Título del Reporte

Compromiso de credenciales mediante ataque de fuerza bruta en el sistema de autenticación web.

Introducción

El día 25 de agosto de 2025 a las 8:35 p.m., se realizó una prueba de seguridad controlada en la plataforma DVWA, donde se detectó la vulnerabilidad del sistema de autenticación frente a un ataque de fuerza bruta. El objetivo del presente informe es documentar el incidente, describir el proceso de reproducción, evaluar su impacto y proponer medidas de mitigación.

Descripción del Incidente

Fecha y hora del incidente: 25/08/2025, 8:35 p.m.
Sistema afectado: Portal de autenticación web (login.php en DVWA).
Vector de ataque: Múltiples solicitudes consecutivas al formulario de inicio de sesión, automatizadas mediante herramienta de fuerza bruta (Hydra).
Credenciales comprometidas: Usuario 'admin' con múltiples contraseñas válidas como 'admin',
'123456', 'qwerty'.

Proceso de Reproducción

1. Se creó un diccionario de contraseñas débiles (passwords.txt).
2. Se ejecutó el siguiente comando:
hydra -l admin -P passwords.txt 127.0.0.1 http-post-form "/DVWA/vulnerabilities/brute/:username=^USER^&password;=^PASS^&Login;=Login:Log in failed"
3. Hydra identificó múltiples contraseñas válidas para el usuario 'admin'.

Impacto del Incidente

- Riesgo de compromiso de cuentas de usuario o administrador.
- Acceso no autorizado a información sensible.
- Posibilidad de manipulación o alteración de datos (afectando la integridad).
- Posible denegación de servicio por sobrecarga de intentos masivos.
- Impacto en los principios de seguridad: Confidencialidad, Integridad y Disponibilidad.

Recomendaciones

- Implementar políticas de bloqueo de cuentas tras múltiples intentos fallidos.
- Configurar captcha o MFA (autenticación multifactor).
- Implementar contraseñas robustas (mínimo 12 caracteres, combinación de letras, números y símbolos).
- Monitorear y alertar en tiempo real patrones de intentos masivos.
- Aplicar listas negras o bloqueo de direcciones IP sospechosas.
- Integrar un sistema de detección y prevención de intrusos (IDS/IPS).
- Realizar auditorías de seguridad periódicas.

-Implementar geobloqueo o restricciones por ubicación:

-Forzar cierre de sesión en todos los dispositivos tras intentos fallidos múltiples:
Si se detectan varios intentos sospechosos, cerrar todas las sesiones activas del usuario afectado para mitigar riesgos.

-Utilizar autenticación basada en certificados o llaves criptográficas:
Reemplazar contraseñas tradicionales en sistemas críticos por métodos más robustos como certificados digitales o llaves SSH.

Conclusión

Se comprobó que el sistema DVWA es vulnerable a ataques de fuerza bruta. El ataque fue exitoso, obteniendo credenciales válidas sin restricción alguna. Aunque se trató de un entorno controlado, esta prueba demuestra la importancia de implementar controles de seguridad efectivos en sistemas de autenticación reales