Project Title:

Recon, Evasion And Vulnerability Exposure tool (REAVER)

Project by

Shaurya (12019002004001, Sec A, Roll 9)

Mentor:

Prof. Dr. Moutushi Singh

moutushi.singh@iemcal.com

ACKNOWLEDGEMENT

I wish to express my heartfelt gratitude to all the people who have played a crucial role in the development of this project, without their active cooperation the preparation of this project could not have been completed within the specified time limit. I am thankful to our respected Director Institute of Engineering & Management, Kolkata, Prof. Satyajit Chakrabarti , my department & all the respected faculties for motivating me to complete this project with complete focus and attention.

I am thankful to my project guide Prof. Dr. Moutushi Singh who supported & motivated me throughout this project with utmost cooperation and patience to learn new resources and improve the project efficiency.

ABSTRACT

The development of an open source reliable and fast reconnaissance and scanning tools have been a challenge for security researchers to find out the missing elements of information security in a web application. Recon, Evasion & Vulnerability Exposure Tool is a python & bash(subprocess) based tool with 14 unique reconnaissance, enumeration & scanning features to scan a web application for vulnerabilities & security misconfigurations. The tool is natively built in python and is currently operable for Ubuntu Distribution of Linux. The tool is able to scan ports , perform enumeration using various techniques, evade firewalls and find vulnerabilities. The tool is in development for 3 versions namely CLI, GUI(Application or software) and Web Application. Tool also integrates pre existing open source, standard tools like Nmap , Nikto & Nuclei.

Keywords: Vulnerability Scanner, Port Scanner, Enumeration, Reconnaissance , Evasion, NMAP, subprocess.

INDEX

Introduction

Comprehensive vulnerability management, which involves evaluating, mitigating, and reporting security flaws and cyber threats within the organization's tech stack, is one of the most important responsibilities of an IT security administrator. An automated vulnerability scanner, which enables the identification and discovery of potential weaknesses, serves as the basis for vulnerability management in order to aid in this.

Over the years, many different scanners have been developed such as Nessus, Netsparker, Acunetix and many more, providing a lot of different options and features. But these scanners often are closed sourced and are available on a periodic subscription model or one time purchase of tools. On the other hand the open source scanners like OPENVAS are very weak in terms of automation and ease of use.

The development of an open source reliable and fast reconnaissance and scanning tools have been a challenge for security researchers to find out the missing elements of information security in a web application. Recon, Evasion & Vulnerability Exposure Tool is a python & bash(subprocess) based tool with 14 unique reconnaissance, enumeration & scanning features to scan a web application for vulnerabilities & security misconfigurations. The tool is natively built in python and is currently operable for Ubuntu Distribution of Linux. The tool is able to scan ports , perform enumeration using various techniques, evade firewalls and find vulnerabilities. The tool is in development for 3 versions namely CLI, GUI(Application or software) and Web Application. Tool also integrates pre existing open source, standard tools like Nmap , Nikto & Nuclei.

Literature Survey

Due to the rapid development in technology stacks and discovery of new vulnerabilities the development of an automated vulnerability scanner has been a challenge for security researchers. SULIMAN ALAZMI & DANIEL CONTE DE LEON published a comprehensive review of several standard Web Application Vulnerability Scanners. The review covered over 30 Web Application Vulnerability Scanners.
There are mainly two approaches towards identifying vulnerabilities in a web application namely Black box Testing & White Box Testing. Security consultants who are proficient in a variety of programming languages, developing algorithms, and examining application code use white-box testing. On the other hand, cyber security experts who are knowledgeable about a variety of technologies, adept at analyzing user input, and able to think innovatively use black-box testing.Black-box testing is the most common approach used for identifying vulnerabilities by testing them dynamically . The review concluded that:

1. Among the OWASP Top Ten vulnerability types, SQLi and XSS vulnerabilities were the most frequently tested.
2. Nearly no tests were conducted on the OWASP Top Ten list's other categories of vulnerabilities.
3. Four other OWASP Top Ten vulnerabilities were only evaluated in one evaluation, and this study only looked at one commercial web vulnerability scanner.
4. 13 studies in total evaluated the performance of SQLi and 8 studies in total evaluated XSS for multiple scanners; however, the majority of studies only evaluated one or two scanners against one or two non-standard, and thus challenging to replicate, web applications.
5. No published evaluations assessing the usability or quality of use of web vulnerability scanners were found.

Based upon the findings of the literature review we incorporated the recommendations made by the latter for development of our Vulnerability Scanner such as:

1. All web vulnerability scanners should have their efficacy evaluated using a set of "benchmark" web applications and for all OWASP Top 10 types of vulnerabilities; however, there are currently no such benchmark web applications. As a result, new benchmark web applications that are standard and representative should be developed. These benchmarks ought to include all relevant niches of web applications. This will help to guarantee complete and comparable results from web vulnerability scanners.
2. Evaluations of web vulnerability scanners from a usability or quality-of-use perspective should also be performed.

Development

1. Planning

The development of Recon, Evasion And Vulnerability Exposure tool (REAVER) was very intricate and had to be planned thoroughly before execution. Hence planning the development procedure is a very crucial step. Automated Vulnerability Scanning works in four different steps:

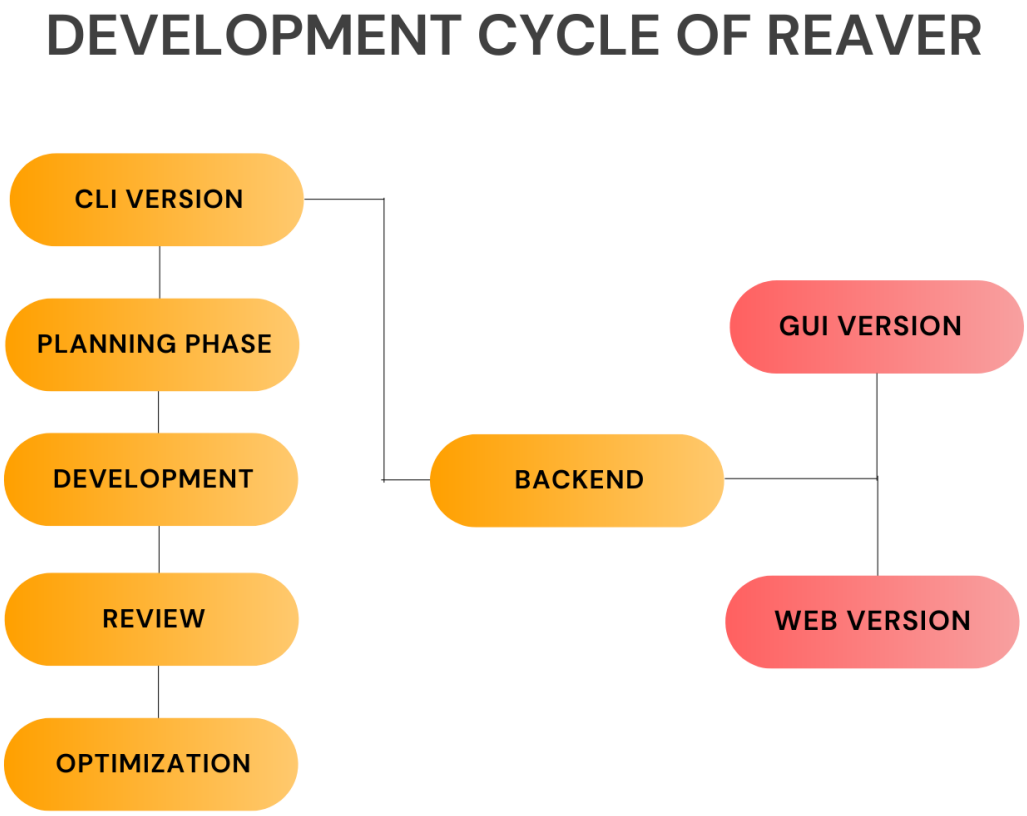
1. **Recognizing the weaknesses** : A vulnerability database is used by a web application security scanner or vulnerability scanning software to find security flaws in the target system. According to pre-established rules, the tool probes into various parts of the target system and looks for response patterns that might point to web application vulnerabilities.
2. **Risk assessment** : The severity and effects on the system of the identified vulnerability should be evaluated using a scoring system. Typically, the CVSS score and the potential harm brought on by a particular vulnerability are used to accomplish this.
3. **Remediation :** Prioritization should be the first step in responding to the security breach. The vulnerabilities should be categorized based on their score, and a remediation inventory should be made as a result. Specific recommendations for addressing the vulnerabilities are produced by a thorough vulnerability assessment.
4. **Reporting :** Any breach that is discovered, assessed, and addressed must be properly reported in order to raise awareness going forward. The vulnerability scanning report ought to include information on the test cases, a summary for everyone's benefit, recommendations for addressing each vulnerability, etc. There are several reporting standards SANS Top 25, PCI DSS Compliance Report, OWASP Top 10, ISO 27001 Compliance etc.

Since REAVER was not only supposed to be a vulnerability scanner but also an all in one reconnaissance & enumeration tool , it was not limited to the given four steps. REAVER also needed to discover security misconfigurations and gather information about the target such as Host Address, Whois Info, Subdomain enumeration, DNS Info, SPF & DMARC Record etc.
Choosing a proper technology stack as well as a good development and testing environment was a challenge as such tools are very hard to build using a single technology stack.

Operation	Technology Stack used
Technology Stack 1	Python
Technology Stack 2	Bash
Development Environment / OS	Ubuntu (based on Debian distribution)
GUI (Software & Web) Development	Tkinter , Django

2. **Development**

REAVER was developed firstly for the cli version which incorporated several unique features . The development cycle has completed the planning , development , and optimization stage of the cli version of the tool. The development cycle for gui and web based versions are in the development phase and will be completed in a span of 5 weeks.

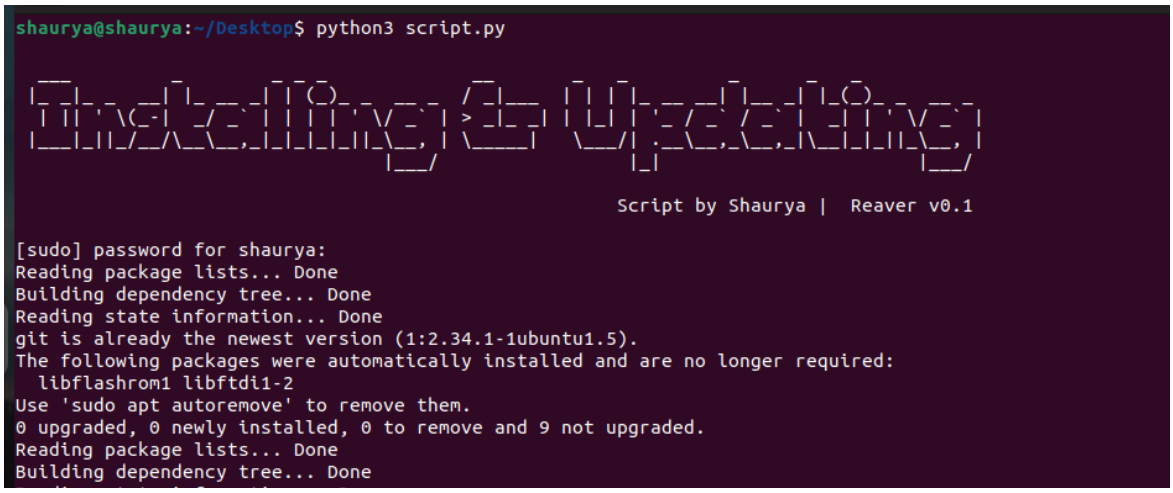


3. **Optimization :** The tool is dependent upon the linux based environment and hence has to be delivered in package and executable versions for platforms such as windows and android before release. The web version of the tool will be based on the technology stack of Django whereas the gui version of the tool will be based on Tkinter. Both gui and web versions will be using the cli version of reaver in the backend. Hence the backend of the tool was optimized multiple times to eliminate errors arising due to user interactions. The runtime of features and processes were also optimized to make the scans faster and efficient.

Working Process & Features

The features and working processes of REAVER are given below in a fragmented manner:

1. **Automated Installation & Updates:** REAVER comes with an installation python based script which installs the tool and its related dependencies .The script is also responsible for updating the tool , operating system , as well as the dependencies.



2. **Host Availability Detection:** Reaver takes the domain of the web application as the input and then scans for the availability of the host by sending different requests and examining the responses.

3. **Tor based firewall evasion:** All the network traffic generated by the REAVER reaches the target through the tor based proxy to maintain the anonymity of the tester as well as

evade the web application firewalls from detecting continuous malicious traffic from a single source.

4. **Port Scanning:** Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. To increase the reliability and contribute towards the open source model , NMAP, an open source port scanning tool was incorporated in REAVER for port scanning as the tool is highly capable and industry standard.

```
2
Executing 2 on iem.edu.in

[sudo] password for shaurya:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-28 07:56 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:56
Completed NSE at 07:56, 0.00s elapsed
Initiating NSE at 07:56
Completed NSE at 07:56, 0.00s elapsed
Initiating NSE at 07:56
Completed NSE at 07:56, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 07:56
Completed Parallel DNS resolution of 1 host. at 07:56, 0.03s elapsed
Initiating SYN Stealth Scan at 07:56
Scanning iem.edu.in (104.21.29.199) [65535 ports]
Discovered open port 443/tcp on 104.21.29.199
Discovered open port 8080/tcp on 104.21.29.199
Discovered open port 80/tcp on 104.21.29.199
Discovered open port 2053/tcp on 104.21.29.199
Discovered open port 8880/tcp on 104.21.29.199
```

5. **Web Based Vulnerability Scanner :** REAVER performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

```
---------------------------------------------------------------------------
+ Target IP:          172.67.149.196
+ Target Hostname:    iem.edu.in
+ Target Port:        80
+ Start Time:         2022-11-28 08:02:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ Uncommon header 'cf-ray' found, with contents: 770fb1990dccf2de-BOM
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400, h3-29=":443"; ma=86400
+ Uncommon header 'nel' found, with contents: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report
rZY1EXEUKLFP8UZzJkifwFxOZznwUfGZaBKrW0fin3XoNqycGFayr6IEfKoEV%2B"}],"group":"cf-nel","max_age":604800}
```

6. **Security Misconfiguration Detection:** REAVER offers scanning for a variety of protocols, including TCP, DNS, HTTP, SSL, File, Whois, Websocket, Headless etc. With powerful and flexible templating, it can be used to model all kinds of security checks.

```
[INF] Templates added in last update: 45
[INF] Templates loaded for scan: 4397
[INF] Templates clustered: 832 (Reduced 767 HTTP Requests)
[2022-11-28 08:03:43] [ssl-dns-names] [ssl] [info] iem.edu.in [iem.edu.in,sni.cloudflaressl.com,*.iem.edu.in]
[2022-11-28 08:03:46] [htaccess-config] [http] [info] https://iem.edu.in/.htaccess
[INF] Using Interactsh Server: oast.fun
[2022-11-28 08:03:50] [tech-detect:google-tag-manager] [http] [info] https://iem.edu.in
[2022-11-28 08:03:50] [tech-detect:youtube] [http] [info] https://iem.edu.in
[2022-11-28 08:03:50] [tech-detect:cloudflare] [http] [info] https://iem.edu.in
```

7. **Subdomain Enumeration:** Subdomain enumeration is the process of identifying all subdomains for a given domain. It helps to broaden the attack surface, find hidden applications, and forgotten subdomains.

```
iem.edu.in
webdisk.iem.edu.in
alumni.iem.edu.in
dev.iem.edu.in
cpcalendars.iem.edu.in
cpcontacts.iem.edu.in
acmiemsb.iem.edu.in
mail.iem.edu.in
naac.iem.edu.in
www.iem.edu.in
ieeeiemsb.iem.edu.in
moodle.iem.edu.in
```

8. **Wordpress Based Scans:** Due to the increasing popularity of wordpress as a method to develop websites over a short span of time, the risk of vulnerabilities which are present in the new releases of technology stack or plugins is very high. To counter the problem REAVER is integrated with a wordpress based vulnerability scanner .

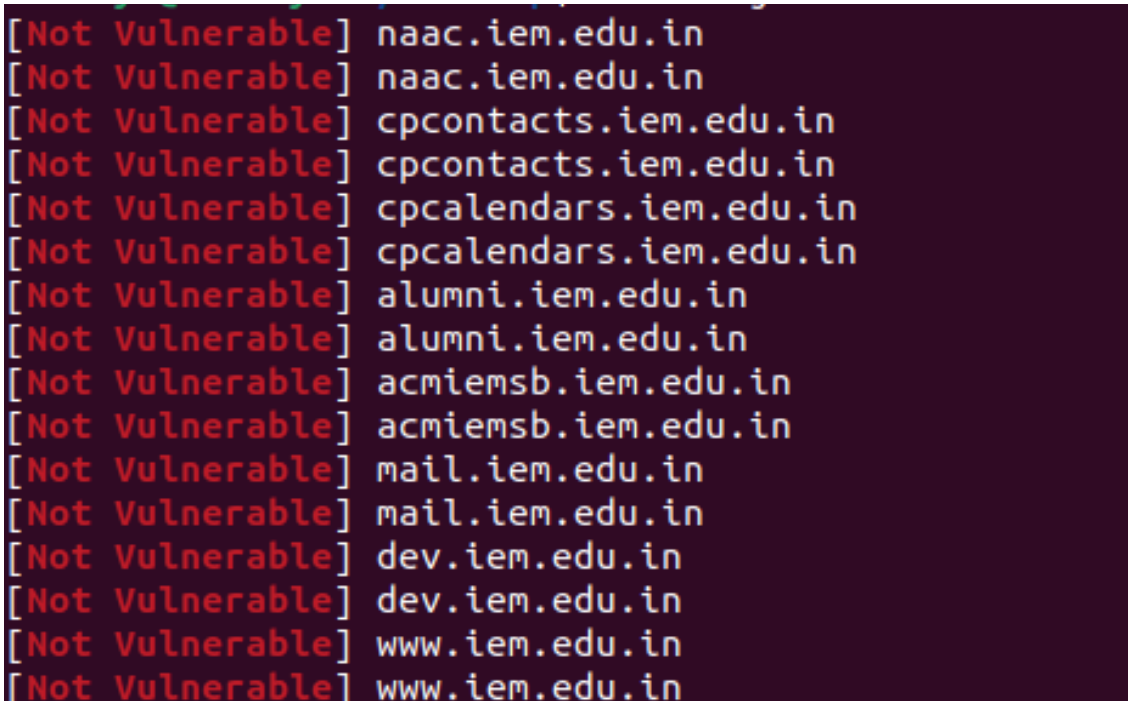
```
[+] URL: https://iem.edu.in/ [104.21.29.199]
[+] Started: Mon Nov 28 08:12:33 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - cf-cache-status: DYNAMIC
 |  - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=vNKEPGE5hS2LSOhDlwHVSmgW4N3ijNvBQaEIp%2B
Q2enW9v%2FHoEMQe5odCxp22ZBwIvdIG2"}],"group":"cf-nel","max_age":604800}
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: cloudflare
 |  - cf-ray: 770fc0400fdf84fe-BOM
 |  - alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://iem.edu.in/robots.txt
 | Interesting Entries:
 |  - /wp/wp-admin/
 |  - /wp/wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%
```

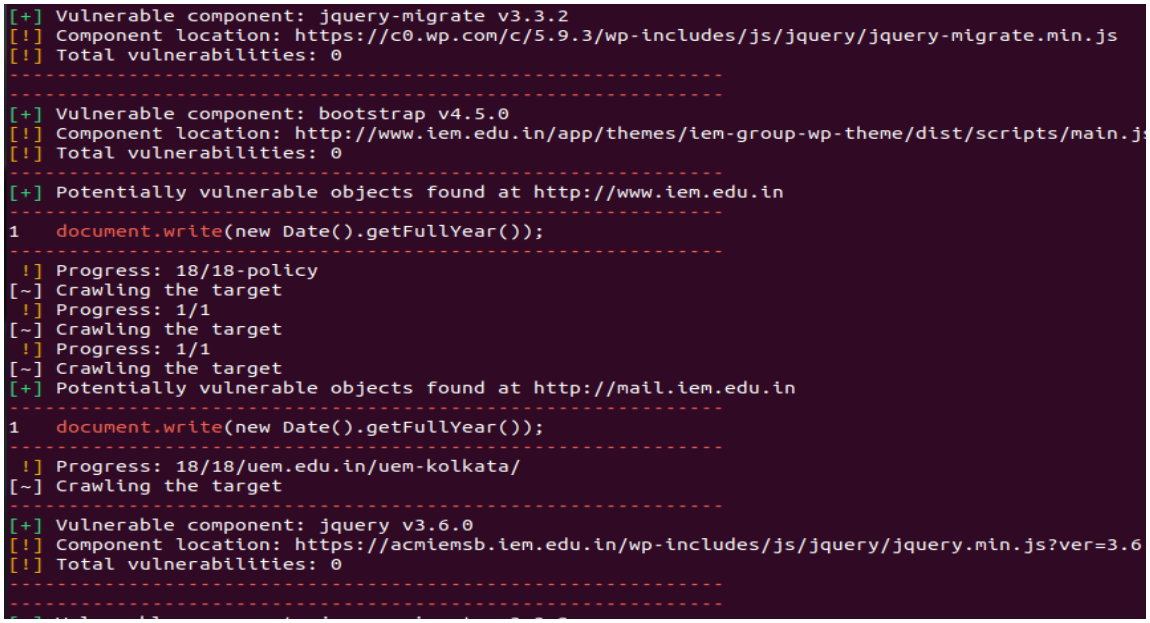
9. **Subdomain Hijack Scan:** When the subdomain has a canonical name (CNAME) in the Domain Name System (DNS), but there is no host who provides content for it , an attacker can gain control over the subdomain. This is known as subdomain hijacking. REAVER is able to enumerate all the subdomains and scans it to test the possibility of subdomain takeover.



10. **DNS toolkit:** The tool sends a Simple and Handy utility to query DNS records and gather information such as A, AAAA, CNAME, PTR, NS, MX, TXT, SOA and DNS information.

11. **XSS Detection:** Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. REAVER performs a comprehensive scan for cross site scripting vulnerabilities. REAVER is equipped with an intelligent payload generator, a powerful fuzzing engine and an

incredibly fast crawler. Instead of injecting payloads and checking it works like all the other tools do, REAVER analyses the response with multiple parsers and then crafts payloads that are guaranteed to work by context analysis integrated with a fuzzing engine.



12. **Complete Scan:** The feature runs all the available processes to discover and report the complete list of valuable information and security vulnerabilities. It utilizes a database of payloads, web based api services like crt.sh, shodan , virustotal, censys search, to inspect the web application for valuable information and vulnerabilities. The report generated by complete scan includes all the reports generated by the previously mentioned features.

Limitations & Scope of Improvement

Since the Tool only completed for cli version there are a lot of limitations and improvements which can be made to increase the usability and platform independence. Some of the limitations of the tool till date which will be removed over the next updates and versions of REAVER are as following:

1. Dependency of tool to run natively on Ubuntu a debian based linux distribution can limit the tool to be compatible for the windows counterparts.
2. The report generation is done in a very generic manner and will be improved to standards like SANS Top 25, PCI DSS Compliance Report, OWASP Top 10, ISO 27001 Compliance.
3. The absence of a database to store previous scans is a necessity ,which needs to be incorporated in the latter versions of the tool.
4. The dependency of REAVER on industry standard open source tools like NMAP is both a curse and a boon. But in future the dependence of REAVER on integration of external tools should be reduced by providing a natively available counterpart of the external tool.

Conclusion

To decrease the risks of vulnerabilities and security misconfigurations the Reconnaissance, Evasion And Vulnerability Exposure Tool was able to detect major vulnerabilities in web applications while also providing the valuable information about the missing elements of information security namely CIAAN - Confidentiality Integrity, Availability , Authentication and Non Repudiation. The tool will be helpful for the security researcher to ease the work of finding vulnerabilities in the system so that they can focus more on the manual testing of web applications which can also bring up several hidden vulnerabilities.

References

[1] A. Doupé, L. Cavedon, C. Kruegel, and G. Vigna, ‘‘Enemy of the state: A state-awareblack-box web vulnerability scanner,’’ in Presented at the 21st USENIX Secur. Symp. (USENIX Secur.), Aug. 2012.

[2] M. Agarwal and A. Singh, Metasploit Penetration Testing Cookbook. Birmingham, U.K.: Packt, 2013.

[3] A. Akbulut, ‘‘VinJect: Toolkit for penetration testing and vulnerability scanning,’’ Düzce Üniversitesi Bilim ve Teknoloji Dergisi, vol. 6, no. 4, pp. 779–790, Apr. 2018. [Online]. Available: https://dergipark.org.tr/en/
download/article-file/517130

[4] M. S. Aliero and I. Ghani, ‘‘A component based SQL injection vulnerability detection tool,’’ in Proc. 9th Malaysian Softw. Eng. Conf. (MySEC), Dec. 2015, pp. 224–229, doi: 10.1109/MySEC.2015.7475225.

[5] M. S. Aliero, I. Ghani, K. N. Qureshi, and M. F. Rohani, ‘‘An algorithm for detecting SQL injection vulnerability using black-box testing,’’ J. Ambient Intell. Humanized Comput., vol. 11, no. 1, pp. 249–266, Jan. 2020, doi:
10.1007/s12652-019-01235-z.

[6] M. Alsaleh, N. Alomar, M. Alshreef, A. Alarifi, and A. Al-Salman, ‘‘Performance-based comparative assessment of open source web vul-nerability scanners,’’ Secur. Commun. Netw., vol. 2017, May 2017,
Art. no. 6158107.

[7] N. Antunes and M. Vieira, ‘‘Comparing the effectiveness of pen- etration testing and static code analysis on the detection of SQLiinjection vulnerabilities in web services,’’ in Proc. 15th IEEE Pacific Rim Int. Symp. Dependable Comput., Nov. 2009, pp. 301–306, doi:
10.1109/PRDC.2009.54.

[8] N. Antunes and M. Vieira, ‘‘Detecting SQL injection vulnerabilities in web services,’’ in Proc. 4th Latin-American Symp. Dependable Comput.,
Sep. 2009, pp. 17–24, doi: 10.1109/LADC.2009.21.

[9] N. Antunes and M. Vieira, ‘‘Benchmarking vulnerability detection tools for web services,’’ in Proc. IEEE Int. Conf. Web Services, Jul. 2010,
pp. 203–210, doi: 10.1109/ICWS.2010.76.

[10] N. Antunes and M. Vieira, ‘‘Enhancing penetration testing with attack signatures and interface monitoring for the detection of injection vulnerabilities in web services,’’ in Proc. IEEE Int. Conf. Services Comput.,
Jul. 2011, pp. 104–111, doi: 10.1109/SCC.2011.67.

[11] N. Antunes and M. Vieira, ‘‘Defending against web application vul- nerabilities,’’ Computer, vol. 45, no. 2, pp. 66–72, Feb. 2012, doi:
10.1109/MC.2011.259.

[12] N. Antunes and M. Vieira, ‘‘Designing vulnerability testing tools for web services: Approach, components, and tools,’’ Int. J. Inf. Secur., vol. 16,
no. 4, pp. 435–457, Jun. 2016, doi: 10.1007/s10207-016-0334-0.