A Survey on Vulnerability Assessment of Indian Police Websites Security

Sahil gurjar[1], Sushma desai[2]
[1, 2] Department of forensic science, Yashvantrao Chavan Institute of Science, Satara, Maharashtra, India

***Abstract*— This abstract highlights the issue of website vulnerability in police traffic challan websites in India. Despite the benefits of having websites, there is a growing concern about the security of such websites due to a lack of secure programming practices, miss-configuration of systems and web application vulnerabilities, or not staying up-to-date with security patches. Attackers may exploit these vulnerabilities and conduct attacks that result in data loss, privacy loss, and other risks. The vulnerability assessment of police traffic challan websites was conducted using online open source tools, where light vulnerability scan tests were performed. The assessment showed that out of the top 5 police traffic challan websites, 4 are at high risk, and one is at medium risk. Improvement in these websites is necessary to mitigate possible cyber-attacks and fix the vulnerabilities.**

***Index Terms*—Information Security, Police Traffic Challan Website Security, Website Vulnerability.**

I.INTRODUCTION

In today's digital age, website security is of utmost importance, especially for traffic challan websites. Web security techniques such as passwords, encryption, authentication, and integrity are used to secure web application layers from unauthorized user attacks. However, despite these security measures, vulnerabilities in websites can still exist, making them susceptible to attacks such as SQL injection, cross-site scripting, header manipulation, and click jacking. To detect these vulnerabilities, scanning the links within URLs and vulnerability assessment of websites are conducted to propose solutions to solve security issues. For instance, Hackers in India studied how to protect traffic challan websites from vulnerabilities, while other authors conducted assessments of Indian government websites using a penetration testing framework (pen test) in four main phases: reconnaissance, scanning, enumeration, vulnerability assessment, and SSL encryption evaluation to discover vulnerabilities that could be exploited by attackers. Furthermore, Positive Technologies published the percentage of the top 10 OWASP vulnerabilities in web applications in 2022, as shown in figure 1, highlighting the need for continued vigilance and improvement in traffic challan website security.

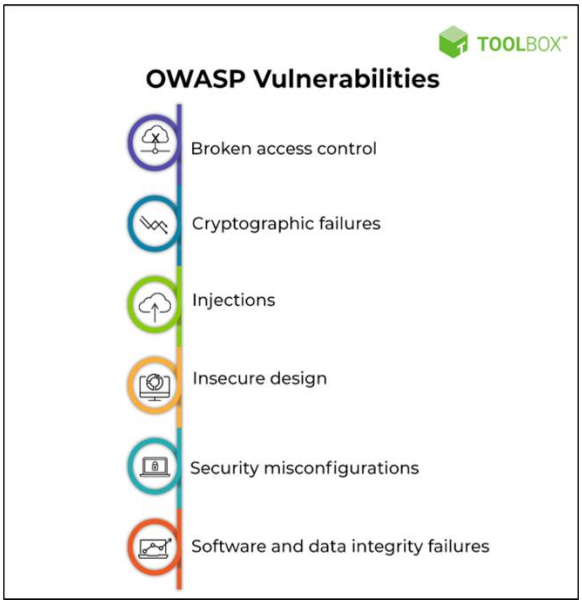
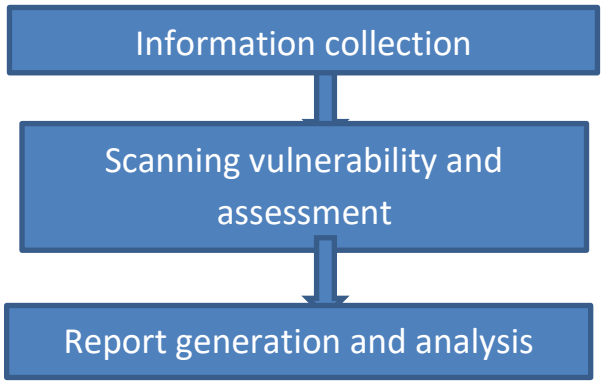


Fig. 1: OWASP Vulnerabilities

To protect against cyber-attacks, it is essential for traffic police challan websites to analyze different types of hacking with their respective phases. These websites must also take measures to safeguard against intruders and investigate the impact of various threats such as DOS, SQL injection, cross-site scripting, and sniffing/request tampering. Additionally, traffic police challan websites should prioritize compliance with information security policies, promote an information security culture, increase information security awareness, and implement effective information security management practices to mitigate the risk of cyber-attacks and ensure the protection of sensitive information.

II. METHODOLOGY

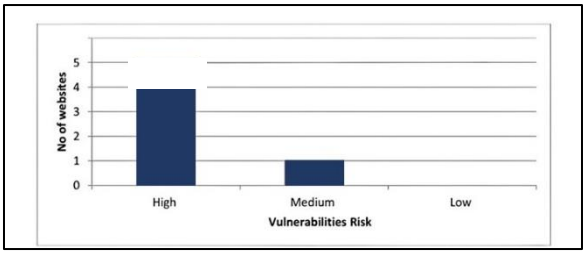
The vulnerability survey in this study was conducted in three stages, with a flow chart of these stages shown in Figure 2.



A. Information collection: Information collection is a critical phase in hacking or pen testing. It involves gathering data about the target system or application, such as network topology, IP addresses, server types, and software versions. This information helps attackers identify vulnerabilities and weaknesses that can be exploited to gain unauthorized access to the system or steal sensitive data. Techniques used in information collection include port scanning, network mapping, OS fingerprinting, and banner grabbing. It is important for organizations to conduct their own information collection activities to proactively identify and address vulnerabilities before attackers can exploit them.

B. Scanning vulnerability and assessment: are important techniques in hacking or penetration testing. They involve identifying potential security vulnerabilities in a system or application. This process helps to identify weaknesses that can be exploited by attackers. Scanning tools and techniques are used to search for vulnerabilities such as SQL injection, cross-site scripting, and other common exploits. Once the vulnerabilities are identified, they are assessed and prioritized based on the potential impact to the system. This information is then used to develop a plan for remediation and risk mitigation.

C. Report generation and analysis: Report generation and analysis are essential components of hacking or pen testing engagements. The purpose of a report is to document the findings of a pen testing or hacking engagement, including vulnerabilities and potential risks. A well-written report should provide a clear and concise overview of the testing process, results, and recommendations for remediation. The report should be tailored to the intended audience, whether that be technical personnel, management, or regulatory bodies. Analysis of the report can inform future security strategies and guide decision-making on how best to address identified vulnerabilities.



	Website vulnerabilities	Host 1	Host 2
1	HTTP Cookie Flags	Insecure	Secure
2	Clickjacking	Insecure	Secure
3	CAPTCHA	Secure	Secure
4	robots.txt	Secure	Secure
5	Mail Server Misconfiguration	Insecure	Secure
	Secuirty Headers		
1	X-Frame-Options	Insecure	Secure
2	Strict-Transport-Security	Insecure	Secure
3	Content Security Policy	Insecure	Insecure
4	Referrer Policy	Secure	Secure
5	XSS protection	Insecure	Insecure

All five hosts have been found to contain vulnerabilities during the discussion of vulnerabilities.

1. Missing HTTP Cookie Flags: This vulnerability was found in Host 1. HTTP cookies are used to store user information, but if the cookies are not properly secured with flags such as HTTP Only and Secure, attackers can hijack the user's session and access sensitive information.

2. Click jacking: Host 1 was also found to be vulnerable to Clickjacking, a type of attack where attackers use transparent or hidden frames to trick

users into clicking on buttons or links that execute unintended actions.

3. Captcha: The study found that all Hosts were not vulnerable to Captcha attacks. Captchas are used to distinguish human users from bots and automated programs. Without Captchas, attackers can launch automated attacks, such as brute-force attacks, on login forms and other sensitive pages.

4. Robots. txt: The study found that all Hosts were not vulnerable to robots.txt attacks. The robots.txt file is used to instruct web robots which pages to crawl and which ones to avoid. Attackers can use this file to identify sensitive pages and exploit them.

5. Mail Server Misconfiguration: Host 1 was also found to have a Mail Server Misconfiguration vulnerability. This vulnerability can allow attackers to access sensitive information, such as email addresses and passwords, and use them for further attacks, such as phishing attacks.

HTTP security headers

1. X-Frame-Options: This header provides clickjacking protection by preventing a webpage from being loaded inside an iframe. Host 1 is vulnerable to clickjacking attacks as it does not have this header enabled.

2. Strict-Transport-Security: This header enforces the use of HTTPS, protecting against man-in-the-middle attacks and SSL stripping. Host 1 and Host 4 are vulnerable to such attacks as they do not have this header enabled.

3. Content Security Policy: This header helps prevent XSS, clickjacking, and code injection attacks by specifying which sources are allowed to execute scripts on a website. All Hosts are vulnerable to these attacks as they do not have this header enabled.

4. Referrer Policy: This header controls how much information is included in the HTTP Referrers header, which can leak sensitive information to third-party sites. All Hosts are not vulnerable to this type of attack as this header is enabled by default in modern browsers.

5. XSS Protection: This header enables the built-in cross-site scripting (XSS) filter in the user's browser to help prevent XSS attacks. Host 1, Host 2, and Host 3 are vulnerable to XSS attacks as they do not have this header enabled.

III.CONLUSION & RECOMMENDATIONS

In conclusion, all five hosts in the study were found to have vulnerabilities that could potentially be exploited by attackers. Missing HTTP cookie flags, click jacking, and mail server misconfiguration were among the vulnerabilities discovered. However, Captcha and robots.txt were not found to be vulnerable in any of the hosts. To prevent such vulnerabilities, implementing HTTP security headers such as X-Frame-Options, Strict-Transport-Security, Content Security Policy, Referrer Policy, and XSS Protection can be effective. Host 1, Host 2, and Host 3 were found to be vulnerable to XSS attacks due to the absence of the XSS Protection header, while Host 1 and Host 4 were vulnerable to man-in-the-middle attacks due to the lack of Strict-Transport-Security header. Therefore, it is crucial to ensure that all websites have the necessary security headers enabled to protect against potential attacks.

IV.FUTURE WORK

After conducting a light vulnerability scan, website fingerprinting, version-based vulnerabilities, and common configuration-based issues were identified. In the future, it is recommended to test for additional vulnerabilities based on OWASP security risks, such as SQL Injection, Cross-Site Scripting, and Remote File Inclusion, on a larger sample size.

B. References

1. Sandeep Kumar, Renuka Mahajan, Naresh Kumar, Sunil Kumar Khatri" A study on web application security and detecting security vulnerabilities" IEEE Xplore: https://ieeexplore.ieee.org/document/8342469 ISBN: 978-1-5090-3012-5
2. R. Hunt PKI and digital certification infrastructure ieee ISBN: 0-7695-1187-4 ISSN: 1531-2216
3. 1Vincent Appiah, 2Michael Asante, 3Isaac Kofi Nti and 4Owusu Nyarko-Boateng "Survey of Websites and Web Application Security Threats Using Vulnerability Assessment " Journal of Computer Science Vincent Appiah et al. / Journal of Computer

Science 2019, 15 (10): 1341.1354 DOI: 10.3844/jcssp.2019.1341.1354
4. Fatemeh Talebzadeh Pirvadlu, Dr.Ghodrat Sepidnam " Assessments Sqli and Xss vulnerability in Several Organizational Websites of North khorasan in Iran and Offer Solutions to Fix these Vulnerabilities " ieee 2017 3th International Conference on Web Research (ICWR) doi:10.1109/icwr.2017.7959303
5. Abdullah Ahmed Ali, Mohd Zamri Murah" Security Assessment of Libyan Government Websites" IEEE PROCEDINGS IEEE Xplore: 28 January 2019
6. K.Bala Chowdappa , S.Subba Lakshmi , P.N.V.S.Pavan Kumar " Ethical Hacking Techniques with Penetration Testing " (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
7. Mr. Vibhurushi Chotaliya, Miss Fiyona Mistr," New Era of Web Security by Implementing of Penetration Testing" International Journal of trend in Scientific Research and Development (IJTSRD 2456-6470 confrence issue 2018
8. Prajnesh Kundar1 Ajinkya Karode2 Rahul Jangida3 Prof. Shweta Sharma4 "Website Vulnerability Scanner "IJSRD - International Journal for Scientific Research & Development Vol. 4, Issue 02, 2016 | ISSN (online): 2321-0613
9. Sadaf Hina & P. Dhanapal Durai Dominic" Information security policies' compliance: a perspective for higher education institutions" Journal of Computer Information Systems ISSN: 0887-4417
10. Positive technologies," Most common OWASP Top 10 vulnerabilities (percentage of web applications" Published on February 13, 2020 https://www.ptsecurity.com/ww- en/analytics/web-vulnerabilities-2020/