*International Journal of Engineering & Technology,* 7 (2.32) (2018) 431-435

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***



# An Integrated Approach Towards Vulnerability Assessment & Penetration Testing for a Web Application

**K. Siva Prasad[1], Dr . K. Raja Sekhar[2], Dr .P. Rajarajeswari[3]**

*[1]M.Tech Cyber Security and Digital Forensics, KLEF, Department of CSE, Guntur, AP, India*
*[2,3]Professor, KLEF, Department of CSE, Guntur, AP, India*
**Corresponding author E-mail: sivaprasad.kram@gmail.com*

**Abstract**

Current digitized world has surpassed the days of mere existence of internet. Furnishing the services through web has become the most often element to be implemented by almost every sector. These ever-changing technologies has also brought about, devastating evading techniques compromising the fragility of the web application. Assessing the existing vulnerabilities of a web application and testing all possible penetrations would be tedious if the tools used are bearing a cost factor. This paper suggests an integrated approach of assessing the vulnerabilities in any web application using free and open source tools where the reports are generated with respect to vulnerabilities and their categories and level of severity. The tools are integrated and correlated for producing the accurate results in better manner similar to the results produced by the commercial ones. The analysis has been done by considering the reports released by OWASP, OSSTMM, ISSAF, CVE, Exploit Database and Microsoft Vulnerability Research. The report produced after vulnerability assessment has been taken for testing different penetrations for a single application. The identified vulnerabilities are therefore exploited for testing the penetrations of a web application. The report will be generated finally stating all possible exploitable vulnerabilities that are encountered in a web application. The final report generated would help the developers to fix the vulnerable issues.

***Keywords***:*Vulnerability assessment, penetration testing, integrated results.*

## 1. Introduction

The evolving nature of the internet has brought about vast transformations in almost every field seeking for furnishing digitized services through online. The client would avail his requested service upon placing his sensitive data on appropriate application databases, thereby he is actually entrusting the application to be safe. But such scenario becomes worse when any of the existing vulnerabilities in the web application happen to be exploited at any time. So, the application needs to be tested under different penetrations by assessing different vulnerabilities. We need to take some defensive security measures to face current attack landscape prioritizing the attacks like Injections, cross-site scripting, remote code execution, cross-site request forgery etc. [1].

Triggering the vulnerabilities through proper identification of the existing backdoors would majorly decide the path to the attacker for an intended exploitation. Such backdoors needs to be identified in prior step before the deployment stage of the software development life cycle. The vulnerabilities will be recognized by the tester, once he has a technical asset on how and what attacks could be possible on a specific application. This paper presents the approaches and tools followed by the pen tester for exploring the vulnerabilities and testing the penetrations. This paper would suggest an innovative approach of integrating the results of the vulnerabilities that are assessed by some of the open source and free tools. The paper goes with a motto of presenting the accuracy in results using free and open source tools relative to the commercial tools, stating the possibility of getting precise data from only free and open source tools rather going with commercial one's. The report produced thereafter would be analyzed under different penetrations like Cross-site scripting, Injections, Directory traversal, Cross site request forgery etc.

## 2. Related Work

The tester's mission would start by analysing attacker's vision. Prioritizing, the attacker's motto the first phase is to gather the information which is actually termed as reconnaissance in penetration testing. The information gathered in this phase would be utilized for further analysis in penetrations. Finding Host names, IP address, domain names, including country, state and city, name of network provider of the target, IP range and maximum frame size of packet. Finding the purpose of organization and how big the organization and verify firewall used by the organization. Examining html code, css code and version of operating system used by organization. Finding open-ports and banner grabbing the target system. Mirroring the website, owner of domain and registration date and owners contact information. IP block address and measuring the route path and transit time of packet across an internet protocol network. Gathering current address, phone number, email address, location history. Extracting Meta data in that particular targeted website. There are many tools exists for information gathering phase. For example *Domain Dossier is an* online tool for investigate domains and IP addresses such as domain "who is" records, DNS records, traceroute, network "who is" record, service scan etc. [4]. Similarly Super Scan is the best tool for enumeration and port scanning which show advanced results about service

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

running in particular port and there versions and also detects open TCP and UDP ports on a target and run queries such as "who is", ping, ICMP traceroute and host name, Net BIOS information, user and group accounts, services on each port etc. [5]. Another interested tool is Nmap (Network Mapper) which is free and open source contain various features like host discovery, scan techniques, service/version detection, script scan, OS detection, firewall/ids evasion and spoofing etc. [6] Scan TCP and UDP ports, analyse host details and their topology, determine various type of packet filters, ping the host, finding host name, ports of target and services, filtered ports, time to live status, web detects, Net BIOS info, MAC address, MAC vender. The following section is giving more related work on Vulnerability scanning and Vulnerability exploitation.

## 2.1 Vulnerability Scanning

In vulnerability scanning phase using automated tools we need to find the vulnerability of particular web application.

**a. Acunetix web vulnerability scanner**

Advanced automated vulnerability scanner which scan the website and perform black box and Grey box hacking techniques which find dangerous vulnerabilities in particular website. Acunetix web vulnerability scanner are can be available for both commercial and free (trail versions are available) [7]

**b. Burp suite:**

Burp suite one of the commercial/free version are available .Burp suite intercepting proxy tool has various features such as Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender. Free version has no scanner but all other features are available. [8]

**c. Nessus:**

Nessus one of the commercial/free home version are available. Advanced automated scanner which contain Advanced Scan, Bad lock Detection, Bash Shell hock Detection, Basic Network scan, Credentialed Path Audit, DROWN Detection, Host Detection, Intel AMT Security Bypass, Malware scan, Shadow Brock Scan, Wanna Cry Ransomware and Web Application Tests etc. here some of the features are not available because of home version. Here I selected a web Application Test. [9]

**d. W3af:**

Web application attack and audit framework contain some advanced features such as audit, brute force, discovery, evasion, grep, mangle, OWAP_Top10, audit_high_risk, fast scan, full audit, Site map etc. We can also exploit the vulnerability by using W3af. [12]

**e. Nikto:**

Nikto free and open source vulnerability scanner. Nikto examines the web server to find potential dangerous problems and security vulnerabilities such as Sever and software misconfigurations, Default programs and files, insecure files and programs and outdated servers and programs. [10]

**f. Vega**

Vega is a free and open source scanner with validate Injection Modules such as SQL Injection, Cross-Site Scripting (XSS), XML Injection, URL Injection, Remote and Local File Inclusion Check, Cross Domain Policy Auditing and other vulnerabilities.Reporting Process Modules such as Directory Listing Detection, Path Disclosure, Cookie Security Module, HTTP Header Check and File upload Detection and other vulnerabilities. [11]

**g. OWASP-ZAP:**

OWASP-ZAP is an all-in-one tool for web application security testing. It is from OWASP. It has a sophisticated GUI and advanced features to do such things as proxy, scripting, spider, Encode/Decode, Active scan, manual request editing, force browsing, fuzzing, compare web pages with extensible through a number of plugins. [13]

**h. Qualys ssl scanner**

Qualys advanced ssl scanner free from Qualys .Qualys commercial vulnerability scanner free versions are available for scanning. Qualys Free SSL Server Test perform in depth analysis of the configuration of any SSL web server. Qualys ssl scanner give better results for analysis over ssl. Qualys Vulnerability scanner trail version are available. [14]

**i. Arachni web Vulnerability scanner**

Arachni is Ruby framework aimed towards helping penetration testers evaluate the security of modern web applications. Its source code public and available for review. [15]

## 2.2 Exploiting Vulnerabilities

Exploiting Vulnerabilities using some automated tools for exploitation of the various vulnerabilities

**a. SQL injection**

A SQL injection means we obtain database by injecting malicious SQL strings this is due to in proper input validation in web application [3].

**Manual exploitation:** SQL injection vulnerability can be exploited by using single quotes (‘), Double quotes (“), backslash (/) and Hash (#). It tested in URLS and all input fields of web application. If it show syntax error then it vulnerable to SQL injection. Use various SQL statements to exploit vulnerability such as order by, union select and information-schema. Tables etc. Here different database has different syntax for manual exploitation it quit difficult.

**Automated exploitation:** SQL map an open source tools written in python .A SQL map best command line tool for sql injection. Here this tool exploit SQL injection vulnerability in any database such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Maria DB etc. Before performing the exploitation take the URL Vulnerable which shown in vulnerability assessment report.

**b. Command:**

Sqlmap.py –u http://www.tesingsite.com/view.php?id=1

**Cross site scripting:** A Cross site scripting Vulnerability occur due to the in proper validation of the JavaScript here attacker inject and execute malicious JavaScript in the application and obtain sensitive information about particular website. [3]

**Manual Exploitation:** Here after executing below java script it will give pop-up then it vulnerable to the Cross site scripting. Here 5000+ payloads are there.

```
<script>alert(123)</script>
<script>window.location=http://facksite.com</script>
<script>alert("document.cookies");</script>
javascript:alert("hellox worldss")
<script>alert("document.domin");</script>
<img src="javascript:alert('XSS');">
```

**Automated Exploitation:** OWASP Xenotix XSS Exploit Framework is exploitation frame work for cross site scripting. It became 2nd World's largest XSS Payloads of about 4800+ distinctive XSS Payloads. It contain excellent three FUZZERS such as Blind FUZZER, INTELLFUZZER and CONTEXT BASED FUZZER.

**c. Directory traversal**

Directory traversal exploitation due to the access of the restricted directories by exploiting the improper input validation. Due to the Directory traversal attack an attacker access the root privileges of the server. [4]

**Manual exploitation:** Directory traversal testing can be done by using …/…/…/…/ at the end of URL.

***Linux:***

../../../../etc/passwd%00

../../../../../etc/passwd

../../../../../etc/shadow%00

../../../../../../etc/shadow

***Windows:***

\..\..\..\..\..\..\..\..\..\..\boot.ini

\..\..\..\..\..\..\..\..\..\..\boot.ini%00

\..\..\..\..\..\..\..\..\..\..\boot.ini

**Automated Exploitation:** Dotdotpwn flexible intelligent fuzzer used to exploiting traversal vulnerabilities in various servers. It attack on specified port and host with desired payload work through protocol-independent modules.

**d. Broken Authentication and session management**

Broken Authentication and session management means by performing Brute force attack on the log in page and verify the Sensitive information over cookies, check cookies with httponly flag and no secure flag, path attributes in session cookie, session prediction, session randomness, check session cookies before and after login and session hijacking.[4]

**Automated Exploitation:** Burp suit and owasp-zap a best tool for broken authentication and session management. By using intruder tool in burp suit we can broken authentication and session management.

**e. Parameter / Form tampering**

A parameter / form tampering due to the manipulation of the parameters in request and response process by using proxy which we can obtain sensitive information in web application [4].

**Automation Exploitation:** Parameter /Form tampering can done by using proxy tools such as owasp-zap, burp suite, vega and web-scrab. Burp suite Use Repeater tool in burp suite along with intercept on. Here we can manipulate parameters in the Repeater.

**f. Denial of Service**

Denial of service attack means attack on computer or network that reduce, restrict or prevent the legitimate user to access their resource in internet. Attacker flood the victim computer with non-legitimate service requests or traffic to overload it resource. [4]

**Automation Exploitation:** Here automated Denial of Service tool means sending multiple request to the server.It send multiple asynchronous sockets to perform Denial of Service attack. LOIC (Low Orbit Ion Canon) tool perform dos attack by sending UDP, TCP or HTTP requests to target. Metasploit Framework can be used to perform dos attack.

**g. Http request header injection**

HTTP Header Injection vulnerabilities occur when user input is insecurely included with in server responses. In this modifying the request and response header of the application and get some critical information about application. [4]

**Automation Exploitation:** Http request header injection vulnerability can be exploited by using net cat tool and proxy tools such as owasp-zap, burp suite, vega and web-scarab.

## 3. Experimental Setup

With a motto of showing the accurate results with open and free tools an architecture has been proposed. The proposed architecture would determine the results of free and open source tools in the most accurate way where the reports of the tools are been integrated and have been well analysed, thereby presenting the précised data report to the developer who could take appropriate preliminary steps without causing the invocation of unintended vulnerabilities.

A pen tester would initially access the testing site through the proxy server. Here my testing site is e-app. The http request sent by the tester would then be intercepted by the proxy before actually sending the request to the application server. The intercepted traffic can then use for further analysis under different penetrations. The information of the testing site will first be gathered actively involving the server machine into the attack process, and then passively not engaging the machine. The tools used for active reconnaissance are nmap and McAfee super scanner, whereas the tools used for passive way of getting the server information has included a domain dossier. Later on after gathering the handful amount of information about the server machine, the vulnerabilities are been scanned using the open and free tools like Nessus, Acute nix, Vega, Nikto,w3af, zap, Qualys and Arachni. The vulnerabilities reports resulted by these tools are been further analysed based on the standards of OWASP, OSSTMM, ISSAF, CVE, Exploit Database, and Microsoft Vulnerability Research. Upon appropriate analysis done manually, the reports are also fed to the FARADAY database where it has generated a final report integrating the results of all the tools taken under vulnerability scanning phase.

The report generated at the end of the vulnerability assessment phase is analysed and tested under vast set of penetrations. The vulnerabilities encountered previously are exploited one by one, using respective appropriate tools for manual exploitation the web application writing custom exploit scripts and injection strings or by using various exploitation tools such as SQL map, XSS Me, OWASP xenotix framework, dotdotpwn, burp suite, owasp-zap, fimap, HTTPDos, metasploit Framework etc. In penetration testing proof of content report a penetration tester made report for exploited flaws in web application and show how much damage a loop hole could be in a real attack, measure the severity of each flaw. Finally report send to the developer team.

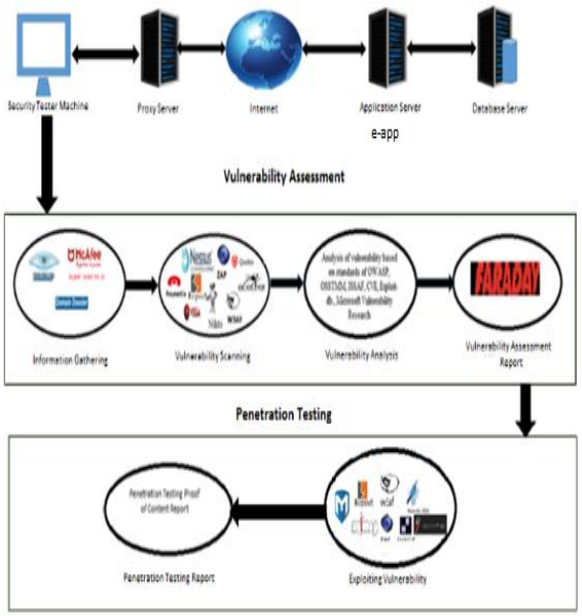



**Fig**.1. Experimental Setup for Vulnerability Assessment and Penetration Testing.

## 4. Results

After scanning the particular e-app web application with multiple vulnerability scanning tools, integrating the results into a single report by using Faraday tools. Faraday report shown in below figure 2.




**Fig**. 2. Vulnerability assessment report.

List of vulnerabilities in vulnerability assessment report shown in the Table 1. After clearly examine each and every vulnerabilities in faraday tool report .Here the vulnerabilities are made some modification according to standards of OWASP, OSSTMM, ISSAF, CVE, Exploit Database, and Microsoft Vulnerability Research. Here the finalized list of vulnerabilities shown in Table 1.

**Table1**: List of vulnerabilities in e-app

| Vulnerabilities | Severity |
|---|---|
| SQL injection | High |
| OS Command Injection | High |
| LDAP injection | High |
| Xpath injection | High |
| Java script injection | High |
| Cross site scripting | High |
| Serialized object in http message | High |
| Cross site request forgery | High |
| File path traversal/manipulation | High |
| Server level issues | High |
| XML entity expansion | High |
| Parameter/Form Tampering | Medium |
| Session token in URL | Medium |
| SSL Cookie without secure flag set | Medium |
| SSL Certificate | Medium |
| SQL Statement in request parameter | Medium |
| Password value set in cookies | Medium |
| Open redirection | Medium |
| Document Domain Manipulation | Medium |
| Database Connection String Disclosed | Medium |
| Log tampering | Medium |
| Hidden Manipulation | Medium |
| Unencrypted communication | Low |
| Source code disclosure | Low |
| Password field with auto completion enabled | Low |
| Link manipulation | Low |
| Cross origin resource sharing | Low |
| Cookies without HTTP only flag set | Low |
| Content type incorrectely stored | Low |
| Cookie manipulation | Low |
| Content type incorrectly stored | Low |
| Ajax request header manipulation | Low |

Penetration testing report is a manual report shows the process of exploiting the vulnerability. In this report penetration tester gives detail description about exploitation and shown in Fig. 3.

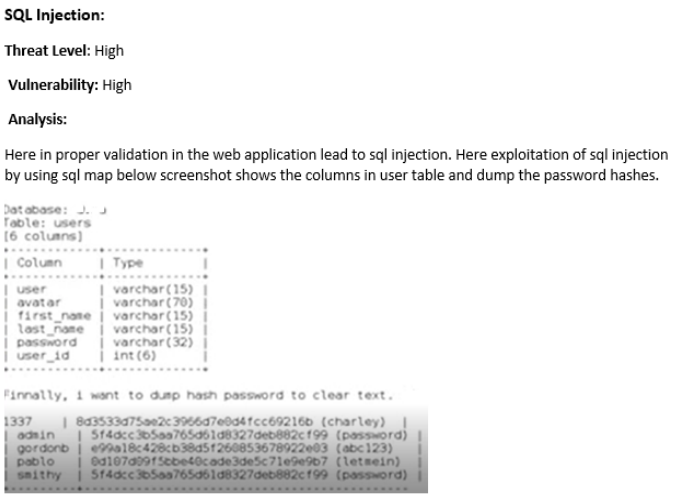



**Fig**. 3. Sql injection exploitation report.

Penetration testing report consist of exploitation of various vulnerabilities such as SQL injection, cross site scripting, path traversal etc. Finally penetration testing report send to the developer for patching purpose.

## 5. Conclusion

The paper has presented a supplementary and complementary way of exploring the vulnerabilities based on the standards of OWASP, OSSTM, ISSAF, CVE and Exploit-db and tested all possible intrusions from traversed vulnerabilities. The accuracy of results using free and open source tools relative to the commercial tools is been well exposed in this paper stating the possibility of getting precise data from only free and open source tools rather going with commercial one's. The analysed report produced finally would extremely be useful to the developer.

## References

[1] Dafydd Stuttard Marcus Pinto: The Web Application Hacker's Handbook Second Edition Finding and Exploiting Security Flaws
[2] Pentesting on Web Applications using Ethical Hacking Central American and Panama Convention (CONCAPAN XXXVI), 2016 IEEE 36th

[3] "Top10 2017-Top10,"OWASP Foundation, 2013; https://www.owasp.org/
[4] Domain Dossier, Investigate domains and IP addresses :
[5] SuperScanv4.1:https://www.mcafee.com/in/downloads/free-tools/superscan.aspx
[6] Nmap : https://nmap.org/
[7] Acunerix :https://www.acunetix.com/vulnerability-scanner/online-scanner/
[8] Burpsuite : https://portswigger.net/burp/communitydownload
[9] Nessus :https://www.tenable.com/products/nessus/select-your-operating-system
[10] Nikto : https://cirt.net/Nikto2
[11] Vega : https://subgraph.com/vega/download/
[12] W3AF Available: http://w3af.org/download
[13] Zap proxy Available: http://www.zaproxy.org/
[14] Qualys : https://www.ssllabs.com/ssltest/
[15] Arachni scanner : http://www.arachni-scanner.com/