IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

WEB VULNERABILITY SCANNER (POC BOMBER)

B. Nishika Reddy, Akarsh Kumar Trivedi, Vijay Krishna,Venkat Kartik, Nava Kishore
Student/Scholar, Student/Scholar, Student/Scholar, Student/Scholar, Associate Professor
Computer Science and Engineering
(Cyber Security)

Hyderabad Institute of Technology and Management (HITAM), Gowdavelly(V), Medchal(M), Medchal-Malkajgiri Dist. 501401, Telangana, India

Abstract:

"POC Bomber" is a flexible vulnerability scanner and exploitation tool that is built for the quick detection of high-risk vulnerabilities for targeted servers. A huge number of Proof of Concepts and Exploits (POCs and EXPs) are used here for the purpose of detection of vulnerabilities e.g. Remote Code Execution (RCE), Arbitrary File Upload and many more. This tool performs complete fuzz testing on the single or more targets, thereby providing effective means of detecting exposed vulnerable devices and winning the target system permissions.

Attacking components supported by the hacker include WebLogic, Tomcat, Apache, JBoss, Nginx, Struts2, ThinkPHP, and the rest. The zero-day exploit may spot security weaknesses such as the flaw in the log4j2 library without the need for visible response from the target system. Thus, the attacker can execute their code on the target system without notice.

"POC Bomber" both has single-target detection mode and batch one. In addition, a high-concurrency thread pool is used in it for scanning quickly. Among its features are the ability to import POCs/EXPs and to generate detailed vulnerability reports. Among RedTeam innovations 3.0 stands out: faster scanning efficiency, bug fixes as well as colorized output, and support for specifying a POC directory, including POCs for vulnerabilities disclosed this year.

In the end, "POC Bomber" is a powerful tool that can be used for discovering vulnerabilities quickly, mapping vulnerability assets, and keeping vulnerability scanners updated, which makes it critical for cybersecurity specialists and researchers.

***Index Terms*:**

Cyber Threats,Security,Salable Design, URL Discovery, Reporting, Ethical Usage,Rigorous Testing, Proactive Security,Vulnerability detection, Exploitation tool, Proof of Concepts (POCs), Exploits (EXPs), Remote Code Execution (RCE), Arbitrary File Upload, Deserialization, Batch detection, Fuzz testing, High-concurrency thread pool, Custom POCs/EXPs import, vulnerability reports, Penetration testing.

1. INTRODUCTION:

Cybercrime is becoming more sophisticated and, in this environment, powerful techniques must be developed to help recognize and prevent weaknesses. "POC Bomber" is a complete tool developed to rapidly identify a vast number of vulnerabilities and facilitate an effective cybersecurity practice. Using its repository of Proof of Concepts (POCs) and Exploits (EXPs), it aims for and analyses urgent security problems such as Remote Code Execution (RCE), Arbitrary File Uploading, Deserialization, and SQL Querying.

With "POC Bomber" you can fix such zombie vulnerabilities that can affect system permissions more quickly than otherwise. Doing an extended fuzz testing of either single or multiple targets will not only help in the discovery of vulnerable areas and the allotment

of target server permissions but also save a lot of time that would have been spent in the process. This tool is a welcome convenience for information security professionals including penetration testers, vulnerability researchers, and exploit developers.

Besides the number of elements, the categories affected include WebLogic, Tomcat, Apache, JBoss, and others. Additionally, the thread pool model adopted by "POC Bomber" ensures speedy vulnerability scanning. It further offers convenient import of POCs/EXPs, helping cover the route in which the user needs most.

The current version, RedTeam 3.0-Red Team Special Edition comes with a scanner that increases efficiency, addresses the lag problem as well as introduces colorized output and progress display. It additionally has POCs for year 2022 vulnerabilities disclosure as well. This guarantees the users stay up to date with the emerging threats statistics.

To sum up, "POC Bomber" is a valuable utility for pinpointing both security loopholes and the associated exploitation, and it thus takes part in the implementation of cybersecurity standards.

2. LITERATURE SURVEY:

The cybersecurity terrain has emerged stronger, owing to many studies that have analyzed software vulnerability detection and exploitation. Researchers have examined wide ranging techniques and technologies to improve the security of organizations and people.

The research focuses on the use of 'Proof of Concepts' (POCs) and Exploits (EXPs) in order to identify and exploit the vulnerabilities. Research shows that POCs are the main crucial players who show the existence of weak points, and EXP's role in portraying the impact of those weaknesses on attackers is crucial. This groundwork is the starting point of tools like "POC Bomber" that with the help of a large database of POC/EXP use the most comprehensive approaches to the vulnerability assessment.

Researchers in the literature tried to raise the accessibility and precision of scanning in the process. Tools like "POC Bomber" have been developed which obtain their capability from advanced scanning techniques such as high-concurrency thread pools and customizable POC/EXP imports that can facilitate fast vulnerability detection.

In addition to that, the latest studies show that the designing of vulnerability detection systems must take into consideration evolving vulnerabilities. Features such as integrating DNSLog platform into "POC Bomber" show the designers' resolve to ensure that the tool is powerful to meet the evolving cybersecurity challenges.

In the last part we notice that literature successfully enlightens both detection and exploitation tools that are vital in securing cyberspace against cyber threats.

4.Purpose and Scope

The main objective of our "POC Bomber" vulnerability scanner is basically to empower cybersecurity staff and researchers with an incredible tool to play tricks on the servers which are at a high risk of being attacked. This tool will effectively combine POCs with EXPs to cut the search time, thereby making it very easy to detect vulnerabilities with the potential to override core network permissions.

The scope of the project includes the following key aspects:The scope of the project includes the following key aspects:

● **Vulnerability Detection:** "POC Bomber" detects web application security flaws across various components that have a high probability of being targeted by cybercriminals, such as WebLogic, Apache, Nginx, Jenkins, and various PHP language vulnerabilities like ThinkPHP, Tomcat, JBoss, Struts2, and Redis.

● **Exploitation:** The risk accolades of the equipment include processing weaknesses like Remote Code Execution (RCE), Deserialization, File upload, and SQL Injection. This gives the users a chance to look into the impact of these vulnerabilities and choose rightful retaliation measures instead.

● **Efficient Scanning:** "POC Bomber" is meant to aim at either single-target or batch detection with the help of a forked thread pool to increase the scanning speed. This allows security personnel to examine the multiple targets quickly, and play a role in identifying the vulnerable ones.

● **Customizability:** This makes it possible for users to import custom POCS/EXPs since this gives them the opportunity to choose which vulnerabilities they want to detect as per their needs and initiatives. The ability to be used for such a wide spectrum of

cybersecurity use cases with end users, including penetration testing, vulnerability research, and exploit development, enables its flexibility.

Ease of Use: Though "POC Bomber" has more sophisticated features, it is made simple by providing a command line user interface and elaborate manual to walk users through the steps of identifying vulnerabilities and actualizing them.

Finally, the "POC Bomber" project is highlighted to improve the security of cyberspace by means of a powerful and multipurpose tool to detect weaknesses and to exploit them, giving a possibility to a user to identify and counteract in an effective way possible vulnerabilities.

5. METHODOLOGY:

The POC Bomber "was developed with" a series of algorithms applied to reduce its attacks and to find vulnerabilities in exploitation. undefined

The methodology can be outlined as follows:

● **Research and Requirements Gathering:** The beginning phase started with carrying out in depth studies on various vulnerability detection tools and identifying common high risk vulnerabilities and their prototype POCs on Exploit. Requirement collection was done based on what is actually required, and being addressed, the cybersecurity problems.

● **Design and Architecture:** The design phase began with visualizing an architecture of POC Bomber that should be capable of handling a large quantity of POCs/EXPs and simultaneously tested for multiple targets. Like architecture, it was also built with ease-to-extend & modify in mind.

● **Implementation:** The execution phase incorporates coding the various components to "POC Bomber" which entails the core scanning section, POC/EXP repository, user interface and the reporting module. We used Python 3 for the framework due to its extensive library support and flexibility.

● **POC/EXP Integration:** High-explosives POC/EXPs were collected and were integrated into "POC Bomber" inventory. These POCs were chosen out of all existing ones based on their ability to demonstrate exploits such as RCE, Arbitrary File Upload, Deserialization, and SQL Injection.

● **Testing and Validation:** The product referred to as "POC Bomber" was subjected to an intense and comprehensive testing process in order to be sure that it was able to identify and utilize the possible vulnerabilities present. Media type validation encompassed unit testing, integration testing, and extensive testing on multiple target servers that was performed to verify the quality of this project.

● **Documentation and User Guide:** Detailed documentation and user manual, were prepared to help home users grasp fundamentals of "POC Bomber". This included installation, configuration, usage of the tool, description of various features and capabilities of the tool.

● **Release and Maintenance:** The last phase of my project delivery involved going live with "POC Bomber" and continuing to provide service and support as necessary. Updates and patches were done after releasing them on a regular basis to take up any software errors or vulnerabilities which were discovered thereafter.

6. Requirements and installation

a) Software Requirements

The following software components are required for the Web Vulnerability Scanner project:

● **Python 3.x:** Considering the core programming language that is going to be used for developing scanner software.

● **PyQt5:** Python bindings for the Qt application framework is an essential tool in building the graphical user interface (GUI) of the scanner.

● **Web Frameworks and Libraries:** Diverse Python web frameworks and libraries may be used for implementing web scanning functions, e.g., request of HTTP communication, BeautifulSoup for HTML parsing.

● **HTML:** The HTML code was used to generate the report on vulnerabilities detected.

b) Hardware Requirements

The following hardware components are required for the Web Vulnerability Scanner project:

● **Processor:** A multicore processor (e.g., Intel Core i5 or AMD Ryzen 5) with sufficient processing power to handle concurrent scanning tasks efficiently.

● **Memory (RAM):** At least 4 GB of RAM to ensure smooth operation and adequate memory allocation for scanning processes and data storage.

● **Storage:** Sufficient storage space for storing the scanner software, scan results, and any additional data or dependencies. SSD storage is recommended for improved performance.

● **Network Connectivity:** A stable internet connection is required for accessing web applications and conducting vulnerability scans. Higher bandwidth may be necessary for scanning large web applications or conducting multiple concurrent scans.

c) Operating System Requirements

The Web Vulnerability Scanner project is a platform-independent, implying it can be run in many different operating systems. The project requirements for operating system:

● **Windows:** The tool has been built using version 10 of Windows and later versions are supported for development as well as deployment.

● **Linux:** The most used Linux distributions like Ubuntu, CentOS, and Debian are given priority when developing and deploying systems, so that the intended purpose of these systems can be achieved.

● **macOS:** macOS 10.13 (High Sierra) or any subsequent version is what you must have for programming on the system and application deployment.

d) Installation

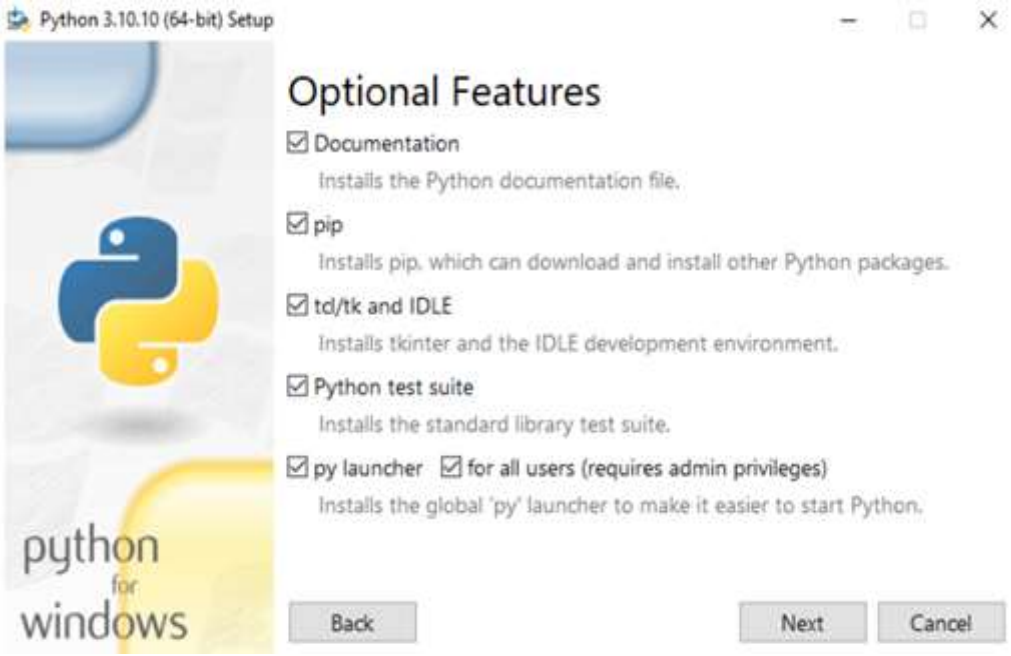
Install Python: Download and set up the latest version of Python 3.x from the official website of Python (https://www.python.org/).

Steps for python installation:

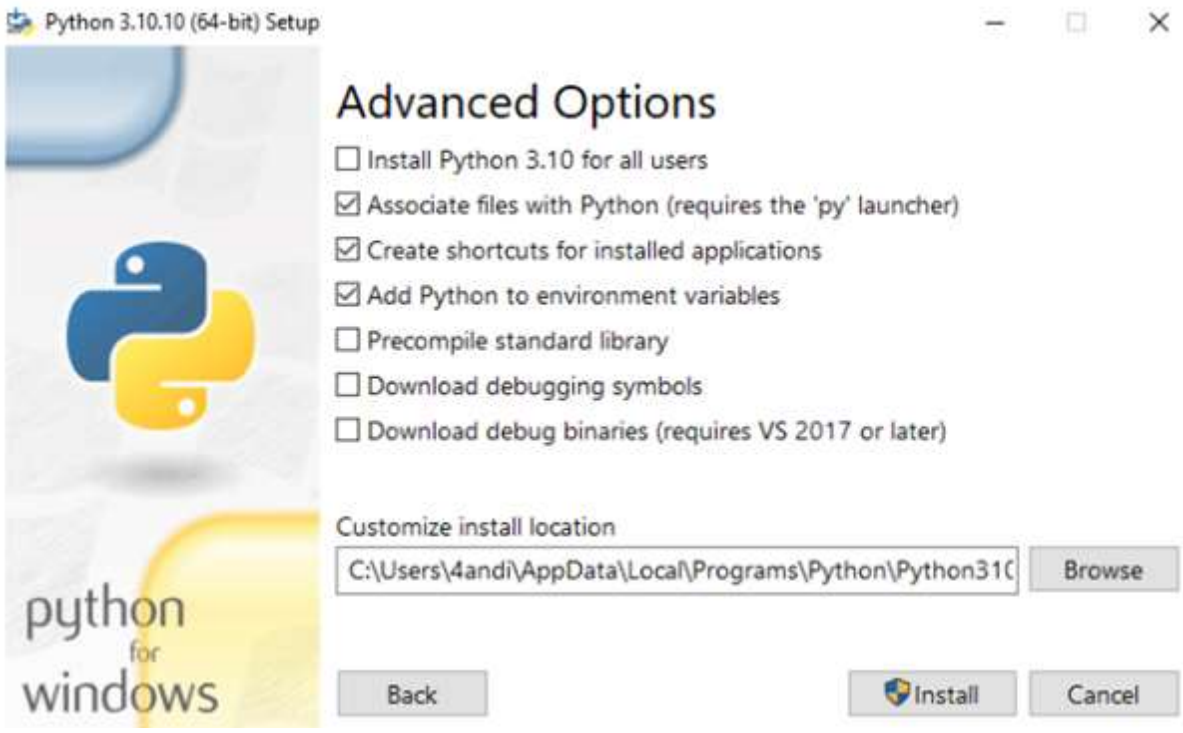
Step 1: Get the python installer from its official website

Step 2: Start the setup.exe. Check two boxes representing the use. Choose “Install now” tab.

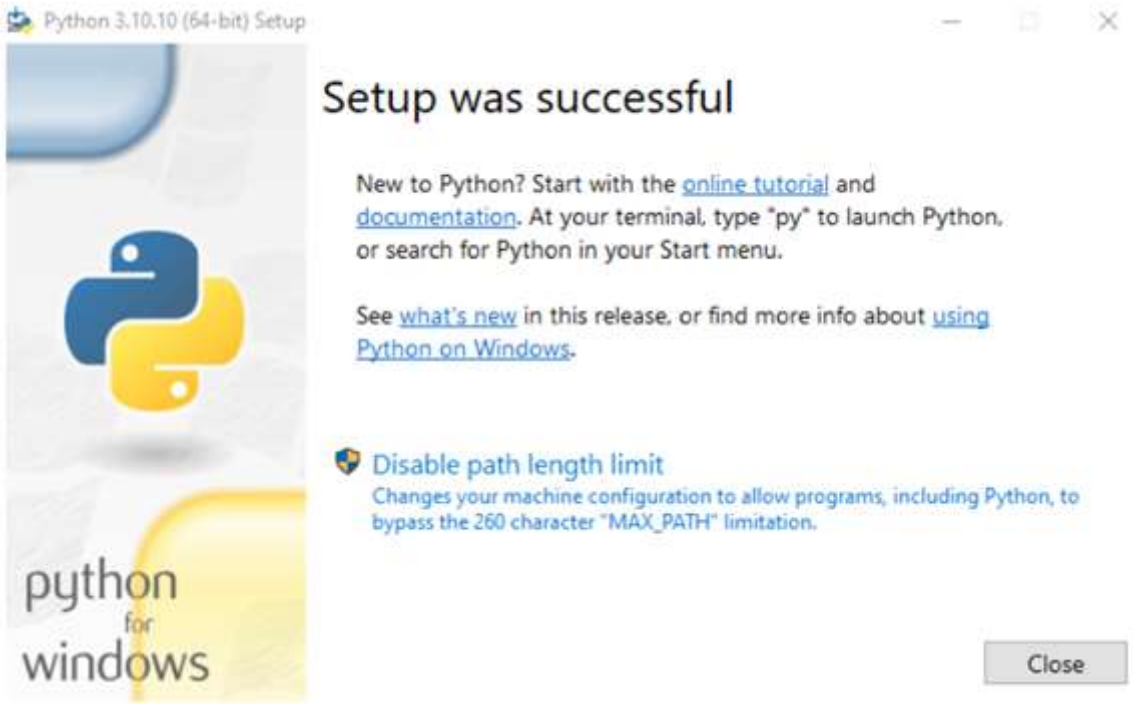
Step 3: Next, you encounter the section that outlines the options. There are only four boxes to check and they are a perfect fit for your needs. Click on “Next”.



Step 4: Then, you go to the advanced options page. One of the checkboxes which is seven in number and made to enable you choose your installation location. Once selected, Click on “Install”.



Step 5: Now, everything is set up and installing python is complete.



Install PyQt5: Install PyQt5 using pip -- a package installer for the Python language -- by executing the following command in the console: pip install PyQt5.

7. Model and Architecture

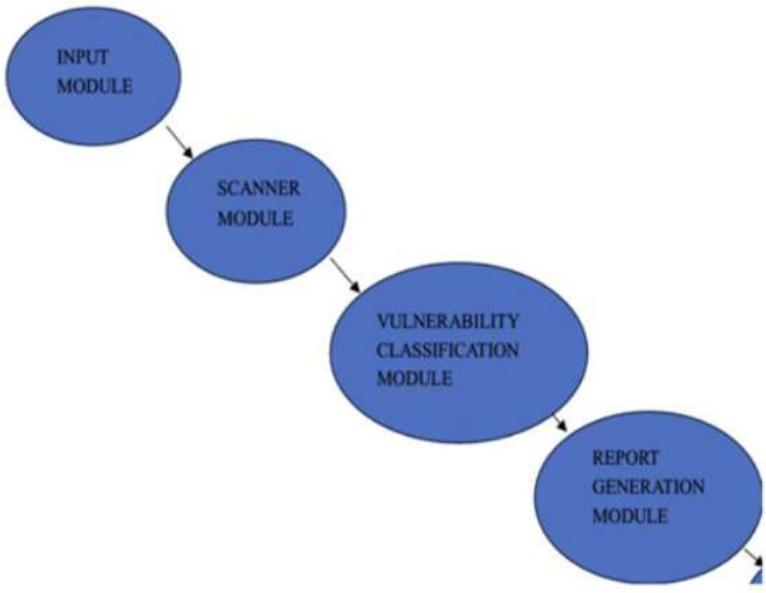


FIG: BLOCK DIAGRAM

● **Input Module :** This part of the tool acts like ears and listens from you—the user—at the same time it reads from a file that contains vulnerable web addresses (URLs). That is the URL you want, one or more, it will wake up to test them.

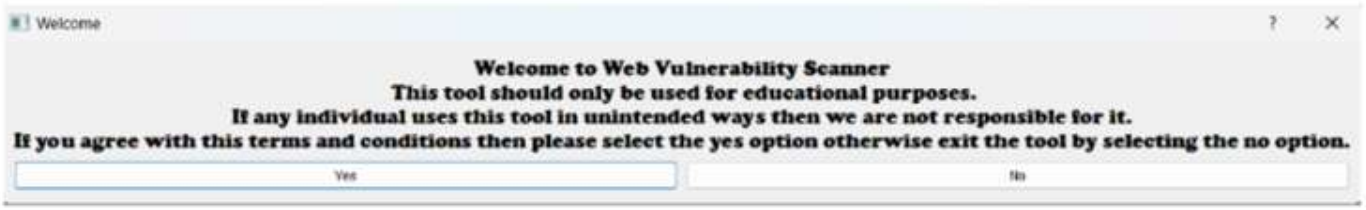
● **Scanner Module:** It is the main factor that makes the tool special. It is just like a squad of investigators looking through each URL for clues that can be vulnerable to any cyber-attacks. It's really speedy and can handle more websites at once.

● **Vulnerability Classification Module:** It operates just like a supercop among the other team members. It is aware of many exploitations that are susceptible to web servers and web applications in particular. It has the ability to spot out these loopholes in the URLs that you type in.

● **Report Generation Module:** After all the data has been collected, the module will combine all the information and will then create a report. It is a summary that identifies vulnerable URLs of your website and the type of assaults they might encounter.

8. Implementation

● Before running the main Python file, users are walked through the terms and conditions regarding the use of the tool on the landing page. Users are given two options: "Yes" or "No". Hitting "Yes" brings the program to execution, but selecting "No" ends the program.



● Once the "Yes" option is selected, the user will see the interface with the "Input dialog", "Scan" button, "Cancel" button and the progress bar. Additionally, there is a menu bar featuring two submenus: "Survey", "Session", and "Reports."

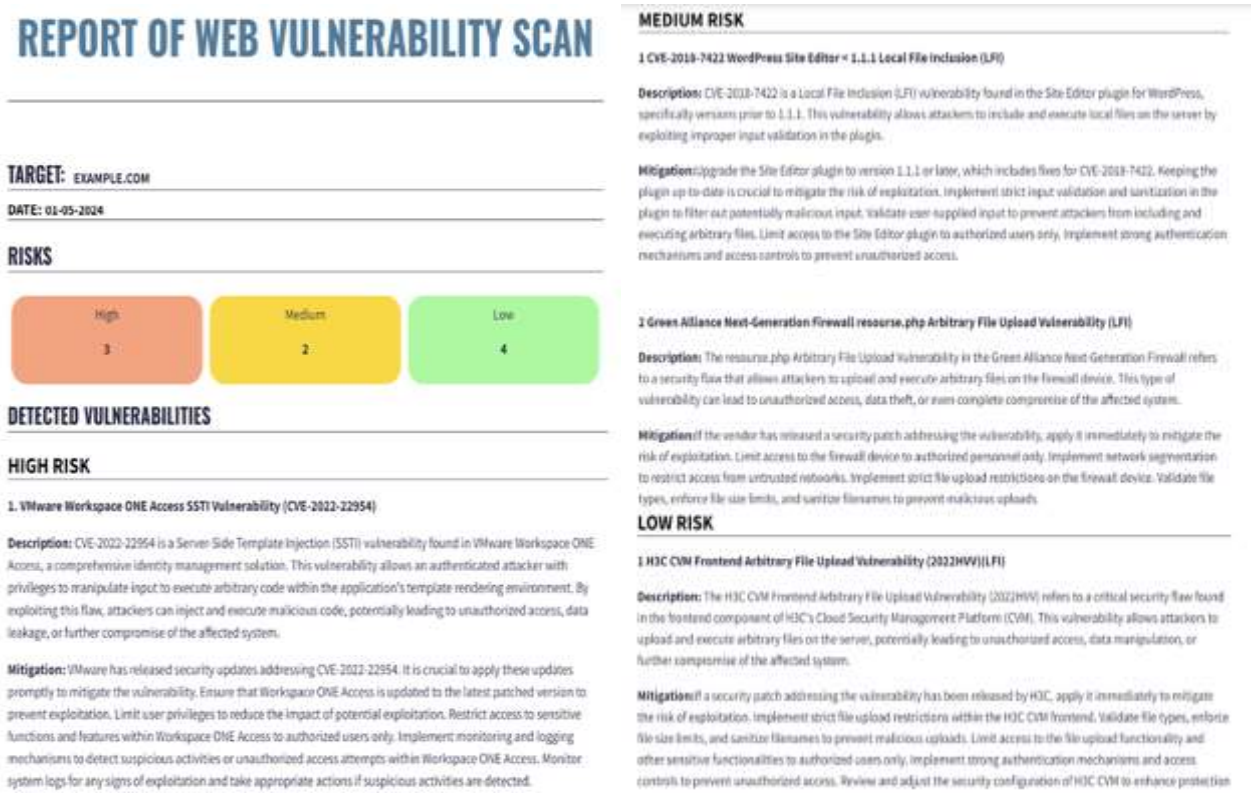
● To use the tool, users must type the URL of the website they want to test in the input dialog and push the "Scan" button. The progress bar provides a physical display of the progress of the scan.

● Upon ending the scan, users will see a report by selecting the "Report" menu and then the report file which is in HTML format.

● If you want to create a new session, you need to use "the Session" menu and choose "Reset," which starts all the session anew.

● If users want to end the session earlier which they find it as not they can click on the "Cancel" button present below the scan button.

● When the report file is clicked on it will be shown in the web browser and the information it contains would be the target URL and the date of scan and as well as the risk classifications (critical, moderate, and low) and the detected vulnerabilities.



REPORT OF WEB VULNERABILITY SCAN

TARGET: EXAMPLE.COM

DATE: 01-05-2024

RISKS

High	Medium	Low
3	2	4

DETECTED VULNERABILITIES

HIGH RISK

1. VMware Workspace ONE Access SSTI Vulnerability (CVE-2022-22954)

Description: CVE-2022-22954 is a Server Side Template Injection (SSTI) vulnerability found in VMware Workspace ONE Access, a comprehensive identity management solution. This vulnerability allows an authenticated attacker with privileges to manipulate input to execute arbitrary code within the application's template rendering environment. By exploiting this flaw, attackers can inject and execute malicious code, potentially leading to unauthorized access, data leakage, or further compromise of the affected system.

Mitigation: VMware has released security updates addressing CVE-2022-22954. It is crucial to apply these updates promptly to mitigate the vulnerability. Ensure that Workspace ONE Access is updated to the latest patched version to prevent exploitation. Limit user privileges to reduce the impact of potential exploitation. Restrict access to sensitive functions and features within Workspace ONE Access to authorized users only. Implement monitoring and logging mechanisms to detect suspicious activities or unauthorized access attempts within Workspace ONE Access. Monitor system logs for any signs of exploitation and take appropriate actions if suspicious activities are detected.

MEDIUM RISK

1 CVE-2018-7422 WordPress Site Editor < 1.1.1 Local File Inclusion (LFI)

Description: CVE-2018-7422 is a Local File Inclusion (LFI) vulnerability found in the Site Editor plugin for WordPress, specifically versions prior to 1.1.1. This vulnerability allows attackers to include and execute local files on the server by exploiting improper input validation in the plugin.

Mitigation: Upgrade the Site Editor plugin to version 1.1.1 or later, which includes fixes for CVE-2018-7422. Keeping the plugin up to date is crucial to mitigate the risk of exploitation. Implement strict input validation and sanitization in the plugin to filter out potentially malicious input. Validate user-supplied input to prevent attackers from including and executing arbitrary files. Limit access to the Site Editor plugin to authorized users only. Implement strong authentication mechanisms and access controls to prevent unauthorized access.

2 Green Alliance Next-Generation Firewall resourse.php Arbitrary File Upload Vulnerability (LFI)

Description: The resourse.php Arbitrary File Upload Vulnerability in the Green Alliance Next Generation Firewall refers to a security flaw that allows attackers to upload and execute arbitrary files on the firewall device. This type of vulnerability can lead to unauthorized access, data theft, or even complete compromise of the affected system.

Mitigation: If the vendor has released a security patch addressing the vulnerability, apply it immediately to mitigate the risk of exploitation. Limit access to the firewall device to authorized personnel only. Implement network segmentation to restrict access from untrusted networks. Implement strict file upload restrictions on the firewall device. Validate file types, enforce file size limits, and sanitize filenames to prevent malicious uploads.

LOW RISK

1 H3C CVM Frontend Arbitrary File Upload Vulnerability (2022HVV)(LFI)

Description: The H3C CVM Frontend Arbitrary File Upload Vulnerability (2022HVV) refers to a critical security flaw found in the frontend component of H3C's Cloud Security Management Platform (CVM). This vulnerability allows attackers to upload and execute arbitrary files on the server, potentially leading to unauthorized access, data manipulation, or further compromise of the affected system.

Mitigation: If a security patch addressing the vulnerability has been released by H3C, apply it immediately to mitigate the risk of exploitation. Implement strict file upload restrictions within the H3C CVM frontend. Validate file types, enforce file size limits, and sanitize filenames to prevent malicious uploads. Limit access to the file upload functionality and other sensitive functionalities to authorized users only. Implement strong authentication mechanisms and access controls to prevent unauthorized access. Review and adjust the security configuration of H3C CVM to enhance protection

CONCLUSION:

The final "POC Bomber" project has been set up to remedy the alarming conditions of incompetent and inefficient security vulnerability detection and exploitation in web servers. The ability of the tool to quickly scan for the critical vulnerabilities, for

instance, Remote Code Execution (RCE), Arbitrary File Upload and SQL injection provides the penetration testers and security professionals with this useful tool.

By way of the introduction of modules such as the input module, scanner module, web vulnerability scanner model, and report generation model, the “POC Bomber” tool delivers a comprehensive solution for scanning and exploiting vulnerabilities found in target or victim servers. Its powerful high-concurrency thread pool enables it to scan quickly and in-depth, while its capability to import POCs/EXPs makes the implementation adaptable and scalable.

The project's concentration on user-friendly operations and comprehensive reporting with the help of this tool helps users to easily understand the vulnerability and act further. The tool performs the job by evaluating the shell and allowing one to acquire a shell once the exploit is confirmed. As a result, the tool accelerates the exploitation process by enabling users to access target server permissions efficiently.

Ultimately, the "POC Bomber" project is a very impactful development in the area of vulnerability discovery and exploitation. Cyber-Attack simulation's innovative approach and robust functionality make it an appropriate tool for security professionals who are looking to enhance their penetration testing capacities with this technology.

ACKNOWLEDGMENT:

We Would like to thank our guide Nava Kishore sir for his valuable suggestions to improve the quality of the paper. We are also grateful to him for helping us review our performance regularly. We would also like to thank the Department of Computer Science Engineering (Cyber Security), HITAM, Hyderabad.

REFERENCES:

● Makino, Y. and Klyuev, V., 2015, September. Evaluation of web vulnerability scanners. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 399-402). IEEE.

●Mburano, B. and Si, W., 2018, December. Evaluation of web vulnerability scanners based on owasp benchmark. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE.

● Khalid, M.N., Rasheed, K. and Abid, M.M., 2020. Web vulnerability finder (WVF): automated black-box web vulnerability scanner. Int J Inf Technol Comput Sci, 12(4), pp.38-46.

● Sagar, D., Kukreja, S., Brahma, J., Tyagi, S. and Jain, P., 2018. Studying open source vulnerability scanners for vulnerabilities in web applications. IIOAB JOURNAL, 9(2), pp.43-49.

● Setiawan, E.B. and Setiyadi, A., 2018, August. Web vulnerability analysis and implementation. In IOP conference series: materials science and engineering (Vol. 407, No. 1, p. 012081). IOP Publishing.