ASSIGNMENT-4

1. OWASP Top 10 Vulnerabilities Overview :

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

1.A01:2021-Broken Access Control

2.A02:2021-Cryptographic Failures

3.A03:2021-Injection

4.A04:2021-Insecure Desig

5.A05:2021-Security Misconfiguration

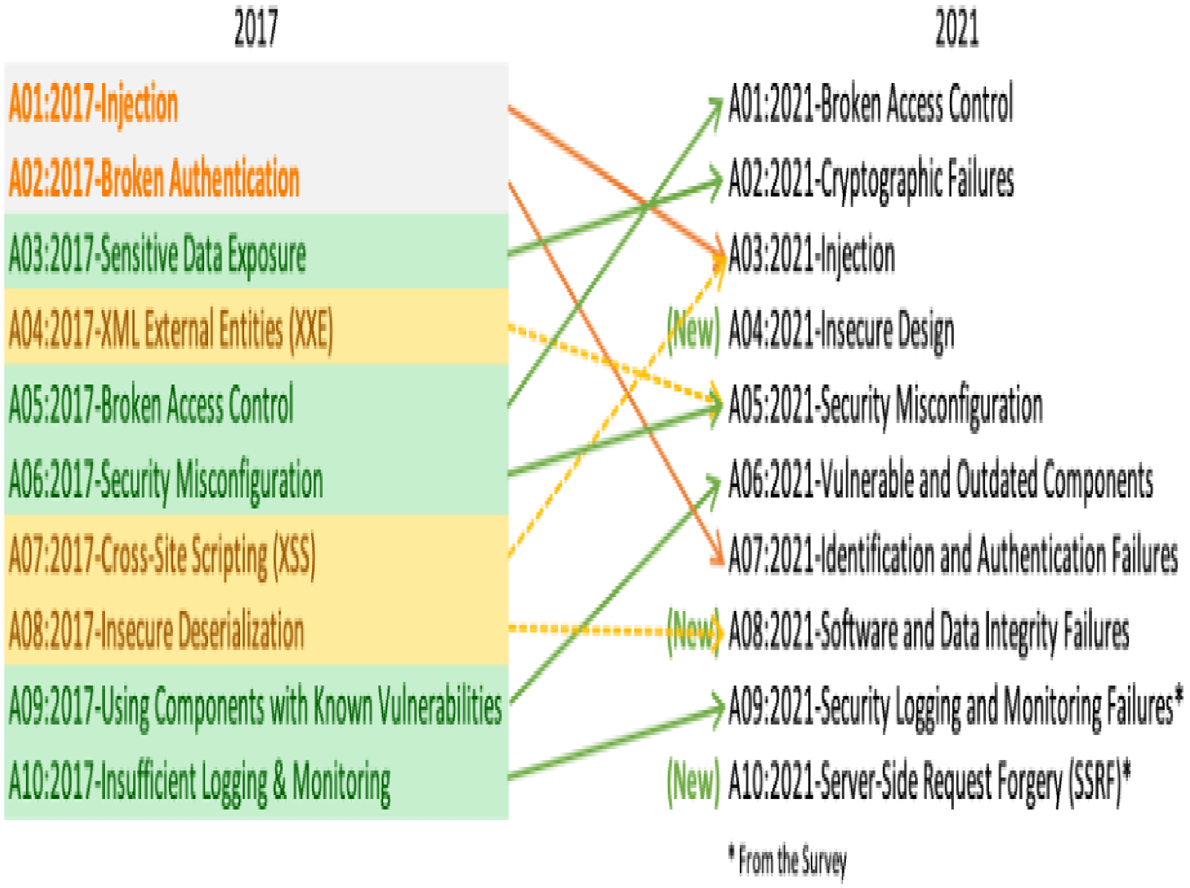
6.A06:2021-Vulnerable and Outdated Components

7.A07:2021-Identification and Authentication Failures

8.A08:2021-Software and Data Integrity Failures

9.A09:2021-Security Logging and Monitoring Failures

10.A10:2021-Server-Side Request Forgery


2017
2021
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

2.Altro Mutual Website Analysis:

"Altro Mutual Website Analysis" likely refers to an analysis conducted on the website of Altro Mutual, a company or organization. Such an analysis typically involves examining various aspects of the website, including design, functionality, user experience, content quality, SEO (Search Engine Optimization) factors, performance, and security.

1.Design: Evaluating the overall aesthetic appeal, layout, typography, color scheme, and visual elements to ensure they align with the brand identity and provide a pleasant user experience.

2.Functionality: Checking for any bugs, errors, or broken links that may hinder navigation or usability. Assessing the responsiveness of the website across different devices and browsers.

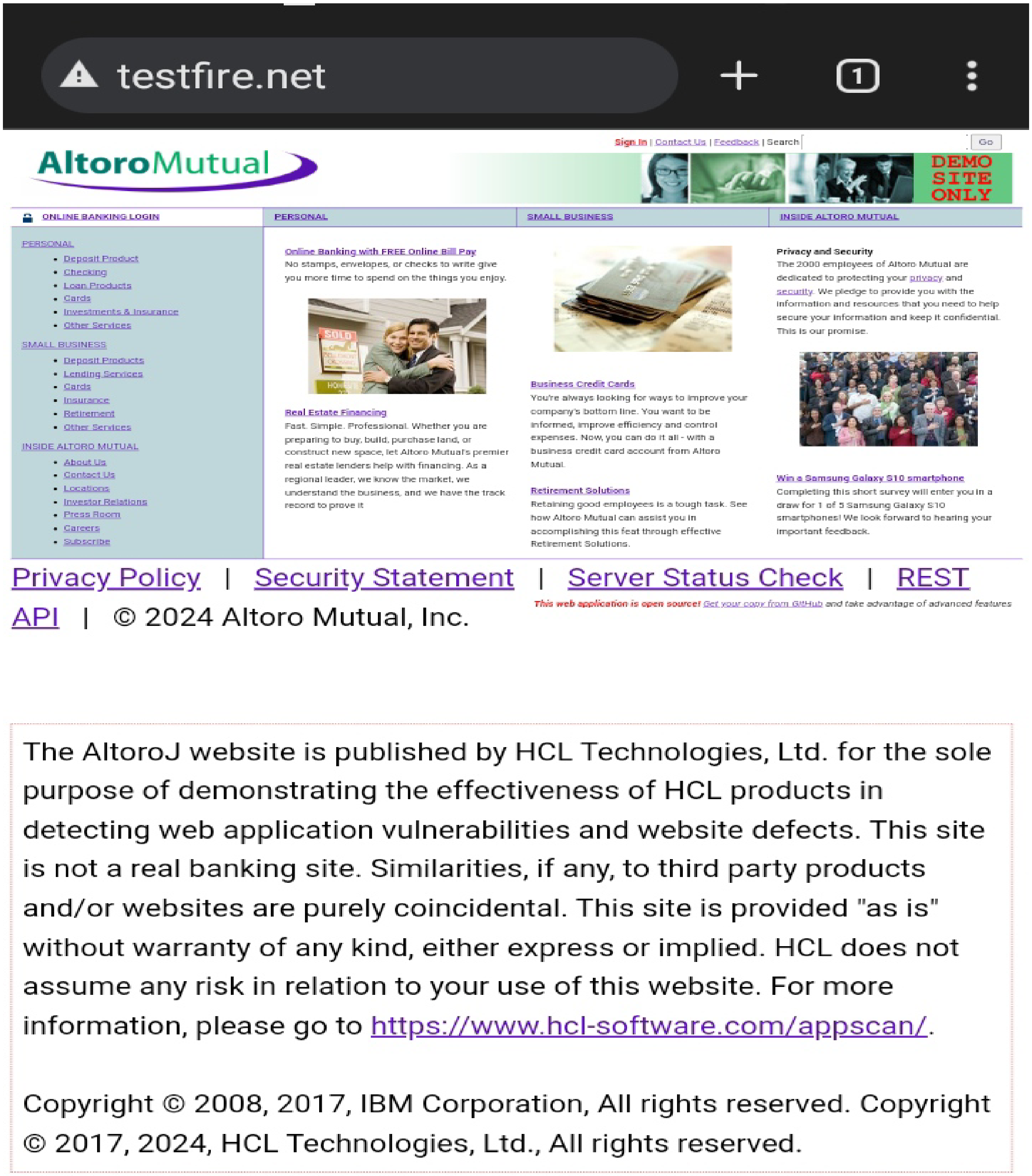
3.User Experience (UX): Analyzing how easily users can interact with the website, find information, and complete tasks. This includes assessing the intuitiveness of navigation, clarity of labels and instructions, and the overall flow of the user journey.

4.Content Quality: Reviewing the accuracy, relevance, and usefulness of the content presented on the website. This involves checking for grammar and spelling errors, outdated information, and ensuring that the content aligns with the target audience's needs and interests.

5.SEO Factors: Examining elements that affect the website's search engine ranking, such as meta tags, keywords, internal linking structure, and page load speed. Optimizing these factors can improve the website's visibility in search engine results.

6.Performance: Assessing the speed and efficiency of the website, including page load times and server response times. Slow performance can lead to a poor user experience and negatively impact SEO.

7.Security: Checking for vulnerabilities and implementing measures to protect user data and prevent unauthorized access. This includes ensuring that the website has SSL encryption, implementing secure login mechanisms, and regularly updating software to patch security vulnerabilities.



Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

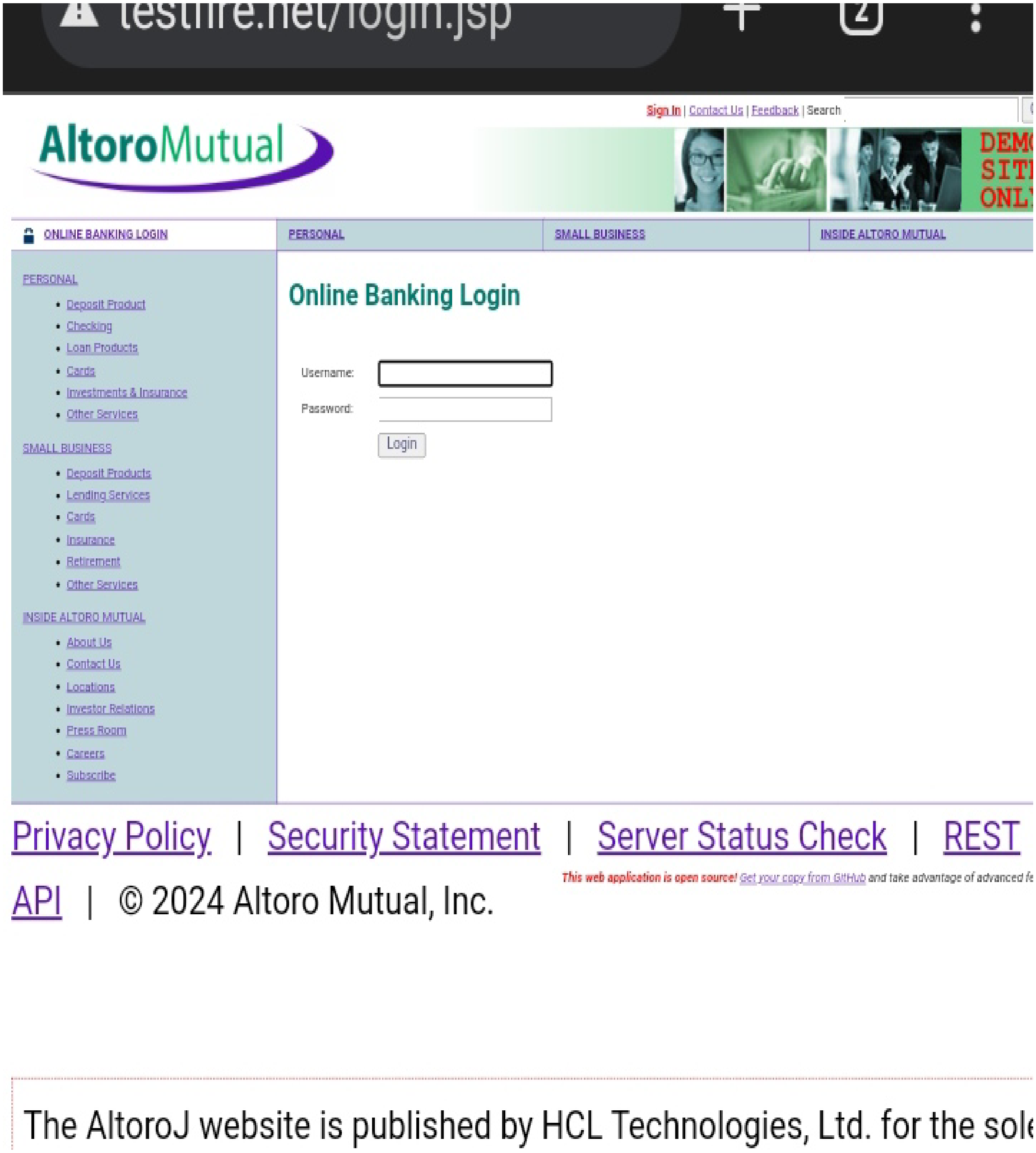
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.



Online Banking Login

Username:

Password:

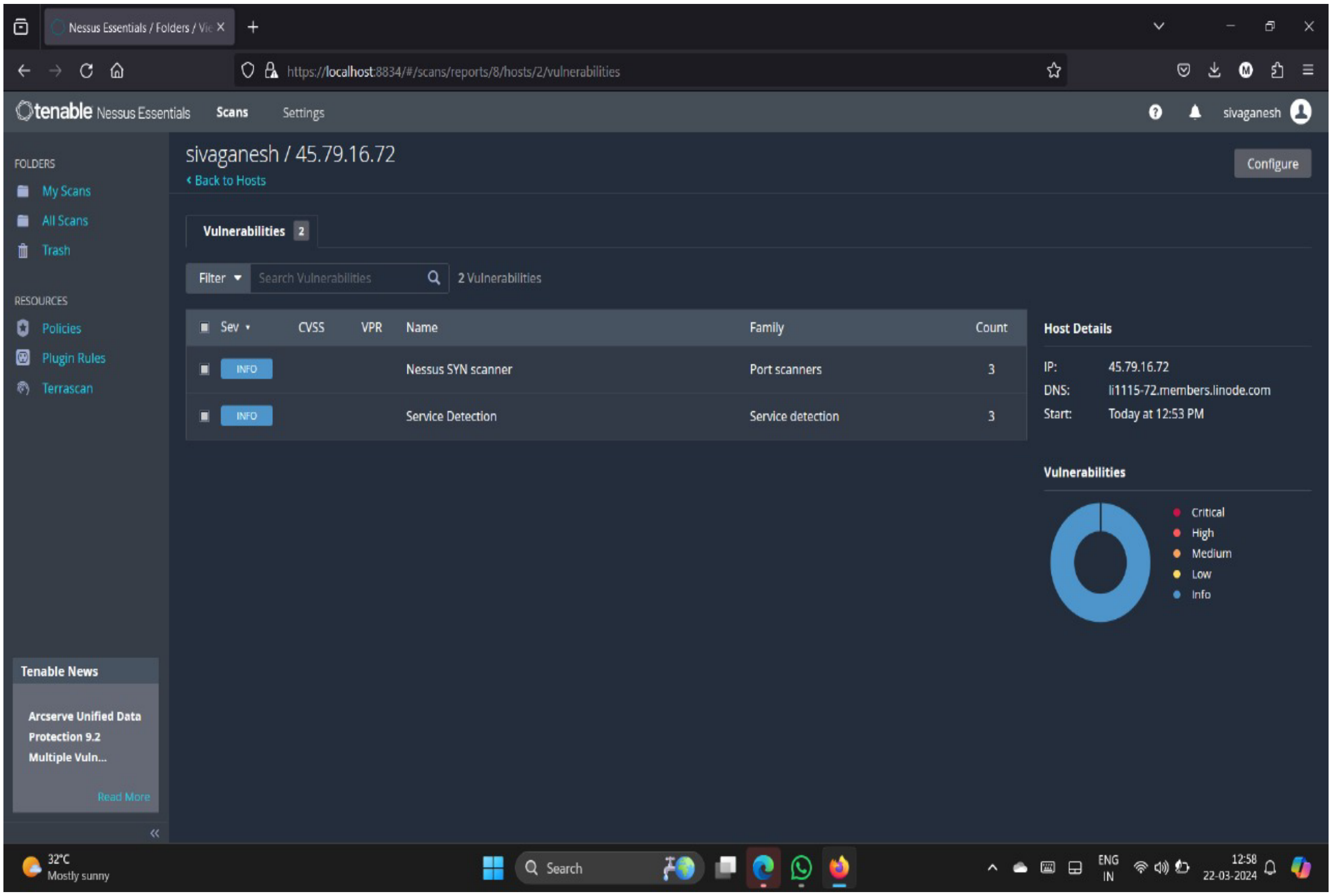
© 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced fe

The AltoroJ website is published by HCL Technologies, Ltd. for the sole

3: Vulnerability Identification Report:

A Vulnerability Identification Report is a document that outlines the vulnerabilities present within a system, network, or application. It typically includes details about each vulnerability, such as its severity, potential impact, affected components, and recommended mitigation measures. The report is often generated by conducting vulnerability assessments or penetration tests, where security professionals systematically scan, test, and analyze the target system for weaknesses. The purpose of the report is to provide stakeholders with a clear understanding of the security posture of the system and to guide efforts to remediate or mitigate the identified vulnerabilities to reduce the risk of exploitation.



sivaganesh / 45.79.16.72

‹ Back to Hosts

2 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	3
INFO			Service Detection	Service detection	3

Host Details

IP: 45.79.16.72
DNS: li1115-72.members.linode.com
Start: Today at 12:53 PM

Vulnerabilities

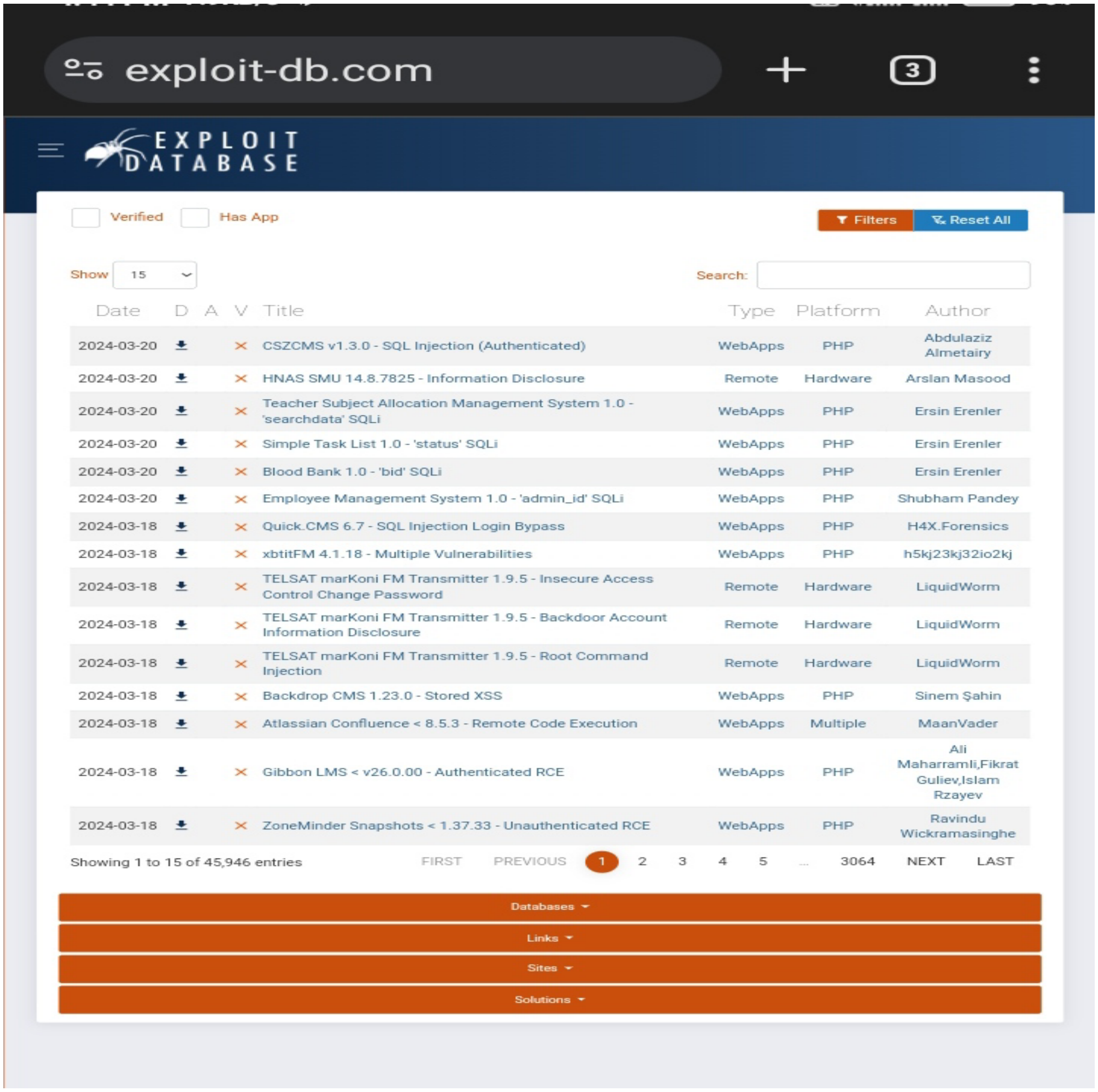
- 🟥 Critical
- 🟥 High
- 🟧 Medium
- 🟨 Low
- 🟦 Info

4. Vulnerability Exploitation Demonstration:

A Vulnerability Exploitation Demonstration is a presentation or practical exercise aimed at illustrating how security vulnerabilities can be exploited in software, systems, or networks. These demonstrations are often conducted by cybersecurity professionals, researchers, or trainers to raise awareness about the potential risks and consequences of vulnerabilities.

During such demonstrations, the presenter typically identifies a specific vulnerability in a system or application, explains how it can be exploited by attackers, and then demonstrates the actual exploitation process. This may involve executing malicious code, bypassing security controls, or gaining unauthorized access to sensitive data or resources.

The purpose of these demonstrations is to educate stakeholders, such as developers, system administrators, and end-users, about the importance of identifying and patching vulnerabilities to mitigate security risks effectively. They also serve to highlight the need for proactive security measures, such as regular vulnerability assessments, penetration testing, and software patching, to minimize the likelihood of successful cyber attacks.

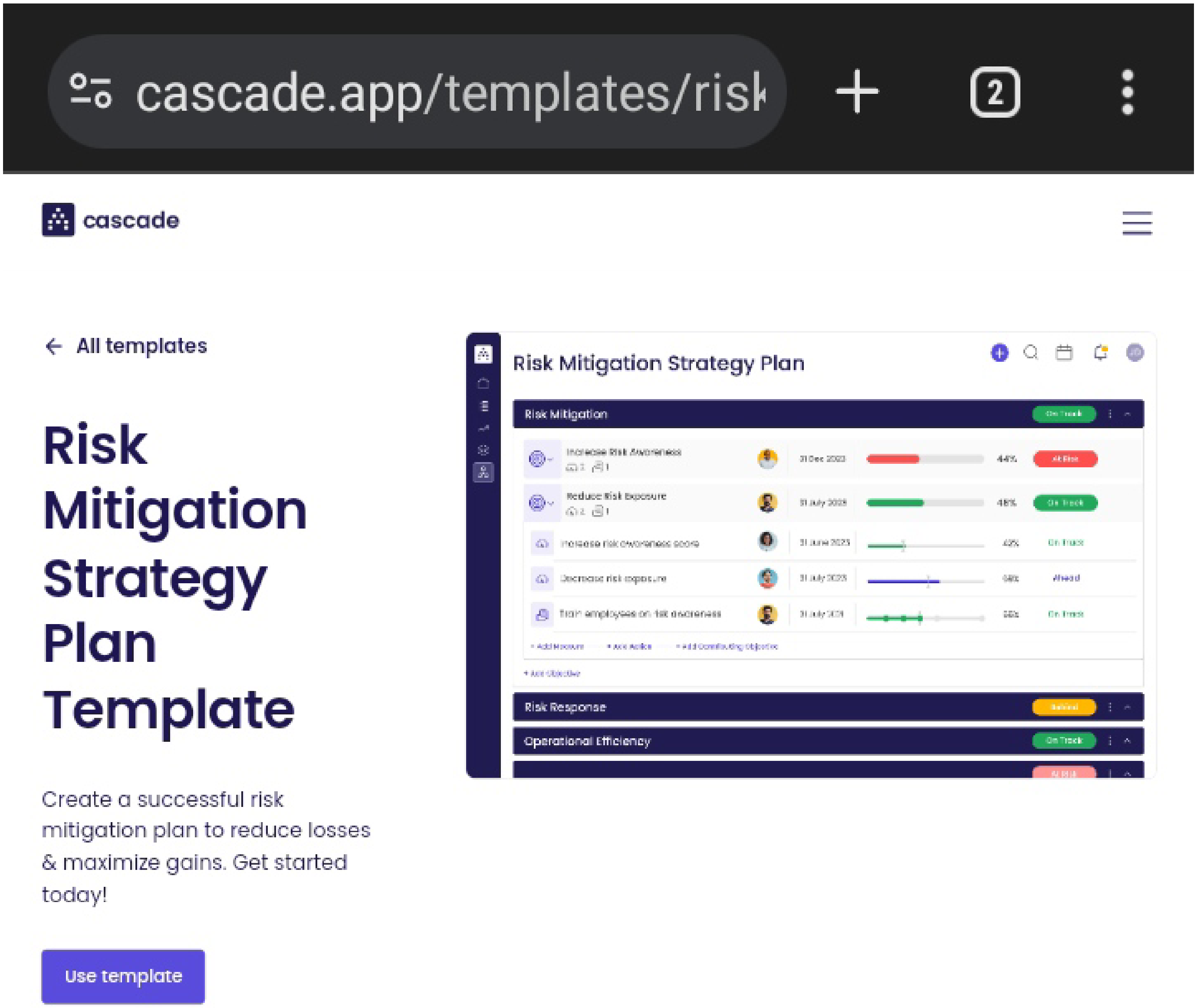


Date	D	A	V	Title	Type	Platform	Author
2024-03-20	⬇		✗	CSZCMS v1.3.0 - SQL Injection (Authenticated)	WebApps	PHP	Abdulaziz Almetairy
2024-03-20	⬇		✗	HNAS SMU 14.8.7825 - Information Disclosure	Remote	Hardware	Arslan Masood
2024-03-20	⬇		✗	Teacher Subject Allocation Management System 1.0 - 'searchdata' SQLi	WebApps	PHP	Ersin Erenler
2024-03-20	⬇		✗	Simple Task List 1.0 - 'status' SQLi	WebApps	PHP	Ersin Erenler
2024-03-20	⬇		✗	Blood Bank 1.0 - 'bid' SQLi	WebApps	PHP	Ersin Erenler
2024-03-20	⬇		✗	Employee Management System 1.0 - 'admin_id' SQLi	WebApps	PHP	Shubham Pandey
2024-03-18	⬇		✗	Quick.CMS 6.7 - SQL Injection Login Bypass	WebApps	PHP	H4X.Forensics
2024-03-18	⬇		✗	xbtitFM 4.1.18 - Multiple Vulnerabilities	WebApps	PHP	h5kj23kj32io2kj
2024-03-18	⬇		✗	TELSAT marKoni FM Transmitter 1.9.5 - Insecure Access Control Change Password	Remote	Hardware	LiquidWorm
2024-03-18	⬇		✗	TELSAT marKoni FM Transmitter 1.9.5 - Backdoor Account Information Disclosure	Remote	Hardware	LiquidWorm
2024-03-18	⬇		✗	TELSAT marKoni FM Transmitter 1.9.5 - Root Command Injection	Remote	Hardware	LiquidWorm
2024-03-18	⬇		✗	Backdrop CMS 1.23.0 - Stored XSS	WebApps	PHP	Sinem Şahin
2024-03-18	⬇		✗	Atlassian Confluence < 8.5.3 - Remote Code Execution	WebApps	Multiple	MaanVader
2024-03-18	⬇		✗	Gibbon LMS < v26.0.00 - Authenticated RCE	WebApps	PHP	Ali Maharramli,Fikrat Guliev,Islam Rzayev
2024-03-18	⬇		✗	ZoneMinder Snapshots < 1.37.33 - Unauthenticated RCE	WebApps	PHP	Ravindu Wickramasinghe

Showing 1 to 15 of 45,946 entries

5. Mitigation Strategy Proposal :

A mitigation strategy proposal outlines actions and measures to reduce or minimize risks, threats, or negative impacts associated with a particular situation or project. This could involve anything from environmental hazards to cybersecurity threats or financial risks. The proposal typically includes an analysis of potential risks, followed by specific strategies or interventions aimed at preventing or mitigating those risks. It may also detail the resources needed, timelines, and responsible parties for implementing the proposed strategies. The goal is to proactively address potential problems before they occur or minimize their impact if they do occur.



cascade.app/templates/risk

cascade

← All templates

Risk Mitigation Strategy Plan Template

Create a successful risk mitigation plan to reduce losses & maximize gains. Get started today!

Use template

6.Documenting the Exploit Process :

Documenting the exploit process involves thoroughly recording the steps taken to identify, analyze, and exploit vulnerabilities in a system or software. This documentation serves several purposes:

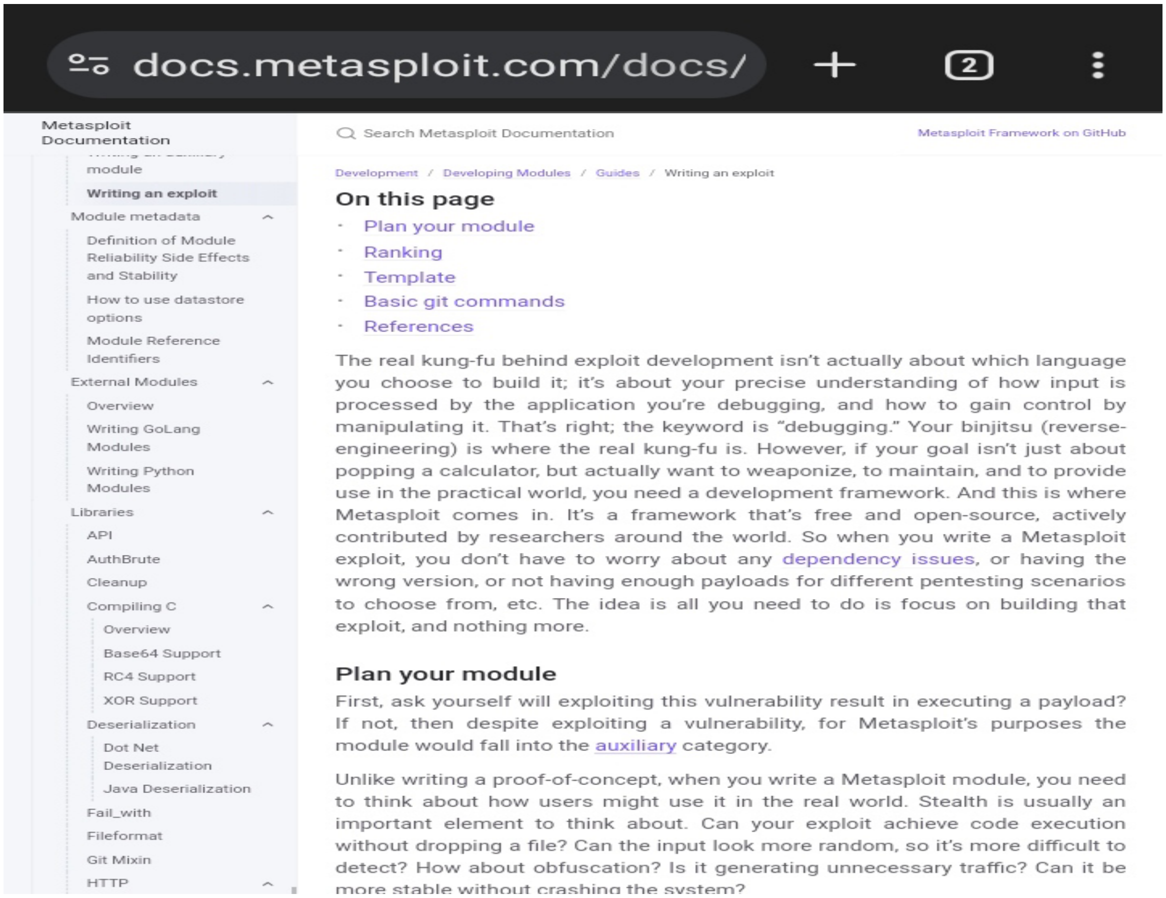
1.Reproducibility: By documenting the exploit process, others can reproduce the steps to verify the vulnerability and understand how it was exploited. This helps in validating the existence of the vulnerability and allows for its effective mitigation.

2.Knowledge Transfer: Documenting the exploit process facilitates knowledge transfer within a team or organization. It ensures that insights gained from discovering and exploiting vulnerabilities are shared among team members, enhancing the collective understanding of security risks and mitigation strategies.

3.Legal Compliance: In some cases, documenting the exploit process may be necessary for legal compliance, particularly when reporting vulnerabilities to vendors or authorities. Detailed documentation can provide evidence of responsible disclosure and ethical behavior.

4.Post-Incident Analysis: Documenting the exploit process enables post-incident analysis to identify weaknesses in the system or processes that allowed the vulnerability to be exploited. This information can be used to improve security measures and prevent similar incidents in the future.

5.Training and Education: Documentation of the exploit process can be valuable for training purposes, helping security professionals and developers understand common attack vectors, exploit techniques, and defensive strategies.



On this page

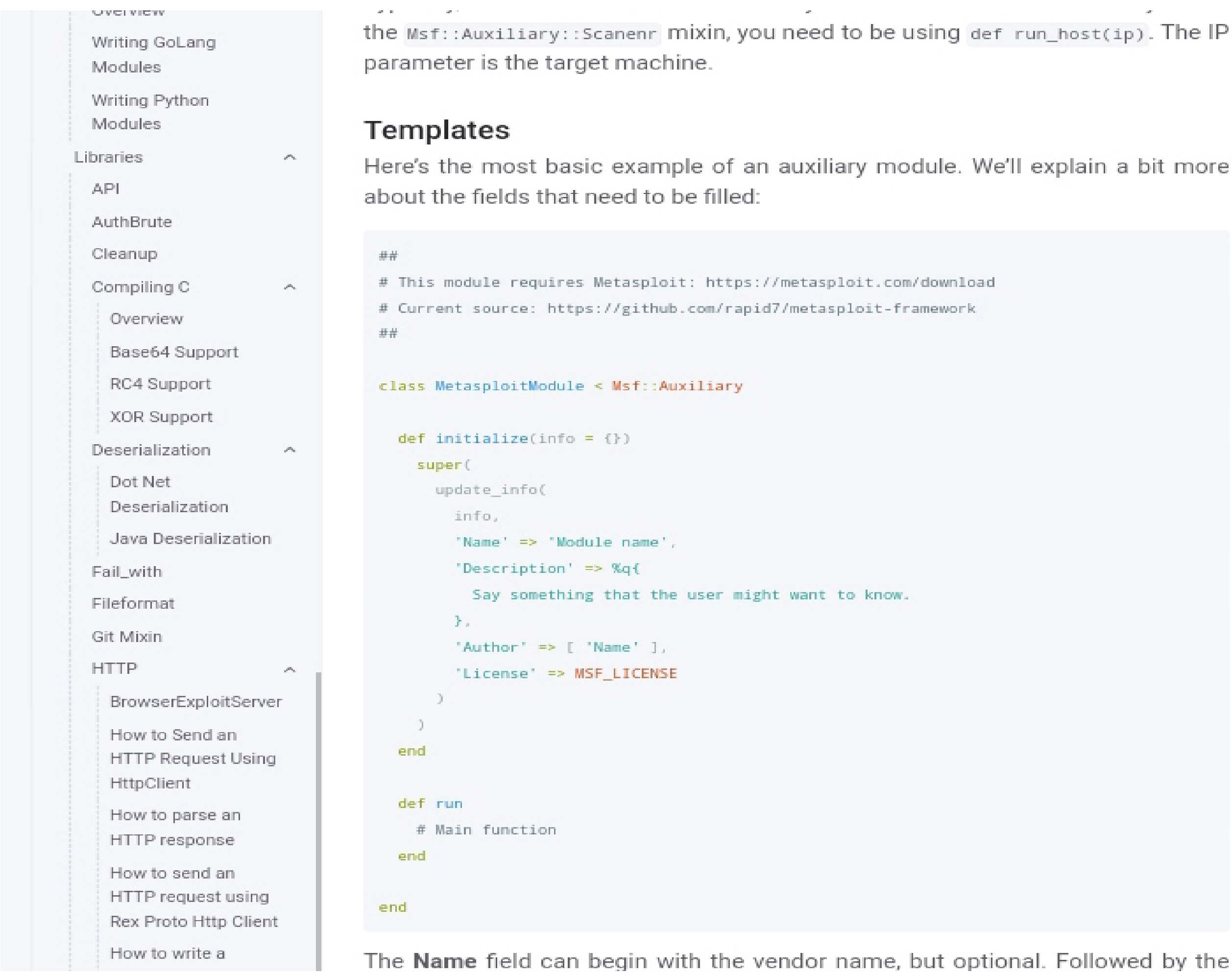
- Plan your module
- Ranking
- Template
- Basic git commands
- References

The real kung-fu behind exploit development isn't actually about which language you choose to build it; it's about your precise understanding of how input is processed by the application you're debugging, and how to gain control by manipulating it. That's right; the keyword is "debugging." Your binjitsu (reverse-engineering) is where the real kung-fu is. However, if your goal isn't just about popping a calculator, but actually want to weaponize, to maintain, and to provide use in the practical world, you need a development framework. And this is where Metasploit comes in. It's a framework that's free and open-source, actively contributed by researchers around the world. So when you write a Metasploit exploit, you don't have to worry about any dependency issues, or having the wrong version, or not having enough payloads for different pentesting scenarios to choose from, etc. The idea is all you need to do is focus on building that exploit, and nothing more.

Plan your module

First, ask yourself will exploiting this vulnerability result in executing a payload? If not, then despite exploiting a vulnerability, for Metasploit's purposes the module would fall into the auxiliary category.

Unlike writing a proof-of-concept, when you write a Metasploit module, you need to think about how users might use it in the real world. Stealth is usually an important element to think about. Can your exploit achieve code execution without dropping a file? Can the input look more random, so it's more difficult to detect? How about obfuscation? Is it generating unnecessary traffic? Can it be more stable without crashing the system?



the `Msf::Auxiliary::Scanenr` mixin, you need to be using `def run_host(ip)`. The IP parameter is the target machine.

Templates

Here's the most basic example of an auxiliary module. We'll explain a bit more about the fields that need to be filled:

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Auxiliary

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Module name',
        'Description' => %q{
          Say something that the user might want to know.
        },
        'Author' => [ 'Name' ],
        'License' => MSF_LICENSE
      )
    )
  end

  def run
    # Main function
  end

end
```

The **Name** field can begin with the vendor name, but optional. Followed by the