

# Web Hacking



# Agenda

- WTF is Web Hacking?!
- “B-A-BA” about Client - Server
- Top 10 OWASP
- Useful Tools
- Let’s Hack!



# \$ whoami

Vinícius Vieira

Pentester e Auditor CyberSec

Guerra Cibernética (Exército)

Professor FIAP

C|EH, CCNASec, DCTS, LPIC



# WTF is Web Hacking?!

De acordo com o Google, 30K sites são hackeados diariamente!

Na maioria dos casos a segurança não é levada em conta durante o desenvolvimento.

Explorar aplicações web envolve muito mais do que “conseguir um shell” em um servidor...

# Vantagens em atacar ambientes Web



- Portas de entrada para ambientes inteiros
- Muitas opções de input de dados
- Confiança nos inputs de usuários

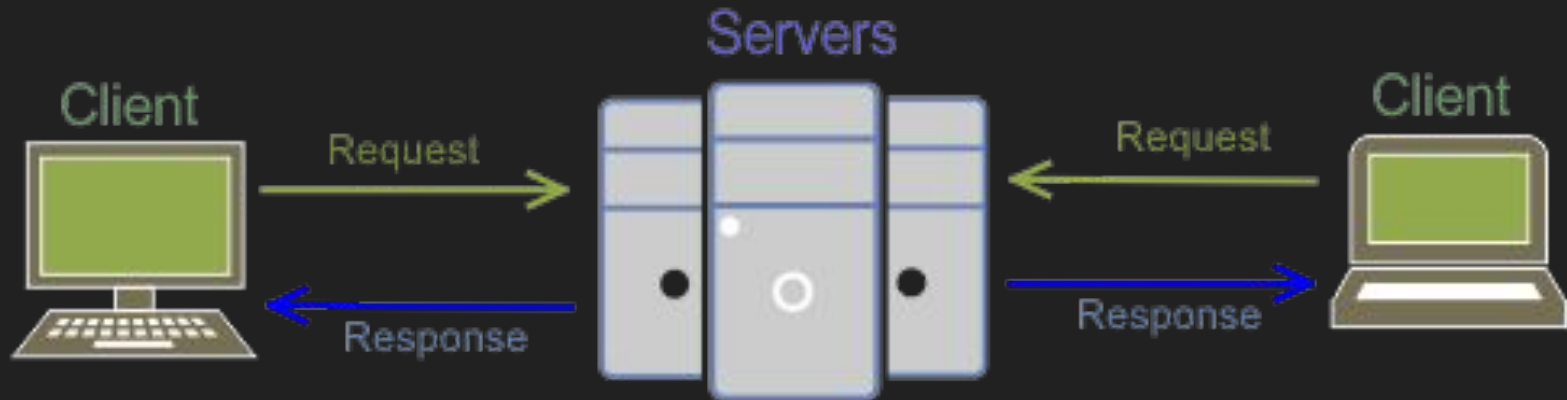
Então como encontrar um alvo vulnerável?

# O que vamos cobrir nessa live?

- Recon and Information Gathering
- SQLi
- Session Management
- XSS
- Broken Access Control
- RCE

...porém antes disso...

## Client Server Architecture



*The Client makes request for service to server.*

*The Server responds to that request.*



# HTTP Request and Response

- (1) User issues URL from a browser  
<http://host:port/path/file>



- (5) Browser formats the response and displays

**Client** (Browser)

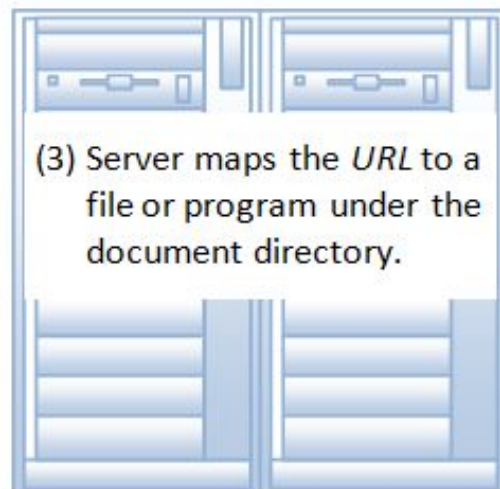
- (2) Browser sends a request message

```
GET URL HTTP/1.1  
Host: host:port  
.....  
.....
```

- (4) Server returns a response message

```
HTTP/1.1 200 OK  
.....  
.....  
.....
```

**HTTP** (Over TCP/IP)

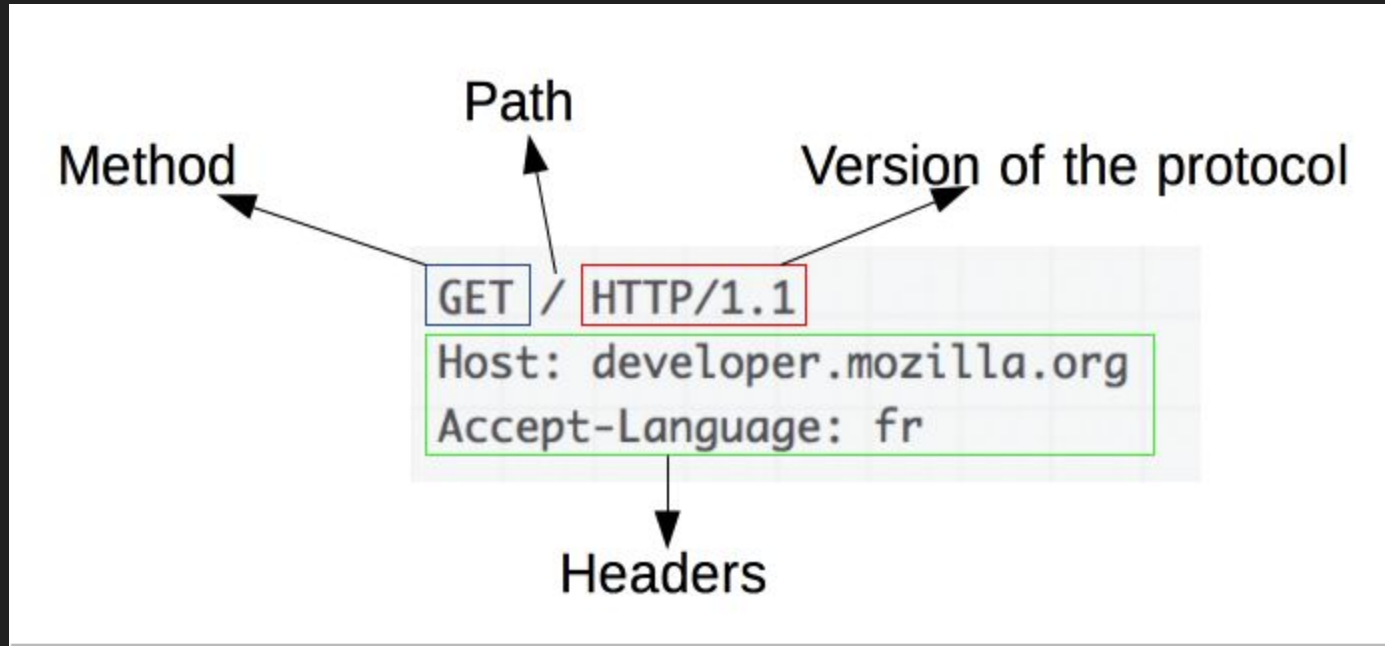


- (3) Server maps the *URL* to a file or program under the document directory.

**Server** (@ [host:port](#))



# HTTP Request and Response



...voltado ao assunto...



# Useful Tools

- Nmap
- DirBuster
- Nikto
- ZAP
- WPScan / Joomscan
- SQLMap
- Burp Suite
- NetCat
- WAppAnalyzer
- WFuzz
- Hydra
- Google ;)

# Let's Hack

- SQLi
- Session Management
- XSS
- Broken Access Control
- RCE



## owaspbwa

### OWASP Broken Web Applications Project

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see <http://sourceforge.net/apps/trac/owaspbwa/report/1>.



!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS

<https://sourceforge.net/projects/owaspbwa/files/>

# Thank you!



A user profile card from the platform HackTheBox. It features a skull profile picture on the left. To the right of the picture, the text reads: 'v1n1v131r4 Pro Hacker'. Below this, it shows 'Rank: 360' followed by a blue plus icon, '265' followed by a yellow star icon, and '6' followed by a green cube icon. At the bottom of the card, the email address 'hackthebox.eu' is displayed in green text.

[vinicius@sejalivre.org](mailto:vinicius@sejalivre.org)