



Florida International University

Fall Semester - 2024

Individual poster

Students: Alejandro Hernandez
Instructor/Faculty: *Masoud Sadjadi*, Florida International University

Team contributions

Brainstorming and Project Direction

- Played a key role in brainstorming alternative ideas for our senior project after the team decided to pivot from our initial concept.
- Actively participated in daily scrum meetings to discuss and refine ideas, leading to the decision to develop a vulnerability scanner.

Custom Template Development

- Researched and learned the YAML syntax required to create custom templates for Nuclei.
- Created three custom templates specifically targeting vulnerabilities in Metasploitable’s Mutillidae webserver.
- Overcame significant challenges in debugging and refining the templates, ensuring they accurately identified vulnerabilities.

Research and Preparation

- Conducted extensive research through articles and videos to determine how to implement the vulnerability scanner using Nuclei and Metasploitable.
- Investigated methods to integrate Nuclei, installed on Kali Linux, with Metasploitable, running as a standalone virtual machine.
- Configured the network setup to enable seamless communication between the two virtual machines, sharing my findings with the team and assisting with implementation.

Custom Template Highlights (detected vulnerabilities)

- Template 1:
Cross-site scripting (XSS) on the host/IP field.
OS command injection on the host/IP field.
SQL injection and XSS vulnerabilities in the log page.
Exploited improper POST/GET method enforcement.
- Template 2:
Focused on:XSS vulnerabilities via any GET, POST, or Cookie parameters.
- Template 3:
Identified:XSS via HTTP Referer header.
JavaScript injection via HTTP Referer header.
XSS via the User-Agent string in the HTTP header.

Testing and Understanding Nuclei

- Experimented with Nuclei's scanning capabilities by testing various vulnerable websites and analyzing the results.
- Shared insights and feedback with the team to help refine our approach to leveraging Nuclei’s powerful scanning features.

Impact

My contributions ensured effective communication between tools, enhanced our understanding of Nuclei’s scanning capabilities, and enabled us to create targeted templates that successfully identified critical vulnerabilities.



ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by XXXXX (name of the project sponsor: federal, state or local government, or corporate partners, where applicable). We/I thank XXXX for his/her/their assistance and mentorship that I/we received throughout the senior design project.