Ahmed Hassan

Cyber Security Consultant & Penetration Tester @ Condignum, AUSTRIA (Vienna)

Title: How to identify CVEs in Open-Source Projects/Applications? Let's hack!

talking @ Hack Red Con 2024 in the
United States of America (USA)

Agenda

1. Self-Introduction
2. What is a CVE?
3. Where can you find a suitable open-source Application for Testing?
4. Installing the open-source Application
5. Identification of a Vulnerability in the open-source Application
6. Reporting Identified Vulnerabilities: Methods and Platforms
7. CVE Acceptance and Publication
8. Questions from the audience & further Explanations (Q&A)?

Self-Introduction

Working since almost 6 years as a Cyber Security Engineer & Penetration Tester @ Condignum, AUSTRIA

Speaker at various international security conferences & Universities (Egypt, UAE, Saudi Arabia, Austria etc.)

Securing the Clients environment (Web, API, Active Directory, Mobile, Infrastructure etc.)

BSIDES COLORADO SPRINGS

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

black hat MIDDLE EAST AND AFRICA

ConstraTech Construction Technology Summit

HACK RED CON

2023 Arab Security Conference & Exhibition

Faculty of Computer and Information Sciences 1995

أكاديمية ربدان
Rabdan Academy

AOU
الجامعة العربية المفتوحة
Arab Open University
Egypt

Where am I from ?

AUSTRIA
ÖSTERREICH
6

Qualifications & professional Certifications

studied and working in Austria in the Cyber Security Field as **Cyber Security Engineer, Penetration Tester and Bug Bounty Hunter**

Certifications for advanced IT professionals

Certified EC-council Instructor

Certified Ethical Hacker

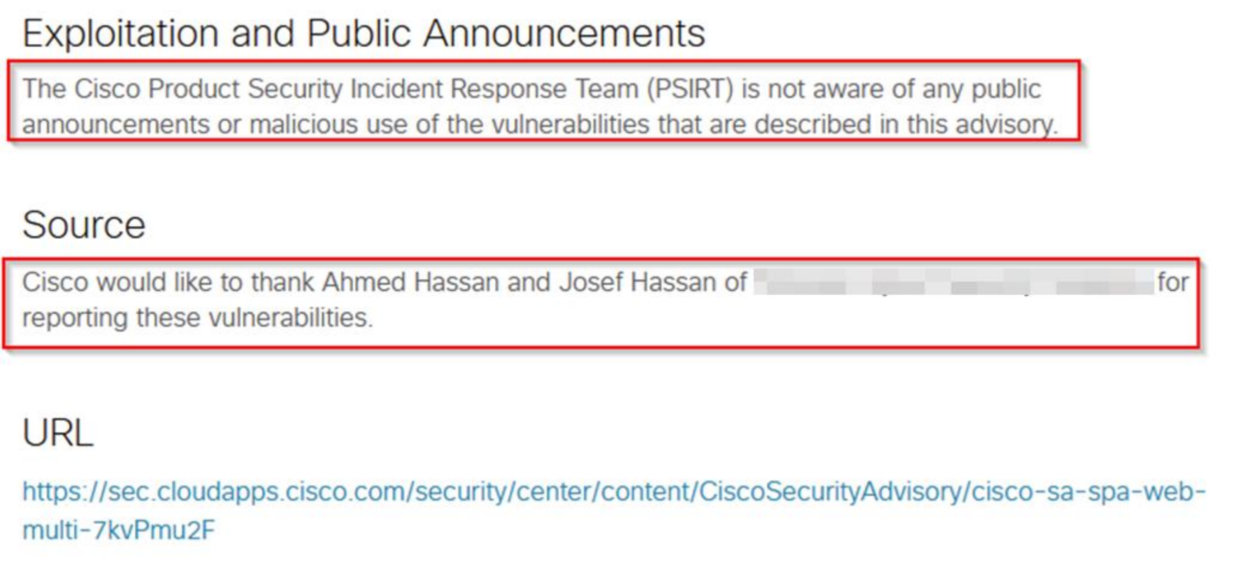
Offensive Security Certified Professional

Offensive Security Web Assessor

Identified Vulnerabilities & 0-day Vulnerabilities

- **Identified more than 52 CVEs. Some as an example:**
- **My GitHub Repo-Link: https://github.com/ahmedvienna/CVEs-and-Vulnerabilities**

  - **CVE-2024-0351**
  - **CVE-2024-0350**
  - **CVE-2024-0349**
  - **CVE-2024-0348**
  - **CVE-2024-0347**
  - **CVE-2024-0262**
  - **CVE-2024-1972**
  - **CVE-2024-1922**
  - **CVE-2024-1919**
  - **CVE-2024-3735**
  - **CVE-2024-7466**



Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

Source

Cisco would like to thank Ahmed Hassan and Josef Hassan of [redacted] for reporting these vulnerabilities.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F

Hall of Fame announcement and CVE assignment, for identifying a Zero-day Vulnerability in CISCO's Devices.

Importance of Cyber Security

This accurately reflects the scenario encountered while providing security services to numerous clients across various industries.

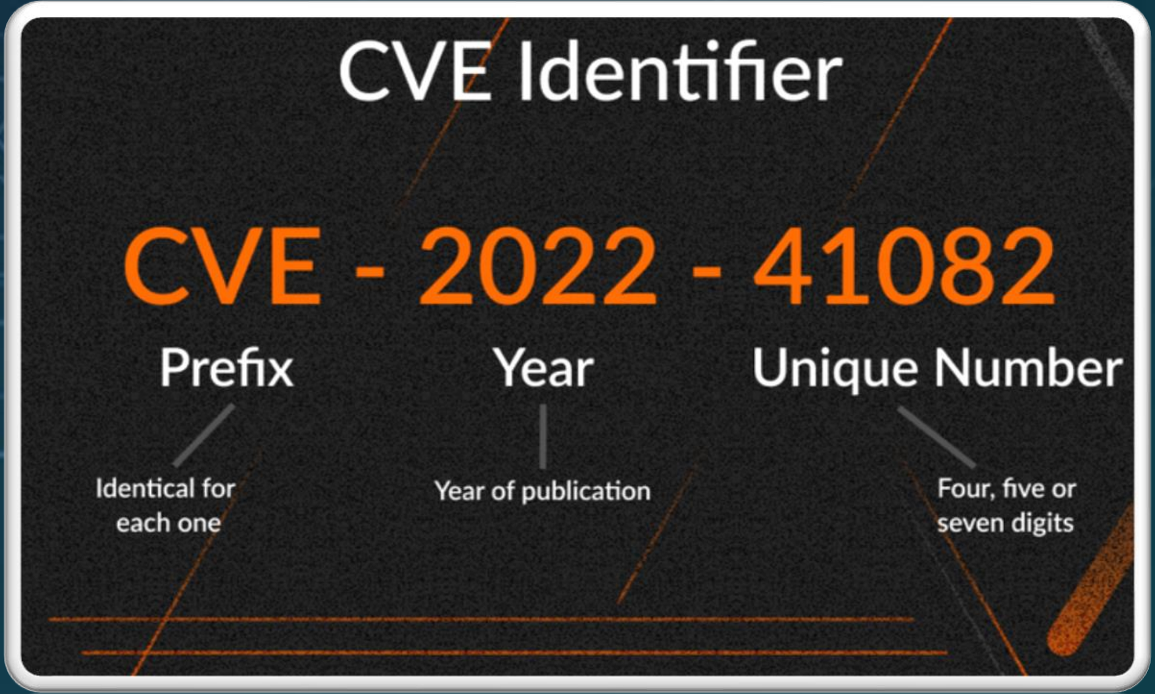
The companies must integrate additional cybersecurity measures into their operations.

What is a CVE ?

CVE Explanation

The Common Vulnerabilities and Exposures (CVE) system is a framework operated by the U.S. National Cybersecurity FFRDC and maintained by the Mitre Corporation. It provides standardized identification and naming of publicly known security vulnerabilities and other weaknesses in computer systems.

The primary goal of the CVE system is to prevent multiple naming of the same threats by different organizations and institutions. Each known vulnerability is assigned a unique identifier, which consists of the prefix CVE, the year of discovery, and a sequential number (e.g., CVE-2020-1234). This ensures the consistent identification of vulnerabilities and facilitates smooth information exchange between the various databases maintained by individual vendors.



CVE Identifier

CVE - 2022 - 41082

Prefix — Identical for each one

Year — Year of publication

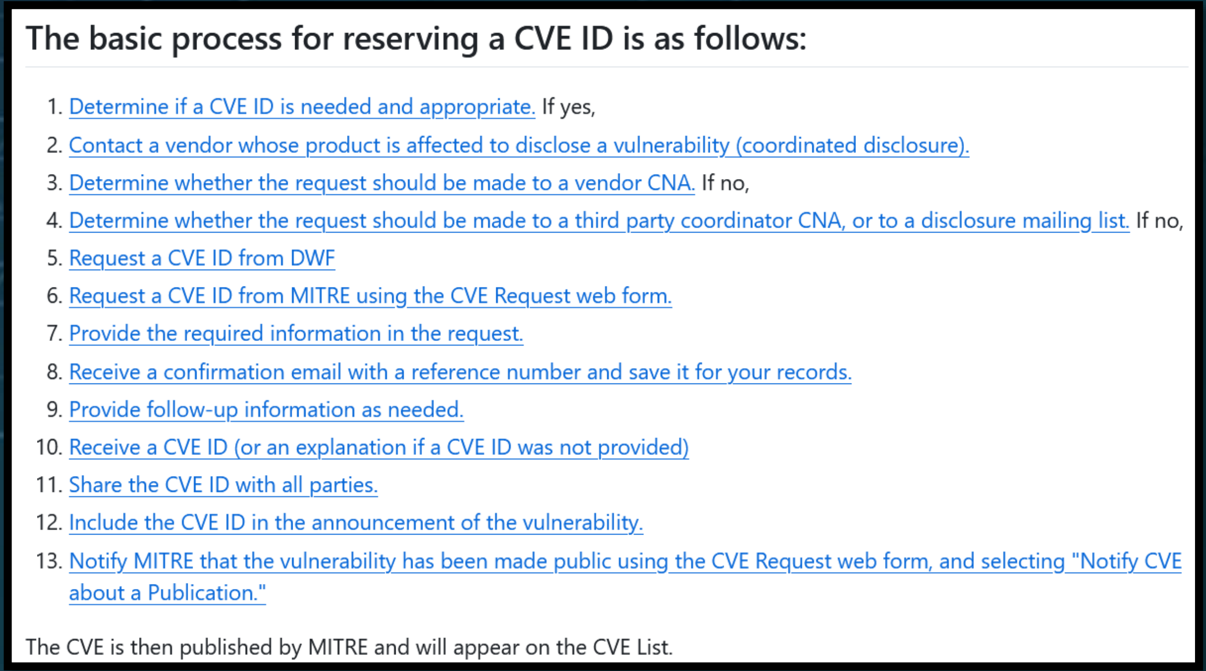
Unique Number — Four, five or seven digits

Criteria for requesting a CVE

Detailed Process how CVEs are reported and assigned: **https://github.com/CVEProject/cveproject.github.io/blob/master/requester/reservation-guidelines.md**

The Common Vulnerabilities and Exposures (CVE) identifier can be requested when a security vulnerability in a software product or system meets specific criteria.

This process typically applies to different applications such as Desktop applications or even Web applications. It is essential to first clarify with the vendor whether they are authorized to request or assign CVEs.



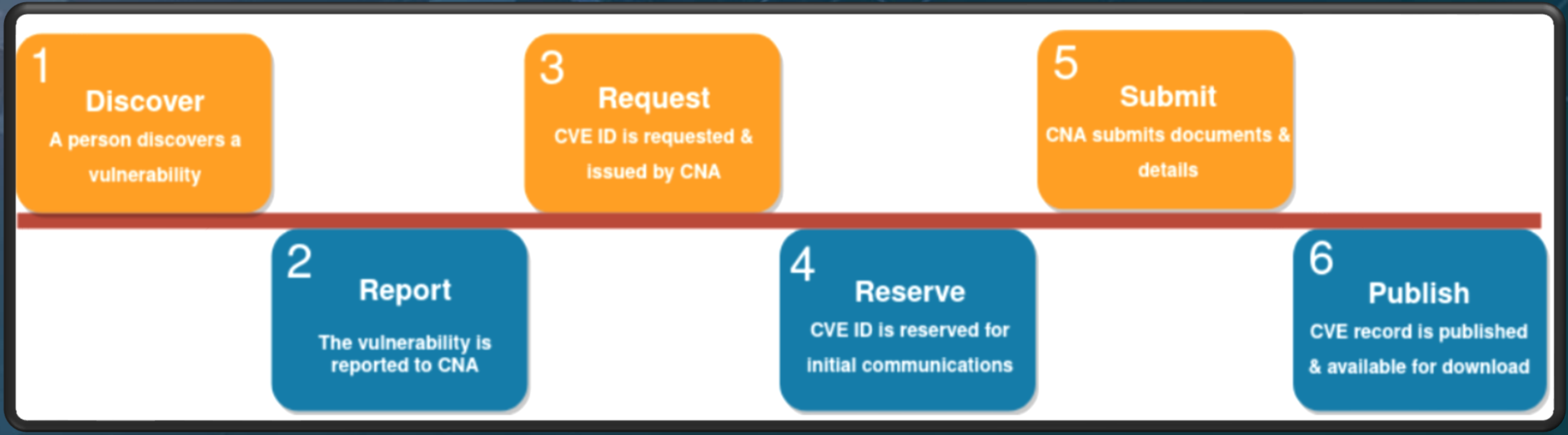
The basic process for reserving a CVE ID is as follows:

1. Determine if a CVE ID is needed and appropriate. If yes,
2. Contact a vendor whose product is affected to disclose a vulnerability (coordinated disclosure).
3. Determine whether the request should be made to a vendor CNA. If no,
4. Determine whether the request should be made to a third party coordinator CNA, or to a disclosure mailing list. If no,
5. Request a CVE ID from DWF
6. Request a CVE ID from MITRE using the CVE Request web form.
7. Provide the required information in the request.
8. Receive a confirmation email with a reference number and save it for your records.
9. Provide follow-up information as needed.
10. Receive a CVE ID (or an explanation if a CVE ID was not provided)
11. Share the CVE ID with all parties.
12. Include the CVE ID in the announcement of the vulnerability.
13. Notify MITRE that the vulnerability has been made public using the CVE Request web form, and selecting "Notify CVE about a Publication."

The CVE is then published by MITRE and will appear on the CVE List.

Workflow for CVE Assignment

This outlines the complete workflow, from identifying the vulnerability to receiving a CVE assignment.



1 **Discover**
A person discovers a vulnerability

2 **Report**
The vulnerability is reported to CNA

3 **Request**
CVE ID is requested & issued by CNA

4 **Reserve**
CVE ID is reserved for initial communications

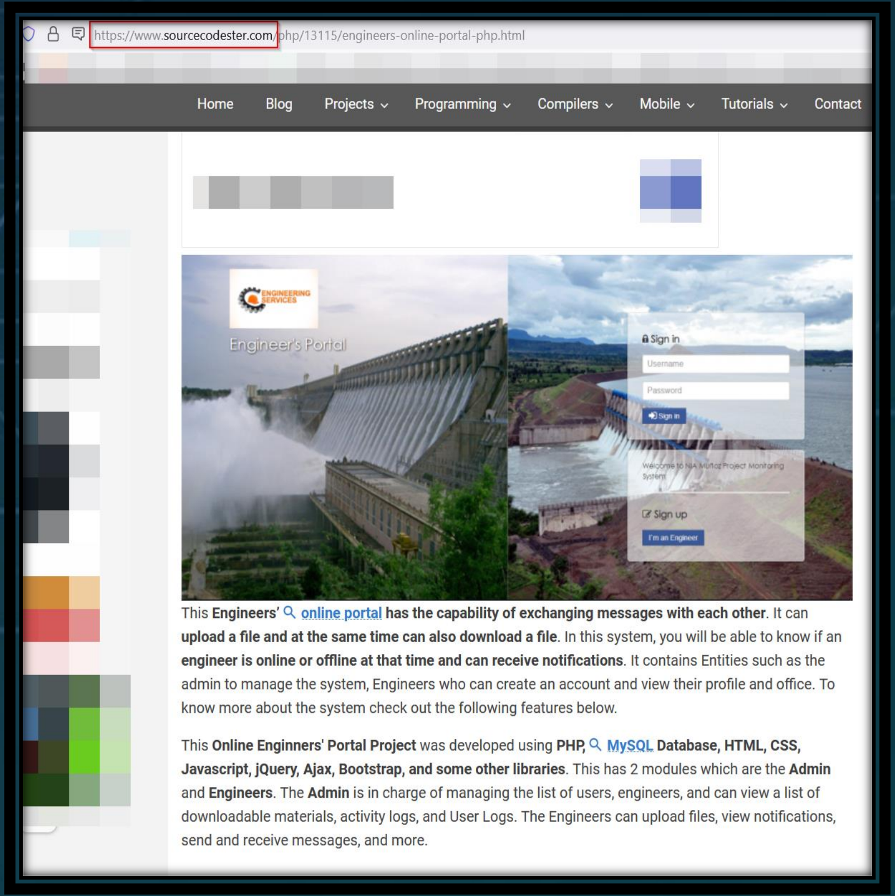
5 **Submit**
CNA submits documents & details

6 **Publish**
CVE record is published & available for download

Where can you find a suitable open-source Application for Testing?

1. **This website hosts a vast collection of open-source applications, of which 99% are legitimate candidates for requesting a CVE.**

2. **The Website link: https://www.sourcecodester.com/**

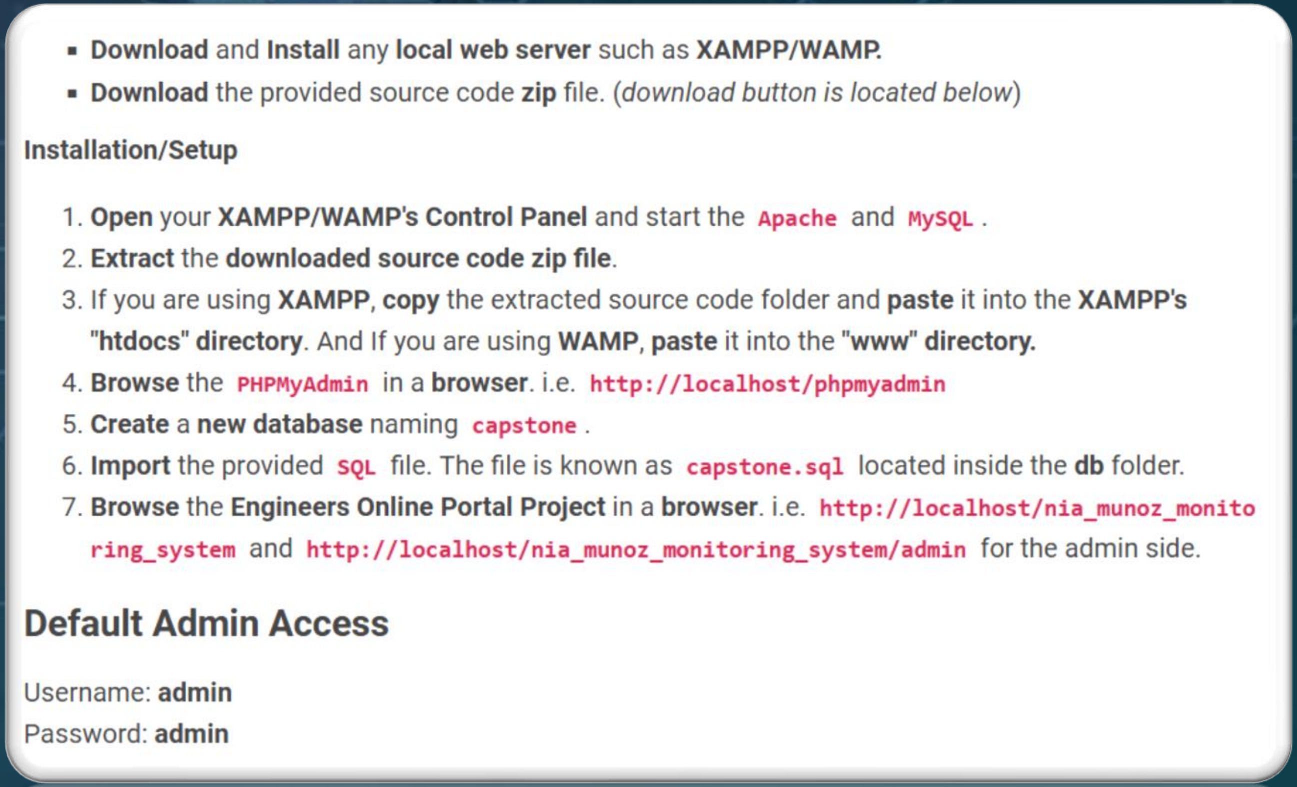


This **Engineers'** online portal **has the capability of exchanging messages with each other**. It can **upload a file and at the same time can also download a file**. In this system, you will be able to know if an **engineer is online or offline at that time and can receive notifications**. It contains Entities such as the admin to manage the system, Engineers who can create an account and view their profile and office. To know more about the system check out the following features below.

This **Online Enginners' Portal Project** was developed using **PHP,** MySQL **Database, HTML, CSS, Javascript, jQuery, Ajax, Bootstrap, and some other libraries**. This has 2 modules which are the **Admin** and **Engineers**. The **Admin** is in charge of managing the list of users, engineers, and can view a list of downloadable materials, activity logs, and User Logs. The Engineers can upload files, view notifications, send and receive messages, and more.

Installing the open-source Application

The installation of the application is well-documented, making it easy and straightforward to download.



- **Download** and **Install** any **local web server** such as **XAMPP/WAMP.**
- **Download** the provided source code **zip** file. (*download button is located below*)

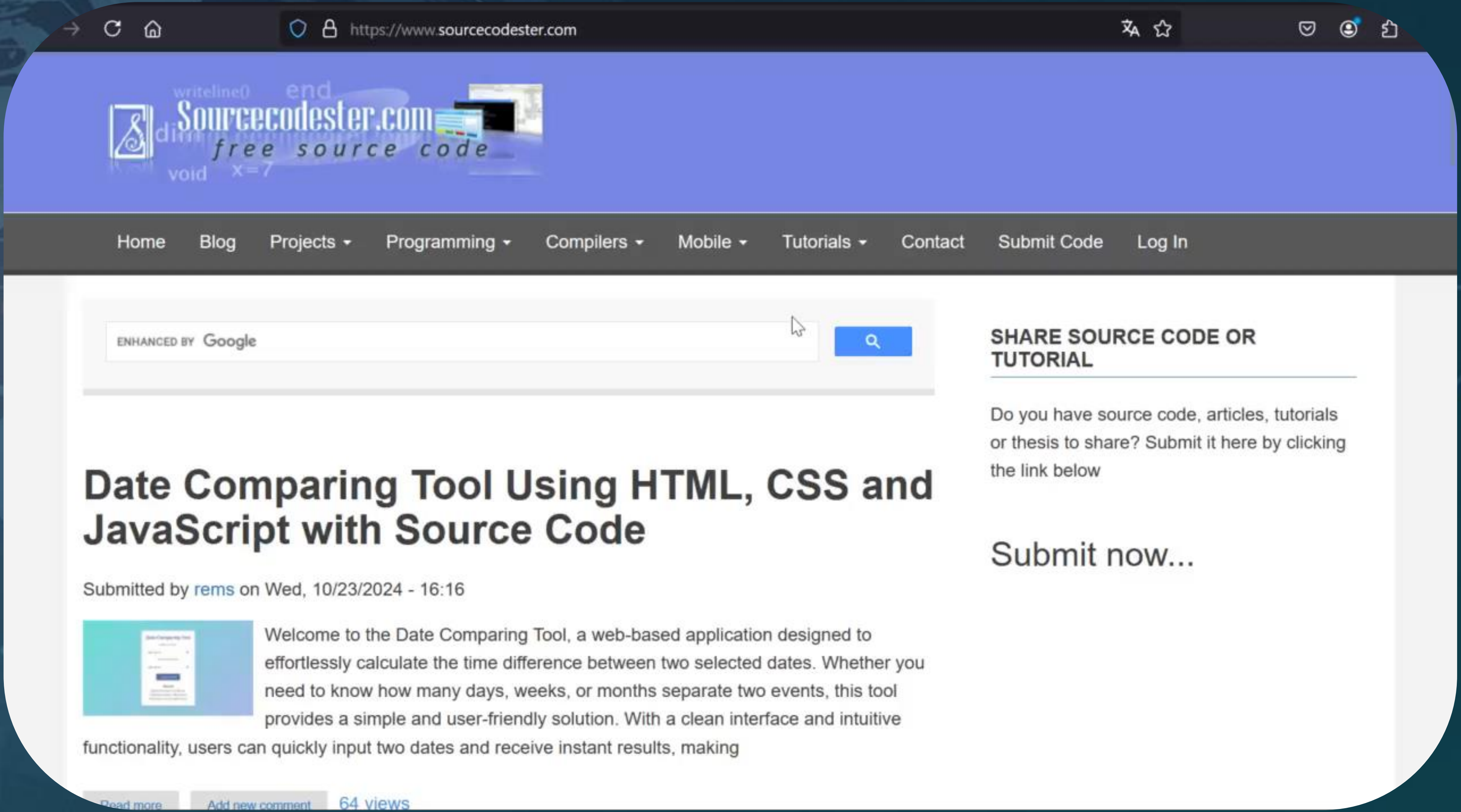
Installation/Setup

1. **Open** your **XAMPP/WAMP's Control Panel** and start the `Apache` and `MySQL` .
2. **Extract** the **downloaded source code zip file**.
3. If you are using **XAMPP**, **copy** the extracted source code folder and **paste** it into the **XAMPP's "htdocs" directory**. And If you are using **WAMP**, **paste** it into the **"www" directory.**
4. **Browse** the `PHPMyAdmin` in a **browser**. i.e. `http://localhost/phpmyadmin`
5. **Create** a **new database** naming `capstone` .
6. **Import** the provided `SQL` file. The file is known as `capstone.sql` located inside the **db** folder.
7. **Browse** the **Engineers Online Portal Project** in a **browser**. i.e. `http://localhost/nia_munoz_monitoring_system` and `http://localhost/nia_munoz_monitoring_system/admin` for the admin side.

Default Admin Access

Username: **admin**
Password: **admin**

Proof of Concept Video



Date Comparing Tool Using HTML, CSS and JavaScript with Source Code

Submitted by rems on Wed, 10/23/2024 - 16:16

Welcome to the Date Comparing Tool, a web-based application designed to effortlessly calculate the time difference between two selected dates. Whether you need to know how many days, weeks, or months separate two events, this tool provides a simple and user-friendly solution. With a clean interface and intuitive functionality, users can quickly input two dates and receive instant results, making

SHARE SOURCE CODE OR TUTORIAL

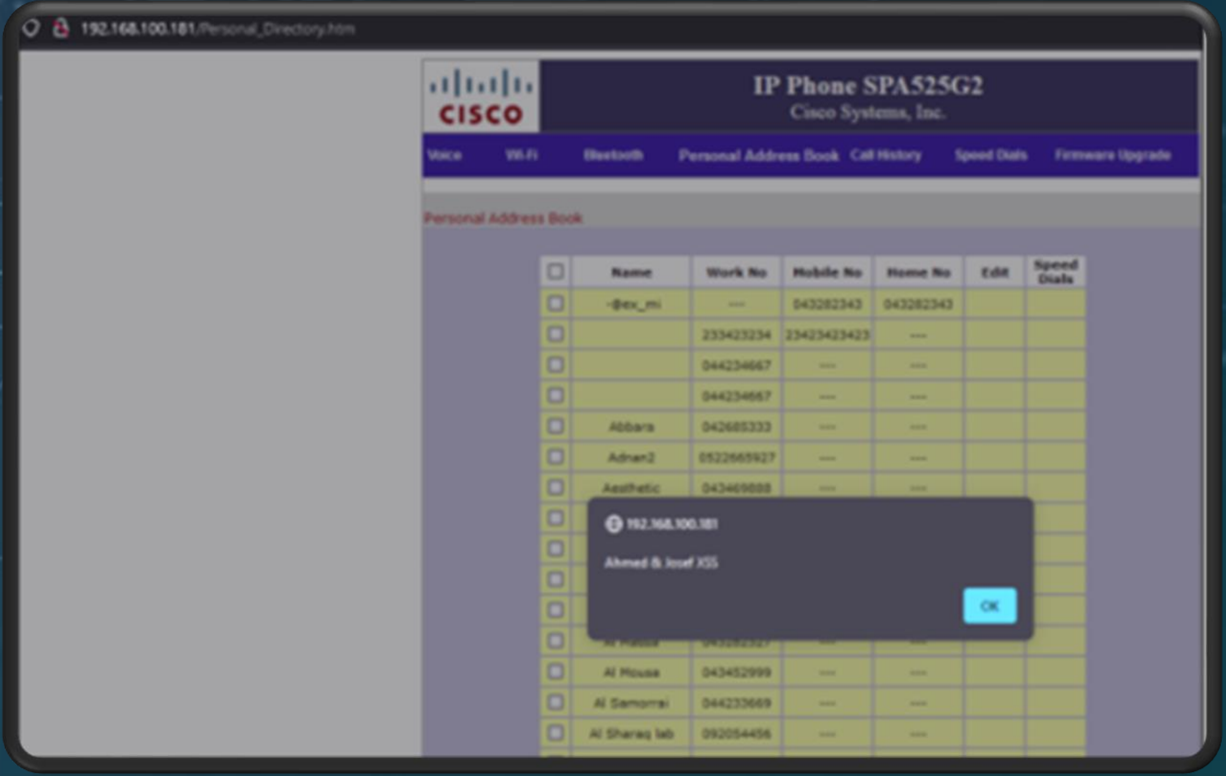
Do you have source code, articles, tutorials or thesis to share? Submit it here by clicking the link below

Submit now...

Identification of a Vulnerability in the open-source Application

Assuming we have identified a vulnerability in this open-source application, it is important to thoroughly document all details before proceeding to the reporting phase.

In this phase, we need to collect screenshots, videos, Payloads used and both the request and response data to ensure we provide the vendor with all necessary information.



IP Phone SPA525G2
Cisco Systems, Inc.

Personal Address Book

□	Name	Work No	Mobile No	Home No	Edit	Speed Dials
□	-@ex_mi	----	043282343	043282343		
□		233423234	23423423423	----		
□		044234667	----	----		
□		044234667	----	----		
□	Abbara	042685333	----	----		
□	Adnan2	0522665927	----	----		
□	Aesthetic	043469888	----	----		
□	[illegible]	[illegible]	[illegible]	[illegible]		
□	[illegible]	[illegible]	[illegible]	[illegible]		
□	[illegible]	[illegible]	[illegible]	[illegible]		
□	[illegible]	[illegible]	[illegible]	[illegible]		
□	[illegible]	[illegible]	----	----		
□	Al Mousa	043452999	----	----		
□	Al Samorrai	044233669	----	----		
□	Al Sharaq lab	092054456	----	----		

192.168.100.181

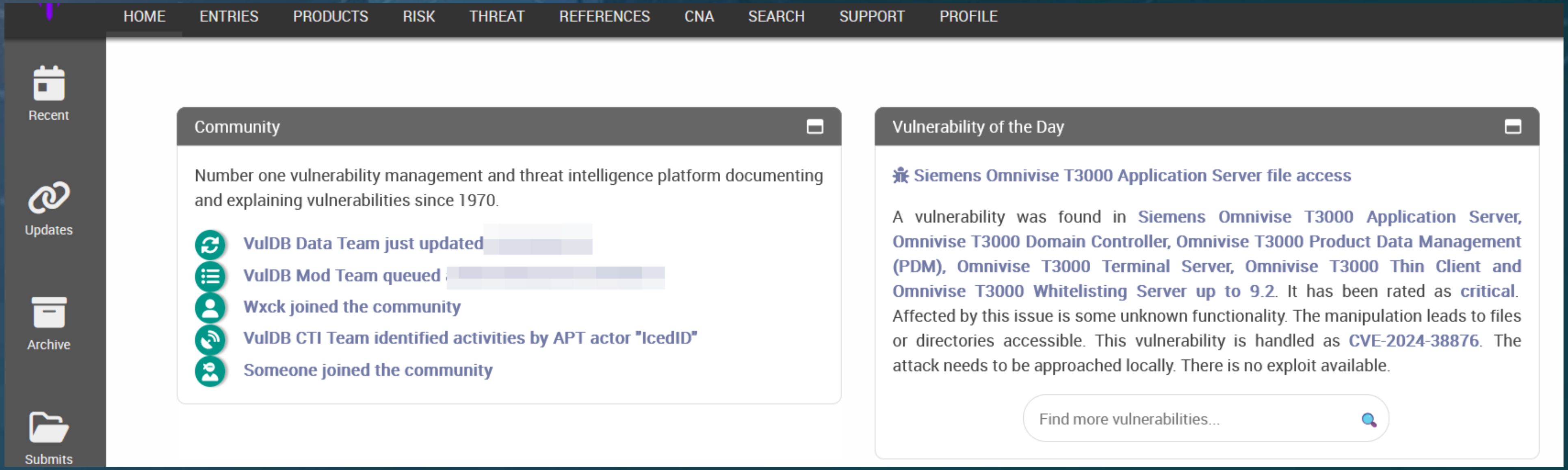
Ahmed & Josef XSS

Reporting identified Vulnerabilities: Methods and Platforms

If you can locate the vendor details, such as those for Cisco, and contact their security team, this should be your first step. They may respond and have the capability to assign a CVE.

In cases where you cannot find the security team or if the company shows no interest in the security aspects of their products, you will need to reach out to a recognized CVE authority for assistance in assigning a CVE after reviewing your vulnerability.

The recognized CVE authority Website: https://vuldb.com/



Community

Number one vulnerability management and threat intelligence platform documenting and explaining vulnerabilities since 1970.

- VulDB Data Team just updated [redacted]
- VulDB Mod Team queued [redacted]
- Wxck joined the community
- VulDB CTI Team identified activities by APT actor "IcedID"
- Someone joined the community

Vulnerability of the Day

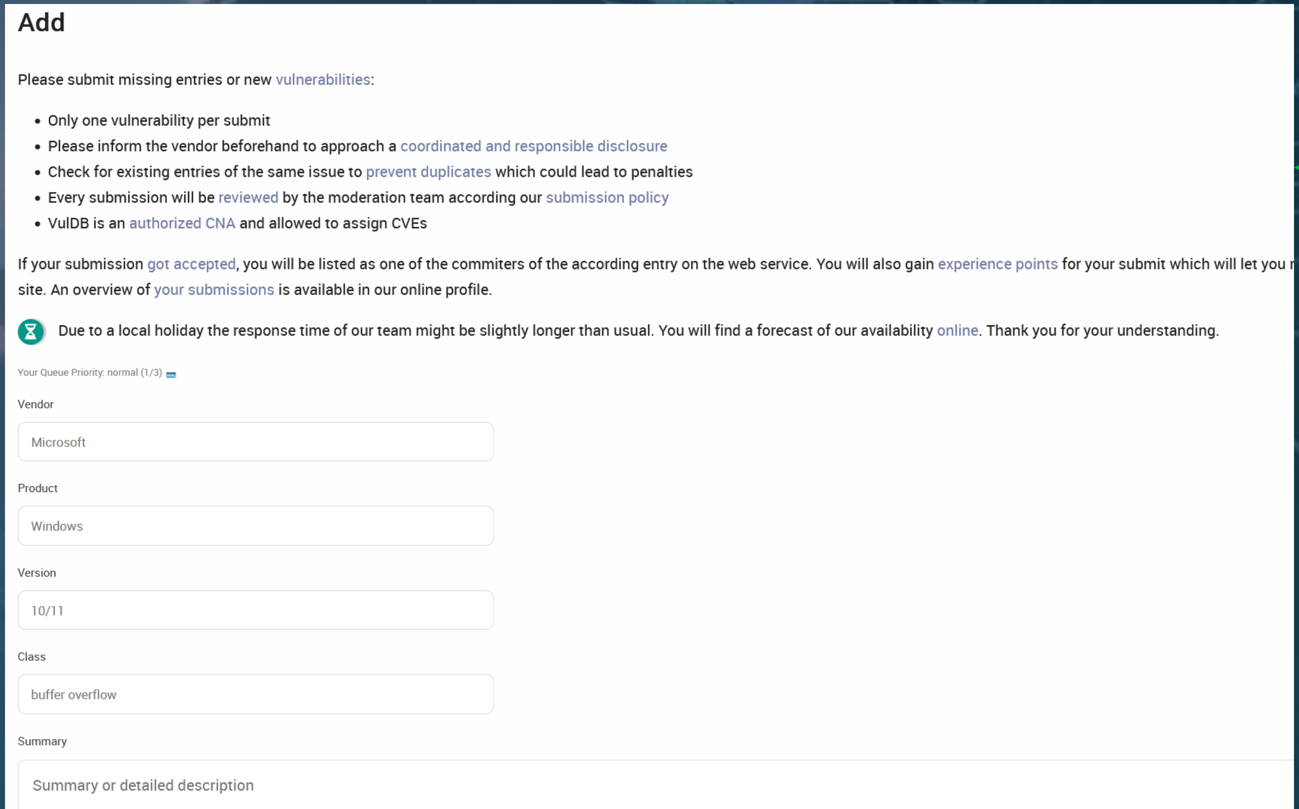
Siemens Omnivise T3000 Application Server file access

A vulnerability was found in Siemens Omnivise T3000 Application Server, Omnivise T3000 Domain Controller, Omnivise T3000 Product Data Management (PDM), Omnivise T3000 Terminal Server, Omnivise T3000 Thin Client and Omnivise T3000 Whitelisting Server up to 9.2. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to files or directories accessible. This vulnerability is handled as CVE-2024-38876. The attack needs to be approached locally. There is no exploit available.

Find more vulnerabilities...

Detailed Procedure for reporting a Vulnerability

To proceed, navigate to the ADD section. Here, you will need to complete all the fields with the information you have, such as details of the vulnerability, proof of concept, and any other relevant data.



Add

Please submit missing entries or new vulnerabilities:

- Only one vulnerability per submit
- Please inform the vendor beforehand to approach a coordinated and responsible disclosure
- Check for existing entries of the same issue to prevent duplicates which could lead to penalties
- Every submission will be reviewed by the moderation team according our submission policy
- VulDB is an authorized CNA and allowed to assign CVEs

If your submission got accepted, you will be listed as one of the commiters of the according entry on the web service. You will also gain experience points for your submit which will let you r site. An overview of your submissions is available in our online profile.

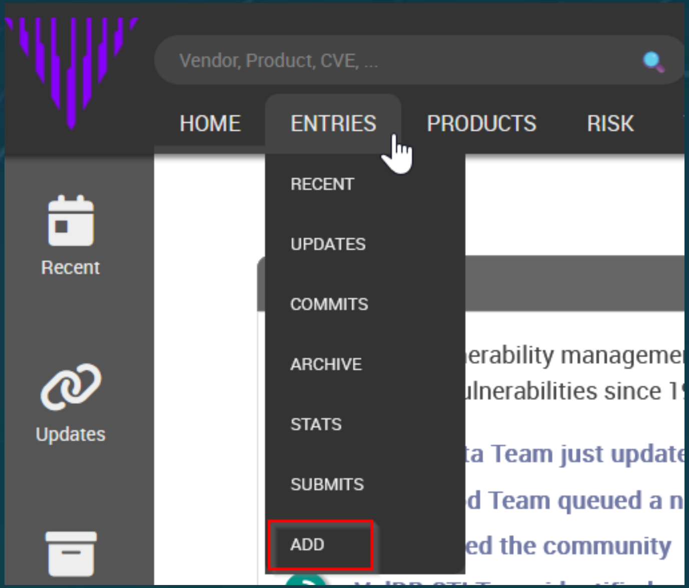
Due to a local holiday the response time of our team might be slightly longer than usual. You will find a forecast of our availability online. Thank you for your understanding.

Your Queue Priority: normal (1/3)

Vendor	Microsoft
Product	Windows
Version	10/11
Class	buffer overflow
Summary	Summary or detailed description

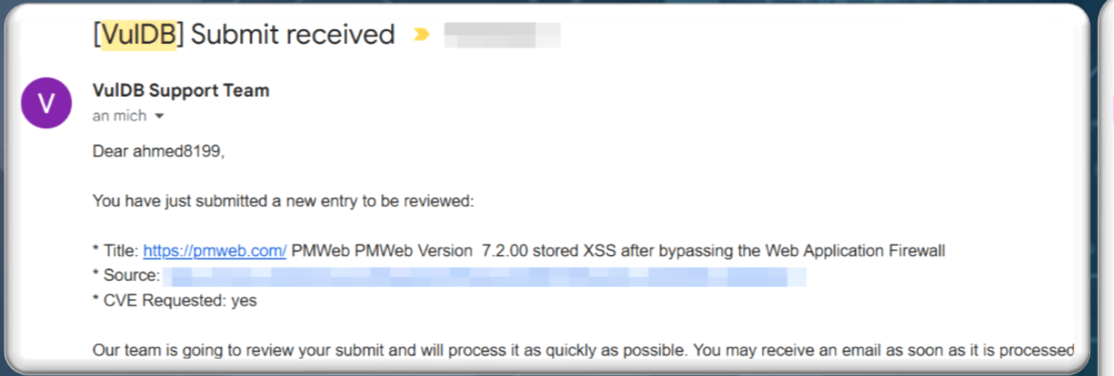
2

1



Submitting the form and receiving the Response

Here we can review the message received after submitting the CVE request, along with the response confirming the approval and issuance of a new, valid CVE.



[VulDB] Submit received [redacted]

VulDB Support Team
an mich

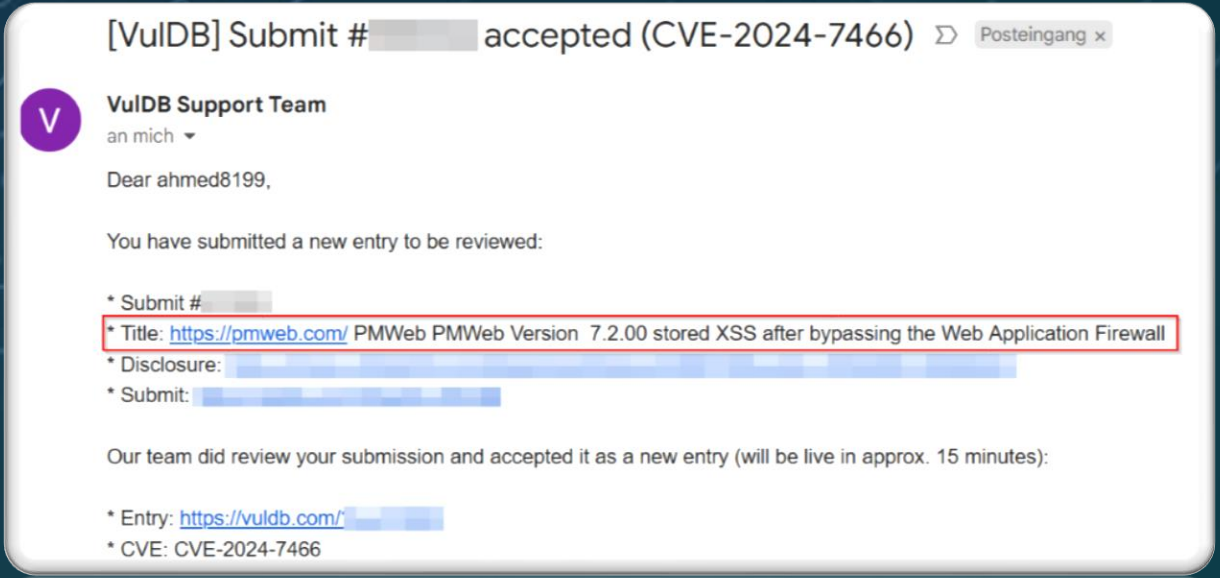
Dear ahmed8199,

You have just submitted a new entry to be reviewed:

* Title: https://pmweb.com/ PMWeb PMWeb Version 7.2.00 stored XSS after bypassing the Web Application Firewall
* Source: [redacted]
* CVE Requested: yes

Our team is going to review your submit and will process it as quickly as possible. You may receive an email as soon as it is processed

1



[VulDB] Submit #[redacted] accepted (CVE-2024-7466)

VulDB Support Team
an mich

Dear ahmed8199,

You have submitted a new entry to be reviewed:

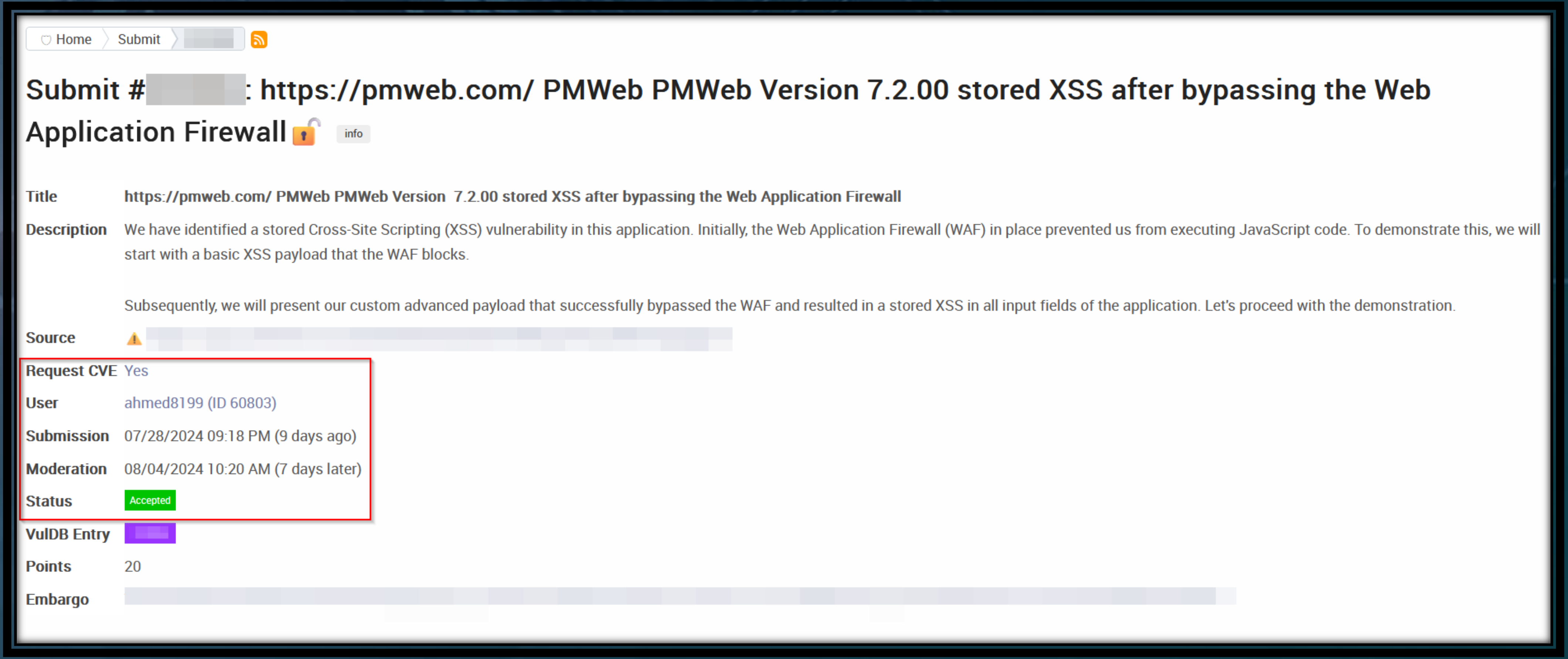
* Submit #[redacted]
* Title: https://pmweb.com/ PMWeb PMWeb Version 7.2.00 stored XSS after bypassing the Web Application Firewall
* Disclosure: [redacted]
* Submit: [redacted]

Our team did review your submission and accepted it as a new entry (will be live in approx. 15 minutes):

* Entry: https://vuldb.com/[redacted]
* CVE: CVE-2024-7466

2

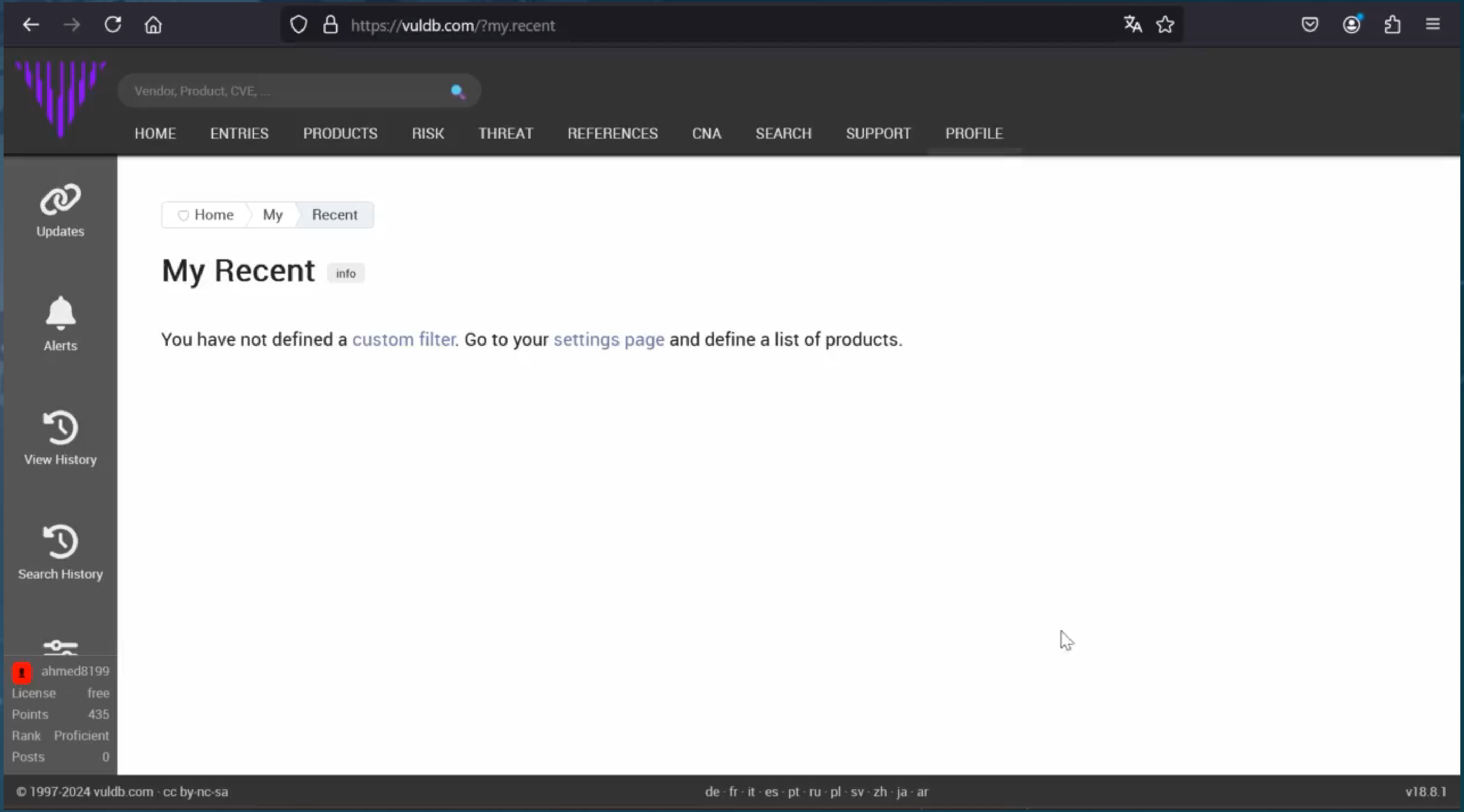
Successful CVE Acceptance and Publication



Submit #[redacted]: https://pmweb.com/ PMWeb PMWeb Version 7.2.00 stored XSS after bypassing the Web Application Firewall

Title	**https://pmweb.com/ PMWeb PMWeb Version 7.2.00 stored XSS after bypassing the Web Application Firewall**
Description	We have identified a stored Cross-Site Scripting (XSS) vulnerability in this application. Initially, the Web Application Firewall (WAF) in place prevented us from executing JavaScript code. To demonstrate this, we will start with a basic XSS payload that the WAF blocks. Subsequently, we will present our custom advanced payload that successfully bypassed the WAF and resulted in a stored XSS in all input fields of the application. Let's proceed with the demonstration.
Source	⚠ [redacted]
Request CVE	Yes
User	ahmed8199 (ID 60803)
Submission	07/28/2024 09:18 PM (9 days ago)
Moderation	08/04/2024 10:20 AM (7 days later)
Status	Accepted
VulDB Entry	[redacted]
Points	20
Embargo	[redacted]

Proof of Concept Video 2



https://vuldb.com/?my.recent
Vendor, Product, CVE, ...
HOME
ENTRIES
PRODUCTS
RISK
THREAT
REFERENCES
CNA
SEARCH
SUPPORT
PROFILE
Updates
Alerts
View History
Search History
Home
My
Recent
info
© 1997-2024 vuldb.com · cc by-nc-sa
de · fr · it · es · pt · ru · pl · sv · zh · ja · ar
v18.8.1

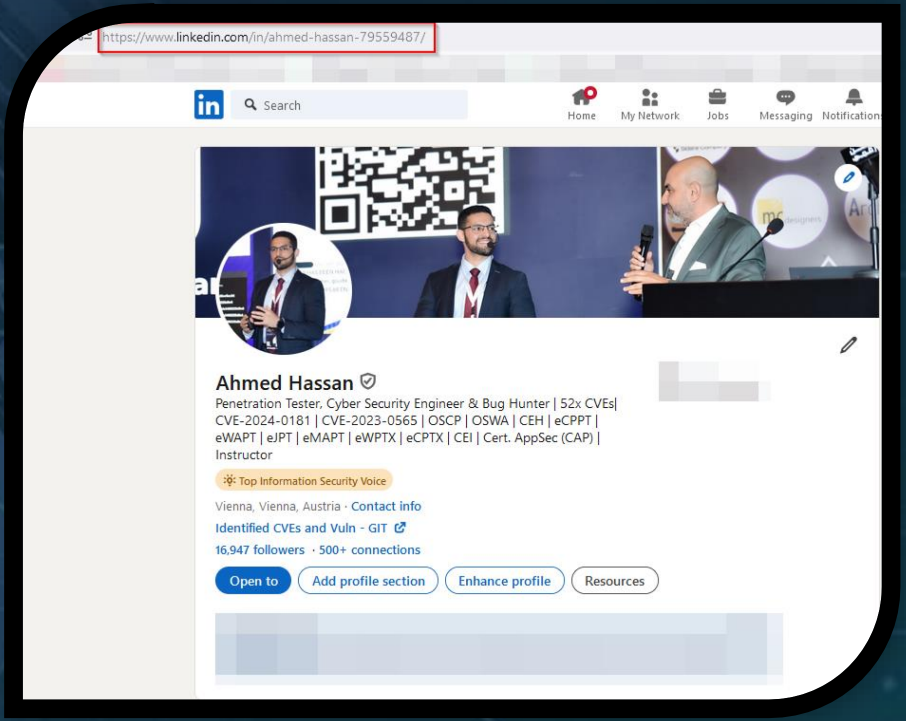
My Recent

You have not defined a custom filter. Go to your settings page and define a list of products.

ahmed8199

License	free
Points	435
Rank	Proficient
Posts	0

This highlighted the vulnerabilities and shortcomings in the cybersecurity measures of certain clients.


https://www.linkedin.com/in/ahmed-hassan-79559487/

Ahmed Hassan

Penetration Tester, Cyber Security Engineer & Bug Hunter | 52x CVEs| CVE-2024-0181 | CVE-2023-0565 | OSCP | OSWA | CEH | eCPPT | eWAPT | eJPT | eMAPT | eWPTX | eCPTX | CEI | Cert. AppSec (CAP) | Instructor

Top Information Security Voice

Vienna, Vienna, Austria · Contact info

Identified CVEs and Vuln - GIT

16,947 followers · 500+ connections

THANK YOU very much ☺

My LinkedIn: https://www.linkedin.com/in/ahmed-hassan-79559487/

Contact -> LinkedIn QR-Code