WEB CC19 - Tools & Challenges

Hydra

Hydra è un tool che permette di fare login bruteforcing su piattaforme web.

Per installarlo:

```
> sudo apt install hydra
```

Hydra

Per attaccare una pagina di login sul web con hydra, i comandi sono i seguenti:

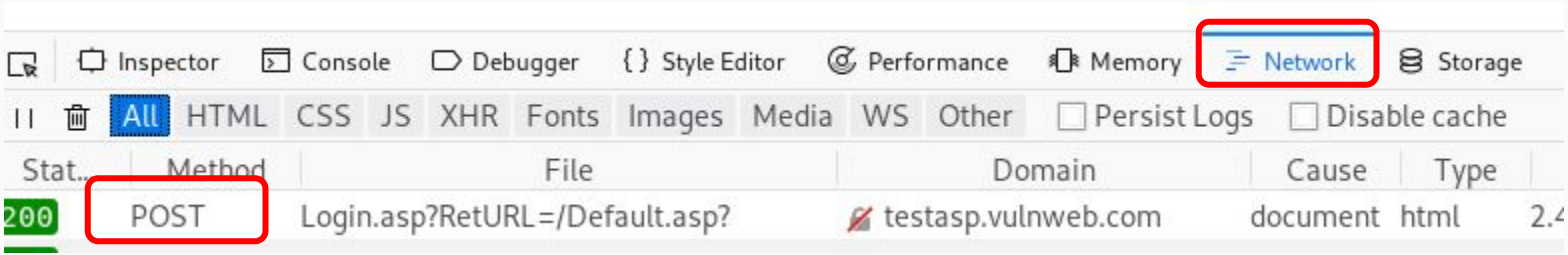
```
hydra -L <username list> -P <password list>
<Targethostname>    <service module>
<uri:parameters:condition> [OPTIONS]
```

Potete trovare queste informazioni facendo un semplice test (e fallendolo) di login sulla pagina web da attaccare, andate al sito:

http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

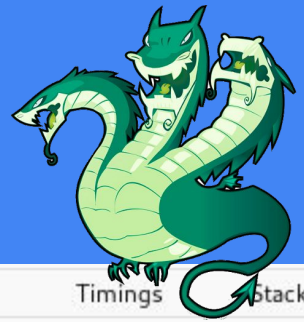
Hydra

Premendo F12 su firefox su qualunque pagina web, vi appare la finestra degli strumenti da sviluppatore. Sulla tab “network” potete vedere le richieste HTTP che mandate dal vostro browser.



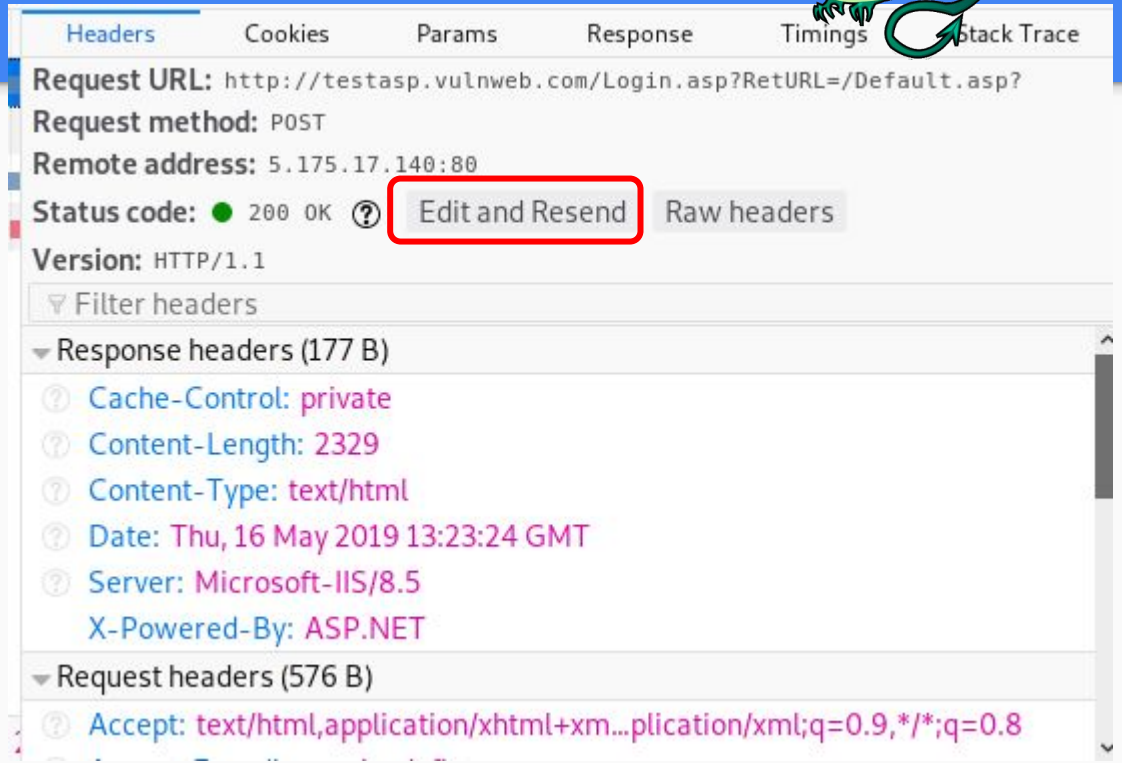
La POST che vedete è un precedente tentativo fallito di login.

Hydra



Facendo doppio click sulla POST, vi si apre questa finestra.

Cliccando su edit and resend, potrete vedere le informazioni contenute nell'header HTTP e il corpo della richiesta.



Hydra

New Request Send Cancel

POST http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F

Query String:

RetURL=/Default.asp?

Request Headers:

Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
Content-Type: application/x-www-form-urlencoded
Content-Length: 19

Request Body:

tfUName=a&tfUPass=a

Curl

A tool to transfer data from or to a server

Curl: simple usage

```
> curl http://info.cern.ch/
```

… what happened?

Curl: parameters list

`-X <ReqMethod>`	Specify a request method (es. POST, GET, …)
`--data <data>`	Sends the specified data in a POST request
`-H “Name: Joe”`	Include extra headers in the request
`-o <file>`	Write the output to the specified output
`-L`	If the page has been moved, follow the redirection
`-i`	Include HTTP response header

URL Encoding

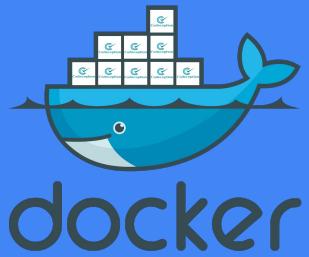
URLs can be sent over the internet using ASCII char-set

If the URL has chars outside the ASCII set, they need to be converted

URL encoding replaces each unsafe char with “%” + 2 hex digits:

- \n → %0A
- ; → %3B
- …

How to RUN a Docker?



1)Install **docker-compose** and **docker** from repository

```
> sudo apt install docker-compose
> sudo apt install docker
```

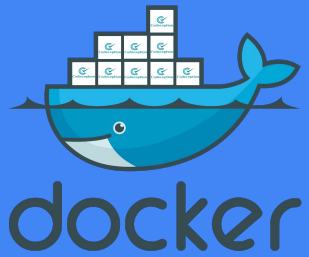
2)If you can find a docker_run.sh file in the directory, run it!

```
> sudo ./docker_run.sh
```

3)If you don’t have a docker_sun.sh file, run the docker using docker-compose

```
> sudo docker-compose up
```

How to STOP a Docker?



1) **CTRL+C** in the terminal running the docker should kill the docker

2) If you face some issues with non-terminated docker:

get the <CONTAINER ID> of the docker running:

```
> sudo docker ps -a
```

Kill the docker:

```
> sudo docker kill <CONTAINER ID>
```

Delete a stopped docker:

```
> sudo docker rm <CONTAINER ID>
```

Time for a challenge!

...Run SMARTCAT1!

MySQL

- Open-source DBMS
- Uses metadata to keep information about dbs, tables, columns, …
- Stores metadata in an internal database called *information_schema*, having tables for:
  - COLUMNS
  - TABLES
  - FILES
  - …
- https://dev.mysql.com/doc/refman/8.0/en/information-schema.html

SQL Injection

Do you remember UNION attack?

1. How many columns does the original query return?
2. What kind of data are they hosting?

… Let’s hack CRIMEMAIL!

Hack Me!

https://hack.me/

1. Very basic SQL injection;
2. Delete all the things;
3. Data verification fail;
4. …

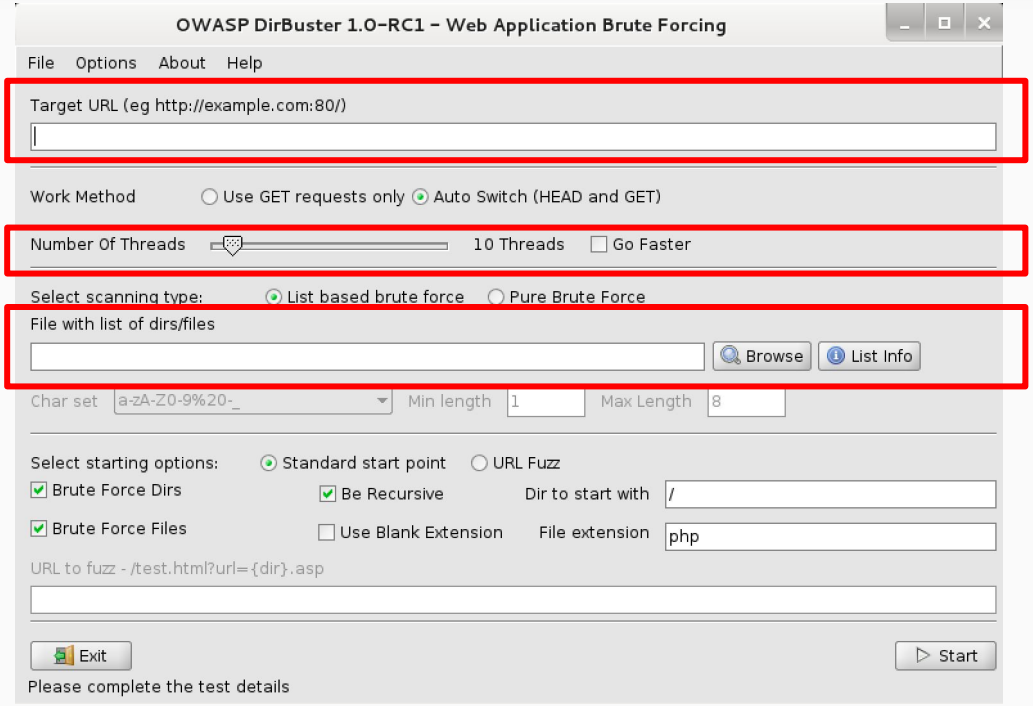
DirBuster

A multi-threaded java application to brute force dirs and files on web/application servers.

Download: https://sourceforge.net/projects/dirbuster/

Dependency: **default-jre**

DirBuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
Exit
Start
Please complete the test details

Challenge “ajax-not-borax”

Take on the challenge

ajax-not-borax

Challenge “ajax-not-borax”

Hint#1

Investigate the javascript-script

Challenge “ajax-not-borax”

Hint#2

localhost:8083/webhooks/get_username.php?username=

Challenge “ajax-not-borax”

Solution

localhost:8083/webhooks/get_pass.php?username=tideade

Challenge “console”

Take on the challenge

console

Challenge “console”

Hint#1

Investigate the html source

Challenge “console”

Hint#2

pressing F12 there is the tab “console”, find out how to use it

Challenge “console”

Solution

Write on the console tab “getThat(‘Y’)

Challenge “OCR”

Take on the challenge

OCR

Challenge “OCR”

Hint#1:

Try to upload an incorrect equation

Challenge “OCR”

Hint#2

In the source, in a comment there is an hint to browse to “/debug”

Challenge “OCR”

Hint#3

The flag is hidden in `x[]`.

Do you know something about the python function ‘`ord`’?

Challenge “OCR”

Solution

Upload multiple PNGs which depict `ord(x[i])=0` where i varies from `0` to whathever index gives you the ‘`}`’ character

Challenge “aart”

Take on the challenge

aart

Challenge “aart”

Hint# 1

Learn the sql database structure. How many tables are there? What are their columns?

Challenge “aart”

Hint# 2

The form should not be injectable, try to write a script using python request.

Challenge “aart”

Hint# 3

Do you know about truncation? What happens if you register a user with a name that is too long? What is the max size of the datatype `TEXT` in `MySQL`?

Challenge “aart”

Solution

Register a new account with a username length > 65535
For example:

```
username = 'A'*65535 + 'B'
```