



Knight Foundation
School of Computing
and Information Sciences



Senior Project Final Presentation Fall 2024

Nuclei – Vulnerability Scanner

Team Members:

Zavier Rodriguez, Frederick Gonzalez, Alejandro Hernandez,
Jean Bagnis, Jonathan Rizo

Product Owner: Jonathan Gil

Professor:

Masoud Sadjadi

School of Computing and Information Sciences
Florida International University

12/06/2024



FLORIDA
INTERNATIONAL
UNIVERSITY

COLLEGE OF ENGINEERING AND COMPUTING



Introduction and Motivation

What is Nuclei?

Potential Risks without proper Scanning

Why we wanted to make this happen.

Our Mission as Cybersecurity Students



Problem Definition

- Different Types of Vulnerabilities
- Challenges in Existing Solutions
- Bug Bounties and Middleman



Solution

Flexibility in Scanning

Ease of Use

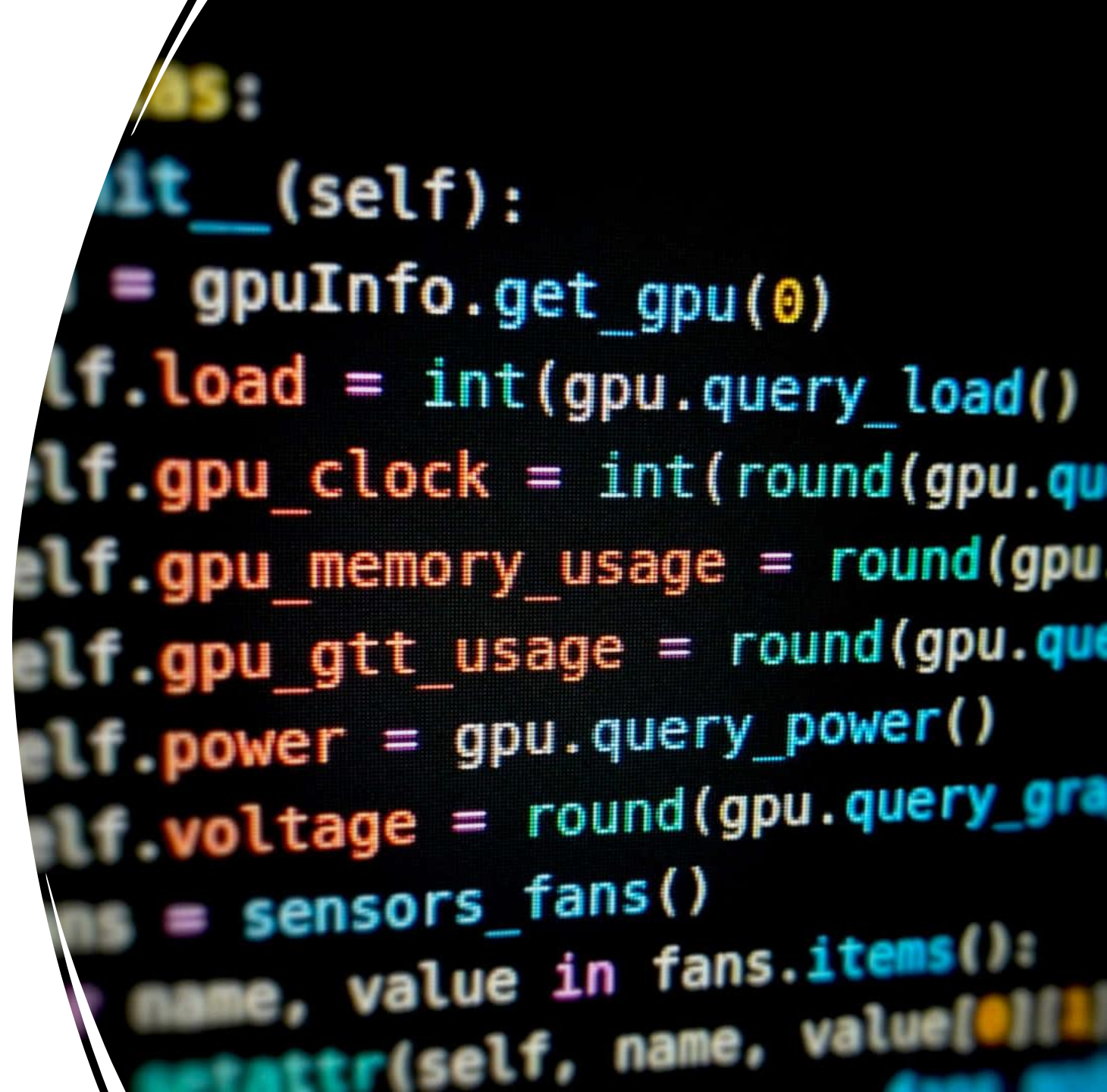
Detailed Vulnerability Insights

Highlighting Specific Risks



System Design

- YAML Templates
 - Purpose
 - Structure
 - Flexibility
- Scanning Engine
 - Supported Protocols: HTTP, DNS, TCP, UDP, and more.
 - Real-World Impact



Verification

- Testing with Metasploitable 2 VM
- Metrics and reports
 - Key Metrics:
 - Severity Level
 - Total vulnerabilities detected
- Detailed Reports



```
nuclei v3.3.4
projectdiscovery.io

[WRN] Found 6 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.1.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 114
[INF] Templates loaded for current scan: 8
[WRN] Loading 8 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[C-Backdoor] [tcp] [critical] 10.0.2.4:3632
[custom-sqli-check] [http] [high] http://10.0.2.4/mutillidae/index.php?page=user-info.php&username='+OR+1=--+&password&user-info-php-submit-button=View+Account+Details
[ssh_auth_methods] [javascript] [info] 10.0.2.4:22 [{"publickey","password"}]
[mutillidae-capture-data-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/capture-data.php?test=<script>alert('XSS')</script> [{"<script>alert('XSS')</script>"}]
[mutillidae-XSS-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/dns-lookup.php [{"XSS"}]
[javascript-injection-check] [http] [high] http://10.0.2.4/mutillidae/index.php?page=password-generator.php&username=<script>alert(1)</script>
[mutillidae-capture-data-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/capture-data.php [{"<script>alert('XSS')</script>"}]
[mutillidae-browser-info-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/browser-info.php [{"<script>alert('XSS')</script>"}]
[mutillidae-XSS-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/dns-lookup.php [{"XSS"}]
[metasploitable-web-weak-passwords] [http] [high] http://10.0.2.4/webdav/
[mutillidae-capture-data-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/capture-data.php [{"<script>alert('XSS')</script>"}]
[mutillidae-browser-info-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/browser-info.php [{"javascript:alert('JS Injection')}"]
[mutillidae-browser-info-vulnerabilities] [http] [high] http://10.0.2.4/mutillidae/browser-info.php [{"<script>alert('User-Agent XSS')</script>"}]
```

Demonstration

FIU

Engineering
& Computing

FLORIDA INTERNATIONAL UNIVERSITY

Thank You!

FIU

Engineering
& Computing

FLORIDA INTERNATIONAL UNIVERSITY



References

- [1] Chinese hackers breach U.S. telecoms, exploiting critical vulnerabilities. (2024, October 5). CNN. ([LINK](#))
- [2] Buy Tenable products: Pricing and licensing. (n.d.). Tenable. ([LINK](#))
- [3] Nuclei: Fast and customizable vulnerability scanner. (n.d.). ProjectDiscovery. ([LINK](#))

