



Arab Security Conference

8th Round
Sponser
2024
22nd - 23rd SEPTEMBER



Ahmed Hassan

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

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



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.)





Arab Security Conference

8th Round
Sponser
2024

22nd - 23rd SEPTEMBER





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.



Arab Security Conference

8th Round
Sponser
2024
22nd - 23rd SEPTEMBER

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

Year

Unique Number

Identical for
each one

Year of publication

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:

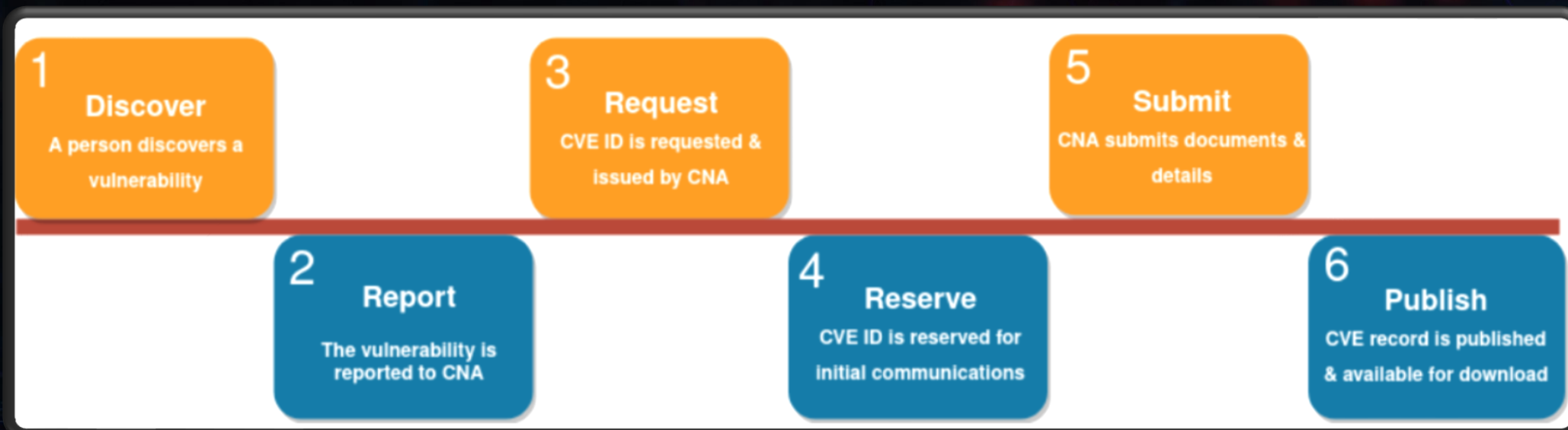
1. [Determine if a CVE ID is needed and appropriate.](#) If yes,
2. [Contact a vendor whose product is affected to disclose a vulnerability \(coordinated disclosure\).](#)
3. [Determine whether the request should be made to a vendor CNA.](#) If no,
4. [Determine whether the request should be made to 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

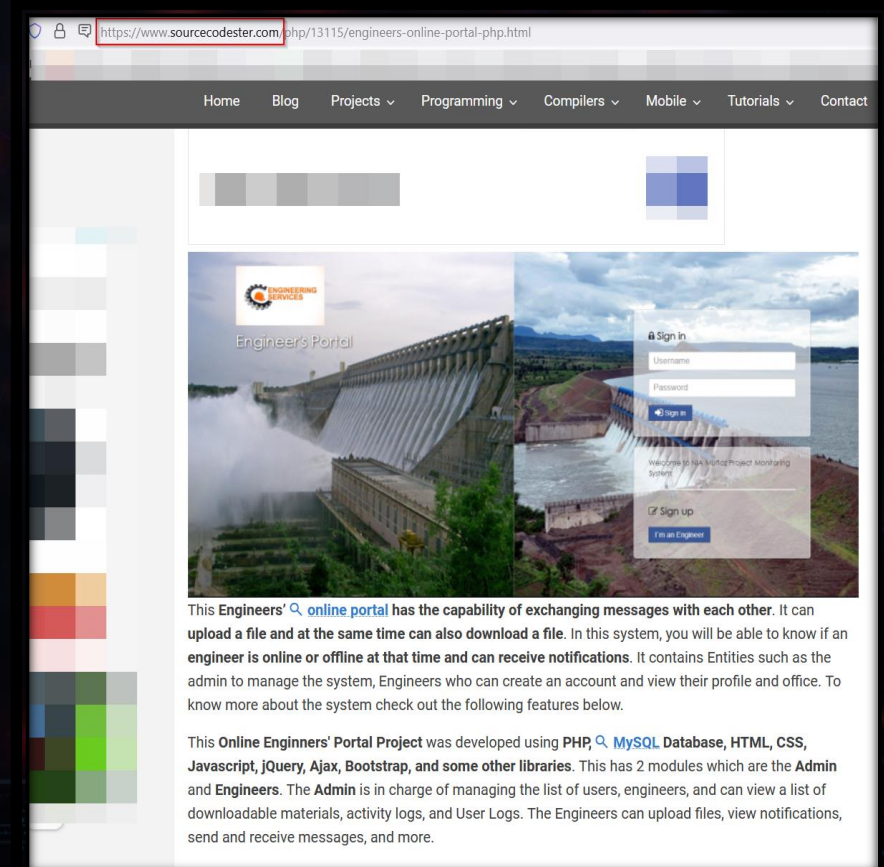
This outlines the complete workflow, from identifying the vulnerability to receiving a CVE assignment.





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/>





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)

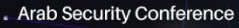
Installation/Setup

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/ring_system and http://localhost/nia_munoz_monitoring_system/admin for the admin side.

Default Admin Access

Username: **admin**

Password: **admin**



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.

The screenshot shows the Cisco SPA525G2 IP Phone's Personal Address Book. A contact entry for 'Ahmed B. Josef X55' is selected, and a pop-up window displays the contact details: 192.168.100.181 and Ahmed B. Josef X55. The interface includes a top navigation bar with options like Voice, VoIP, Bluetooth, Personal Address Book, Call History, Speed Dials, and Firmware Upgrade.

	Name	Work No	Mobile No	Home No	Edit	Speed Dials
<input type="checkbox"/>	-Bex_mi	----	043282343	043282343		
<input type="checkbox"/>		233423234	23423423423	----		
<input type="checkbox"/>		044234667	----	----		
<input type="checkbox"/>		044234667	----	----		
<input type="checkbox"/>	Abbara	042685333	----	----		
<input type="checkbox"/>	Adnan2	0522665927	----	----		
<input type="checkbox"/>	Aesthetic	043409088	----	----		
<input type="checkbox"/>	192.168.100.181					
<input type="checkbox"/>	Ahmed B. Josef X55					
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>	Al Housse	043282327	----	----		
<input type="checkbox"/>	Al Housse	043452999	----	----		
<input type="checkbox"/>	Al Samarra	044233669	----	----		
<input type="checkbox"/>	Al Sharaf lab	092054456	----	----		



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/>

The screenshot displays the VulDB website interface. The top navigation bar includes links for HOME, ENTRIES, PRODUCTS, RISK, THREAT, REFERENCES, CNA, SEARCH, SUPPORT, and PROFILE. On the left, a sidebar contains icons for Recent, Updates, Archive, and Submits. The main content area is divided into two sections. The 'Community' section on the left features a header 'Community' and a description: 'Number one vulnerability management and threat intelligence platform documenting and explaining vulnerabilities since 1970.' Below this, a list of recent community updates is shown, including 'VulDB Data Team just updated', 'VulDB Mod Team queued', 'Wxck joined the community', 'VulDB CTI Team identified activities by APT actor "IcedID"', and 'Someone joined the community'. The 'Vulnerability of the Day' section on the right features a header 'Vulnerability of the Day' and a detailed entry for 'Siemens Omnivise T3000 Application Server file access'. The entry describes a critical vulnerability 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 states that the vulnerability is critical, affects unknown functionality, and is handled as CVE-2024-38876. The attack needs to be approached locally, and no exploit is available. At the bottom of this section, there is a search bar with the text 'Find more vulnerabilities...' and a magnifying glass icon.



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 committers of the according entry on the web service. You will also gain [experience points](#) for your submit which will let you [rank up](#) on the 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)

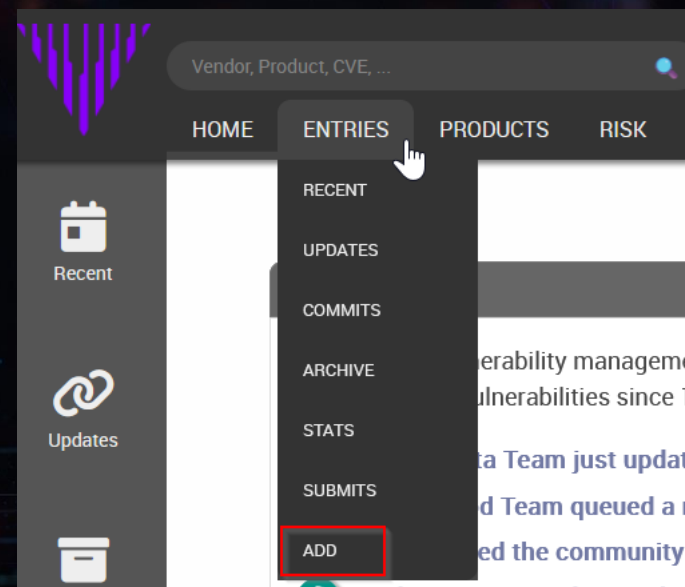
Vendor

Product

Version

Class

Summary





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 >



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) > Posteingang x



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


[Home](#) [Submit](#)

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

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

Points 20

Embargo [redacted]



Arab Security Conference

8th Round

THANK YOU

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