

Set up for SQLMAP

The image shows a screenshot of a Kali Linux desktop environment with two windows open. The left window is Burp Suite Community Edition v2023.3.5, showing the 'Proxy' tab with 'Intercept is on' selected. A red box labeled '1' highlights the 'Intercept is on' button. A red box labeled '3' highlights the 'Raw' tab in the HTTP history panel, which displays the raw HTTP request for a GET request to `http://10.0.2.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit`. The right window is a web browser showing the DVWA (Damn Vulnerable Web Application) interface. A red box labeled '2' highlights the 'User ID' input field, which contains the value '1'. The browser address bar shows `10.0.2.5/dvwa/vulnerabilities/sqli/`. The DVWA interface also shows a sidebar with various vulnerability categories, including 'SQL Injection' which is highlighted.

In order to be able to execute sqlmap every time with the same parameters and without having to write them over and over, it is possible to make an HTTP request file from which sqlmap takes the information.

The 3 simple passages are explained below and refer to the image.

1. Switch the interception ON
2. Submit a value from web application page
3. Copy the HTTP GET request into a file called req.txt

In this way, to run sqlmap it is only needed the following code:

```
sqlmap -r req.txt --OTHER-PARAMETERS
```