2018

Sqlmap 视频课程

Sqlmap请求参数设置

课程内容

1. Sqlmap设置HTTP协议认证
2. Sqlmap设置HTTP代理
3. Sqlmap设置Tor隐藏网络
4. Sqlmap设置延迟

01

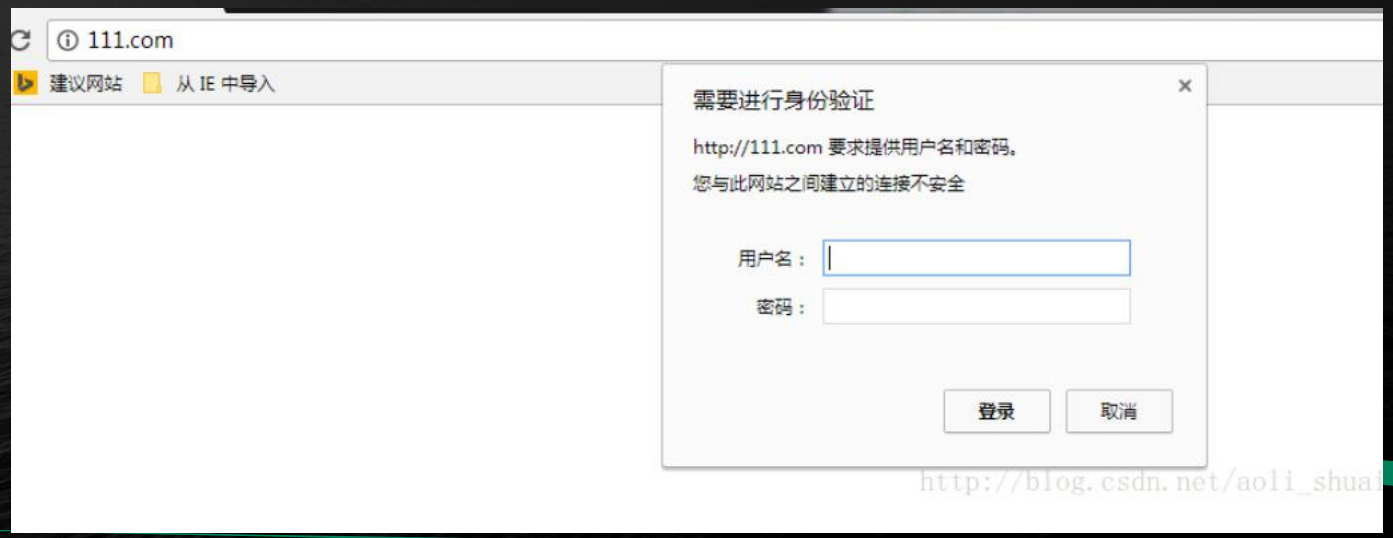
Sqlmap设置HTTP协议认证

Sqlmap中设置HTTP协议认证的参数：--auth-type和--auth-cred

其中--auth-type支持 Basic、Digest、NTLM

--auth-cred认证语法为：username:password

例如：python sqlmap.py -u "http://url/arit.php?id=1" --auth-type Basic --auth-cred "testuser:testpass"



02

Sqlmap设置HTTP代理

Sqlmap中设置代理的参数：--proxy, --proxy-cred, --proxy-file ， --ignore-proxy

其中--proxy用来设置HTTP代理服务器位置 格式：--proxy http(s)://ip[:端口]

--proxy-cred用来设置HTTP代理服务器认证信息 格式：--proxy-cred username:password

--proxy-file用来设置多条代理在文件中

--ignore-proxy当您希望通过忽略系统范围内的HTTP(S)代理服务器设置来针对本地网络的目标部分运行sqlmap时，应该使用这种方法。

03

Sqlmap设置Tor隐藏网络

Sqlmap中设置Tor网络的参数：--tor, --tor-port, --tor-type --check-tor

```
root@kali:~/Desktop# sqlmap -u "http://www.asp.com.cn/index.php?m=search&c=index&a=init&typeid=53&siteid=1&q=XP19" --tor --tor
-type=SOCKs5 --check-tor

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.3#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's resp
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting at 03:25:22

[03:25:22] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[03:25:22] [INFO] setting Tor SOCKS proxy settings
[03:25:22] [INFO] checking Tor connection
```

04

Sqlmap设置延迟

Sqlmap探测过程中会发送大量探测Payload到目标，如果默认情况过快的发包速度回导致目标预警。为了避免这样的情况发生，可以在探测设置Sqlmap发包延迟。默认情况下，不设置延迟。

--delay 0.5 设置延迟0.5秒

```
root@kali:~/Desktop# sqlmap -u "http://192.168.1.100/sqli/Less-1/?id=1" --delay 0.5

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.3#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's resp
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting at 03:27:00

[03:27:01] [INFO] testing connection to the target URL
[03:27:03] [INFO] testing if the target URL content is stable
[03:27:05] [INFO] target URL content is stable
[03:27:05] [INFO] testing if GET parameter 'id' is dynamic
```

总结

1. Sqlmap设置HTTP协议认证
2. Sqlmap设置HTTP代理
3. Sqlmap设置Tor隐藏网络
4. Sqlmap设置延迟

谢谢

欢迎关注 后续课程