Scripting Web Attacks with Python

Matt Brown (nmatt)

Whoami

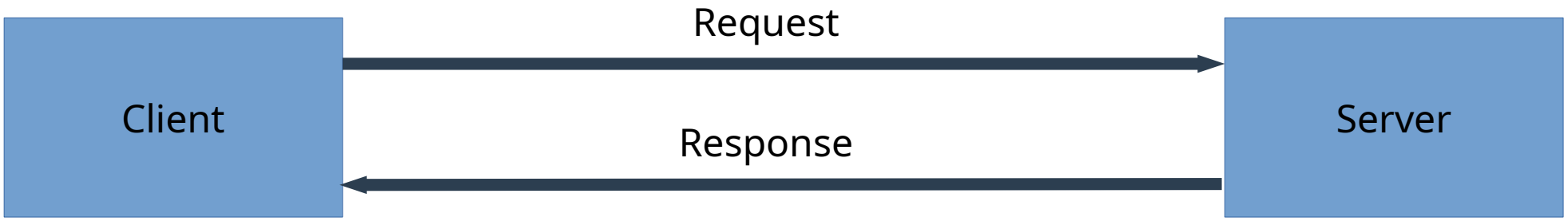
- **Hacker handle: nmatt**
- **Day Job: Security Engineer**
- **Other Interests/Passions:**
  - CTFing
  - Gaming on a Windows VM
    - (See: PCI passthrough via OVMF)
  - Philosophy/Theology

Agenda

- Intro to HTTP
- Browser Dev Tools Walkthrough
- Get Python setup and ready
- Write Python scripts to attack vulnerable webapp code

Intro to HTTP

- **HTTP = Hypertext Transfer Protocol**
  - Lets you transfer files to/from a web server
  - Clients make requests and Servers give responses
  - Text-based Protocol



Intro to HTTP – Requests and Responses

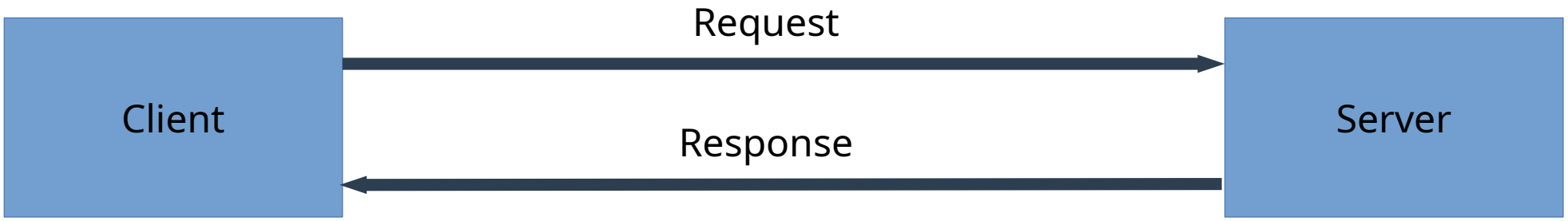
Request

```
GET /index.html HTTP/1.1
Host: example.com
User-Agent: curl/7.61.0
```

Response

```
HTTP/1.1 200 OK
Server: ECS (dca/53DB)
Content-Length: 1270

<html>
.............
```



Intro to HTTP – GET Request

- **HTTP GET**
  - Used to request data from a web server
  - Example: **http://example.com/index.html?var1=value1&var2=value2**

```
GET /index.html?var1=value1&var2=value2 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
```

Intro to HTTP – POST Request

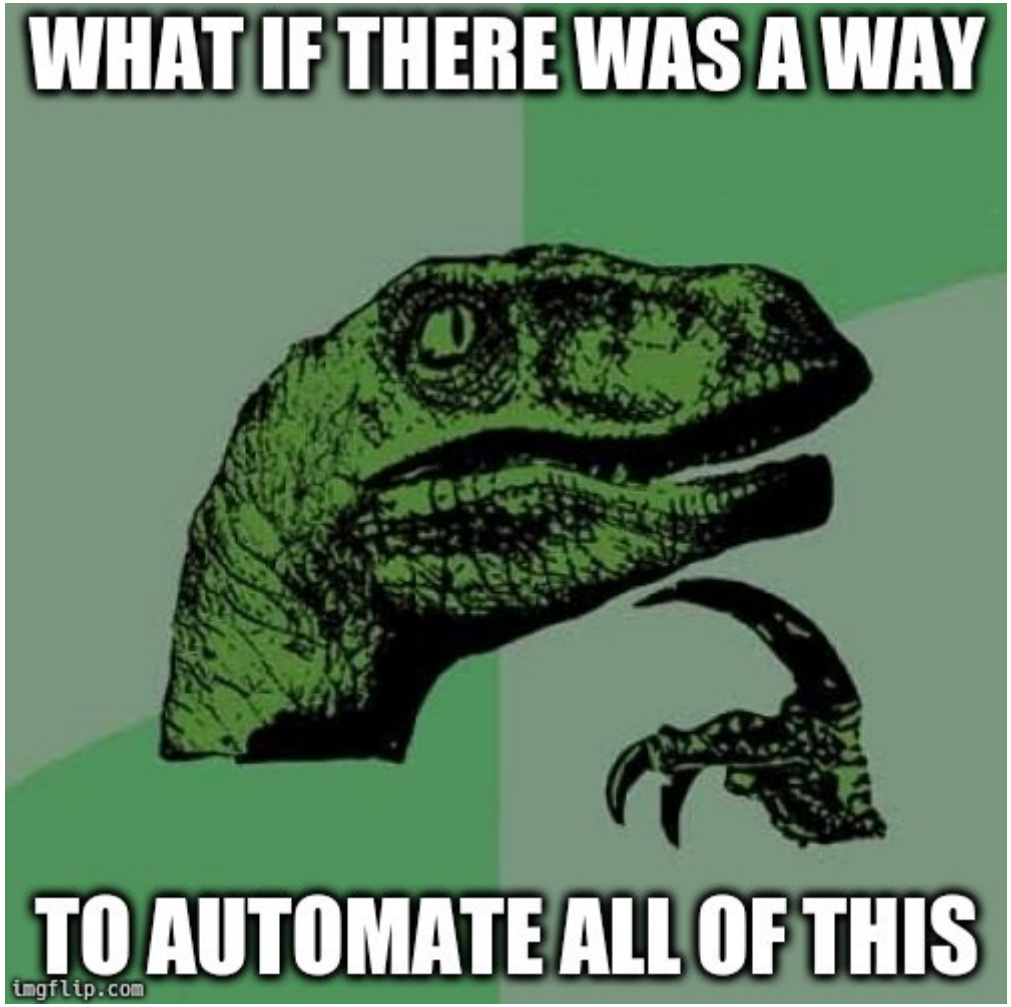
- **HTTP POST**
  - Used to send data to a web server
  - Example: POST to **http://example.com/index.html**
    - With data payload: **var1=value1&var2=value2**

```
POST /index.html HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Length: 23

var1=value1&var2=value2
```

Intro to HTTP – Hands On Example

- **Browser Dev Tools**
  - This demo works best in Firefox or Chrome
- **Browse to http://ctf.nmatt.com/example.php**
  - Observe GET request and response
- **Submit FAKE username and password to the login form**
  - Observe POST request and response


WHAT IF THERE WAS A WAY
TO AUTOMATE ALL OF THIS
imgflip.com

Scripting Web Attacks w/ Python

- **Why Python?**
  - Easy to learn
  - Great HTTP library: Requests
- **Getting things setup**
  - Install Requests library
    - `apt-get install python3 python3-requests` or `pip3 install requests`
  - Have the following open:
    - Text editor of choice
    - Shell to execute python scripts

Scripting Web Attacks w/ Python

- DEMO 1
- http://ctf.nmatt.com/demo1.php
- Write a python script that will:

1) send a GET request to the target page

2) Modify the script to pass the user agent check

Scripting Web Attacks w/ Python

- DEMO 2
- http://ctf.nmatt.com/demo2.php
- Write a python script that will:

1) Send a GET request to the target page

2) Set the correct cookie name and value

Scripting Web Attacks w/ Python

- DEMO 3
- http://ctf.nmatt.com/demo3.php
- Write a python script that will:

1) Send a POST request to the target page

2) Set the “username” and “password” in the data payload

Scripting Web Attacks w/ Python

- DEMO 4
- http://ctf.nmatt.com/demo4.php
- Write a python script that will:

1) Send a POST request to the target page

2) Set the “cmd” field in the data payload

3) Read the flag off the filesystem of the web server: “/flag.txt”

Scripting Web Attacks w/ Python

- **Questions?**

Link to webapp and attack scripts:
https://gitlab.com/nmatt0/WebAttackDemos