Security Assessment Tool

Riza Gujarati[1], Dr. Ravi Sheth[2]
[1.] *Student at M.Tech., School of Information Technology & Cyber Security, Raksha Shakti University, Lavad, Dahegam, Gandhinagar, Gujarat, India.*
[2.] *Asst. Prof, School of Information Technology & Cyber Security, Raksha Shakti University, Lavad, Dahegam, Gandhinagar, Gujarat, India*

***Abstract*- This paper describes the in-depth technical approach. This paper describes the in-depth technical approach to perform manual test in web applications for testing the integrity and security of the application and also serves as a guide to test top 10 security vulnerabilities. The main objective is to find out the effectiveness in detecting the vulnerability in web application. The main motive of the scanner is to identify the vulnerability and produce a better result/report of each web application in effective manner. This tool is an Open Vulnerability scanner, it scans for Specific Vulnerabilities which can be easily identified by the Hacker and can be exploited, and Security Team can use this Tool in order to scan the Results.**

***Index terms*- Web application, Web security scanners, Web security vulnerability, Security tool**

I.INTRODUCTION

Web application is the most important, kinds of communication channels service providers and clients. On the internet vulnerability may compromise all the sensitive information and give report continuously which results in damage of cost. Web page contain HTML, images, script code and become more user friendly but it also exploits security vulnerability. Web application mechanisms include a web browser that may interacts with one or more number of web servers via a series of HTTP requests and HTTP responses. The main reason behind this is developers having limited programming skills and lack of security awareness. In this paper it is mainly explained about Security headers -CSP Header checker, Open port Scanner, SPF and DMARC records check, subdomains finding, TLS/SSL ciphers & protocols, Web Application Firewall, technologies Detections. All these tools are already available and all are open source and build in python language. Here I have just combined them in a single tool for ease of user. This tool allows a user to find top 10 vulnerability in the website.

- SSI Endpoint Vulnerability
  - Heart bleed Attack
  - BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)
  - POODLE(Padding Oracle On Downgraded Legacy Encryption)
  - Sweet32 or Birthday attack
  - FREAK (Factoring Attack on RSA-EXPORT Keys)

- Content Security Policies
  - Mitigating cross site scripting
  - Mitigating packet sniffing attacks
- HSTS Header
- WAF- Detection
- Outdated content in websites.
- Scanning Open Currently Open Port
- X-Content-Type-Options
- X-XSS-Protection
- Technology Lookup
- Subdomain Checker

II. TOOL INFORMATION

1. Security Header Checker

Applications can set secure HTTP response headers as an additional layer of defense that prevents browsers from running into easy preventable vulnerabilities. The script in this repository validates whether the headers pertaining to security are present and if present, whether they have been configured securely.

2. Spoof Check

A program that checks if a domain can be spoofed from. The program checks SPF and DMARC records for weak configurations that allow spoofing. Additionally it will alert if the domain has DMARC configuration that sends mail or HTTP requests on failed SPF/DKIM emails.

www.cyberoctet.com has no SPF record!
Sender Policy Framework (SPF) is a method of fighting spam

No DMARC record found. Looking for organizational record
No DMARC Record found, this means that your domain does not have a published DMARC record. DMARC Records are published via DNS as a text (TXT) record. They will let receiving servers know what they should do with non-aligned email received from your domain.

Organizational subdomain policy set to none
Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

3. TestSSI.sh

Tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as some cryptographic flaws.

Header	FType	Severity	Directive	Value	Description
expect-ct	not_ enforced	LOW	enforce		

The Expect-CT header lets sites opt in to reporting and/or enforcement of Certificate Transparency requirements, to prevent the use of misused certificates for that site from going unnoticed.

feature-policy missing_header INFO

The HTTP Feature-Policy header provides a mechanism to allow and deny the use of browser features in its own frame, and in content within any <iframe> elements in the document.

referrer-policy missing_header INFO

The Referrer-Policy HTTPheader controls how much referrer information (sent via the Referer header) should be included with requests.

content-security-policy missing_header INFO

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

strict-transport-security no_subdomains LOW

The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP

4. Web application/ Technology Detection

WAD lets you analyze given URL(s) and detect technologies used by web application behind that URL, from the OS and web server level, to the programming platform and frameworks, as well as server- and client-side applications, tools and libraries.
For example, results of scan of server might include:

- OS: Windows, Linux...
- Web server: Apache, Nginx, IIS...
- Programming platform: PHP, Python, Ruby, Java...
- Content management systems: Drupal, WordPress...
- Frameworks: AngularJS, Ruby on Rails, Django...
- Various databases, analytics tools, JavaScript libraries, CDNs, comment systems, search engines and many others.

5. Open Port Checker (nmap)

Finds open ports on the website.

6. Web Application Firewall (WAF)

Sends a normal HTTP request and analyses the response; this identifies a number of WAF solutions. If that is not successful, it sends a number of (potentially malicious) HTTP requests and uses

simple logic to deduce which WAF. If that is also not successful, it analyses the responses previously returned and uses another simple algorithm to guess if a WAF or security solution is actively responding to our attacks.

7. Subdomains Checker

It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

III. WORKING

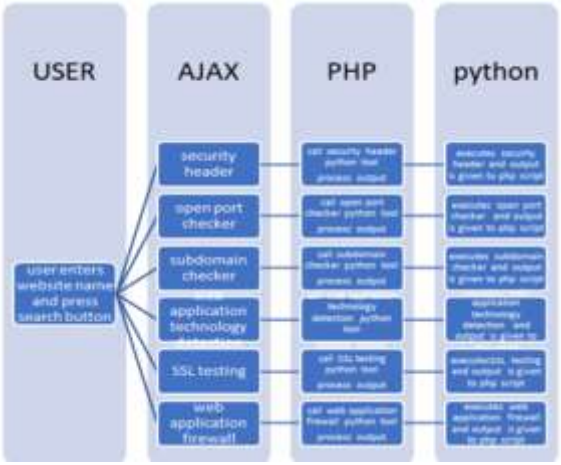
User enters website name and then press search button, function is called which is developed in JavaScript and that JavaScript function calls AJAX. There are six AJAX for each request i.e., Security header, subdomain checker, Web application technology detection, Secure socket layer (SSL) testing, web application firewall.

This ajax request send to server where for every ajax is handled separately by PHP technology script for all this ajax Security header, subdomain checker, Web application technology detection, Secure socket layer (SSL) testing, web application firewall.

AJAX call have the website name pass to php script and stored in variable and then php script have the command to call python function for Security header, subdomain checker, Web application technology detection, Secure socket layer (SSL) testing, web application firewall than python script is executed by using shell_exec() in php where it executes python script after than result is stored in json format which is then processed in php script.

This json data is decoded and checked for error of website after than if the website have high risk of vulnerability than it is processed accordingly by showing red color , orange, yellow, green as in sequence of high, medium, low, not vulnerable risk.

And this output after processing stored in table form for to display at user side in html format and given response to ajax function and that displays to the user to screen.



IV. REPORT DETAIL

The report generated is on the basics of the scan and give the user detail about the vulnerability present on the website and also on the server. It also give user an idea which vulnerability is crucial and which is not on the basic risk scan low, medium, high. Tables given below will be generated after the scan of the web application is completed. User can download the report after the scan. The report will give user the idea about how vulnerable the website is.

1. Summary of Findings:

Severity	Vulnerabilities	Affected Items	Mitigation
High	Name of Vulnerability	Module	It is recommended to update the software to its latest version.
Medium	Name of Vulnerability		
Low	Name of Vulnerability		

Based on severity whether it is high, low or medium, what items are affected and what steps should be taken to remove risk will be given on report. Also the what type of vulnerability found will also be shown in the report.

2. Vulnerabilities Identified:

URL/Hosts	Severity		
	High	Medium	Low
198.168.x.x	3	3	3
demo.com	1	2	4

The generated report also shows what is the host or url and its risk based on scan whether it is very risky or there is a low risk.

3. Severity Classification:

Impact	Definition
Low	Minimal impact on the business if exploited. Information disclosed is of no significant detrimental value, no repudiation or legal consequence, minimal to no impact.
Medium	Moderate financial impact, possible legal consequence and reputational ramifications.
High	Significant financial loss, damage to brand and bussiness identity through potential media involvement, exposure and compromise of data.

Severity classification is based on low, medium and high. Depending on what kind of impact is there, report will show what level of damages could be done on the web application.

4. Open Port Scanner:

Port	Service	Version
21	FTP	FileZilla 1.2
22	SSH	OpenSSH 2.2
23	Telnet	

This tool finds open ports on the website and scanning shows what is the port and what the port service is and what version the web is using.

5. Detected Technologies:

Technology	Version
PHP	5.4.3
Apache	2.4.4
AngularJS	1.2.1

The report shows the example of technologies that are used in web application and thus those technologies with their version will be detected.

V. CONCLUSION

Security Assessment Tool is an online website assessment tool that allow full scan of a website and provide us all the detail about the top 10 vulnerability. And also rate the website on the basics of risk low, medium, high. After a deep scan a detail report is generated for the user in pdf format. All processing of the website is done on the server side. This tool scans for Specific Vulnerabilities which can be easily identified by the Hacker and can be exploited, Security Team can use this Tool in order to scan the Results

VI. ACKNOWLEDGMENT

My topic has been possible with the help of my guide Dr. Ravi Sheth and other various people at Raksha Shakti University. I am grateful to Dr. Ravi Sheth for giving me all the possible support for my Mtech research paper. Thank you for all the advice, ideas, moral support, and patience in guiding me through this topic. Thank you for the golden opportunity to do this topic which helped me came to know about lots of new things. I am grateful for the consthant support and help. I am also very thankful to all the faculty at Raksha Shakti University who have always been helping me and encouring me throughout the final year of my Mtech.

REFERENCES

[1] https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/
[2] https://hackr.io/blog/top-10-open-source-security-testing-tools-for-web-applications
[3] https://www.softwaretestinghelp.com/penetration-testing-tools/
[4] Metasploit, Available at http://www.metasploit.com.
[5] CERT liveview available at: http://liveview.sourceforge.net/.
[6] GNU netcat. Available at http://netcat.sourceforge.net.
[7] Microsoft Baseline Security Analyzer (MBSA). Available at: http://www.technet.microsoft.com/enus/security/cc184924.aspx.
[8] Nmap. Available at http://nmap.org/.
[9] Ounce, http://www.ouncelabs.com/
[10] Nikto. Web Server Scanner. http://www.cirt.net/code/nikto.shtml.
[11] Z. Su and G. Wassermann. The Essence of Command Injection Attacks in Web Applications. In The 33rd Annual Symposium on Principles of Programming Languages (POPL 2006), Jan. 2006.
[12] PortSwigger. Burp Scanner. Available at: http://portswigger.net/.

[13] G. F. Lyon. NMAP.ORG. Available at: http://nmap.org/.
[14] N-Stalker. N-Stalker The Web Security Specialists. Available at: http://nstalker.com, 2010