Defend with Jasmin Shield 2.0; Protect with your Cyber Sword

"Security used to be an inconvenience sometimes, but now it's a necessity all the time."

— Martina Navratilova

Imagine a world of convenience, where refrigerators order groceries, thermostats learn & follow schedules, and blood pressure monitors alert Doctors in real-time. This is the promise of the Internet-of-Things; an interconnected web of smart devices enhancing our lives. And we will rely on these smart devices, with no option to get off this grid. The proliferation of IoT and mobile devices thus introduce additional security challenges that require the advanced tools for performing security testing.

If the legendary advice is repeated today, it now would be more cautious and say - with great connectivity comes great vulnerability.

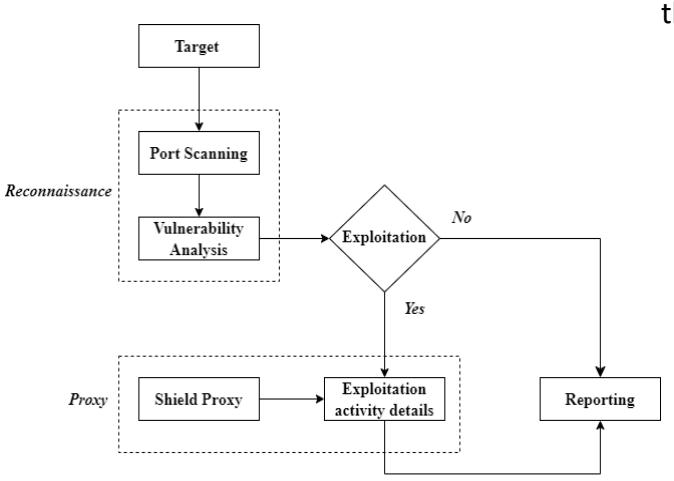
Jasmin Shield, your Defender

Created exclusively for Penetration Testing as a Service (PTaaS); Jasmin Shield is a customized "in-house" penetration testing tool. Meant to test our customers' own designed & prototyped products. It allows security professionals to perform thorough security assessments, detect vulnerabilities, and analyse the security posture of application, networks, and systems.

Organizations can use Jasmin Shield to proactively address security concerns and strengthen their defence.

Jasmin shield's Summary of Testing Report provides a comprehensive analysis of security vulnerabilities in the target system, including detailed findings, impact assessments, CVSS scores, and mitigation strategies.

Jasmin Shield tool is available in several versions, each version with a set of benefits and limits that suit specific user needs and scenarios.



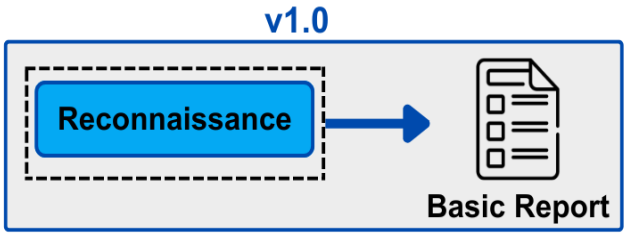
Jasmin Shield - Basic Workflow:

Jasmin Shield 1.0

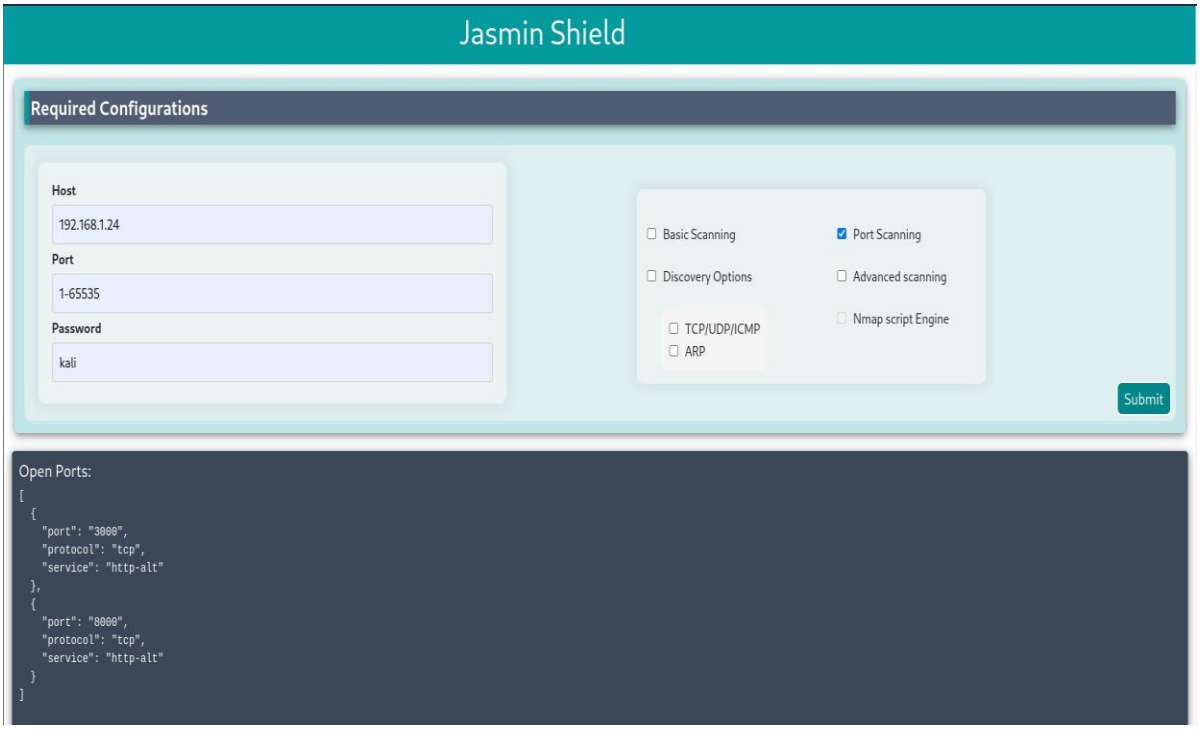
Jasmin Shield 1.0 was developed as a reconnaissance and reporting tool; with scanning & discovery capability, to capture information from the target system. It employed features such as port scanner, subdomain enumeration, and information lookup. Also reported the basic system information of the target.

Limitations:

- Essentially pre-penetration scanning tool for information gathering; with no capability of attacks on the target
- Provides minimal reporting and executing a limited number of test cases.



Jasmin Shield v1.0 port scanning result



Jasmin Shield v2.0

Jasmin shield tool v2.0 now additionally supports penetration testing and vulnerability scanning. One can now utilize reconnaissance to obtain information, vulnerability scanners to detect common flaws, and shield proxy to exploit system weaknesses. In addition, we included a Web application firewall detector for reconnaissance.

Web application and network vulnerability scanners generate extensive reports with CVSS scores and remediation recommendations for vulnerabilities in the system.

Shield proxy offers multiple features, including proxy, intercept, repeater, comparer, and decoder. As a result, Jasmin Shield 2.0 can be deployed as a proxy to examine, change, and remove existing system communication. This capability is key to use Jasmin Shield V2.0 as a penetration testing tool.

Why a Proxy - the Sword - with Jasmin Shield v2.0?

Jasmin Shield v1.0 without the inclusion of any exploitation tool; works towards information gathering, with no aggression. As we know, offence is the best defence, - hence the proxy Sword.

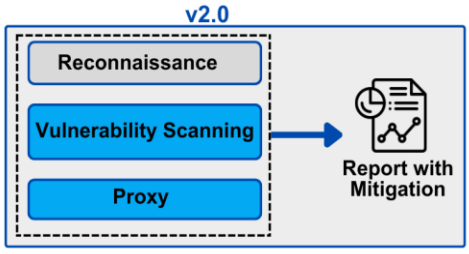
Implementing Proxy capabilities in Jasmin Shield v2.0 was deemed essential for thorough penetration testing. The following are some of the advantages of using a proxy for penetration testing.

- Allows for real-time interception and inspection of traffic between clients and servers, providing deep insights into communication patterns.
- Enables identification of vulnerabilities such as insecure data transmission, weak encryption, and sensitive information leakage
- Simulates various attack scenarios such as Man-In-The-Middle (MITM) attacks, helping to identify weaknesses in data validation and handling
- Allows testers to modify requests and responses in transit to test how systems handle manipulated data

Advanced tools of Jasmin Shield v2.0

Jasmin shield v1.0 has limitations in - not suitable for - scanning the large domains.

Jasmin shield v2.0 has many reconnaissance tools, proxies and vulnerability scanners are available to do thorough testing. Also, it provides detailed reporting with its impact, CVSS score and mitigation.



Jasmin Shield v2.0 port scanning and web vulnerability Result

Jasmin Shield

Port Probe Scanner Report

Port probe scanner generate detailed reports containing information about open ports, including their number, status, and the services associated with them. This output helps users assess the security posture of the target system and prioritize further investigation.

192.168.1.24

Scan Information:

Nmap 7.94SVN was initiated at Mon Jul 22 14:04:59 2024 with these arguments:

nmap -T5 -sV -p 1-65535 -n --min-parallelism 100 --max-parallelism 256 --max-retries 1 --min-host-group 64 --max-hostgroup 128 --max-rtt-timeout 1000ms --min-rate 10000 -oA nmap_scan_results 192.168.1.24

IPv4 Address: 192.168.1.24

Ports:

The 65535 ports are scanned and only open ports are Filtered below:

65533 ports are closed and replied with: conn-refused

Port	Protocol	State	Reason	Service	Product	Method	Tunnel	Confidential
3000	tcp	open	syn-ack	http	Node.js Express frame-work	probed	N/A	10
8000	tcp	open	syn-ack	http	Node.js Express frame-work	probed	N/A	10

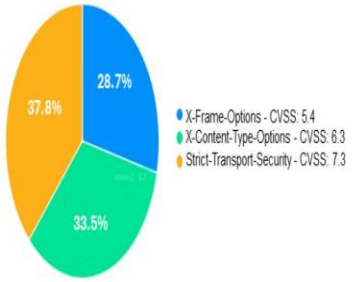
Web Vulnerability Scanner Report

Target Information:

Site	example.com
IP Address	xxx.xx.xxx.x
Headers	X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, Permissions-Policy

Graphical Summary

The below graphical representations will provide you with an overall summary of the security audit scan results, including vulnerabilities discovered, severity & respective CVSS Score.



Missing Headers:

Header	Description
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared con-tent-type. The only valid value for this header is "X-Content-Type-Options: nosniff"
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; include Subdomains".

Potential Risks from Missing Security Headers

X-Frame-Options	
Attack Name	Clickjacking
Description	Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.
CVSS	5.4
References	https://owasp.org/www-community/attacks/Clickjacking
Mitigations	Use the X-Frame-Options HTTP header to prevent your web pages from being loaded inside a frame or iframe by other sites. Setting this header to DENY or SAMEORIGIN helps to prevent clickjacking attacks.

X-Content-Type-Options	
Attack Name	MIME-Type Sniffing
Description	MIME-type sniffing is a security issue where a web browser or other client incorrectly guesses the MIME type of a resource and processes it in a way that can lead to vulnerabilities. This occurs when the declared MIME type is ignored, and the content is instead interpreted based on its actual content, potentially leading to security risks such as cross-site scripting (XSS) attacks.
CVSS	6.3
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
Mitigations	Use the X-Content-Type-Options HTTP header with the value nosniff. This instructs browsers not to perform MIME type sniffing and to trust the Content-Type header provided by the server

Strict-Transport-Security	
Attack Name	MITM (Man-in-the-middle attack)
Description	If a website accepts a connection through HTTP and redirects to HTTPS, visitors may initially communicate with the non-encrypted version of the site before being redirected, if, for example, the visitor types http://www.foo.com/ or even just foo.com. This creates an opportunity for a man-in-the-middle attack. The redirect could be exploited to direct visitors to a malicious site instead of the secure version of the original site
CVSS	7.3
References	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
Mitigations	Implement HSTS to enforce secure connections over HTTPS and prevent downgrade attacks. This ensures that communication between the client and server is always encrypted, reducing the risk of MitM attacks.

The **Jasmin Shield v2.0** penetration testing report offers detailed findings, including impact assessment, CVSS scores, and mitigation recommendations. Additionally, it enhances readability with visual representations such as graphs and charts.

Reason for Upgrading the Jasmin shield 2.0 to 3.0

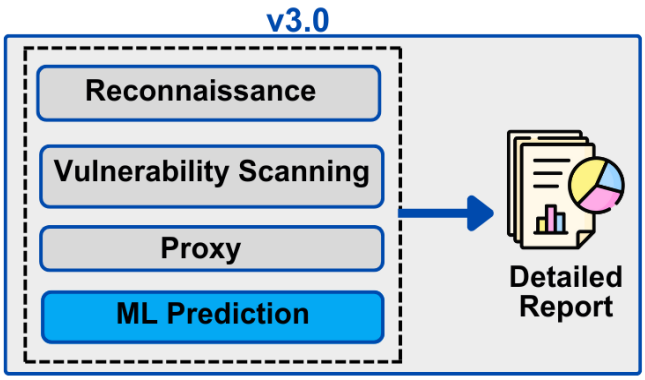
With the incorporation of Machine Learning tools within the platforms, in subsequent versions we will not be limited to eliminating common & existing vulnerabilities. In fact, with targeted training models & vast test data; Jasmin Shield platform will leverage the prediction capability of AI to identify potential vulnerable spots in the target device under test.

Plan about Jasmin Shield v3.0

We intend to include ML-based penetration testing and sophisticated reporting in Jasmin Shield Tool v3.0. This function uses the training data set to foresee & forecast new vulnerabilities in the system and gives sophisticated reports with vulnerability, severity, mitigation solutions, and reports tailored to user interests. This is also beneficial for identifying unknown vulnerabilities in the system.

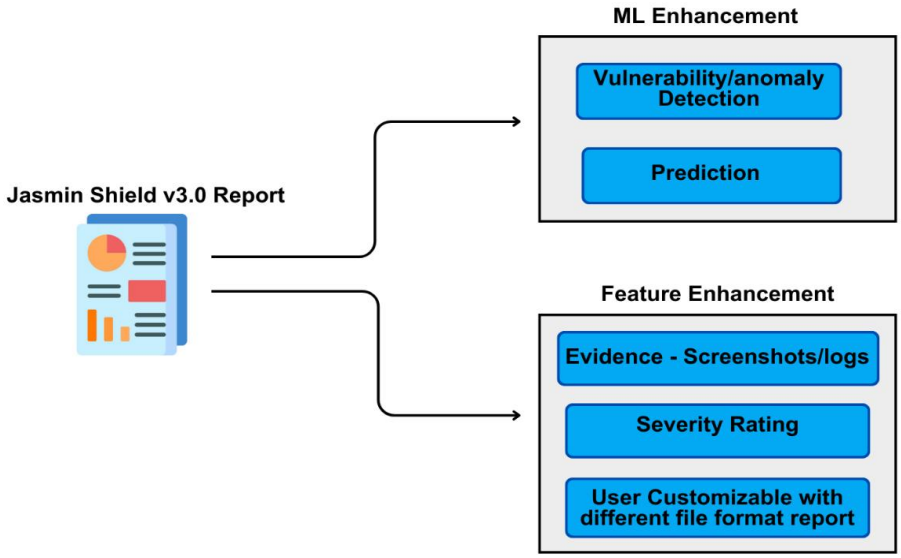
Benefits of ML in Jasmin shield 3.0:

- ML models can analyse patterns and behaviours to detect sophisticated and emerging threats that traditional methods might miss, including zero-day vulnerabilities
- It reduces the extensive manual labour and generate detailed reports



Jasmin Shield v3.0 Report

Jasmin shield v3.0 report shall outline the results of an ML-enhanced penetration test on the target system. By utilizing machine learning algorithms, the analysis will provide a deeper understanding of potential vulnerabilities, their impact, and recommendations for remediation.

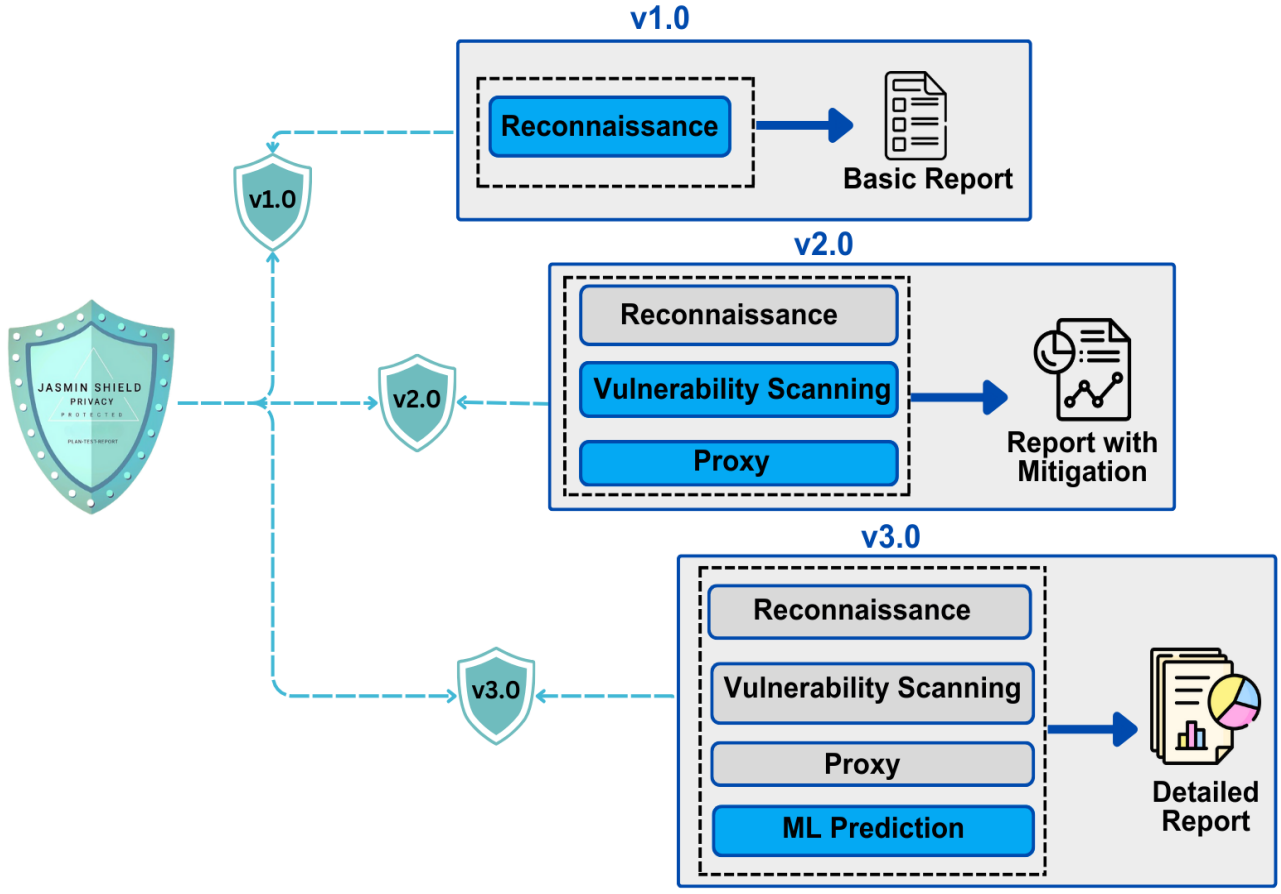


ML Features:

1. **Vulnerability/anomaly Detection**
    - Identify unusual patterns in network traffic that correlate with potential attack vectors.
    - Detected repeated patterns of misconfigurations and weaknesses that are commonly exploited.
2. **Predictive Analysis:** Forecast the vulnerabilities based on historical data and emerging threats.

Feature Enhancement in Jasmin shield:

1. **Evidence – Screenshot/logs**
    - Screenshots and logs provide evidence of identified vulnerabilities.
    - Raw data logs that show the sequence of events leading up to the issue
2. **Severity Rating**
    - Each vulnerability or finding is assigned a severity level (e.g., critical, high, medium, low).
    - Severity helps prioritize remediation efforts.
3. **User customizable with different file format report**
    - Users can tailor the report to their specific needs.
    - User can select the file format based on the requirement. Reports can be generated in various formats (PDF, HTML, CSV, DOCX)



Jasmin Shield different version and its features:

Jasmin Shield Version	v1.0	v2.0	v3.0
Features list: Port Probe	✓	✓	✓
Subdomain Enumeration	✓	✓	✓
Information Lookup	✓	✓	✓
WAF Detector		✓	✓

Jasmin Shield Version	v1.0	v2.0	v3.0
Web Vulnerability Scanner		✓	✓
Network Vulnerability Scanner		✓	✓
Proxy		✓	✓
Report with mitigation, CVSS Score		✓	✓
Anomaly Detection			✓
Prediction			✓
Advanced Report (Evidence, Logs)			✓

Use case 1: Testing a web application using Jasmin Shield v2.0

Objective: To ensure the security of a web application by identifying and mitigating potential vulnerabilities using Jasmin Shield

Steps:

- **Information Gathering:**
  - Use Jasmin Shield Reconnaissance tools to gather information about the target website, such as domain details, server configurations, and software versions.
  - It will Identify open ports and running services to detect potential entry points for attackers.

- **Vulnerability Scanning:**
  - We will conduct automated scans to identify common vulnerabilities like SQL injection, XSS, CSRF, and insecure configurations using Jasmin shield vulnerability scanners
- **Exploitation using Proxy:**
  - Use Jasmin Shield's proxy capabilities to intercept and analyse traffic between the browser and web server.
  - We can test how the website handles manipulated requests and responses by simulating real-world attack scenarios.
- **Report with mitigation:**
  - It will generate comprehensive reports detailing identified vulnerabilities, their severity with CVSS score, and potential impacts.
  - It provides actionable recommendations for mitigating identified risks and enhancing the website's security posture.

Conclusion:

Jasmin Shield is a sophisticated penetration testing tool that uses automation, machine learning, and proxy capabilities to enhance security and resilience of IoT devices and networks.

****** STAY TUNED ******

**** Next article Update - Test a Home automation device using Jasmin shield ****

The goal of the next article will be doing security testing to evaluate the data transmission security of the home automation device using Jasmin shield 3.0 and how it identifies vulnerability detection and predictive analysis using ML in addition with potential flaws that how it could compromise the data's integrity and confidentiality.

Contact Details

Jasmin Infotech Private Limited (HQ)
Plot 119 Velachery Tambaram Road
Pallikaranai, Chennai 600100
India

MS. JEYASUDHA / MR. NARENDRAN OVI

M: +91 89251 09996
narendran.ovi@jasmin-infotech.com