



Florida International University

Fall Semester - 2024 - Senior Design Project

Nuclei – Vulnerability Scanner

Students: Jonathan Rizo

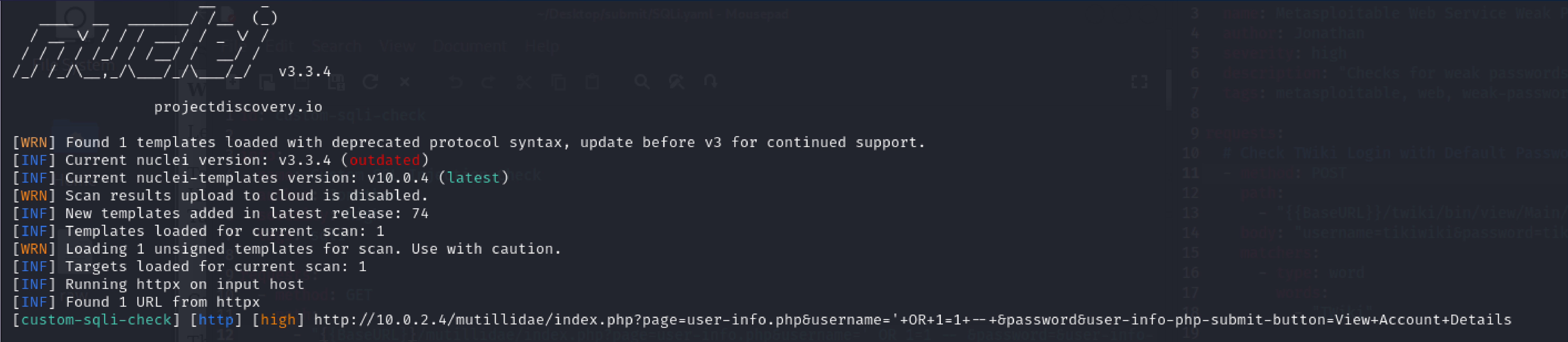
Instructor/Faculty: *Masoud Sadjadi*, Florida International University

PROBLEM

There is an increasing number of data breaches/systems compromised that contain very sensitive information that should never be made public. The increase can be due to many things most of which usually results from sloppy/unpolished code and or hidden vulnerabilities.

Companies that do not feel secure may also release bug bounties which basically means “help us out and compensated.” Many web experts take the offer with a mutual sign of respect and do not leak/compromise any data if they push further.

Vulnerabilities and backdoors are bound to happen, it is almost impossible to have anything 100% secure but knowing where your vulnerabilities and backdoor are located is very crucial information.



SYSTEM DESIGN

We focused on using Nuclei, a public customizable vulnerability scanner, it attracted us mainly because it supports YAML Templates and Frequent CVE Updates. (Common Vulnerabilities and Exposures) ¹

Additionally, for testing purposes we opted to use **Metasploit** and scan the webapps automatically installed on it, though it works just fine without it.

Since Nuclei does not support any other type of code. Our team had to learn how to use YAML. The templates we created are original and work with any other website.

Current System

In this short term, we developed various types of YAML templates focused on different types of vulnerabilities.

- I was the first to create their YAML template that served as a blueprint and guided our team
- Additionally, I was among one of the first to get the testing environment properly set up.
- Among the team, we had all mutually agreed to do at least 1 template, however some of us including me were comfortable enough to do at least 2 or more.

VERIFICATION

Testing: Focused scans using real-world common vulnerabilities. Furthermore, due to using a controlled testing environment, we can 100% report and confirm the vulnerabilities and their locations which were all accurate.

Verification: In Nuclei you will usually be told where and what caused the vulnerability so in the image on top you can see ‘ OR 1=1 -- ’ is what causes the vulnerability. If it is not given back, it is usually in the code, so for example for password checking like scanning for default passwords, it does not give feedback, but the passwords are coded into the templates.

SUMMARY

To conclude, the **System Vulnerability Scanner** is an easily accessible and free alternative to top existing security tools used by real industry professionals. By using Nuclei and YAML-based customed templates it ensures accurate detecting of vulnerabilities and few false positives due to enhanced searching methods. **Additionally, our coded templates ensure to find multiple different common vulnerabilities that could be present in any network or web-app.**

REQUIREMENTS

False Positives: We do want any false positives present at all, we coded are our templates with a strong focus on some key word manipulation, i.e for default passwords it looks for clues that the login work like Welcome User! Or Hello User!

Customization and Flexibility: Different scenarios are present for any given website we want to be able to scan whichever website and get feedback and info from it.

Feedback: We want to gain as much information as possible specifically where the vulnerability is and what causes the vulnerability!

REFERENCES

- [1] <https://github.com/projectdiscovery/nuclei>
<https://www.yamllint.com/> (YAML Validator)
<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>



Engineering
& Computing

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.

FLORIDA INTERNATIONAL UNIVERSITY