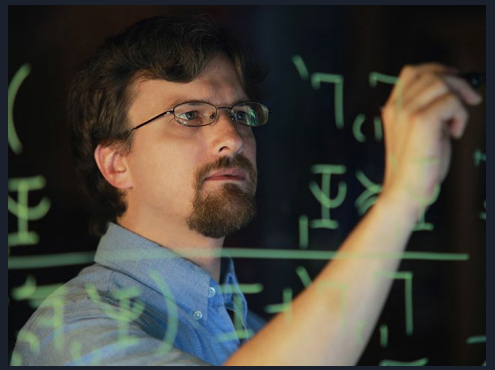
Welcome to ACM Research!

ACM Research Info!

- Director: Roman Hauksson-Neil
- Faculty: Advisor: Dr. Kevin Hamlen
- Team Lead : Pranav Nair



- Meetings every Monday at 8:30 PM CST - 10:00 PM CST

Introductions!

Name, pronouns, major/minor, fun fact about yourself

- Rishit Viral
- Lawson Lay
- Adith Talupuru
- Sai Kanchan-Javalkar
- Christopher Back

Finding Security Vulnerabilities

- Our team will work together to find security vulnerabilities in a pre-existing open-source software project.
  - Where? We will try to find them on GitHub
  - How? We will use Dr. Hamlen's own vulnerability scanner and try to spot vulnerabilities

- We will start by learning about what a vulnerability is and how they're documented.

- Timeline for the semester
  - Learn about common real-life vulnerabilities through CVE
  - Find an open-source software
  - Try to find a vulnerability (Dr. Hamlen's scanner will assist us!)
  - Submit a pull request with a fix ?
  - Report + Presentation

Vulnerability

- CVE (Common Vulnerabilities & Exposures) = founded in 1999, documents known vulnerabilities
  - funded by the U.S. Department of Homeland Security (DHS)
  - CNA are the organization that publish new CVE IDs
  - Can help us see examples of vulnerabilities that we may see in our research

- Types of cyberattacks:
  - XSS (Cross-site scripting)
  - SQL Injection
  - DoS (Denial of Service) attack

CVE example

Example:

Printer-Friendly View

CVE-ID

CVE-2022-38550 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A stored cross-site scripting (XSS) vulnerability in the /weibo/list component of Jeesns v2.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.

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://github.com/Pick-program/JEESNS/issues/1

Assigning CNA

MITRE Corporation

Date Record Created

20220822 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20220822)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

GitHub: https://github.com/Pick-program/JEESNS/issues/1

HW:

- Look at 5 CVEs and try to understand the vulnerability, how it works, and the vulnerable code.
- Take a look at the resources below in case you did not get time during the build night.

Feedback?