



Fundação Universidade Federal de Mato Grosso do Sul

Serviço Público Federal  
Ministério da Educação



## ATIVIDADE ORIENTADA A ENSINO

*Segurança Computacional com foco em Pentest*

### Identificação

Atividade Orientada a Ensino

Acadêmico: Pedro Augusto Paião Figueiredo

RGA: 2016 1907 0260

Professor: Carlos Alberto da Silva

Atividade: Atividade Orientada a Ensino sobre Segurança computacional (Pentest + OSINT)

### 1. Introdução

Esta atividade orientada a ensino aplica, em ambiente controlado, conceitos do TCC “Superfície de ataque em SaaS: impacto do OSINT na autenticação”. O objetivo pedagógico é demonstrar como fontes abertas (OSINT) reduzem o espaço de busca de identificadores de conta e como controles de autenticação (mensagens, rate limiting, MFA) influenciam o risco prático.

### 2. Objetivos de Aprendizagem

- Empregar OSINT para inferir padrões de e-mail institucionais.
- Mapear e validar endpoints de autenticação com ferramentas de inspeção.
- Conduzir tentativas controladas e éticas de login com telemetria.
- Avaliar consistência de mensagens, presença de rate limiting e esforço temporal.
- Propor mitigações mensuráveis e alinhadas a boas práticas (OWASP/NIST/ANPD).



### 3. Escopo Ético e Autorização

**Escopo restrito:** 1 conta autorizada + 1 controle inexistente para observar mensagens/códigos.

**Sem exaustão:** amostras curtas; sem contornar WAF/CDN; sem dumps privados.

**Registro:** coleta de evidências (prints, CSV, fluxos) e descarte seguro pós-aula.

### 4. Ambiente de Laboratório

- **Virtualização:** Oracle VirtualBox; VM com Kali Linux.
- **Rede:** uso de proxy HTTPS local para inspeção; sem varreduras intrusivas no “origin”.
- **Reprodutibilidade:** scripts versionados e resultados em CSV.

### 5. Ferramentas Utilizadas

- Fiddler / Burp / mitmproxy: interceptação TLS e mapeamento de rotas de autenticação.
- Censys / CT logs / buscadores: OSINT para padrões de e-mail e superfície exposta.
- curl/httpie, jq, grep/awk: checagens rápidas, extração e sumarização.
- Python 3 + requests: script de tentativas controladas com concorrência por threads.
- Crunch: geração de wordlists determinísticas (amostras).
-



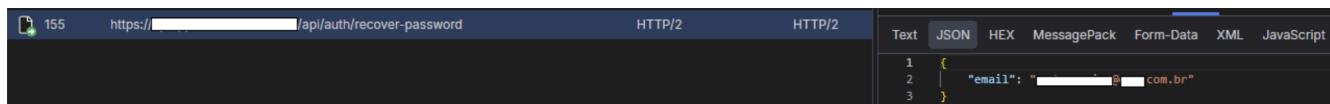
## 6. Metodologia

Análise do que funcionou bem, pontos de melhoria, e ajustes previstos para próximas turmas.

Passo 1 — Proxy HTTPS e mapeamento

Inspeção de chamadas do app e identificação de /api/auth/login e /api/auth/recovery-password (método, headers, corpo, padrões de resposta).

**A Figura 1** mostra a captura de uma requisição para o endpoint de recuperação de senha /api/auth/recovery-password, destacando o método HTTP, a URL completa e o corpo JSON contendo apenas o campo "email"

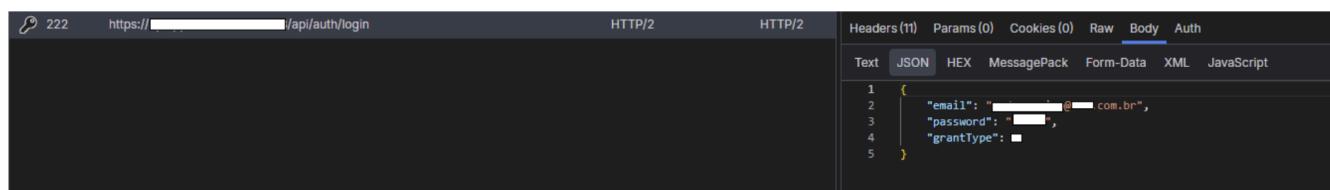


```
155 https://[REDACTED]/api/auth/recovery-password HTTP/2 HTTP/2
Text JSON HEX MessagePack Form-Data XML JavaScript
1 {
2   "email": "[REDACTED]@ufms.br"
3 }
```

**Figura 1. Rota de recuperar senha com o corpo enviado (/api/auth/recovery-password).**

**A Figura 2** apresenta a requisição para o endpoint de login /api/auth/login, na qual, além do "email", são enviados os demais parâmetros de autenticação (por exemplo, senha e tipo de grant). Essas capturas serviram de base para reproduzir o mesmo padrão de chamadas nos testes controlados com outras ferramentas.

**controlados com outras ferramentas.**



```
222 https://[REDACTED]/api/auth/login HTTP/2 HTTP/2
Headers (11) Params (0) Cookies (0) Raw Body Auth
Text JSON HEX MessagePack Form-Data XML JavaScript
1 {
2   "email": "[REDACTED]@ufms.br",
3   "password": "[REDACTED]",
4   "grantType": "password"
5 }
```

**Figura 2. Rota de login com o corpo enviado (/api/auth/login).**



## Passo 2 — Reconhecimento (OSINT)

Navegação por buscadores, CT logs e Censys para inferir padrão institucional de e-mail, camada WAF/CDN e metadados públicos.

Após o mapeamento de endpoints, foi realizado um reconhecimento da camada de exposição para caracterizar o front do domínio e verificar a presença de WAF/CDN. A sequência adotada incluiu varredura com nmap (portas/serviços e metadados TLS/SNI), consulta a whois (propriedade/ASN) e busca no Censys (OSINT) para levantar possíveis IPs candidatos por correlação de certificado/hostname.

### Procedimento.

1. **nmap**: confirmação de portas expostas e coleta de metadados.
2. **whois**: verificação de propriedade/ASN, com indicação de Cloudflare como WAF/CDN.
3. **Censys**: correlação por certificados/hostnames para identificação de IPs candidatos.

```
(Kali㉿Kali)-[~]
$ nmap [REDACTED].com.br
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 12:38 EST
Nmap scan report for [REDACTED]
Host is up (0.0071s latency).
Other addresses for [REDACTED] (not scanned): [REDACTED] 146 [REDACTED].9
[REDACTED]
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
```

**Figura 3.** nmap: portas/serviços e metadados TLS/SNI observados para o domínio.



Serviço Público Federal  
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



```
whois

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange: [REDACTED]
CIDR: [REDACTED]
NetName: CLOUDFLARENET
NetHandle: NET-[REDACTED]
Parent: NET-[REDACTED]
NetType: Direct Allocation
OriginAS:
Organization: Cloudflare, Inc. (CLOUD14)
RegDate: 2015-02-25
Updated: 2024-09-04
Comment: All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Comment: Geofeed: https://api.cloudflare.com/local-ip-ranges.csv
Ref: https://rdap.arin.net/registry/ip/[REDACTED]
```

**Figura 4.** whois: evidência de CDN/WAF (Cloudflare) como camada de exposição.



Serviço Público Federal  
Ministério da Educação  
Fundação Universidade Federal de Mato Grosso do Sul



censys

---

**Results**

**Host Filters**

Labels:

- 4 open-dir
- 3 file-sharing
- 3 google-analytics
- 3 google-tag-manager
- 3 ipv6

More

Autonomous System:

- 7 CLARO S.A.
- 5 CLOUDFLARENET
- 4 Century Telecom Ltda
- 3 ALGAR TELECOM SA
- 1 Claro NXT
- Telecommunicacoes Ltda

Location:

- 15 Brazil
- 5 United States

**Service Filters**

Service Names:

- 60 HTTP
- 3 FTP
- 2 IKE
- 2 SNMP
- 1 SSH

**Hosts**  
Results: 20 Time: 0.07s

<a href="#">.181 (</a>	<a href="#">.com.br)</a>			
Microsoft	CLARO S.A. (4230)	Minas Gerais, Brazil		
<a href="#">google-analytics</a>	<a href="#">google-tag-manager</a>	<a href="#">jquery</a>	<a href="#">jquery-ui</a>	<a href="#">slick</a>
<a href="#">443/HTTP</a>	<a href="#">2053/HTTP</a>	<a href="#">2083/HTTP</a>	<a href="#">8443/HTTP</a>	
 <a href="#">.178</a>				
Microsoft Windows Server 2012	CLARO S.A. (4230)	Minas Gerais, Brazil		
<a href="#">google-analytics</a>	<a href="#">google-tag-manager</a>	<a href="#">jquery</a>	<a href="#">jquery-ui</a>	<a href="#">slick</a>
<a href="#">443/HTTP</a>				
 <a href="#">.142 (</a>				
Microsoft Windows Server 2012	Century Telecom Ltda (21574)	Minas Gerais, Brazil		
<a href="#">443/HTTP</a>				
Microsoft Windows Server 2012	CLARO S.A. (4230)	Minas Gerais, Brazil		
<a href="#">443/HTTP</a>				
Microsoft	ALGAR TELECOM SA (16735)	São Paulo, Brazil		
<a href="#">open-dir</a>				
<a href="#">443/HTTP</a>	<a href="#">7090/HTTP</a>	<a href="#">9090/HTTP</a>		

**Figura 5.** Censys: correlação por certificado/hostname indicando possíveis IPs candidatos



### Passo 3 — Validação controlada

Reprodução da requisição de login via IP/hostname em cliente HTTP, comparando códigos/latências com o fluxo original.

POST https://api/auth/login

Body (application/json)

```
1 {  
2   "email": "██████████",  
3   "password": "██████████",  
4   "grantType": "██████████"  
5 }
```

200 OK 3.62 s 455 B

**Figura 6.** Postman — requisição POST para `https://api/auth/login` com `Content-Type: application/json` e corpo equivalente ao mapeado no Fiddler.

### Passo 4 — Obtenção de identificadores (OSINT)

Coleta passiva de endereços e seleção de 1 e-mail autorizado para os testes; um e-mail inexistente serve de controle.

#### Start your Search

- Company search
- Person search
- Decision Maker search
- LinkedIn URL search

Domain (recommended) or company name:

company.com

Search

#### Search history

.br

Valid 17 emails found

@ com.br	@ .br		r@ .com.br	t@ com.br
@ com.br	i@ com.br	:	@ .com.br	i@ com.br
i@ com.br	)@ com.br	@	.com.br	i@ com.br
@ com.br	i@ com.br	i@t	.com.br	@ com.br
i@ com.br				

Copy 17 emails

**Figura 7.** Exemplo de consulta OSINT para extração de padrões de e-mail no domínio de interesse.



## Passo 5 — Recovery

Comparação de respostas do /recovery-password (válido vs. inexistente) para avaliar granularidade e potencial de enumeração.

A Figura 8 ilustra o teste controlado realizado sobre o endpoint de recuperação de senha /api/auth/recovery-password. Na parte superior da captura, observa-se a requisição HTTP contendo apenas o campo "email" no corpo JSON. Na parte inferior, são exibidas as respostas retornadas pela aplicação para diferentes cenários (endereço cadastrado e endereço inexistente), com variações tanto no conteúdo da mensagem quanto nos campos estruturados da resposta. Essa diferença de granularidade fornece ao atacante um canal de enumeração de contas, permitindo inferir se um determinado e-mail está ou não registrado no sistema a partir do texto de erro e dos códigos retornados.

The screenshot shows a network traffic capture interface. At the top, a POST request is shown to the endpoint `/api/auth/recover-password`. The request body is a JSON object with a single field `"email": "██"`. The response section shows two entries. The first response (labeled 'Response (CERTIFICATE VALID)') is for a valid email and contains a JSON object with fields like `"ResponseType": 2`, `"Key": "██"`, and `"Message": "E-mail: ██████████@████████.████ não cadastrado."`. The second response (labeled '(BODY: 200.00 B) (TLS 1.3) (HTTP/2) (404)') is for an invalid email and contains a JSON object with fields like `"Error": "E-mail: ██████████@████████.████ não cadastrado."`. The interface includes tabs for Headers, Cookies, Raw, Preview, and Body, with the Body tab selected. The JSON tab is also visible.

**Figura 8.** Evidência de granularidade de mensagens no endpoint /api/auth/recovery-password (exemplo sanitizado).



## Passo 6 — Login com script fixo (threads)

Execução de amostra: threads concorrentes lendo wordlist curta; registro por tentativa: timestamp, código, latência e snippet em CSV; resumo por categorias (200/401/403/429/5xx).

```
CONST URL      = "https://<host>/api/auth/login"
CONST EMAIL    = "usuario_autorizado@dominio"
CONST WORDLIST = "wordlist_8digitos.txt"
CONST THREADS  = 8
CONST OUT_CSV  = "login_results.csv"

fila_senhas = carregar_linhas(WORDLIST)
iniciar_csv(OUT_CSV, "timestamp,attempt,http_status,elapsed_ms,snippet")

contador = 0
função worker():
    enquanto houver senha em fila_senhas:
        senha = puxar_proxima()
        ini = agora()
        resp = POST(URL, json={email: EMAIL, password: senha})
        fim = agora()
        escrever_csv(OUT_CSV, [ini, ++contador, resp.status, millis(fim-ini), trecho(resp.mensagem)])
        se resp.status == 200: sinalizar_sucesso_e_parar_todos()

lançar THREADS workers
aguardar_todas
resumir_por_codigo(OUT_CSV)
```

## 7. Resultados (resumo didático)

- **Recovery:** respostas distintas (ex.: 200 para e-mail válido vs. 401 para inexistente) → canal de enumeração.
- **Login (amostra):** predominância de 401; 0 ocorrências de 429 na janela observada; 1 retorno 200 isolado (não conclusivo).
- **Esforço prático:** sem reação defensiva explícita na amostra curta; latência estável.

## 8. Evidências

- Capturas do Fiddler/Burp (requisições e respostas sanitizadas).



Serviço Público Federal  
Ministério da Educação

**Fundação Universidade Federal de Mato Grosso do Sul**



- Fluxograma do procedimento do script.
- Saída do terminal com resumo por código HTTP e caminho do CSV.
- Excertos de CSV (5-10 linhas) e gráfico simples (barra) de códigos.

## 9. Discussão

- Impacto do OSINT: reduzir o espaço de busca de identificadores encurta o caminho até o ponto de autenticação.
- Superfície de login: mensagens não uniformes e ausência de limites claros elevam o risco de enumeração/tentativas repetidas.
- Medibilidade: métricas como tempo até 429, tentativas até bloqueio, variação de latência e taxa de indistinguibilidade das respostas permitem acompanhar evolução.

## 9. Mitigações Recomendadas

- Mensagens uniformes em login/recovery (indistinguíveis para falhas).
- Rate limiting com janela deslizante por conta e origem (IP/ASN), atraso progressivo e bloqueio temporário.
- MFA por risco e checagem contra senhas comprometidas.
- Higiene de exposição pública: reduzir previsibilidade de e-mails e remover artefatos acessíveis.
- Telemetria de abuso: dashboards de códigos/latências, bursts por ASN, alertas de spraying/stuffing.



Serviço Público Federal  
Ministério da Educação

**Fundação Universidade Federal de Mato Grosso do Sul**



## 7. Assinaturas

Acadêmico(a): \_\_\_\_\_

Professor(a): \_\_\_\_\_