Exemplos Pentest Básicos

***Command Injection**

1° Acessar https://pentest-ground.com/

2° Clicar na URL **Damn Vulnerable Web Application** e selecione "**Command Injection**";

3° Executar o CMD do Windows e digitar o comando nslookup para obter o IP do Website;

```
C:\Users\User> nslookup pentest-ground.com
```

4° Digite no campo Enter an IP address [178.79.134.182;cat /etc/passwd] e clique em Submit;

Obs: Ataques de injeção de comando são possíveis quando um aplicativo não valida dados fornecidos pelo usuário (por exemplo, dados inseridos em formulários da Web, cookies, cabeçalhos HTTP e outros elementos). O sistema vulnerável passa esses dados para o "shell" do sistema.

***SQL Injection**

1° Selecione "**SQL Injection**"

2° No campo User ID digite [**' OR 1=1 #**] e Submit.

Obs: A saída confirma que existe uma vulnerabilidade que permite a execução de instruções SQL inseridas diretamente nos campos de entrada.

3° No campo User digite [**1' OR 1=1 UNION SELECT 1, VERSION()#**] e Submit.

Obs: A saída confirma que foi possível identificar o serviço de banco de dados Database Management System (DBMS) e o sistema operacional rodando no servidor.

4° No campo User digite [**1' OR 1=1 UNION SELECT user, password FROM users #**] e Submit.

Obs: A saída retorna uma lista de usuários e o hash das senhas armazenadas na base de dados.

5° Acesse https://crackstation.net/ copiar e colar o hash da conta de admin para ver a senha.

***Cross-site scripting (XSS)**

1° Selecione **"XSS (Stored)"**

2° No campo Name * digite um nome qualquer.

3° No campo Message * [**<script>alert("DIGITE SUA SENHA")</script>**], e Sign Guestbook.

Obs: A exploração bem-sucedida pode resultar na instalação ou execução de código malicioso, comprometimento da conta, sequestro de "cookies" de sessão, revelação ou modificação de arquivos locais e redirecionamento de site.