IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

WEB APPLICATION SECURITY

Dr.Shalu Tandon[1], Devasnshi Chopra[2], Ankit Bewal[3] , Sayantika Manna[4]

Assistant Professor[1], Jagannath International Management School, Vasant Kunj, New Delhi-110070

Student[2], Jagannath International Management School, Vasant Kunj, New Delhi-110070

Student[3], Jagannath International Management School, Vasant Kunj, New Delhi-110070

Student[4], Jagannath International Management School, Vasant Kunj, New Delhi-110070

ABSTRACT

Cyber Security plays a robust role in the area of information technology. Safeguarding information has become a massive problem in the current world scenario.

As this paper describes the in-depth technical approach to perform manual penetration testing as well as automated testing using ZAP in web applications for testing the integrity and security of the web application and also serves as a guide to test OWASP top 10 security vulnerabilities.

The paper is focused on providing detailed knowledge about manual and automated web application penetration testing methodologies to secure them from malicious contents which can be used to manipulate the application.

Keywords: Cyber Security, web application security, OWASP Top 10 (2021), penetration testing, Automated And Manual Testing

INTRODUCTION

In today's world each and every information about a person is on the web. From email id to phone number everything is stored on the internet in the form of data. This type of data is always authenticated. But sometimes due to lack of enough security the data gets leaked. Although a data breach can be the result of an innocent mistake, real harm is possible if the person with unauthorized access steals and sells personal information or corporate intellectual data for financial gain or to cause harm. Data breaches can occur due to an accidental insider, a malicious insider or malicious outside criminal. Now to avoid data breach web application testing or penetration testing plays a vital role.

We will be testing two dummy sites namely acunetix, bwapp by manual and automated testing. The tool we will be using for automated testing is ZAP Proxy. OWASP ZAP is a security scanner for opensource web applications. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Some of the recent data leaks in the world are of 2021's Domino's user data and of Fortinet VPN as well. In 2020 as the video conferencing app sky rocketed with zoom being the first priority of the workers, it's credentials over 500,000 were compromised. As focused to our country in 2018 security breach of India's national ID database Aadhaar, with over 1.1 billion records lost. This included biometric information such as iris and fingerprint scans which could be used to open bank accounts and receive financial aid, among other government services.

CLASSIFICATION OF WEB APPLICATION

1. CLIENT-SIDE ATTACKS

Attacks which are on client-side are carried out by attackers against clients of a certain website in order to steal their data. Cross Site Request Forgery (CSRF), Cross Origin Resource Sharing
(CORS), Cross Site Scripting (XSS), Clickjacking, HTML Injection, and other client-side assaults are frequent. Server-side attacks do not necessitate user intervention. These attacks are applicable to web servers. We may even use them against a regular PC that people use in their daily basis.

2. SERVER-SIDE ATTACKS

Server-side assaults don't need client cooperation. These assaults can be utilized with web servers. We can likewise utilize this against an ordinary PC that individuals use consistently. In server-side assaults, the aggressor focuses on a weak end-point of the web application and sends a malignant payload to the server. After the effective execution of payload in the server, it reacts to the aggressor with the secret information he mentioned with the payload.

REVIEW OF LITERATURE

Web security is an important aspect for web applications, today web security is a real concern in the context of the Internet and is considered to be the main frame of the global data society. There are two common important security vulnerabilities today: SQL injection and cross-site scripting. These types of vulnerabilities have a direct impact on the web server, application server, and the web application environment.

Extensive literature research suggests cyber security research for testing web applications using manual tools and automated software. Cyber security has become a major issue in our daily lives, not even individuals, but large companies or organizations face huge setbacks as their confidential information is at risk as there are many ways to compromise security, but we only focus on the internet application.

OWASP TOP 10 (2021)

The Open Web Application Security Project (OWASP) is a non-benefit establishment devoted to working on the security of programming. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Globally recognized by developers as the first step towards more secure coding. So, OWASP is a vault of everything web-application-security, sponsored by the broad information and experience of its open local area patrons.[3]

A01:2021-Broken Access Control goes up from the fifth position; 94% of the applications were tested for some form of broken access control. The 34 Common Weaknesses, enumerations (CWE) assigned to Broken Access Control had, more occurrences in applications than any other category.

A02:2021-Cryptographic Failures shifts up one role to #2, formerly referred to as Sensitive Data Exposure, which changed into broad symptom in place of a root cause. The renewed consciousness right here is on screw ups associated with cryptography which regularly results in sensitive information publicity or gadget compromise.

A03:2021-Injection slides right all the way down to the 1/3 position. 94% of the programs had been examined for a few shapes of injection, and the 33 CWEs mapped into this class have the second one most occurrences in programs. Cross-Site web page Scripting is now element of this class on this edition. A04:2021-Insecure Design is a brand new class for 2021, with a awareness on dangers associated with layout flaws. If we honestly need to “pass left” as an industry, it requires greater use of threat modeling, steady layout styles and principles, and reference architectures.

A05:2021-Security Misconfiguration movements up from #6 in the preceding edition; 90% of programs had been examined for a few form of misconfiguration. With greater shifts into fantastically configurable software, it’s now no longer unexpected to peer this class flow up. The former class for XML External Entities (XXE) is now element of this class.

A06:2021-Vulnerable and Outdated Components previously referred to as under the heading Use of Components with Known Vulnerabilities and is ranked 2nd in, the Top 10 Community Survey Assess Risk), assigned to the CWEs included, so a standard vulnerability and an impact weighting of 5.0 are included in their scores.

A07:2021-Identification and Authentication
Failures was formerly Broken Authentication and is sliding down from the 2nd position, and now consists of CWEs which are greater related to identity failures.
This class remains an essential component of the Top 10, however the elevated availability of standardized frameworks appears to be helping.

A08:2021-Software and Data Integrity Failures is a brand-new category for 2021, that specialize in making assumptions associated with software updates, vital records, and CI/CD pipelines without verifying integrity. One of the best weighted affects from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) records mapped to the ten CWEs in this category.[7]

A09:2021-Security Logging and Monitoring Failures was formerly Insufficient Logging & Monitoring and is brought from the enterprise survey (#3), shifting up from #10 formerly. This class is multiplied to encompass greater kinds of screw ups, is hard to check for, and isn’t properly represented in the CVE/CVSS data. However, screw ups on this class can directly effect visibility, incident alerting, and forensics.

A10:2021-Server-Side Request Forgery The facts suggest an especially low prevalence charge with above common testing coverage, alongside abovecommon rankings for Exploit and Impact potential. This class represents the situation where the safety network contributors are telling us that is important, despite the fact that it’s now no longer illustrated withinside the facts at this time.

PENETRATION TESTING

Penetration testing and vulnerability evaluation are specific terms. The latter consists of uncovering the safety flaws and group while the previous consists of exploiting the found paper, we are able to be discussing approximately the flaw and trying statistics ex-filtration or privilege strategies used for checking out net applications.[10] escalation or another feasible malignant motion at the goal host.[4]

Penetration testing out facilitates the builders to locate safety flaws of their utility and hold their utility secure. Performing real-time assessments on internet packages has validated to be useful in hardening the safety of the website. Regular penetration checking out is obligatory after making the utility online to keep away from capability risks.

MANUAL TESTING VS AUTOMATED TOOLS

Manual penetration checking out desires lot of information in gambling with HTTP requests and response. An Expert penetration tester might understand the viable assaults that may be executed on a selected stop factor via way of means of fuzzing the HTTP requests. The principal drawback of the use of automatic gear are fake positives. The automatic gear paintings primarily based totally at the use instances coded via way of means of the developer. And each developer has their very own checking out technique. Some of them can be powerful at the same time as a few may also now no longer. So now no longer all of the automatic gear brings about success. It's higher to observe very own approach whilst it comes for penetration checking out. But automatic gear play's an essential function in content material discovery and reconnaissance and it allows in saving loads of time. Within few years, the entire Pentesting system might be automatic with included Penetration testing and may be widely categorized into five phases

1. Reconnaissance
2. Scanning
3. Exploitation
4. Maintaining Access
5. Clearing Tracks and Reporting

reporting it to the involved safety Because, new zero-day vulnerabilities are found daily and its developer's number one obligation to have an eager eye on what form of third-celebration offerings they're depending on. Penetration checking out isn't most effective restrained to net apps, however additionally completed on IoT Devices, Networks, Computer Systems, Mobile Applications etc. But on this

1. Reconnaissance

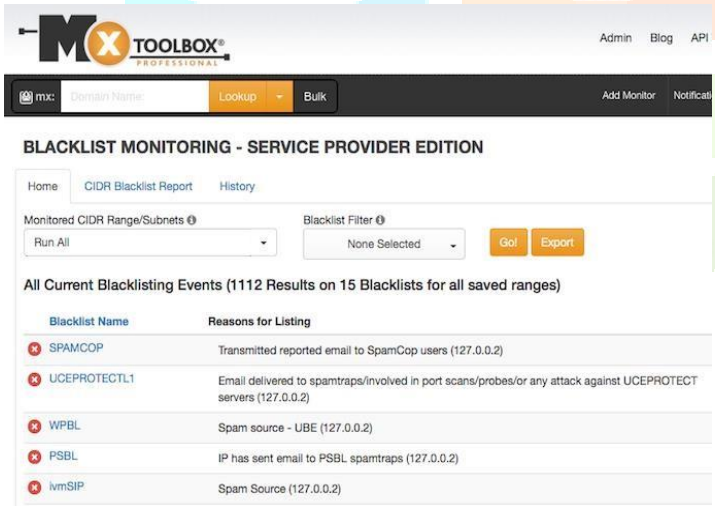
Reconnaissance is the primary section of the penetration testing, take a look at in which the attacker obtains the important records approximately the target. This enables the attacker to benefit foothold on what are the technology, the utility is and the usage of which in addition enables him to discover the vulnerabilities. For example, so that you can hack something, the attacker doesn't constantly hack to locate the direct manner to interrupt in. He may even compromise the hosts on which the goal is counting on after which pivot into the target. There are many web sites and frameworks to be had for performing reconnaissance.[5]

Online Apps for Recon

- dnsdumpster.com – provides data concerning DNS servers, magnetic flux unit records, TXT records, Host records and domain map.

- virustotal.com – checks for malicious files within the web site and provides the DNS information and subdomain info.

- mxtoolbox.com – offers basic functions like reverse DNS lookup, transmission control protocol UDP port scan, reverse IP lookup, and finding shared DNS servers.



- Shodan.io – helps the attackers to seek out internal infrastructure of an organization that are exposed to the internet. Also, Shodan makes the work easier by creating a port scan on the target IP address.

- Wayback.com – excellent place to find sensitive information. Sometime, once you get a 403 forbidden error, there are prospects that back then, the page might be left accessible in public. Similarly, once you notice a 404 page not found error, there are possibilities that back then, there could also be sensitive data left publicly thereon page.

2. Scanning

Scanning is the second segment of penetration checking out which makes use of the records amassed from recon and dig deep into the offerings and contents. It includes host discovery, content material discovery, scanning ports and offerings, vulnerabilities, OS fingerprinting etc. The statistics amassed from the Scanning segment could deliver the attacker, sufficient understanding pick the proper cease factor to start sporting out his exploitation segment Similar to reconnaissance, net apps and frameworks are usually to be had to do this, frameworks do the fine activity of scanning. Some fine frameworks for scanning include.

- Nmap - most prominent and traditional tool for port scanning and OS fingerprinting. Nmap has its own scripting engine called Nmap Scripting Engine (NSE) which allows users to write their own script and automated their tasks. NSE scripts such as nmap-vulners, vulscan retrieves the CVE IDs associated with the target port, operating system etc. Nmap supports different types of scans to detect and evade various types of IDS and Firewall. NSE scripts like smtp-strange port, dns-blacklist, HTTP Enum are most commonly used for website scanning purposes.

- Dmitry, or Deepmagic Information Gathering Tool, is a command line utility included in Kali Linux. It is designed to allow a user to collect public information about a target host. It can be used to gather a number of valuable pieces of information, such as: The whois details of a target host.

```
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting fi
ts
* -b      Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```

3. Exploitation

Although computerized gear do a respectable paintings over recon and scanning, they can't compete with guide techniques. A vulnerability may be exploited in superuser permissions withinside the net server, he thousand methods however guide checking out reveals the can delete the log report leaving no hint for him. But maximum suitable manner (i.e., the manner which has the accomplishing superuser permission isn't always that

As of the device is the Metasploit Framework (MSF) is a the ones logfiles. That relies upon at the UNIX long way greater than only a series of exploits–it's also a distribution, but the maximum not unusual place could stable basis that you could construct upon and without be in /var/log. Any authentication login thru SSH, difficulty customize to fulfill your needs. This permits you Telnet, FTP, SCP are written to those files, it's miles to pay attention for your particular goal surroundings and essential which you take away YOUR ENTRY from now no longer must reinvent the wheel. We remember the those log files. MSF to be one of the unmarried maximum beneficial safety auditing gears freely to be had to safety specialists today.

```
msf > use  exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > help
...snip...
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    pry           Open a Pry session on the current module
    rcheck        Reloads the module and checks if the target is vulnerable
    reload        Just reloads the module
    rerun         Alias for rexploit
    rexploit      Reloads the module and launches an exploit attempt
    run           Alias for exploit

msf exploit(ms09_050_smb2_negotiate_func_index) >
```

Metasploit Framework may be accessed withinside the Kali Whisker Menu, and also can be released at once from the terminal.[4]

very best impact & severity). The severity of the vulnerabilities is represented in one-of-a-kind phrases relying upon the organization. OWASP summarizes the vulnerabilities from A0 to A10 consistent with their severity. Likewise, a web crowdsourcing platform like BugCrowd has its very own vulnerability evaluation taxonomy wherein every vulnerability is assigned a price from P1 - P5 relying upon the Vulnerability severity and impact. HackerOne uses Industrial standardized severity calculator like Common Vulnerability Scoring System (CVSS).

Many human beings round the sector are getting interested by the sector of hacking. This is probably because of sci-fi films or different futuristic titles which have attracted customers to discover ways to hack. There are numerous exploitation gear in Kali Linux 2020.1 to exercise this skill.

clean and it relies upon what form of kernel model and different inclined software's, the server is using. So, in place of clearing logs, it's higher to apply proxy mechanisms to penetration take a

4. Clearing Tracks and Reporting

All the incoming requests to an internet server could guide checking out reveals the can delete the log report leaving no hint for him. But maximum suitable manner (i.e., the manner which has the accomplishing superuser permission isn't always that

It is VERY essential which you delete your access from

```
root@linux:~# locate access.log
/var/log/apache2/access.log
/var/log/apache2/other_vhosts_access.log
/var/log/apache2/xplico_access.log
/var/log/apache2/xplico_access.log.1
/var/log/nginx/access.log
```

/var/log/auth.log This is where are the activity and login's are stored, including failed attempted login's

/var/log/lastlog Contents of accounts, port, and last login date & time.

/var/log/wtmp Records all logins and logouts.

The shell history can be found in the home directory of a specific user, if you logged in as root, then in

/root.

look at a website. Reporting is the very last procedure withinside the penetration testing. Write an in depth file which includes, To begin with we need to pay attention to the following files:
To start with we want to be aware of the subsequent files:

- WTMP – every log in/out, with timestamp + tty and host
- UTMP – who is logged in at the moment
- LASTLOG – what accounts did the logins come from

RESULTS

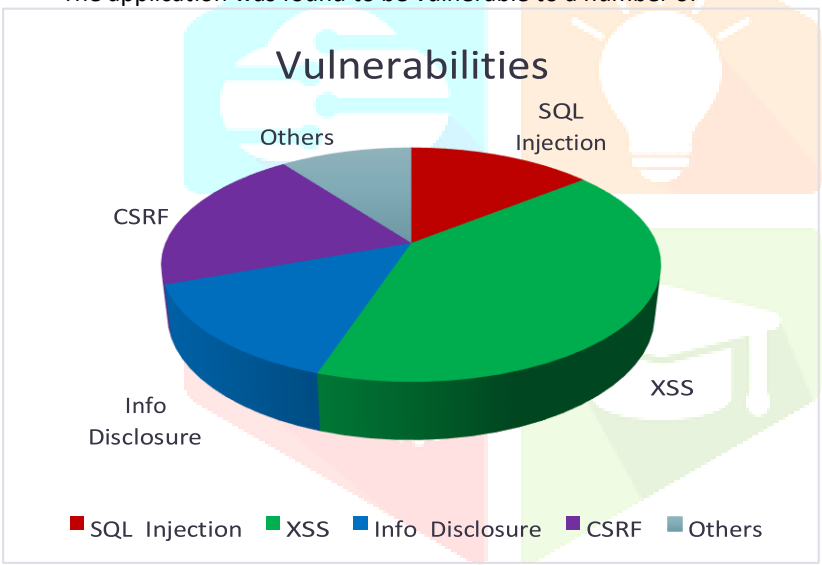
In the beginning of the test phase, the first step was to obtain relevant information such as code language used, script validation information, type of framework used, and website information relevant to test analysis. At the time the test phase started a total of 2 website domains were scanned.

The domain described as www.test.vulnhub.org present a big list of resources, database information, classes, libraries, templates, modules and a long file structure in general. With the help of ZAP Proxy, the scanner test showed relevant results.

From the 100 % of the test the majority of the falsepositive test results were related directly to cross-site scripting under the folder /listings..php that is consider a medium risk. Other medium risk results that the scanner showed were possible Database identification, internal path leakage and blind SQL injection, but are considered a false-positive result.

Finally under the path …/include/get_info.php, a programming error message was detected by the scanner. This has been identified as a minor issue as it could lead to the disclosure of important information to hackers.[6]

The application was found to be vulnerable to a number of



attacks related to the authentication and authorization controls. The application does not implement an account lockout threshold or any password complexity rules. Error messages presented upon valid and invalid login attempts differ, allowing an attacker to determine valid and invalid usernames.

These problems combined allow for the creation of a very effective brute force attack; that would ultimately result in unauthorized access to the application and compromise of the application and user's data. The application's session handling mechanism implementation is vulnerable to several well-known classes of vulnerabilities such as OWASP top 10; its identifiers are predictable, they can be fixed, captured, and trivially inverted through the use of a well-known coding implementation.

These combined issues allow an attacker to hijack user sessions and gain unauthorized and unauthenticated access to application and user data. Client-side script can be bypassed simply by changing web browser security settings.[8]

CONCLUSION

There are also many tools available to automate the exploitation of the application in this manner and the Internet has many step-by-step guides to enable even the lowest skilled attacker to successfully execute an attack. An attacker could feasibly use the vector to embed malicious code that would be run in the security context of the user's browser.

The application has been deployed in a manner that is not in line with best practice guidelines for application and web servers deployed in a hostile environment such as the Internet. A significant amount of test and default content was found to be present on the web server's file system; the file system permissions allowed for the viewing of sensitive.[9]

REFERENCES

1. HTTP://WWW.THESPANNER.CO.UK/2014/05/06/MXSS/
2. Https://Hackernoon.Com/Timing-Based-Blind-Sql-AttacksBd276dc618dd
3. HTTPS://SIMPLYSECURE.BLOG/2017/07/05/FIVE-PHASES-OFPENETRATION-TESTING/
4. https://securityboulevard.com/2021/09/owasptop-10-vulnerabilities-avast/
5. https://securityboulevard.com/2021/09/owasptop-10-vulnerabilities-avast/
6. https://ieeexplore.ieee.org/document/4085599
7. https://www.scitepress.org/Papers/2016/64506/64506.pdf
8. https://ieeexplore.ieee.org/abstract/document/8342469
9. https://ieeexplore.ieee.org/document/8777558
10. https://www.irjet.net/archives/V5/i12/IRJET-

V5I1236.pdf

11. https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1179&context=etd_projects
12. https://ieeexplore.ieee.org/document/8777558
13. CEH V10 MODULES SECURITY COMPROMISING PHASES
14. Earl et al.,. "The oracle problems in Software testing". IEEE transaction on software engineering, Vol. 41, No. 5, 2015, pp 507525.
15. Yuhua et al.,."The Efficient Automated Program Repair through Fault-Recorded Testing Prioritization". 2013 IEEE
16. Chirstopher and Hyunsook "Model-Based Exploratory Testing: A Controlled Experiment ". 2014 IEEE 7th international conference on software testing, ISBN 978-1-4799-5790-3., Acc No. 14363377, 2014

CITATIONS

[1]https://ieeexplore.ieee.org/abstract/document/8342469

[2]https://ieeexplore.ieee.org/abstract/document/6227054

[3]https://securityboulevard.com/2021/09/owasptop-10-vulnerabilities-avast/

[4] X. Li and Y. Xue, "BLOCK: A Black-box Approach for Detection of State Violation Attacks Towards Web Applications," in ACSAC'11: Proceedings of 27th Annual Computer Security Applications Conference, 2011.

[5] R. Wang, S. Chen, X. Wang, and S. Qadeer, "How to shop for free online - security analysis of cashier-as-a-service based web stores," in Oakland'11: Proceedings of the 32nd IEEE Symposium on Security and Privacy, 2011.

[6] M. Balduzzi, C. T. Gimenez, D. Balzarotti, and E. Kirda, "Automated discovery of parameter pollution vulnerabilities in web applications." in NDSS'11: Proceedings of the 8th Annual Network and Distributed System Security Symposium, 2011.

[7] B. J. Corcoran, N. Swamy, and M. Hicks, "Cross-tier, label-based security enforcement for web applications," in SIGMOD '09: Proceedings of the 35th SIGMOD international conference on Management of data, 2009, pp. 269–282.

[8] N. Swamy, B. J. Corcoran, and M. Hicks, "Fable: A language for enforcing user-defined security policies," in Oakland '08: Proceedings of the 29th IEEE Symposium on Security and Privacy.

[9] A. Yip, X. Wang, N. Zeldovich, and M. F. Kaashoek, "Improving application security with data flow assertions," in SOSP'09: Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles, 2009, pp. 291–304.

[10] A. Chlipala, "Static checking of dynamicallyvarying security policies in database-backed applications," in OSDI'10: Proceedings of the 9th USENIX conference on Operating systems design and implementation, 2010

IJCRT