Lab Sheet 3

Security

In our third lab, we will use hydra, a tool in Kali Linux, to perform a Brute Force attack on a Web based login. Hydra is the fastest network logon cracker which supports numerous attack protocols. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

1 Task 1: Brute Force Web-based Login with hydra

We will use http to run a brute force attack on a vulnerability testing site.

1.1 Get to know your tool

Type `hydra -h` (`h` for help) in your Kali terminal and find out what *hydra* is all about and how it might work.

1.2

One of hydra's brute force attackingservices is used on Web-based logins, such as social media login forms, user banking login forms, your router's Web-based login, etc. That's `http[s]-get|post-form` which will handle this request.

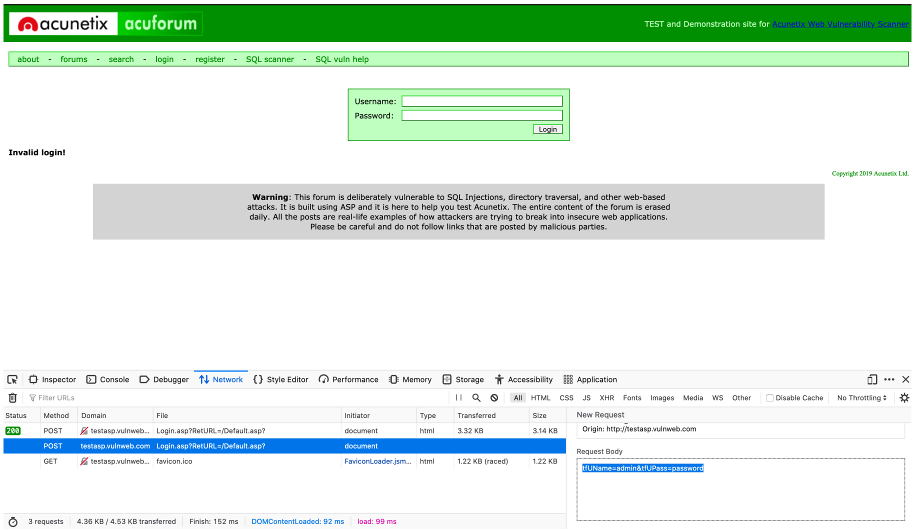
Before we fire up hydra, we should know some of the arguments:

- **Target:** http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
- **Login username:** admin (if you're not sure, bruteforce this)
- **Password list:** "The location of the dictionary file list containing possible passwords."
- **Form parameters:** "Here we will be using iceweasel or firefox network developer toolbar."
- **Service module:** http-post-form

1.3 Obtaining post parametres

Visit http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F and open the *Network* tool in the *Web Developer* menu.

To obtain the post-form parameters, type anything in the *username* and/or *password* form. You will notice a new **POST** method on the network developer tab. Click on that line and on the *Headers* tab click *Edit and Resend* on the right side. From the *Request Body* textbox, copy the last line, e.g. `tfUName=admin&tfUPass=password`. The *tfUName* and *tfUPass* are parameters we need (see Figure 1).



Invalid login!

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	testasp.vulnweb...	Login.asp?RetURL=/Default.asp?	document	html	3.32 KB	3.14 KB
	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document			
	GET	testasp.vulnweb...	favicon.ico	FaviconLoader.jsm...	html	1.22 KB (raced)	1.22 KB

3 requests | 4.36 KB / 4.53 KB transferred | Finish: 152 ms | DOMContentLoaded: 92 ms | load: 99 ms

Origin: http://testasp.vulnweb.com

Request Body

```
tfUName=admin&tfUPass=password
```

Figure 1: Copying Request Body.

1.4 Wordlists

Kali Linux has a bunch of wordlists, so you can choose the appropriate one or just use rockyou.txt from `/usr/share/wordlists/`. So copy the worlist into your home directory and use *gzip* to unzip the archive. Type `cat rockyou.txt` to see how many passwords the wordlist contains.

1.5 Run the attack

Alright, now that we got all arguments, we are ready to fire up hydra. Here is the command pattern:

```
hydra −l <username> −P <password list> <Target hostname>
<service module> <post request parameters>[/code]
```

Based on information we have gathered, our command should look something like this:

```
hydra −l admin −P /usr/share/wordlists/rockyou.txt
testasp.vulnweb.com http−post−form
”/Login.asp?RetURL=\%2FDefault\%2Easp\%3F:tfUName=
ˆUSERˆ&tfUPass=ˆPASSˆ:S=logout” −vV −f
```