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

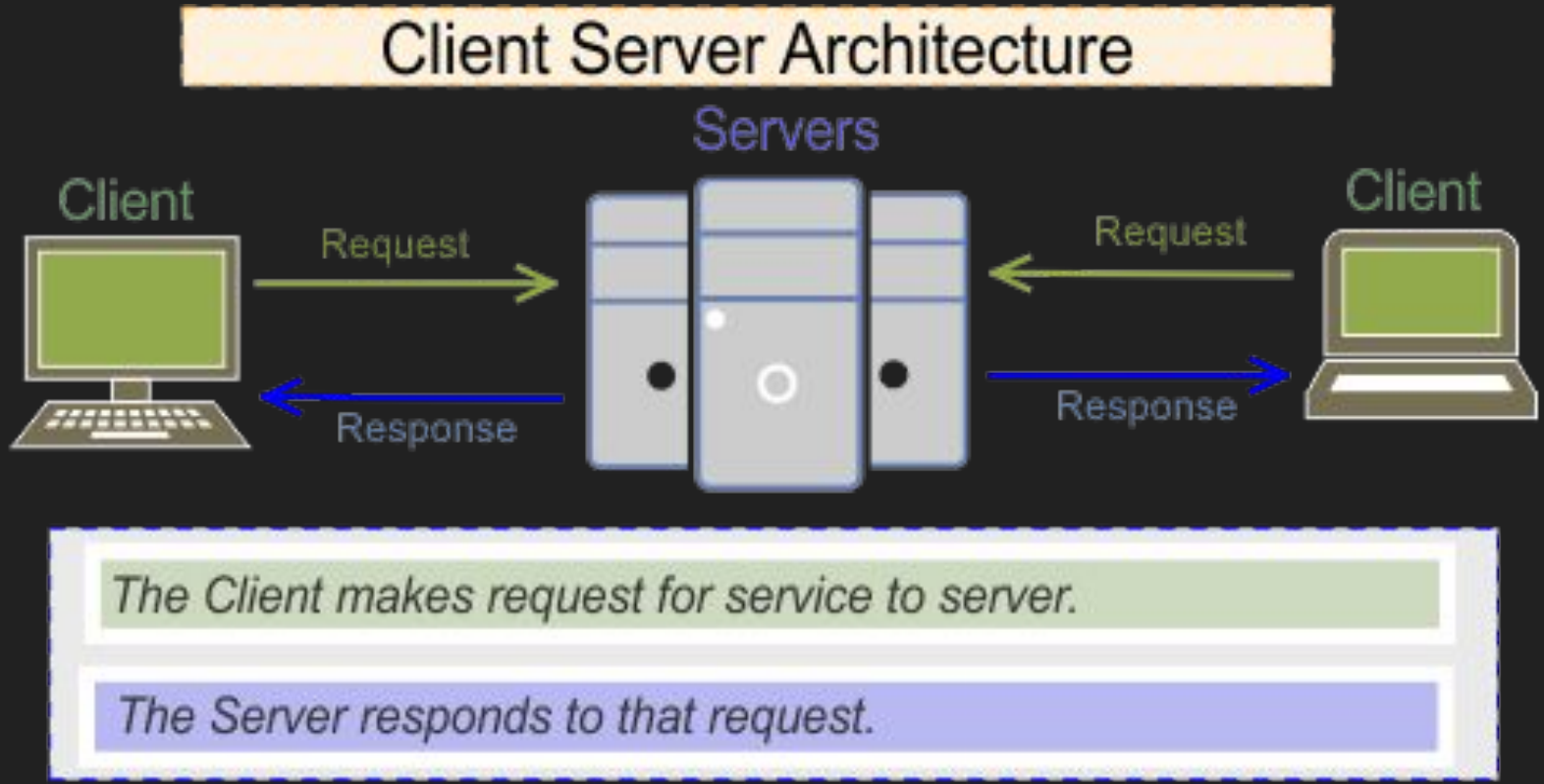
- Portas de entrada para ambientes inteiros
- Muitas opções de input de dados
- Confiança nos inputs de usuários

Então como encontrar um alvo vulnerável?

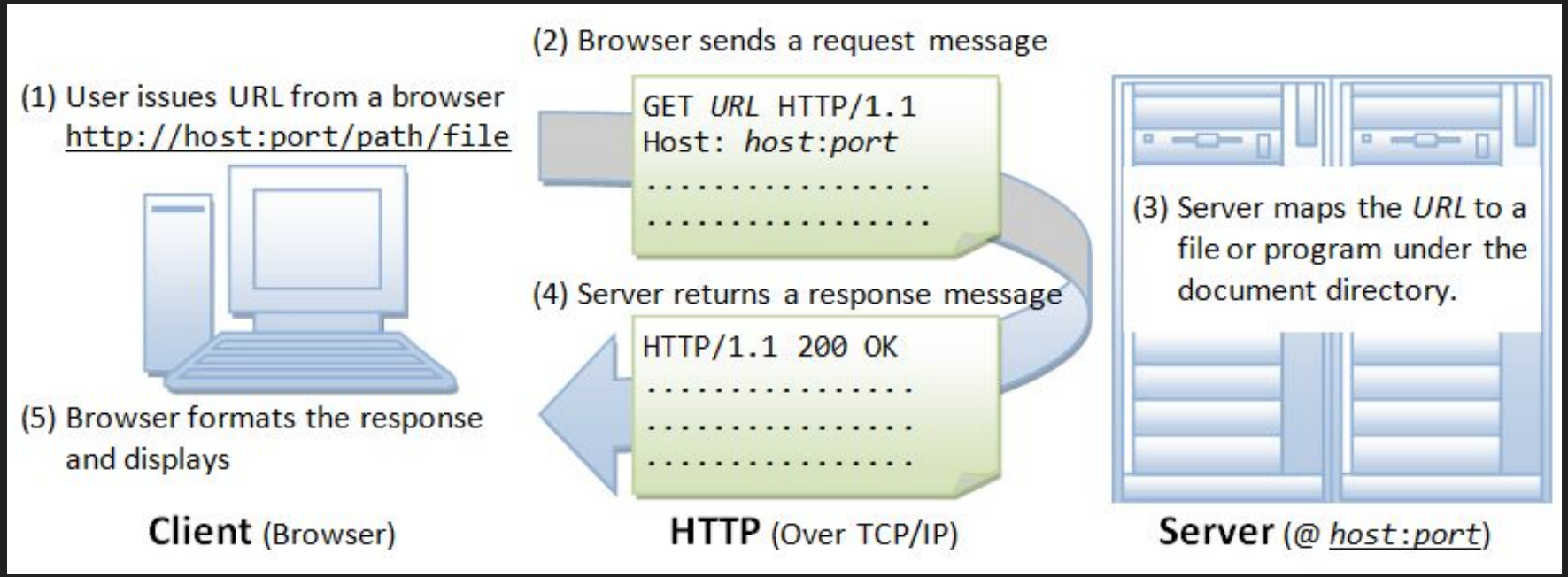
O que vamos cobrir nessa live?

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

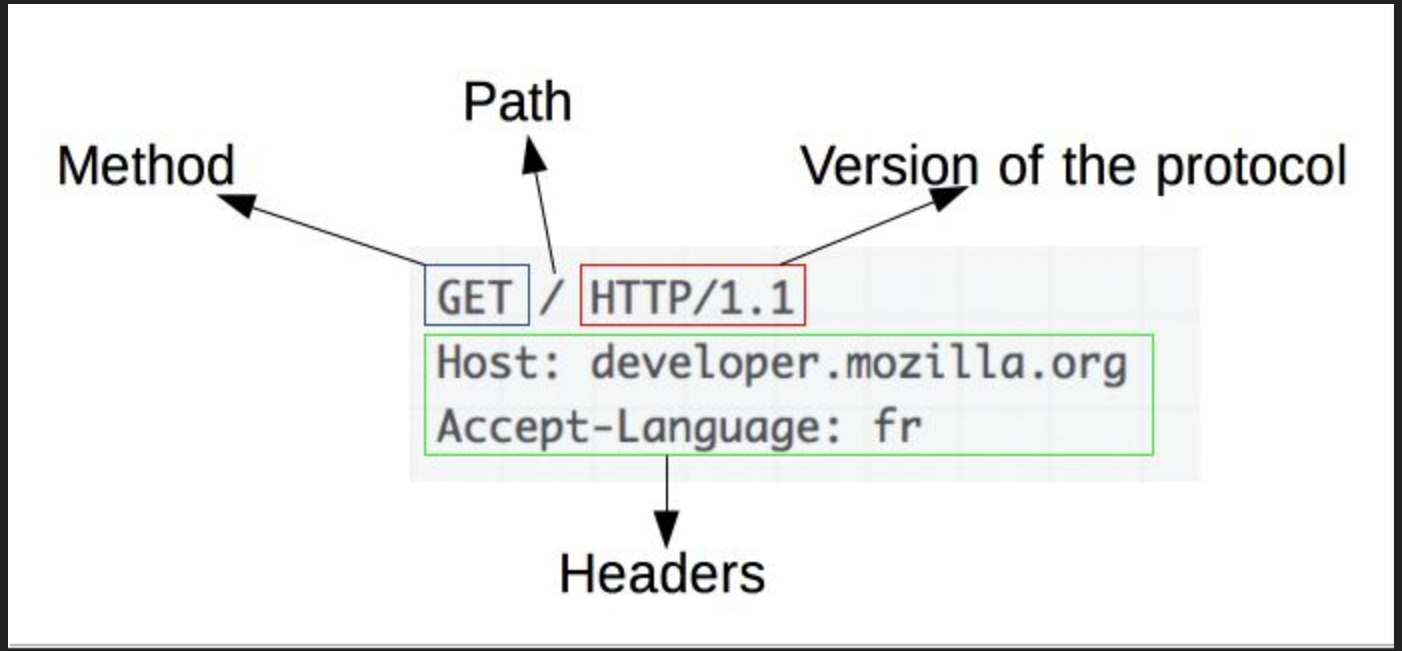
...porém antes disso...



HTTP Request and Response



HTTP Request and Response



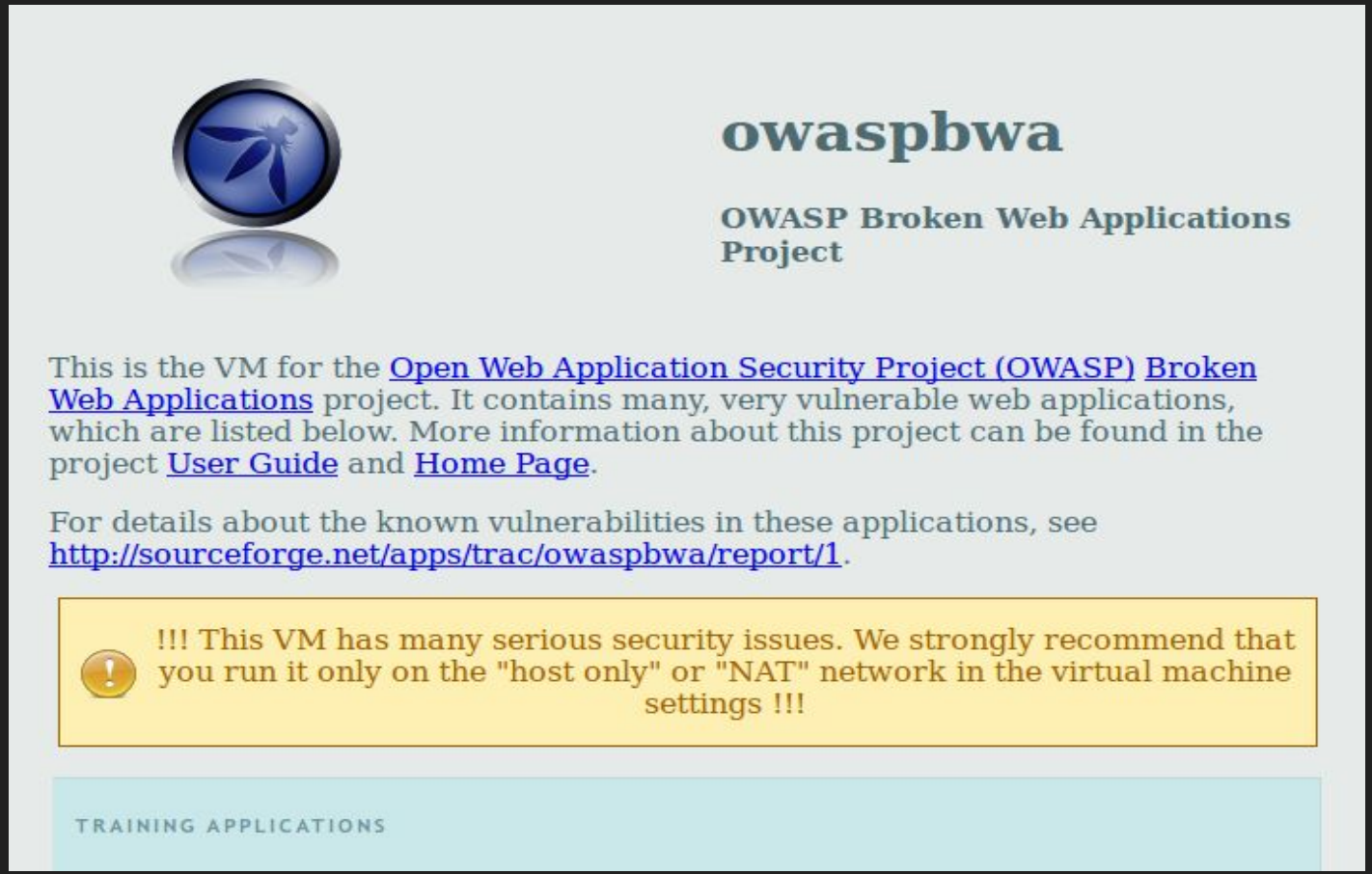
...voltado ao assunto...

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



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

Thank you!

vinicius@sejalivre.org