Reporte Vulnerabilidades

4Geeks Academy

FELIPE ALONSO GOMEZ HENRY
ESTUDIANTE BOOTCAMP CIBERSEGURIDAD

4Geeks

Contenido

4Geeks

Información General

Analista: Felipe Gómez Henry

Fecha: 14-04-2025

Entorno: Red Local privada con VM (Debian) con DVWA

Objetivo general: Práctica para reconocimiento de vulnerabilidades en una máquina virtual con DVWA ejecutando módulos de inyección SQL e inyección de comandos.

Control de Versiones

- Máquina Vulnerable: Debian + DVWA sobre Apache/PHPMySQL
- Nmap: 7.9
- DVWA detectado en /var/www/

Alcance

- Evaluación de funciones disponible en DVWA (DAMN VULNERABLE WEB APPLICATION), en nivel Low.
- Identificar vectores de entrada para ejecución de código y acceso a datos.
- Validar explotación real de vulnerabilidades.

Objetivos y metodologías de trabajo

- Identificación y ejecución de comandos y sus efectos.
- Evidenciar resultados

Resultado Vulnerabilidades Expuestas

I. Nivel alto – Inyección SQL

Playload utilizado: 1’ OR ‘1’ =’1

Consecuencias

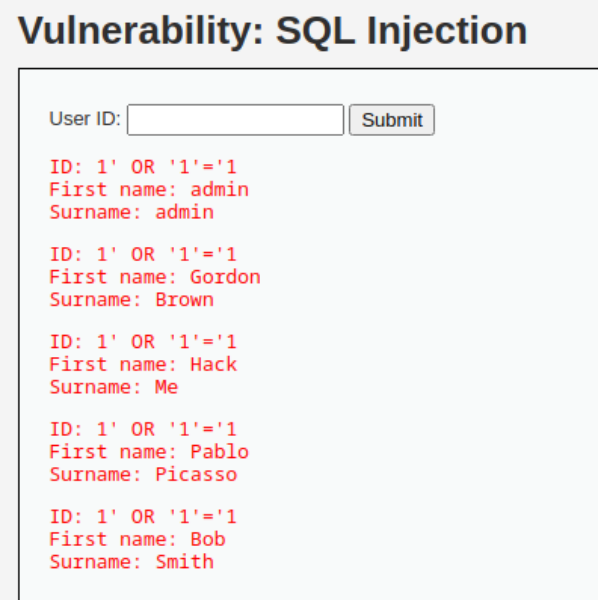
- Acceso remoto a la base de datos dvwa.
- Extracción de información sensible de la base de datos como usuarios y contraseñas.
- Alteración de la integridad de la base de datos.
- Probabilidad alta de abuso para dump completo de la base de datos.

4Geeks

Solución

1. Implementación de consultas parametrizadas en el código PHP/MySQL
2. Validar y sanear todas las entradas de usuarios.
3. Aplicar un WAF y controles de detección de inyecciones.

Evidencias



II. Nivel alto – Inyección de comandos

- Playload utilizados:
  - 127.0.0.1; ls -la
  - 127.0.0.1; cat /etc/passwd

Consecuencias

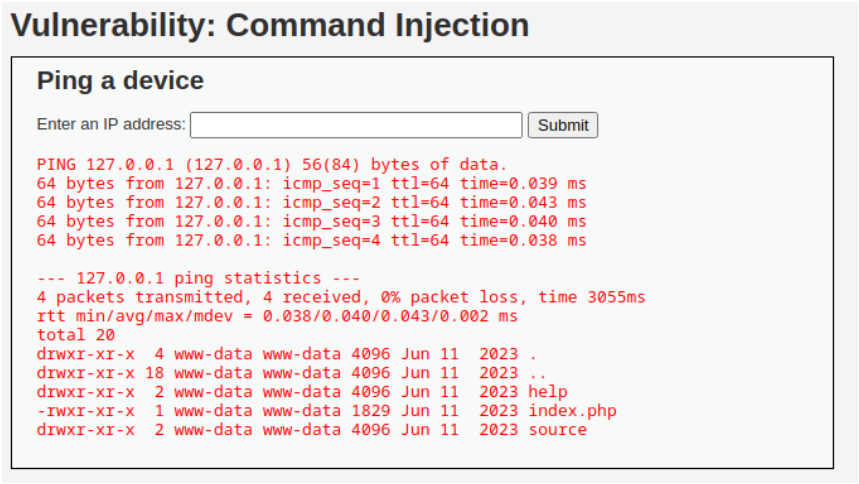
- Obtención de Shell remota, que da control total sobre el servido o maquina como si tuviera acceso físico.
- RCE ejecución remota de comandos, lo que implica un impacto directo sobre la integridad y confidencialidad de los datos del sistema.

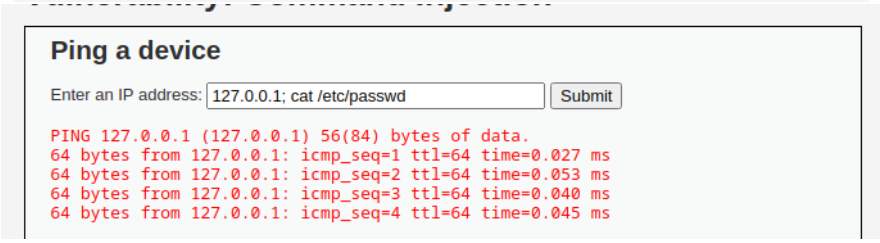
- Exfiltración de información de datos sensibles.
- Escalamiento de privilegios consecuencia de la Shell remota establecida.
- Crear cuentas de usuario con intenciones maliciosas.

Solución

1. Validación estricta de las entradas de los usuarios.
2. Implementación de una whitelist, es decir se permite acceso solo a entidades conocidas.
3. Deshabilitar funciones en php.ini como: exec, shell_exec, system, passthru, popen, proc_open. Ya que no deberían usarse en producción.
4. Aplicar un WAF y controles de detección de inyecciones.
5. Auditorías y monitoreos.

Evidencias





4Geeks

```
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3083ms
rtt min/avg/max/mdev = 0.027/0.041/0.053/0.009 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
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,,:/nonexistent:/bin/false
```

4Geeks

Conclusiones

Como proyecto práctico sobre las vulnerabilidades de Inyección SQL e Inyección de Comandos. Se logró con éxito identificar, explotar y documentar exitosamente ambas fallas en un entorno controlado, ejecutando comandos directos del sistema. Este enfoque metódico permitió no solo comprometer la aplicación DVWA, sino también analizar el impacto de las fallas en términos de confidencialidad, integridad y disponibilidad.