Alcapdemy:
Curso de SQL injection (básico)

1.SQL injection

La inyección SQL es una vulnerabilidad web que permite a un atacante manipular la base de datos de una aplicación. Esto ocurre cuando los datos del usuario no son validados correctamente y se insertan directamente en una consulta SQL, permitiendo ejecutar comandos maliciosos. Así, el atacante puede ver, cambiar o borrar datos sin autorización

2.Explotar una SQL injection

1.Identifica el punto vulnerable:

-Encuentra una entrada de usuario en la aplicación web (por ejemplo, un campo de búsqueda o login, o una URL con parámetros)

-Introduce caracteres comunes de SQL, como ' o " y observa si se produce un error de base de datos

2.Insertar la inyección:

-Supongamos que has encontrado un formulario de inicio de sesión

-Intenta introducir caracteres comunes de SQL, como ' o " en los campos de entrada. Por ejemplo, en el campo de usuario, ingresa:

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

-Supongamos que el formulario de login envía los datos a una consulta SQL como esta:

```
SELECT * FROM users WHERE username = 'usuario' AND password = 'contraseña';
```

-Al ingresar `' OR '1'='1` en el campo de usuario y cualquier cosa en el campo de contraseña, la consulta se convierte en:

```
SELECT * FROM users WHERE username = '' OR '1'='1' AND password = 'cualquier cosa';
```

-Debido a que `'1'='1'` es siempre verdadero, la consulta se convierte en:

`SELECT * FROM users WHERE '' = '' OR '1'='1' AND password = 'cualquier cosa';`

-Esta consulta puede permitir el acceso sin necesidad de proporcionar credenciales válidas, ya que `'1'='1'` siempre es verdadero y puede omitir la verificación de la contraseña.

-Ahora supongamos que en una aplicación de productos online usa la siguiente consulta SQL:

`SELECT * FROM products WHERE id = '1';`

Al modificar la URL a:

`http://example.com/products?id=1' OR '1'='1`

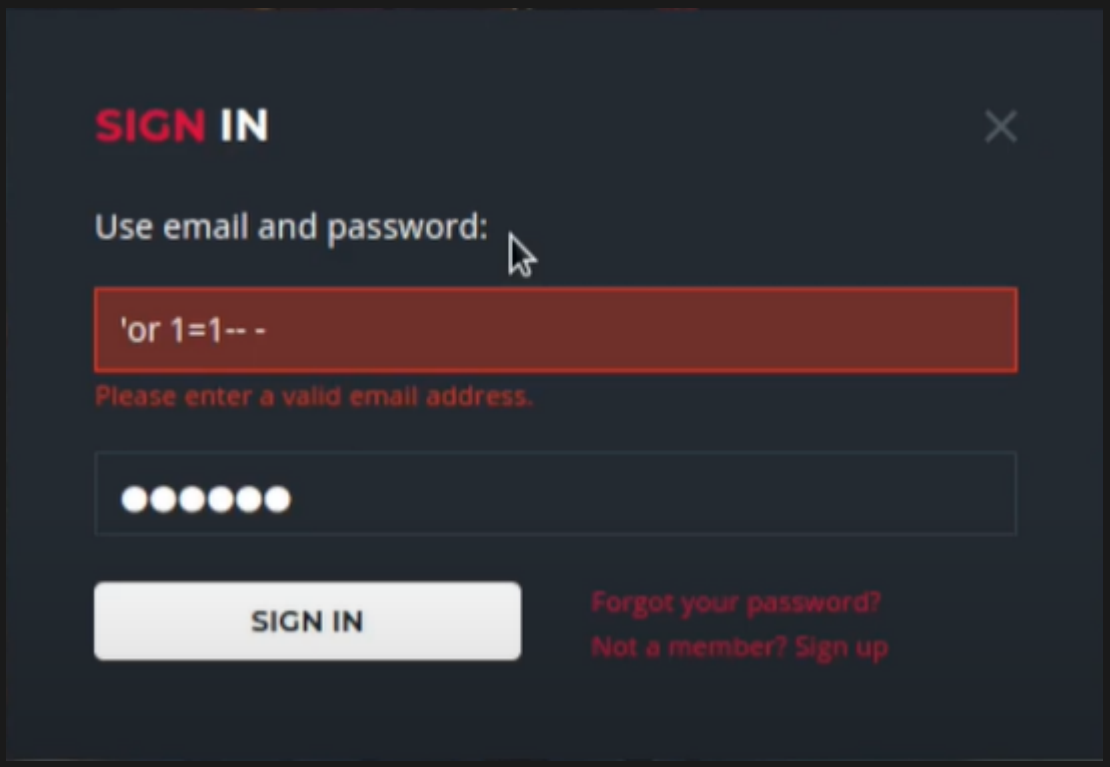
La consulta se convierte en:

`SELECT * FROM products WHERE id = '1' OR '1'='1';`

Esto puede devolver todos los productos porque `'1'='1'` es siempre verdadero.

3.Posible errores:

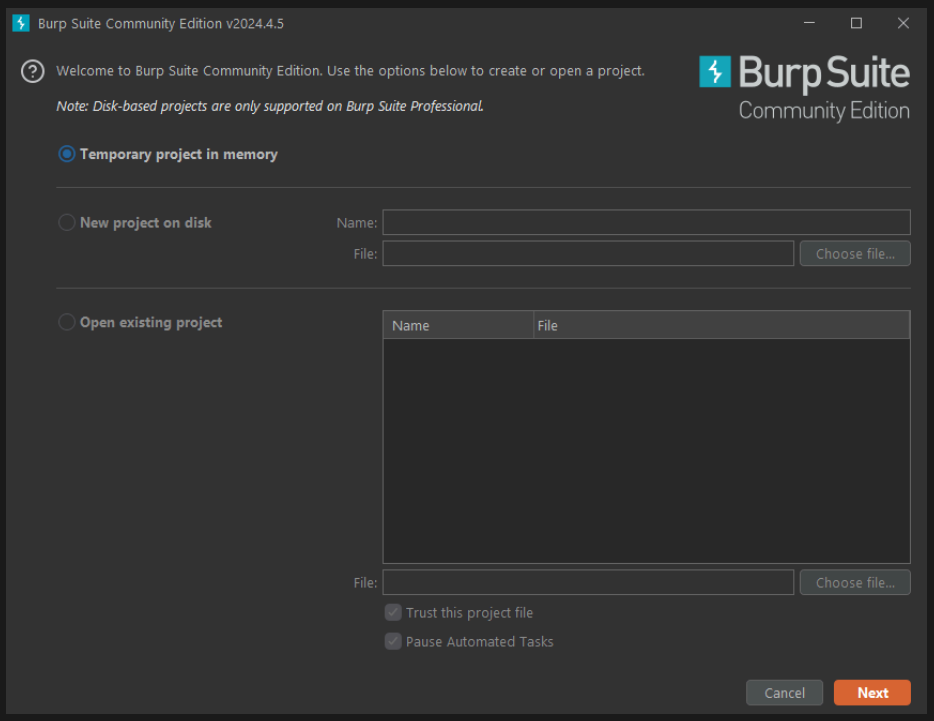
Es posibles que algunos formularios de login no te permiten introducir ciertos caracteres, haciendo imposible la inyección

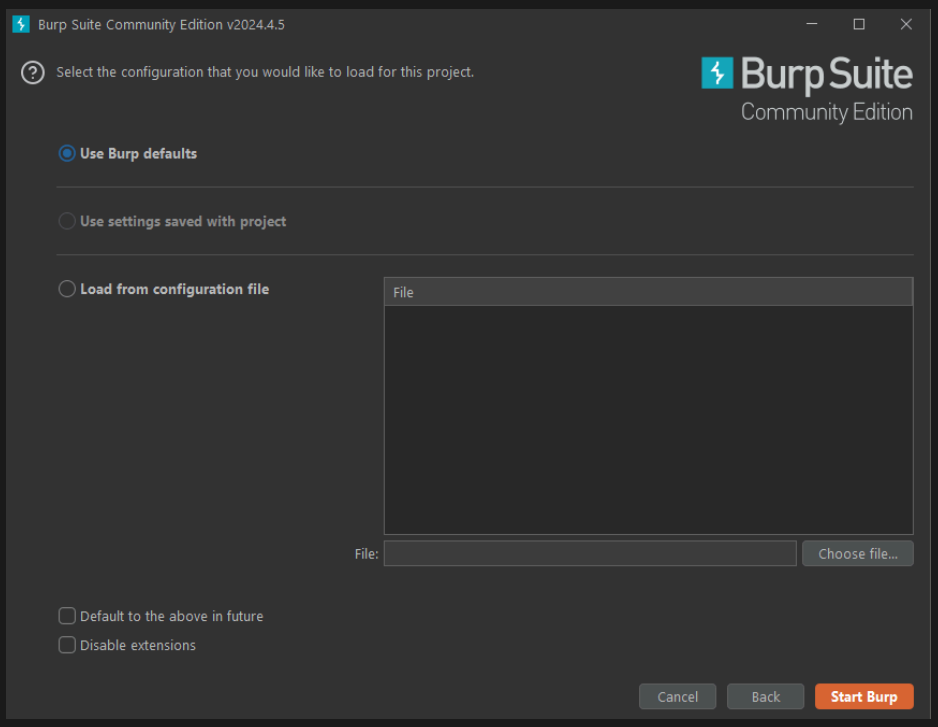


-Para solucionar esto usaremos una herramienta gratuita y muy usada en pentesting llamada “Burp Suite”

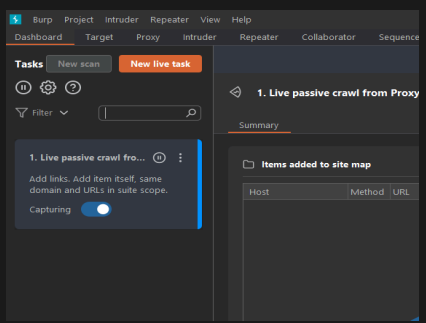
4.Pasos para utilizar Burp Suite:

-Abre Burp Suite, selecciona “Temporary project in memory” dale a next y después a Start Burp

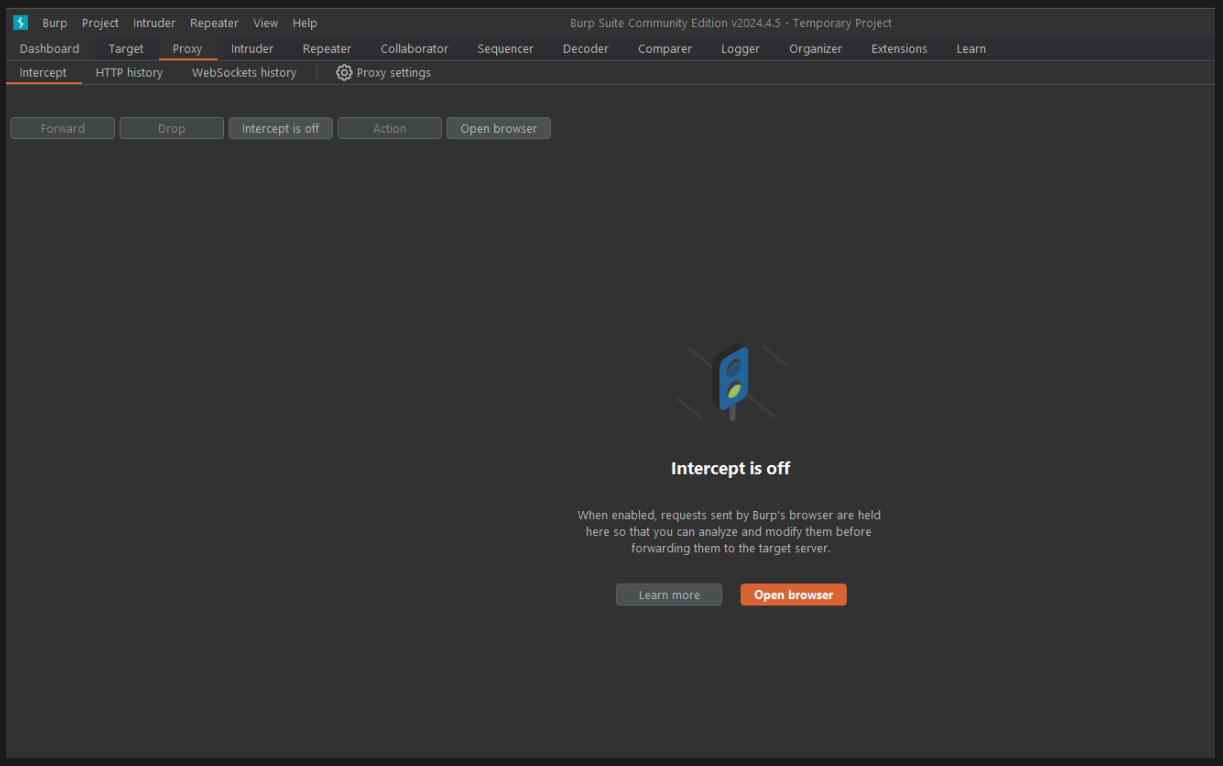




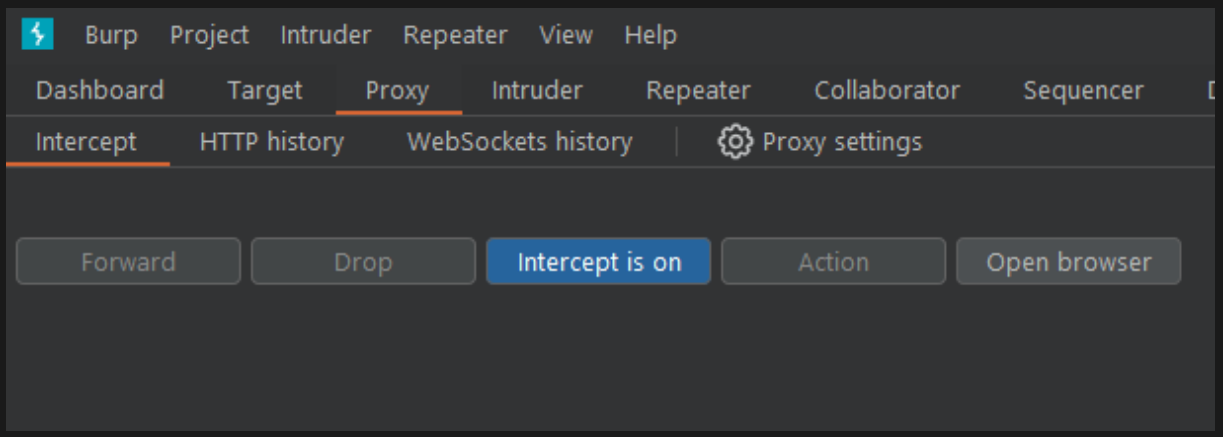
-Cuando Burp Suite haya terminado de crear el proyecto estaremos ubicados en el panel de dashboard, debemos ir al apartado de proxy



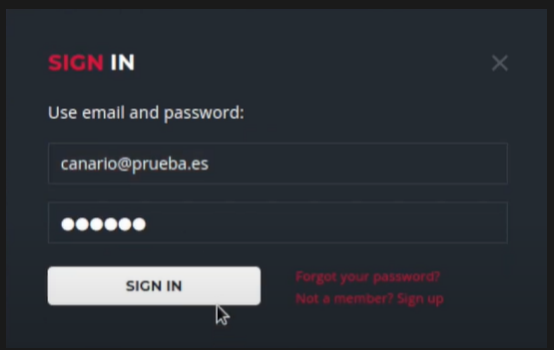
-En el apartado de proxy debemos de darle al botón de open browser



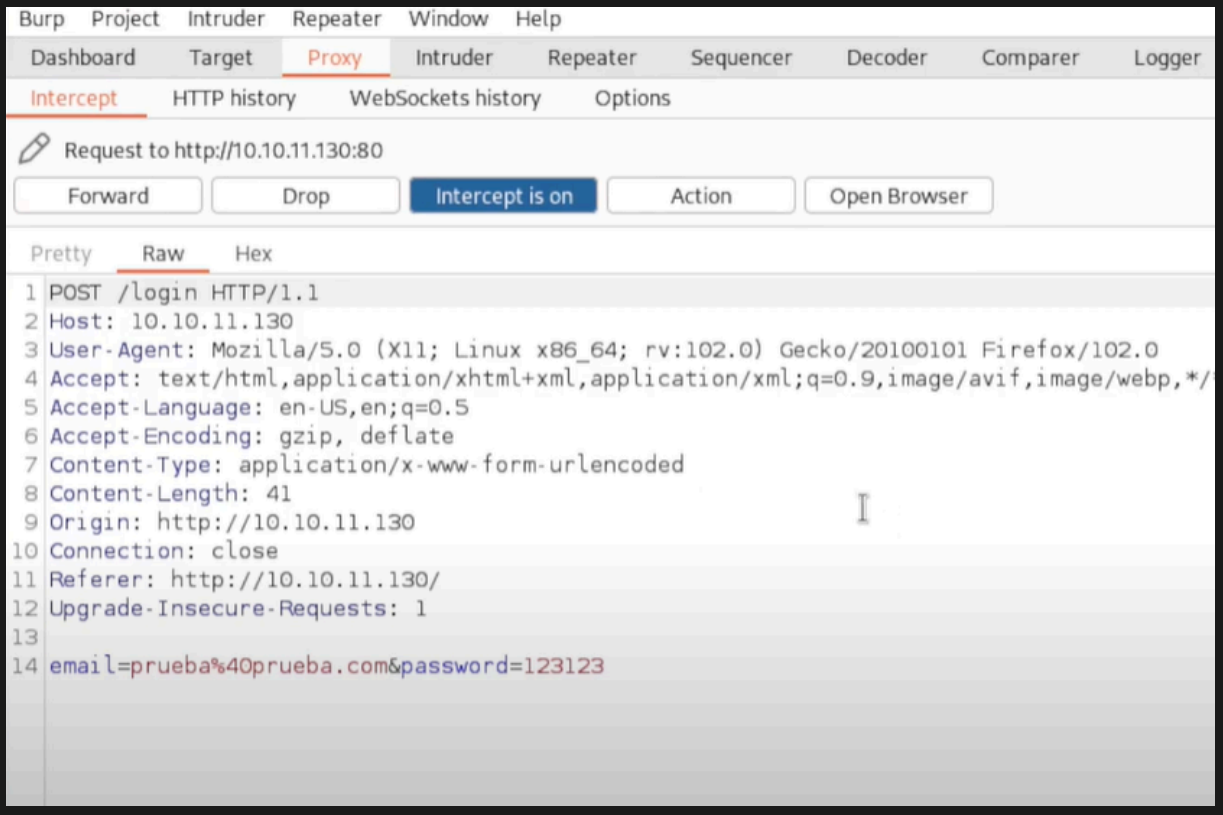
-Cuando el navegador de Burp Suite se habrá dirígete a la página que quieras realizarle el ataque
-Una vez ubicado en la página, debes de interceptar la petición pulsando el botón de intercept is off



-Una vez hecho esto dirígete de nuevo a la página y prueba a iniciar sesión con unas credenciales aleatorias

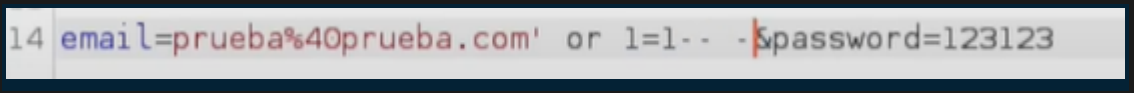


-Ahora dirígete de nuevo a Burp Suite (deberías tener algo parecido a esto)

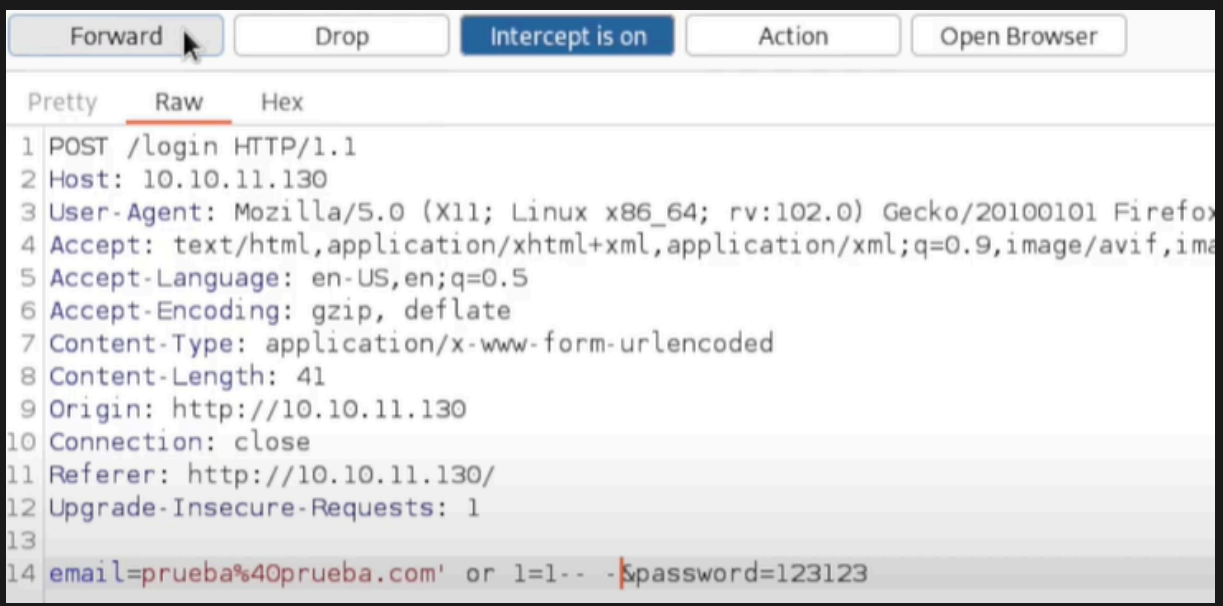


-Esto es una petición, debemos modificar la última línea de la petición donde se encuentra las credenciales que hemos puesto anteriormente

-Modificamos la línea ingresando `' or 1=1— -`



-Por último enviamos la petición con el botón forward



-Al enviar la petición vemos que hemos conseguido vulnerar el panel de login