BD

Post Data SQL Injection using SQLMAP

⌛ 2 min read

The best thing about sqlmap is that it is free & you can use it for SQL INJECTION even for POST data. This post is meant to provide you a quick look into the options that sqlmap provides for performing sql injections in post data. For all those who don't know about sqlmap, it is a database automated sql injection & database takeover tool :). If you have some experience using the free version of Havij, then I urge you to try this tool because this is the best open source tool (by default it doesnot have any GUI), but you can get one if you like. (I suggest you to stick with CLI version).

The important arguments that are available for you are -

- **-u** : This is the most important parameter, because this is where you give the url where the request is supposed to be made.(For a POST request make sure you give the correct url i.e the place where the corresponding form is posting rather than the page where the form is present :P)
- **--data** : When you provide this argument with some data, sqlmap will perform POST requests automatically. The POST data of a request can be written directly, if help needed use some tool like ZAP or Burp Suite or Live HTTP Headers to get the post data

Some other important arguments that are usefull -

- **--proxy** : This is used when you wish to tunnel all your requests through a proxy. The protocol must also be mentioned here.
- **--proxy-cred** : This is used to provide credentials for proxy server.
- **--tor** : This allows you to use tor anonymity network.(--tor-port & --tor-type are used if these settings are different from the default values)

So a command using all these arguments would look like -

```
./sqlmap.py -u "URL WHERE THE DATA WILL BE POSTED" --data="POST DATA" --proxy="P
```

For example if we have a form posting data to **www.example.com/submit.php** & the data is **search=hello&value=submit** then the command will look like this - (we are using tor network this time :P)

```
./sqlmap.py -u "http://www.example.com/submit.php" --data="search=hello&value=su
```

2013-03-11 :: {tools}