Roteiro Técnico 1: Injeção de SQL (SQL Injection) com DVWA

Objetivo

Simular um ataque de injeção de SQL em uma aplicação web vulnerável e identificar como detectar e mitigar a falha.

---

1. Preparação do Ambiente

Ferramentas necessárias:

- VirtualBox ou VMWare
- Máquina Linux com **Kali Linux**
- Máquina com **DVWA (Damn Vulnerable Web Application)** instalada (pode ser um LAMP server)

Instalação do DVWA:

```
# Em uma VM Ubuntu
sudo apt update
sudo apt install apache2 php php-mysqli mariadb-server git -y
sudo systemctl start apache2
sudo systemctl start mariadb

# Clone o DVWA
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo chown -R www-data:www-data DVWA/
sudo chmod -R 755 DVWA/

# Configurar banco de dados
sudo mysql_secure_installation
sudo mysql -u root -p
CREATE DATABASE dvwa;
CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapassword';
GRANT ALL ON dvwa.* TO 'dvwauser'@'localhost';
FLUSH PRIVILEGES;
EXIT;

# Configurar DVWA
cd /var/www/html/DVWA/config
cp config.inc.php.dist config.inc.php
# Edite config.inc.php e insira as credenciais do banco
# Acesse via navegador: http://[IP-DA-VM]/DVWA
```

---

2. Configuração do DVWA

1. Acesse: `http://[IP da máquina DVWA]/DVWA`
2. Vá em **"Setup"** → "Create / Reset Database"
3. Faça login:
   Usuário: `admin`
   Senha: `password`
4. Vá em **DVWA Security** e defina o nível como **"Low"**

---

3. Execução do Ataque

1. Vá na aba **SQL Injection**
2. No campo de busca de usuários, digite:

```
1' OR '1'='1 --
```

3. Você verá uma lista completa de usuários sendo retornada — isso confirma a falha de SQLi.
4. Teste outras variações, como:

```
' OR 1=1 LIMIT 1 OFFSET 1 --
```

5. Capture as requisições com **Burp Suite** ou **Wireshark** (opcional).

---

4. Detecção e Auditoria

Verificar logs:

```
# Em DVWA (servidor web)
      cat /var/log/apache2/access.log
      cat /var/log/apache2/error.log
```

Identificar comandos maliciosos:
Procure por `OR 1=1` ou outros padrões de injeção nas requisições HTTP.

Ferramenta alternativa: sqlmap
Execute no Kali:

```
sqlmap -u "http://[IP]/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --
cookie="security=low; PHPSESSID=xxxx" --dbs
```

---

5. Mitigação da Falha

1. Volte à aba "DVWA Security" e mude o nível para "High".
2. Refaça os testes e verifique que o ataque não é mais possível.
3. Discuta no relatório:
    - Validação de entradas
    - Uso de prepared statements
    - Monitoramento de logs

---

6. Evidências e Documentação

Inclua no relatório:

- Capturas de tela do ataque com sucesso.
- Linhas de log com a tentativa de injeção.
- Resultados com `sqlmap`.
- Demonstração de mitigação ao mudar o nível de segurança.
