This document outlines findings from a comprehensive security assessment of several public-facing web applications and servers. The evaluation identified critical vulnerabilities, including misconfigurations, weak access controls, and exploitable code flaws. These vulnerabilities highlight the potential for unauthorized access, data breaches, and system compromise. Immediate remediation measures are recommended to mitigate these risks and enhance the overall security posture.

Scope

The assessment focused on public-facing web servers and applications hosted on the following domains and servers:

- **L-SRV01**: Web server hosting multiple virtual hosts.
- **S-SRV01**: Server containing a password reset functionality.

The evaluation included:

1. Enumeration of virtual hosts and directories.
2. Identification of hidden files and sensitive information.
3. Analysis of critical vulnerabilities such as Local File Inclusion (LFI) and Remote Code Execution (RCE).
4. Exploitation of password reset token leakage.

Objectives

The primary objectives of this assessment were to:

1. Identify and document hidden files, directories, and misconfigurations.
2. Detect and exploit critical vulnerabilities to evaluate their impact.
3. Provide actionable recommendations for mitigating the identified risks.

Methodology

A systematic approach was adopted to identify and exploit vulnerabilities using industry-standard tools and techniques:

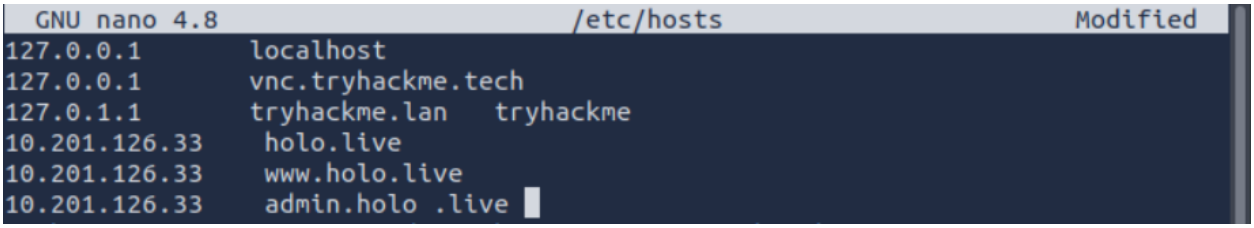
1. **Enumeration Tools**:
    - Gobuster and WFuzz for brute-forcing subdomains and directories.

2. **Exploit Development**:
    - Manual exploitation of LFI and RCE vulnerabilities.
    - Interception of JSON responses using browser developer tools.
3. **Risk Assessment**:
    - Severity analysis based on the potential impact of each vulnerability.
4. **Evidence Collection**:
    - Screenshots, command outputs, and captured traffic logs.

Technical Details

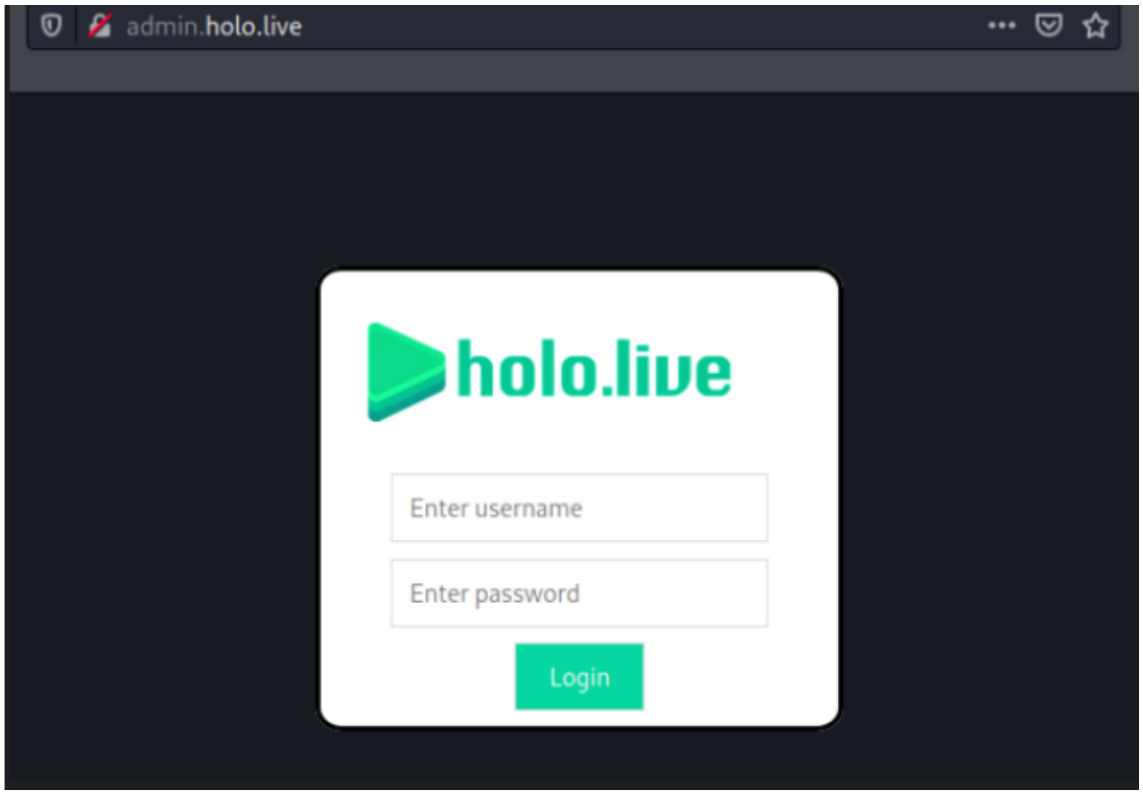
Task 9: Virtual Host Enumeration

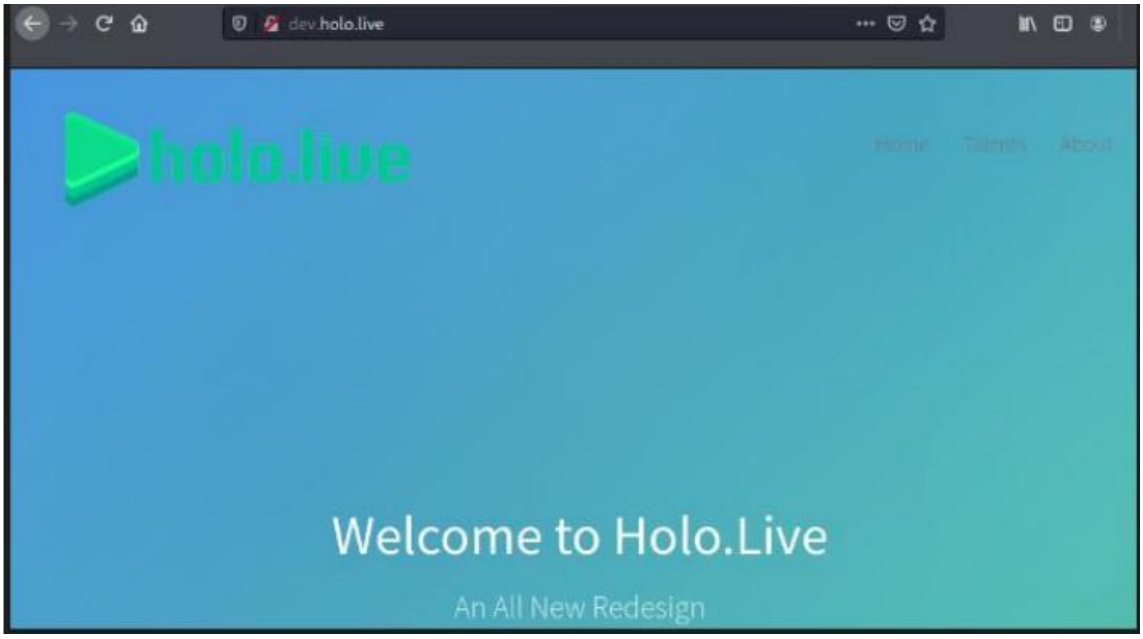
- **Target**: L-SRV01
- **Method**:
    - Tools like Gobuster and WFuzz were used to identify hidden virtual hosts (vhosts).
    - Wordlists were employed to brute-force subdomains without causing server crashes.
- **Findings**:
    - Multiple vhosts were discovered, increasing the attack surface.



```
root@ip-10-10-235-220:~# sudo nano /etc/hosts
root@ip-10-10-235-220:~# gobuster vhost -u holo.live -w /usr/share/wor
dlists/SecLists/Discovery/DNS/subdomains-top1mllion-110000.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://holo.live
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/SecLists/Discovery/DNS/subdomai
ns-top1million-110000.txt
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
023/03/08 00:11:35 Starting gobuster
===============================================================
```

```
Found: www.holo.live (Status: 200) [Size: 21405]
Found: dev.holo.live (Status: 200) [Size: 7515]
Found: admin.holo.live (Status: 200) [Size: 1845]
ound: gc._msdcs.holo.live (Status: 400) [Size: 422]
ound: WWW.holo.live (Status: 200) [Size: 21405]
rogress: 1330 / 114533 (1.16%)
```





What domains loads images on the first web page?

www.holo.live

✓ Correct Answer

What are the two other domains present on the web server? Format: Alphabetical Order

admin.holo.live, dev.holo.live

✓ Correct Answer

Task 10: Directory Enumeration

- **Target**: Web server L-SRV01
- **Command Example**:
- **Results**:
    - Hidden directories and sensitive files such as backup and configuration files were identified.


```
User-agent: *
Disallow: /var/www/admin/db.php
Disallow: /var/www/admin/dashboard.php
Disallow: /var/www/admin/supersecretdir/creds.txt
```

What file leaks the web server's current directory?

robots.txt ✓ Correct Answer

What file loads images for the development domain?

img.php ✓ Correct Answer

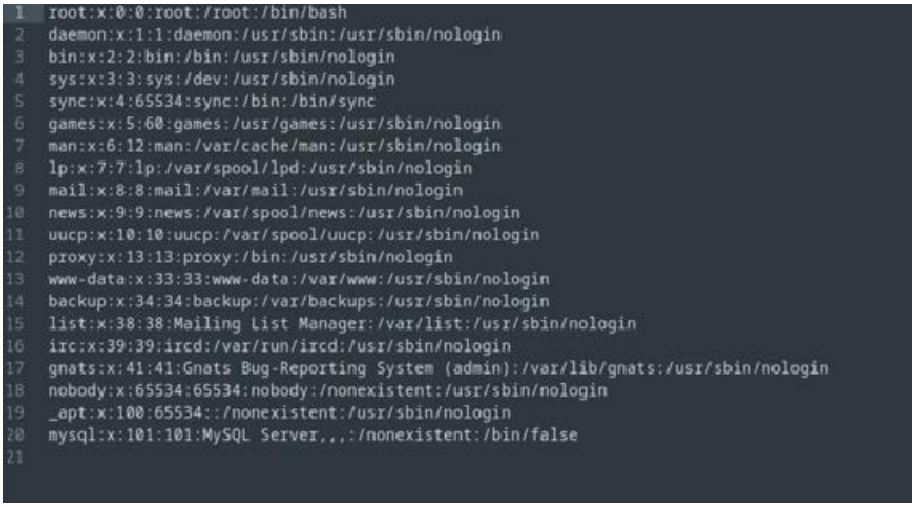
What is the full path of the credentials file on the administrator domain?

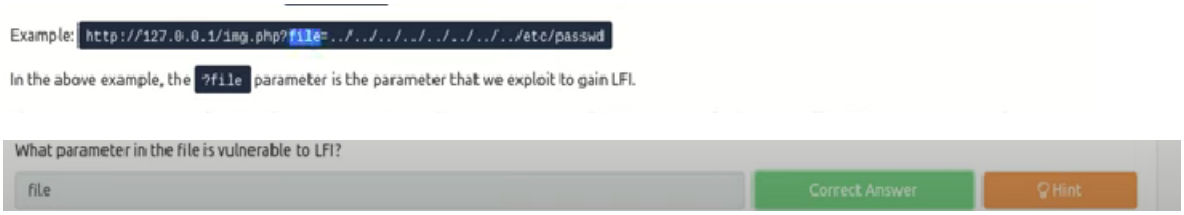
/var/www/admin/supersecretdir/creds.txt ✓ Correct Answer Hint

Task 12: Local File Inclusion (LFI)

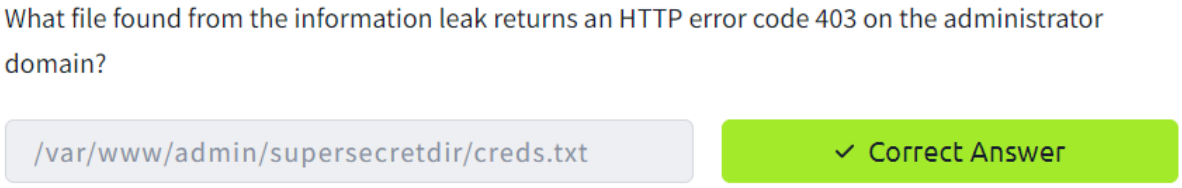
- **Vulnerability**: Improper input validation in HTTP request parameters.
- **Exploitation**:

- Manipulated URL parameters to access /etc/passwd and a sensitive credentials file at /var/www/admin/supersecretdir/creds.txt.





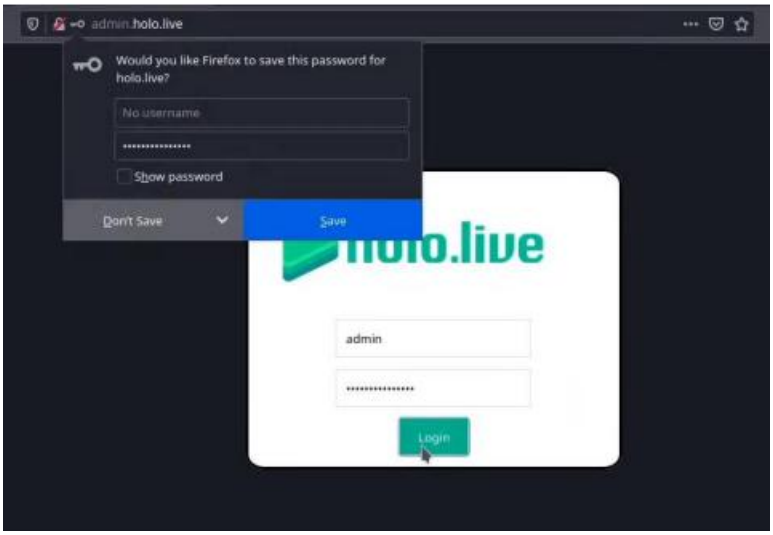
The server response includes the /etc/passwd file. This confirms that we've successfully exploited LFI. Additionally, recall the credentials file mentioned in robots.txt located at /var/www/admin/supersecretdir/creds.txt.



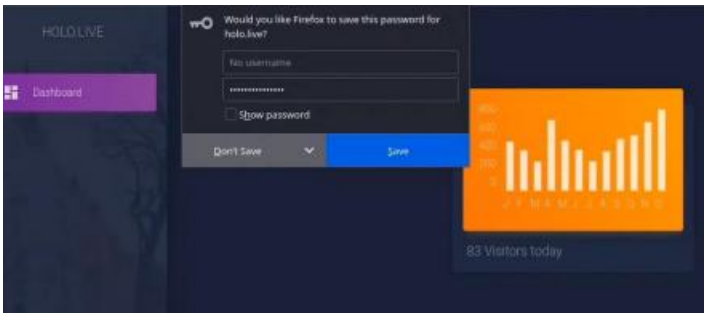

```
I know you forget things, so I'm leaving this note for you:
admin:DBManagerLogin!
- gurag <3
```

Task 13: Remote Code Execution (RCE)

- **Vulnerability**: Exploitable command parameters in Dashboard.php.
- **Command Example**:
    - Executed whoami to confirm access to the server.



Dashboard.php appear



What user is

Use who ami

What file is vulnerable to RCE on the administrator domain?

dashboard.php ✓ Correct Answer Hint

What parameter is vulnerable to RCE on the administrator domain?

cmd ✓ Correct Answer Hint

What user is the web server running as?

www-data ✓ Correct Answer Hint

Task 28: Password Reset Token Leakage

- **Vulnerability**: Reset tokens exposed in JSON responses.
- **Impact**: Unauthorized account takeover.
- **Exploitation Steps**:
    1. Captured token via browser developer tools.
    2. Used token in the reset URL to successfully change the password.

Recommendations

1. **For Virtual Hosts and Directory Security**:
    - Restrict access to sensitive directories.
    - Regularly audit DNS and HTTP headers for misconfigurations.
2. **For LFI and RCE Mitigation**:
    - Validate and sanitize all user inputs.

- Implement strict access controls for sensitive files.

3. **For Password Reset Security**:
    - Avoid exposing reset tokens in client-facing responses.
    - Use secure delivery mechanisms like email or SMS.
    - Enforce multi-factor authentication.
    - Implement short expiry times for reset tokens.

Findings and Conclusion

The assessment revealed significant vulnerabilities that could be exploited to compromise systems and sensitive data. Addressing these issues promptly is critical to reducing the attack surface and preventing potential breaches. The recommended measures aim to enhance the security of the identified systems and prevent similar vulnerabilities in the future.