



De noobs a Investigadores de vulnerabilidades

Natan Morette



>\$ Whoami

- [+] Natan Morette - nmmorette.github.io
- [+] Analista Senior de Seguridad de la Información
- [+] Instructor de Seguridad Ofensiva
- [+] En tecnología desde los 15 años
- [+] Certificaciones – Un verdadero “alfabeto en sopa”
- [+] 30+ CVEs gracias a CVE-Hunters
- [+] Interested in:
 - └ 🎮 Videojuegos
 - └ 🏄 Surf
 - └ 📖 Libros de Ciencia ficción



>\$ Agenda



- 1** Contexto y Problema
- 2** Proyecto CVE-Hunters
- 3** Ola 1
- 4** Ola 2

- 5** Lecciones
- 6** Travessuras de CVE-Hunters
- 7** Números
- 8** Conclusión

>\$ Contexto y Problema

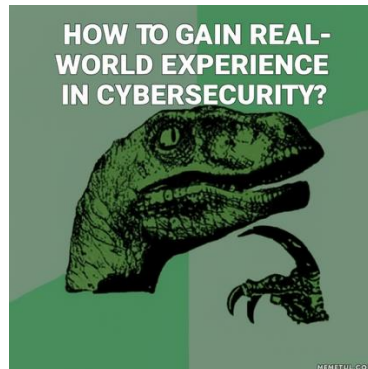


Contexto

- Durante mis clases, muchos me **preguntan cómo obtener experiencia en ciberseguridad.**
- Mis consejos:
 - Participa en CTFs
 - Estudia para certificaciones

La industria exige experiencia

La mayoría de las oportunidades, incluso para junior, requieren algo de experiencia. Y conseguir tu primer trabajo en ciberseguridad puede ser muy difícil.



>\$ Proyecto CVE Hunters



El comienzo

En noviembre de 2024, decidí reunir a algunos estudiantes para investigar vulnerabilidades en proyectos de código abierto.

Con solo tres personas: yo y dos estudiantes, ni siquiera sabíamos si lograríamos publicar un solo CVE — yo mismo aún no había publicado ninguno.

Ola-1

Llamamos a esa primera fase *Ola-1* y nos enfocamos en un pequeño proyecto local de código abierto llamado **Wegia**.

No teníamos una hoja de ruta clara — solo curiosidad, motivación y las ganas de aprender juntos.

The Process

La idea era: como miembro más experimentado del grupo, encontraría algunas vulnerabilidades, publicaría unos cuantos CVE y luego transmitiría la metodología a los estudiantes para que ellos pudieran compartirla más adelante con otros.



>\$ Ola 1 – Proyecto Wegia

Por qué este Proyecto?

Wegia es un software de código abierto utilizada por programas sociales y ONG en Brasil. Nos brindó la oportunidad perfecta para aprender seguridad ofensiva mientras aportábamos algo a la comunidad..

Uso Real

Usado activamente por orfanatos, residencias de ancianos y centros de adopción de mascotas – lugares que atienden a quienes más necesitan protección.



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%

>\$ Ola 1 – Resultados

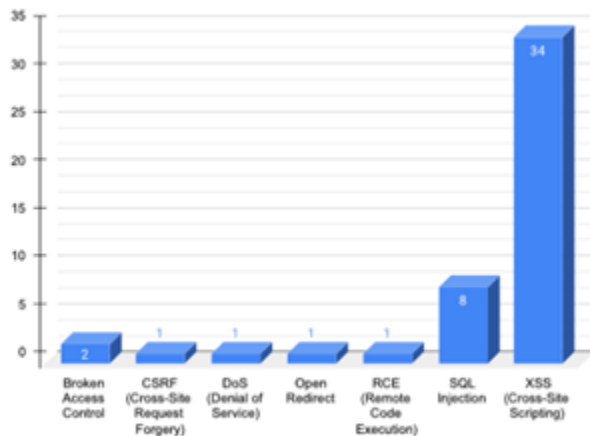


Resultados Directos

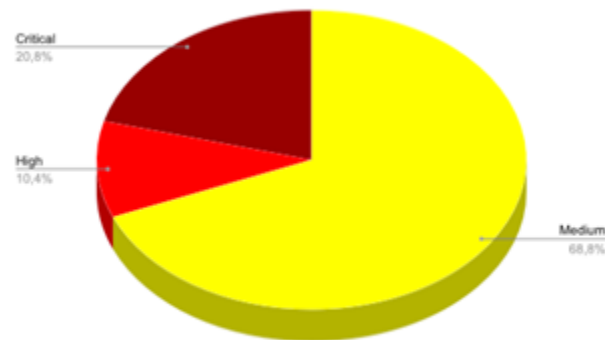
48 CVEs publicados

- 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 provinieron de uma estudante: Elisangela Mendonça



(a) Vulnerabilities



(b) Severity

Credits



elisangelasilvademendonca

Finder

Resultados Indirectos

Dos estudiantes consiguieron sus primeros empleos en ciberseguridad.
Los desarrolladores de **WeGia** contactaron para agradecer y colaborar más.
Nuevos investigadores externos comenzaron a contribuir al proyecto.

>\$ Ola 2 – Portabilis



Más estudiantes

10 nuevos estudiantes

Nuevos proyectos

Comenzar a identificar nuevos proyectos que se alineen con la misión de nuestro grupo
— no solo proyectos aleatorios.



¿Cómo encontramos este software?

<https://ieducar.org>

portabilis/i-educar

Lançando o maior software livre de educação do Brasil!



62 Contributors 4 Issues 643 Stars 463 Forks

portabilis/i-diario-app

Aplicativo para o professor com lançamento de frequência e registro de conteúdos offline, integrado com o software livre i-Diário e...



10 Contributors 0 Issues 22 Stars 16 Forks

>\$ Portabilis – Números

Quiénes lo usan?



Varias escuelas públicas en todo Brasil.



Brazilian Airforce

Fuimos proactivos y nos pusimos en contacto con Portabilis — fueron muy receptivos a nuestro proyecto y abiertos a una colaboración estrecha.

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

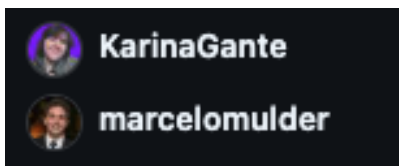
Students reached

<https://ieducar.org>

>\$ Ola 2 – Resultados

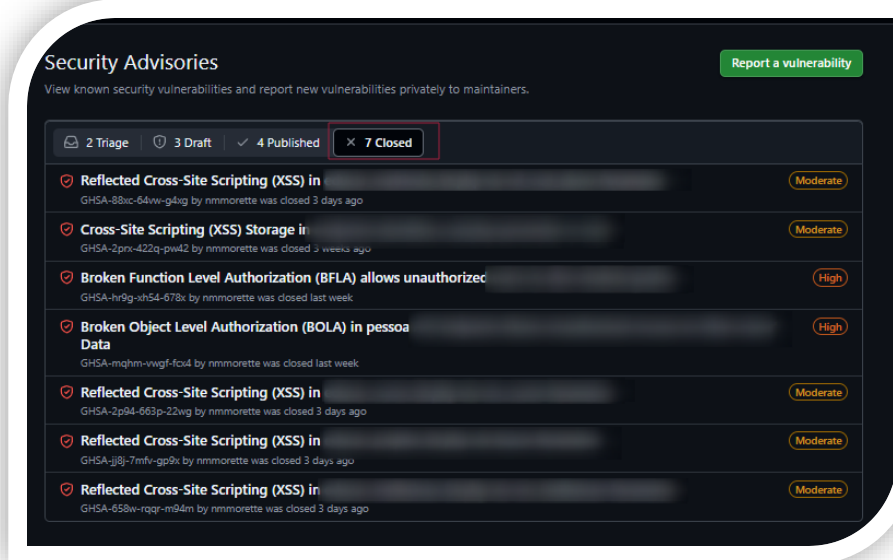


98 vulnerabilidades encontradas no I-Educar 72 CVE publicadas
19 vulnerabilidades encontradas no i-Diário 12 CVE publicadas



>\$ Lecciones

- Priorizamos proyectos con la seguridad habilitada en GitHub para seguir el flujo completo de divulgación.
- Es una calle de doble sentido: nosotros reportamos vulnerabilidades, ellos corrigen y solicitan CVE.
- Sin embargo, algunos desarrolladores no están realmente abiertos a la colaboración en materia de seguridad.
- Corrigen el problema y cierran el aviso sin solicitar un CVE. O dejan el aviso abierto sin la solicitud de CVE, incluso después de haber hecho el *commit* con la corrección.



La mayoría de los proyectos en los que estamos trabajando ahora utilizan **VulnDB** para la notificación.

Dec 26, 2024.

>\$ Ola 3 – En ejecución ahora



scada-
LTS



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

Nuevos proyectos | Nuevos Estudiantes | Abierto a todos

> \$ Travessuras de CVE-Hunters



✓ Vulnerable o no?



✓ Sueño de todo estudiante



>\$ Vulnerabilidades en API



✓ BOLA

Broken Object Level Authorization

Puedes acceder a cosas de otra persona (como su cuenta, datos, etc.) — incluso cuando no deberías, simplemente modificando el ID en un request.

API1:2023

✓ BFLA

Broken Function Level Authorization

Puedes realizar acciones no autorizadas llamando a funciones a las que no deberías tener acceso — como eliminar a otros usuarios, ascenderte a administrador, etc.

API5:2023



>\$ Indico



Indico es:

- 📅 una herramienta de gestión de eventos de propósito general;
 - 🌐 completamente basada en la web;
 - 🌱 rica en funciones pero también extensible mediante el uso de complementos;
 - 🔧 software de código abierto bajo la licencia MIT;
- hecha en el CERN, ¡el lugar donde nació la web!

indico/indico

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



113
Contributors

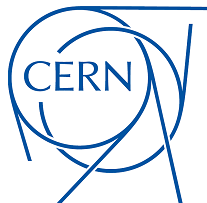
83
Used by

2k
Stars

480
Forks



¿Quién lo usa?



European Council for Nuclear Research.



**United
Nations**



esa
European Space Agency



Muchas instituciones
académicas em el
mundo usan Indico.

			Response			
Request			Pretty	Raw	Hex	Render
Pretty	Raw	Hex				
1 POST /api/princi			1 HTTP/1.1 200 OK			
2 Host: 10.10.10.10			2 Server: nginx/1.26.3			
3 Cookie: aHR0cH			3 Date: Tue, 10 Jun 2025 19:02:32 GMT			
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0			4 Content-Type: application/json			
5 Accept: application/json			5 Connection: keep-alive			
6 Accept-Language: pt-BR			6 Vary: Accept-Encoding			
7 Accept-Encoding: gzip, deflate			7 X-Indico-URL: /api/principals			
8 Content-Type: application/json			8 Vary: Cookie			
9 X-Requested-With: XMLHttpRequest			9 Content-Length: 344			
10 X-Csrf-Token: 69			10 {			
11 Content-Length: 69			11 {			
12 Origin: https://10.10.10.10			12 "User:1":{			
13 Referer: https://10.10.10.10			13 "affiliation": "Root",			
14 Sec-Fetch-Dest: empty			14 "affiliation_id": null,			
15 Sec-Fetch-Mode: cors			15 "affiliation_meta": null,			
16 Sec-Fetch-Site: same-origin			16 "avatar_url": "/user/1/picture-default/MQ.V4G8HTnUj_MahUnFFdb7Yp1Dd4s",			
17 Te: trailers			17 "detail": "servnac@rnp.br (Root)",			
18 Connection: keep-alive			18 "email": "servnac@rnp.br",			
19 {			19 "first_name": "admin",			
20 {			20 "identifier": "User:1",			
21 {			21 "invalid": false,			
22 {			22 "last_name": "GTI",			
23 {			23 "name": "admin GTI",			
24 {			24 "title": "none",			
25 {			25 "type": "user",			
26 {			26 "user_id": 1			
27 {			27 }			
28 {			28 }			
29 {			29 }			
30 {			30 }			
31 {			31 }			
32 {			32 }			
33 {			33 }			
34 {			34 }			
35 {			35 }			
36 {			36 }			
37 {			37 }			
38 {			38 }			
39 {			39 }			
40 {			40 }			
41 {			41 }			
42 {			42 }			
43 {			43 }			
44 {			44 }			
45 {			45 }			
46 {			46 }			
47 {			47 }			
48 {			48 }			
49 {			49 }			
50 {			50 }			
51 {			51 }			
52 {			52 }			
53 {			53 }			
54 {			54 }			
55 {			55 }			
56 {			56 }			
57 {			57 }			
58 {			58 }			
59 {			59 }			
60 {			60 }			
61 {			61 }			
62 {			62 }			
63 {			63 }			
64 {			64 }			
65 {			65 }			
66 {			66 }			
67 {			67 }			
68 {			68 }			
69 {			69 }			
70 {			70 }			
71 {			71 }			
72 {			72 }			
73 {			73 }			
74 {			74 }			
75 {			75 }			
76 {			76 }			
77 {			77 }			
78 {			78 }			
79 {			79 }			
80 {			80 }			
81 {			81 }			
82 {			82 }			
83 {			83 }			
84 {			84 }			
85 {			85 }			
86 {			86 }			
87 {			87 }			
88 {			88 }			
89 {			89 }			
90 {			90 }			
91 {			91 }			
92 {			92 }			
93 {			93 }			
94 {			94 }			
95 {			95 }			
96 {			96 }			
97 {			97 }			
98 {			98 }			
99 {			99 }			
100 {			100 }			





Parrot Terminal

File Edit View Search Terminal Help

`[root@parrot]-[/home/crv157/Desktop]`

#

crv157's Home

Trash

XSStrike

Indico.py

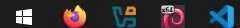


Firefox



Calico

Menu [Burp Suite Commun... [Home - Indico - Moz... Parrot Terminal

11:28
27/06/2025

>\$ Vulnerable o no?



CVE-2025-53640

¿Quién cree que esto es una vulnerabilidad?

BOLA


Un usuario común es capaz de recuperar datos de todos los usuarios dentro de la aplicación, incluyendo:

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

CVE ID
CVE-2025-53640

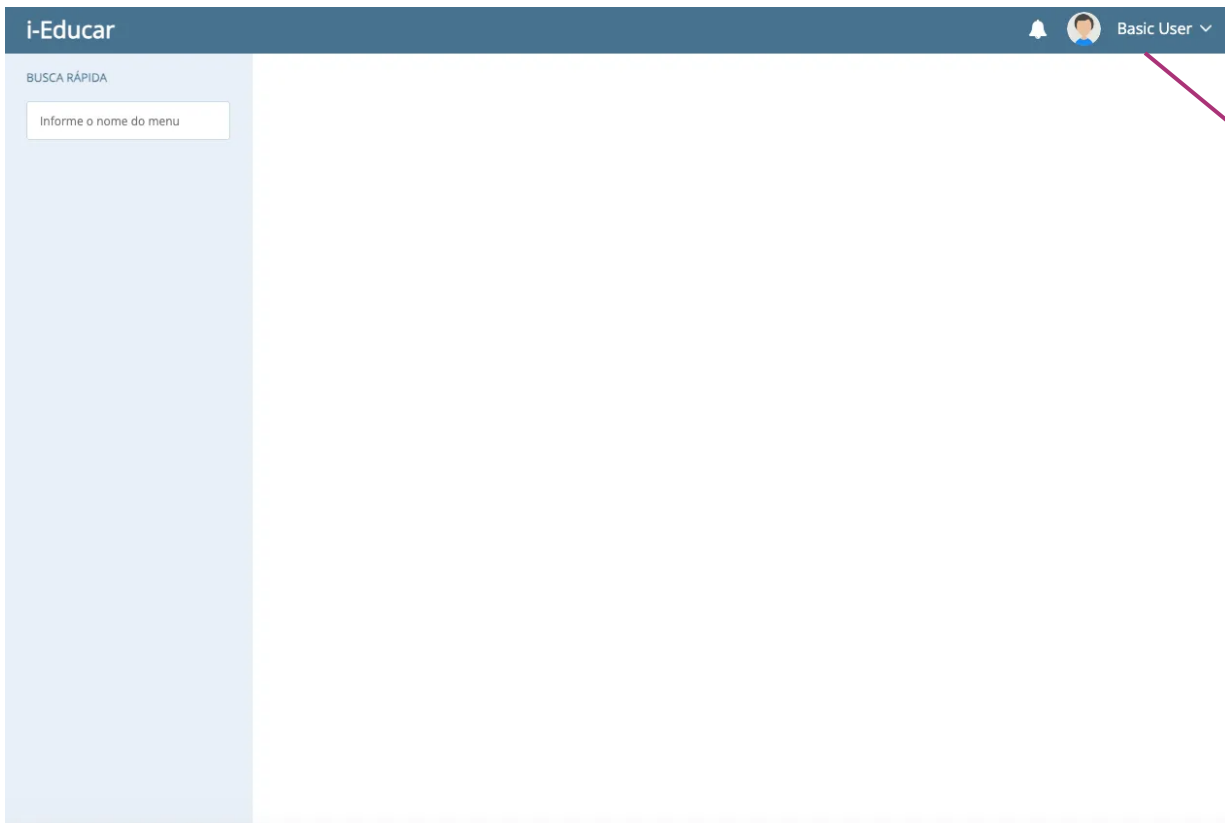
GHSA ID
GHSA-q28v-664f-q6wj

Source code
[indico/indico](#)

Credits
 [rafaelfcorvino1](#) [Finder](#)

>\$ Sueño de todo estudiante

CVE-2025-8789



Un usuario sin privilegios no podía hacer nada a través de la interfaz.

\$> CVE-2025-8789



```
1 GET /module/Api
  %5B770%5D%5B2
2 Host: comunida
3 Connection: ke
4 sec-ch-ua: "No
5 sec-ch-ua-mobi
6 sec-ch-ua-plat
7 Accept-Languag
8 Upgrade-Insecu
9 User-Agent: Mo
  37.36
10 Accept: text/h
  exchange;v=b3;
11 Sec-Fetch-Site
12 Sec-Fetch-Mode
13 Sec-Fetch-User
14 Sec-Fetch-Dest
15 Accept-Encodin
16 Cookie: i_educ
17
18 |
```

API

Edinei Valdameri edited this page on Jan 18, 2023 · [5 revisions](#)

API i-Educar

O i-Educar conta com uma API JSON que permite o acesso externo de outras aplicações. Para utilizá-la é necessário possuir o token que cada aplicação possui configurado no seu arquivo `ieducar.ini`.

Endpoints

Existem inúmeros endpoints disponíveis para consultar informações do i-Educar, mais abaixo há a listagem completa.

Como fazer uma requisição

A maior parte das requisições do i-Educar é feita utilizando o método HTTP GET e passando seus parâmetros via query string na URL para o endpoint que sempre começará com `https://seudominio.com.br/module/Api/`.

URL `https://seudominio.com.br/module/Api/Aluno?access_key=abc123&oper=get&resource=aluno&id=1`

\$> CVE-2025-8789

```
1 HTTP/1.1 200 OK
2 Date: Fri, 16 May 2025 16:10:42 GMT
3 Content-Type: application/json; charset=UTF-8
4 Connection: keep-alive
5 X-Xss-Protection: 1; mode=block
6 X-Frame-Options: SAMEORIGIN
7 Server: cloudflare
8 Vary: Accept-Encoding
9 Cache-Control: no-cache, private
10 Cf-Ray: 940c258a087764ea-GIG
11 Strict-Transport-Security: max-age=63072000
12 Cf-Cache-Status: DYNAMIC
13 Server-Timing: cfCacheStatus;desc="DYNAMIC"
14 Report-To: [{"endpoints":[{"url":"https://a-nel.cloudflare.com/v/report/v4?s=17ggmEL8XYFLi90p0F0uHxUl9h18439q6FZF0sKMas9Vld1os44uBB60hxhQoKU13ZozkT5aQ39aet57tbz8CFhSBQCrrNMZFvME%2B0LLARG6doksaj1zicnmRRoLiZZM5%2B8ia0ZfkHygN5Jc0l1T"}],"group":"cf-nel","max_age":604800}
15 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
16 Expect-Ct: max-age=86400, enforce
17 Referrer-Policy: same-origin
18 X-Content-Type-Options: nosniff
19 Set-Cookie: 1_educar_session=zRwb2f27m1K3FC1t1MeFsJjymzAhbRRBzHtIrv5H; HttpOnly; SameSite=Lax; Path=/; Max-Age=0; Expires=Fri, 16 May 2025 18:10:42 GMT
20 alt-svc: h3=":443"; ma=86400
21 server-timing: cf;desc="?proto=TCP&rtt=27676min_rtt=21096rtt_var=12615sent=56recv=66lost=0&retrans=0&comp_by=8366recv_bytes=15436delivery_rate=1917496&cwnd=2526unsent_bytes=0&cid=83c01f20270589b8&ts=5846"
22 Content-Length: 120
23
24 {
25   "oper": "post",
26   "resource": "notas",
27   "msgs": [
28     {
29       "msg": "Notas postadas com sucesso!",
30       "type": "success"
31     }
32   ],
33   "any_error_msg": false
34 }
```



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

>\$ Y la Plata?

0-Day

CONCLUÍDO ⓘ

Transferência de
Trend Micro

+ US\$ 275,00

5 set 2025 - 04:02



ZERO DAY
INITIATIVE



CVE-2025-10023

MARCELOQJ ✓

7.2 HIGH
CVSS SCORE FRI, 5 SEP 2025

+35 pts ↗

€500

SQL INJECTION **CWE-89**

YesWeHack



centreon

> \$ Numeros



~~170~~ **236** Vulnerabilidades

2 Alianzas directas (Wegia e Portabilis).

~~116~~ **201** CVE Publicadas.

3 Participaciones en Eventos



~~20~~ **85** Miembros

~~0~~ **1** Patrocinador



~~0~~ **2** Bounty

~~5~~ **9** Proyectos activos

<https://www.cvehunters.com/stats>

> \$ Agradecimiento Especial



>\$ El Fin – Nos vemos

www.cvehunters.com



www.future.com.br



nmmorette.github.io



