Web Application Penetration Automation Testing Tool - WAPATT

Nitesh Kumar Singh[1], Prajwal Bajpai[2], Dr. Raju Ranjan[3]
[1,2,3] *School of Computer Science & Engineering, Galgotias University, Grater Noida, India*

***Abstract*— We are making a automation Tool for Finding a bugs in website or web application. There are many tools available on OPEN SOURCE Platforms (github, gitlab.) in this project tools are used perform specific working. To find bugs like XSS, SQL Injection, OPEN REDIRECTION, and also find CVE (Common Vulnerabilities & Exposures) based Vulnerabilities.**

Project Hunt Bull is a collection of OPEN SOURCE tools, this project helps to find larger amount of subdomains, filter out the live or dead host and save in list and increase the chances of vulnerability exists in websites.

The tool first of all enumerate all subdomains of the provided target domain using AMASS, SUBLISTER, SUBFINDER, and ASSETFINDER, then filters all valid domains from the entire subdomain list, then uses httpx to extract subdomain titles, and finally uses nuclei-tool to scan for CVE based vulnerability. Then it uses way back url tool to extract url parameters, then run gf-patterns tool to filter the xss, ssti, ssrf, and sqli parameters from those subdomains, and last it checks The output will be stored as target xss.txt in a text file, then manual testing of this parameter and increase the chances of vulnerability exists in websites, then send notifications on discord, telegram using the notify-tool.

Index Terms: **Automation, Tool, Scan, XSS, Open Redirect, internet (key words), CVE, SQL.**

I.INTRODUCTION

Meaning of Automated Penetration Testing? first we should momentarily explain penetration testing. It is the process where a gifted security analyzer attempts to find weaknesses, & breach the security of your frameworks. An automated penetration test is simply an automated rendition of this, correct?

In reality penetration tests include a range of activities, some of which are manual & some of which can & ought to be automated. For example, when speculating passwords, a human analyzer may look at the individuals in a company, & tailor a portion of their estimates based on birthdays or pets' names viewed as on the web; they may even manipulate the company name or office address in the hope it may yield something fascinating. Be that as it may, with regards to distinguishing known software flaws – like a server that's missing security patches, normal passwords, or accidental exposure to the web – this can & ought to be automated. The instruments that find these flaws are actually utilized by penetration analyzers, & so are once in a while called automated pen-testing apparatuses, are most generally known as vulnerability scanners. [1]

Historically, penetration tests were usually carried out a few times per year. In any case, as the prevalence of automated attacks increases, organizations can no longer afford to depend on a couple of check-ups per year. As a result, they are searching for more automated penetration testing devices (which we currently know are also called vulnerability scanners).

II.PENETRATION TESTING

For many years, penetration testing has been a popular method of assessing network security. Black box testing or ethical hacking are other terms for it. Penetration testing is the "skill" of remotely evaluating a functioning application for security flaws without knowing the application's internal workings. Typically, the penetration testing team would have user-level access to an application. The tester takes on role of an attacker, looking for and exploiting flaws. A genuine account on system will be offered to the tester in many circumstances. [2]

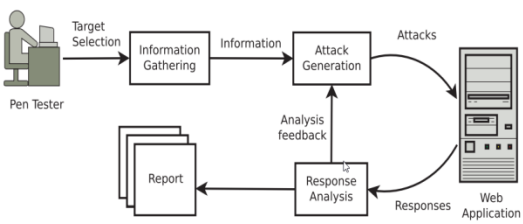

Figure 1. The penetration testing process. [3]

III.TOOL DESCRIPTION

1. Subfinder : It is a subdomain discovery tool that uses passive online sources to find acceptable subdomains for websites. It has a straightforward modular design that is intended for speed. Subfinder was designed to accomplish one thing and one thing well: passive subdomain enumeration. Subfinder has been developed to conform with all passive source licences and usage restrictions, as well as to maintain an uniform passive model that will be valuable to both penetration testers and bug bounty hunters. [4]

2. Sublist3r: It is a python tool that enumerates website subdomains using OSINT. It helps the collect subdomains for the website they're looking at. Sublister searches for subdomains using a number of search engines, including Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also searches for subdomains using Netcraft, Virustotal, etc. [5]

3. Subbrute : It's a community-driven effort with the goal of creating the fastest and most accurate subdomain enumeration tool available. It works in part because open resolvers are used as a proxy to bypass DNS rate limitations. It doesn't send traffic to the target's name servers directly, which adds an extra layer of anonymity. [6]

4. httpx: It's a multi-purpose HTTP toolkit that lets you run many probers using the retryable http library, and it's meant to keep the results consistent as the number of threads increases. [4]

5. Waybackurls: Accept line-delimited domins on stdin, fetch known URLs for *.domin from the Wayback Machine, and output them to stdout. [7]

6. Nuclei: Nuclei is used to send requests to several targets based on a template, resulting in zero false positives and quick scanning of a large number of hosts. TCP, DNS, HTTP, File, and other protocols are among those scanned by Nuclei. Nuclei can model many types of security checks thanks to its powerful and flexible templating. We have a dedicated repository with over 200 security researchers and engineers contributing various types of vulnerability templates. . [8]

7. DalFox: It is a robust open source cross site scripting scanning tool, parameter finder , and utility that makes finding and verifying XSS problems much faster. It includes a robust testing engine as well as other niche features for cool hackers. I discuss the topic of naming. Moon is pronounced Dal() in Korean, while Fox is translated as "Finder Of XSS" or "Finder Of XSS.". [9]

8. Naabu: Naabu is a Go-based port scanning tool that allows you to fast and reliably enumerate valid ports for hosts. It's a very basic programme that performs quick SYN/CONNECT scans on a host/list of hosts and displays all ports that respond. [10]

9. Notify: Notify is a Go-based assistance package that enables you to stream the output of several apparatuses (or read from a document) & publish it to a variety of supported platforms. [10]

10. Httprobe: httprobe which is a apparatus for rapidly probing for active http & https servers. If you have a list with subdomains you can quickly check which are active by using this tool.[7]

IV. TYPES OF VULNERABILITY IN WEB APPLICATION

1.Cross site Scripting: It is one of the most famous and widely used vulnerabilities, and it has been on the OWASP top 10 list for quite some time. XSS gives attackers the ability to run javascript code in the target browser. Tokens, sessions, cookies, and much more can all be stolen using this method. Reflected, stored, and DOM based XSS are the three forms of XSS.

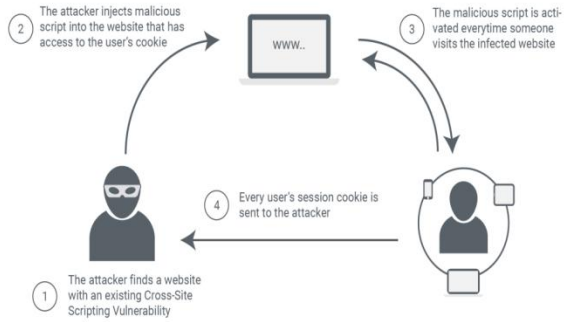

Figure 2. Cross Site Scripting. [11]

2.SQL Injection : SQL Injection (SQL) is a well known flaw that doesn't seem to be going away anytime soon. This flaw can be used to dump the contents of a database in an application. Because databases usually store sensitive information like usernames and passwords, obtaining access to them is effectively game over. MySQL is the most prevalent database, although you'll also come across MSSQL, PostgreSQL, Oracle, and others. [12]

3.Open Redirect: Basically we force the application to redirect to an attacker controlled site. This is typically considered a low impact vulnerability. However, this vulnerability can be chained with other bugs giving you greater impact. As mentioned earlier our goal is to make the application redirect to our site. Looking at the code below we can clearly see user supplied input is being passed to a redirect function. [13]
https://example.com/redirect.php?redirecturl=http://attacker.com/test

4.Insecure Direct Object Reference(IDOR): IDOR is one of my favorite vulnerabilities to search for as it is easy to find & can have a high impact depending on the context. The vast majority of the time you can spot this vulnerability by looking for a request which contains your user id, username, email, or some other id tied to your user. Some applications will use this id to serve you content based on the id supplied. Under normal circumstances you would only supply your users id so developers might forget to include authentication checks when retrieving this data. If that's the case attackers can supply other users id to retrieve data belonging to them. This could be anything such as a user's shipping address, credit card number, email, or anything. Not only can you retrieve information but sometimes you can exploit IDOR to send commands to the application such as adding an admin account, changing a user's email, or removing a set of permissions. As you can see above there are two requests. One will set a users email & the other will get a users email. The backend application uses the “userId” value supplied by the user when performing these actions without any other verification. So as an attacker we could easily modify & retrieve any user's email on the application.
As you can see above there are two requests. One will set a users email & the other will get a users email. The backend application uses the “userId” value supplied by the user when performing these actions without any other verification. So as an attacker we could easily modify & retrieve any user's email on the application. [14]

5.Directory Traversal: Directory traversal is a vulnerability that occurs when developers improperly use user supplied input to fetch files from the operating system. As you may know the “../” characters will traverse back one directory so if this string is used to retrieve files you can retrieve sensitive files by traversing up or down the file structure. If you see an application utilizing user supplied input to fetch files you should immediately test to see if its vulnerable to directory traversal. This can be fairly easy to spot as shown below:
https://example.com/?page=index.html
As you can see there is a GET parameter called page which is used to load the contents of “index.html”. If improperly implemented attackers leverage the “../” technique to load any file they want. [15]

6.Server-Side Template Injection (SSTI) : When user-controlled input is inserted into a server-side template, allowing users to inject template directives, this is known as server-side template injection. This allows an attacker perform to inject malicious template directives into the server and potentially execute arbitrary code.

7.Cross-Site Request Forgery (CSRF): It is an exploit that causes a logged-on victim's browser to make a bogus HTTP request to a vulnerable web application, which includes the victim's session cookie and any other automatically included authentication credentials. This allows the attacker to manipulate the victim's browser to send requests to the vulnerable application that it misinterprets as legitimate victim requests. [16]

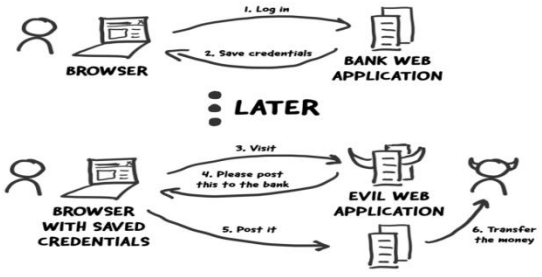

Figure 3. Cross -Site Request Forgery (CSRF)[3]

8.HTML Injection: Injecting HTML code through weak parameter of the website is the essence of this sort of injection attack. The malicious user injects HTML code into any vulnerable field with the intent of altering the website's appearance or any information presented to the user.

As a result, the user may be able to see the data that the unauthorized user transmitted. As a result, HTML Injection is just the injection of markup language code into the page's document.

The data that is delivered during an injection attack might be completely different. It might be a few HTML elements that just display the data supplied. It might also be the entire fake form or page. When this happens, the browser normally perceives malicious user data as legitimate and shows it to the user.

This form of assault poses more than just a threat to the aesthetic of a website. It's analogous to an XSS attack, in which a rogue user takes the identities of others. As a result, identity theft might occur as a result of this injection attack.[17]

9.Broken Authentication: some applications are frequently implemented incorrectly. When authentication and session management procedures are done poorly, attackers can get access to passwords, keywords, and sessions. This can result in the theft of a user's identity, among other things.[17]

10.Server-Side Request Forgery: Server-side request forgery (also known as SSRF) is a web security flaw that allows an attacker to force a server-side application to send HTTP requests to any domain the attacker chooses.

The attacker may force the server to connect to internal-only services within the organization's architecture in a conventional SSRF attack. They may also be able to compel the server to connect to arbitrary external systems, exposing sensitive data such as authorisation credentials.[17]

V.WORKING OF TOOL

We can make a simple automation penetration testing tool using the bash programming language, this tool finding the bugs in the website. It is also find CVE based vulnerability find by using nuclei tool.[18]

First of all run the subdomain finder tools are Sublister, findomain, amass, asset finder, subfinder,[4][5][6] after completing the subdomain enumeration all subdomain save in sub_domain.txt this subdomain are without http or https . so next step is automate the add the http/https with help of HTTPX tool or HTTPROBE tool then save in http_domain.txt, now filter out the live or dead host from the http_domain.txt using the help of HTTPX[4] tool its show with status code in output. then crawl the all domain using the waybackurl and save it new file crawl_domain.txt, then find filter out the vulnerable parameter using GF tool its help the find parameter in the website like XSS parameters, SSRF[17] parameters, OPEN REDIRECT[13] parameters, SQL injection parameters many more. After all vulnerable parameter urls save in txt file, its increase the chances of vulnerability exists in websites. And complete all the process then nuclei tool run with subdomain list its find the CVE based vulnerability, after complete the all scanning notification send on my discord slack, using the help of notify tool, its save my reconnaissance process and easily find the bugs on website.

VI.CONCLUSION

Successful tool automation requires not just the correct tools, but also a consistent testing procedure and the right roles, responsibilities, and abilities from the test team. Therefore, the automated test team must possess a mix of testing, development, and tool expertise. If a company wishes to reap the benefits of automation offered by tool suppliers, it must utilise the tool in conjunction with manual testing. It also includes using a solid testing approach.

REFERENCES

[1] S. M. a. S. Pourdavar, "Penetration test: A case study on remote command execution security hole," in Fifth International Conference on Digital Information Management (ICDIM), July 2010.

[2] S. N. a. S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in International Conference on Computing, Communication, Control and Automation, ICCUBEA, 2017, 2018..

[3] S. R. C. a. A. O. William G. J. Halfond, "Improving penetration testing through static and dynamic analysis," Published online in Wiley Online Library, 2010.
[4] Project discovery, "Subfinder is a subdomain discovery tool that discovers valid subdomains forwebsites".https://github.com/projectdiscovery/subfinder.
[5] I. M. Ahmed Aboul-Ela, "Sublist3r - Fast subdomains enumeration tool for penetration testers," https://github.com/aboul3la/Sublist3r, 2016.
[6] TheRook, "SubBrute - A DNS meta-query spider that enumerates DNS records, and subdomains.".https://github.com/TheRook/subbrute.
[7] T. Hudson, "waybackurls tool - ".https://github.com/tomnomnom/waybackurls.
[8] projectdiscovery, "Nuclei Tool- Fast and customizable vulnerability scanner based on simple YAML based DSL.".https://github.com/projectdiscovery/nucle
[9] hahwul, "DalFox Tool - Xss parameter finder".https://github.com/hahwul/dalfox.
[10] projectdiscovery, "Naabu - Fast Port scanning tool".https://github.com/projectdiscovery/naabu.
[11] F. 2., "Cross Site Scripting".https://crashtest-security.com/cross-site-scripting-xss/.
[12] OWASP, "OWASP TOP 10 - SQL Injection [ONLINE]".https://owasp.org/www-community/attacks/SQL_Injection.
[13] Acunetix, "Open Redirection". https://www.acunetix.com/blog/web-security-zone/what-are-open-redirects/.
[14] Owasp Top 10, "Owasp.org, 'Top 10 2017-Insecure Direct Object [online]".https://owasp.org/www-project-web-security-testing-guide/latest /4-Web_Application_Security_ Testing/05-Authorization_Testing/04-Testing_for_Insecure_ Direct_Object_References.
[15] Portswigger, "Directory traversal [online]". https://portswigger.net/web-security/file-path-traversal.
[16] R. K. Muhammad Zulkhairi Zakaria, "Risk Assessment of Web Application Penetration Testing on Cross-Site Request Forgery (CSRF) Attacks and Server-Side Includes (SSI) Injections," in International Conference on Data Science and Its Applications (ICoDSA), 2021.
[17] R. Ramgattie, "Cracking Java's RNG for CSRF [ONLINE]".https://blog.securityevaluators.com/cracking-javas-rng-for-csrf-ea9cacd231d2.
[18] S. K. Lala, A. Kumar and S. T., "Secure Web development using OWASP Guidelines," in 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021.
[19] NIST, "NATIONAL VULNERABILITY DATABASE [online]".https://nvd.nist.gov/vuln .