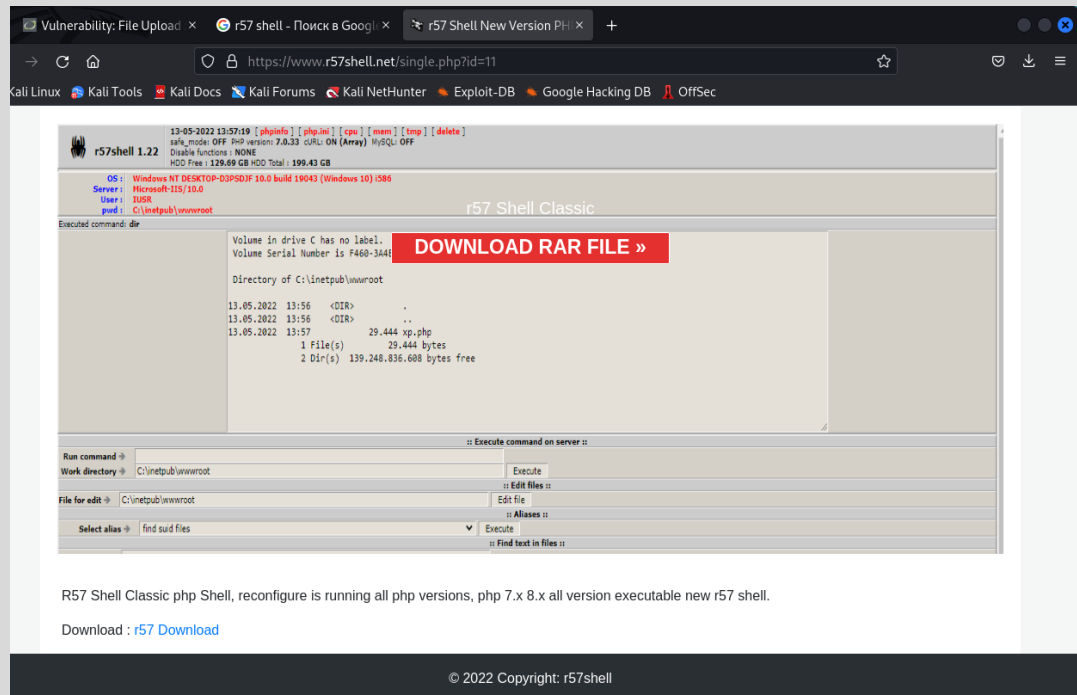


Задание выполнил студент группы 2345 Романенко Кирилл Д.

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

Настроил DVWA

Скачал r57shell 1.22



Загрузил

Vulnerability: File Upload

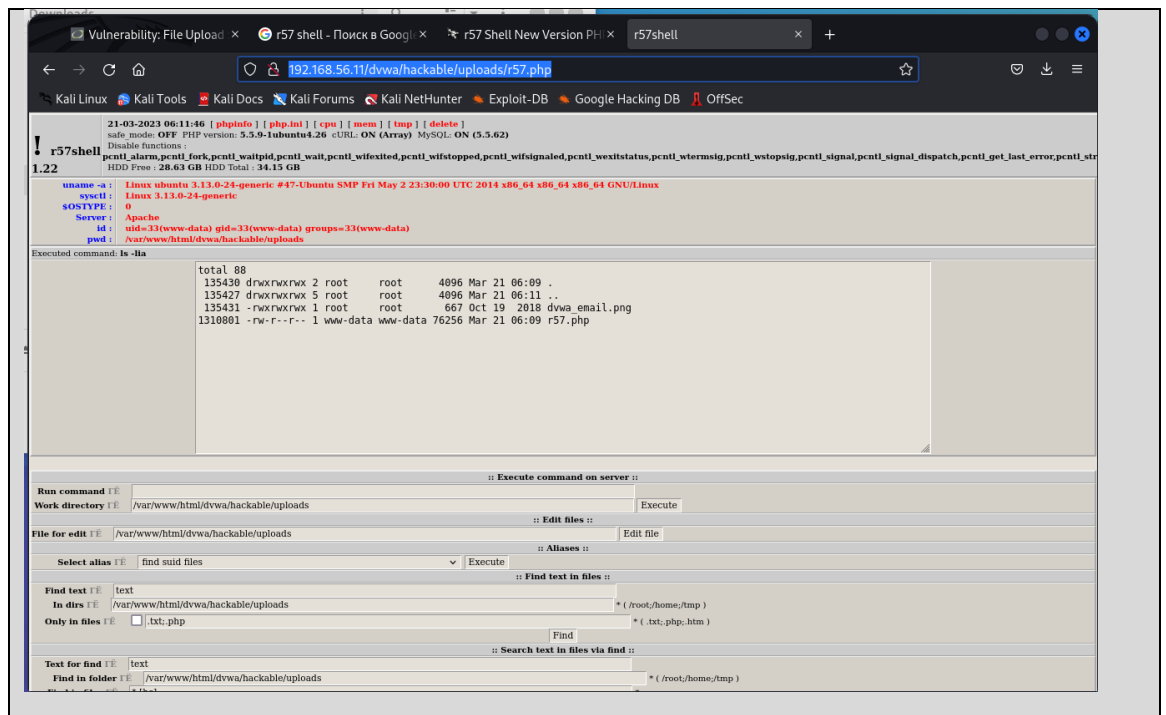
The PHP module **GD** is not installed.

Choose an image to upload:

No file selected.

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

Готово



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

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

Зашёл на страницу

Просканировал

nikto -host http://192.168.56.11/bwapp/sm_obu_files.php

```

(kirill@kali)-[~]
└─$ nikto -host http://192.168.56.11/bwapp/sm_obu_files.php
- Nikto v2.1.6
-----
+ Target IP:      192.168.56.11
+ Target Hostname: 192.168.56.11
+ Target Port:    80
+ Start Time:     2023-03-21 12:06:24 (GMT5)
-----
+ Server: Apache
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 7915 Requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:      2023-03-21 12:07:24 (GMT5) (60 seconds)
-----
+ 1 host(s) tested

```

Версия сервера и бэка

Просканировал

dirb http://192.168.56.11/bwapp/sm_obu_files.php

```
(kirill@kali)-[~]
$ dirb http://192.168.56.11/bwapp/sm_obu_files.php/hi>

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Mar 21 12:07:55 2023
URL_BASE: http://192.168.56.11/bwapp/sm_obu_files.php/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

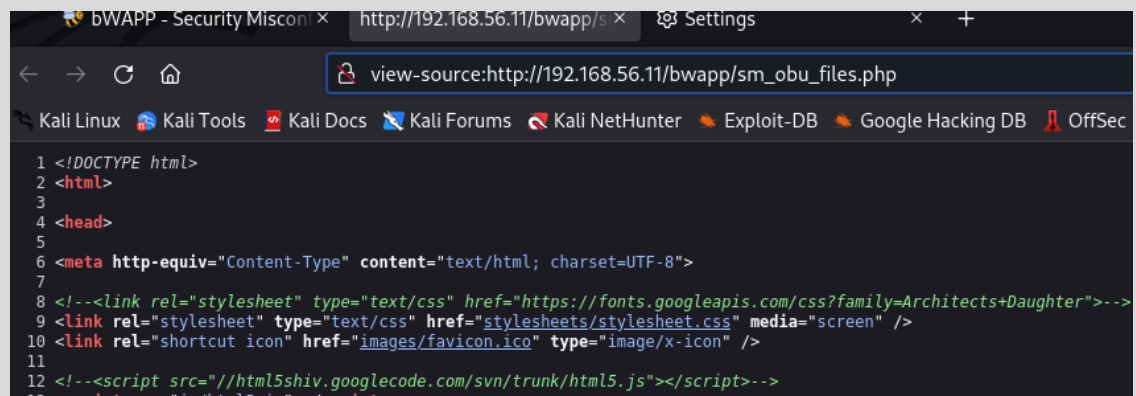
---- Scanning URL: http://192.168.56.11/bwapp/sm_obu_files.php/ ----

-----

END_TIME: Tue Mar 21 12:07:58 2023
DOWNLOADED: 4612 - FOUND: 0
```

Ничего не дало

Открыл Page Source

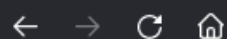


```
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5
6 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
7
8 <!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
9 <link rel="stylesheet" type="text/css" href="stylesheets/stylesheets.css" media="screen" />
10 <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />
11
12 <!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
13 <script src="js/html5.js"></script>
```

Ничего не дало

Предположил, что это просто страница с файлами, в которых есть уязвимости. Открыл их:

Заменял 0 на o и перешел по ссылке, например backd00r.php -> backdoor.php



192.168.56.11/bwapp/backdoor.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

NSA file uploader

No file selected.

to directory:



Есть возможность загрузить shell в нужную директорию. Заменяю to directory: **/var/www/html/bwapp** и загрузил shell **r57.php**

Загрузка прошла, шелл работает