International Journal in IT & Engineering (IJITE)
Volume 7 Issue 6, June 2019 ISSN: 2321-1776 Impact Factor: 6.493
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

"A STUDY OF WEB APPLICATION PENETRATION TESTING"

Kailash Kumar Pareek
Assistant Professor, School of Engineering & Technology, RNB Global University

ABSTRACT

Web Application Penetration Testing plays an important role in the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. In today time it is very difficult to secure company data from the cyber-attacks. Whenever we think about the attacks the first thing that comes to our mind is 'cyber attacks' which are increasing immensely day byday. Various Governments and companies are hiring experts to prevent these cyber arracks. Besides various experts hiring cyber security is still a very big issue. This paper mainly focuses on types of web application penetration testing, phases of web application penetration testing, OWASP top 10 web application security risks and tools of web application penetration testing.

Keywords: Vulnerability, Types of Web Application Penetration Testing, Security Risks, Web application penetration tools.

1. INTRODUCTION

Vulnerability Assessment and Penetration Testing (VAPT) are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serves a different purpose and are carried out to achieve different but complimentary goals. Vulnerability Assessment focuses on internal organizational security, while Penetration Testing focuses on external real-world risk. Vulnerability Assessment (VA) is a rapid automated review of network devices, servers and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage off. Its generally conducted within the network on internal devices and due to its low footprint can be carried out as often as every day.

Penetration Testing (PT or PenTest)is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.

Web Application Penetration Testing is security testing methods for security holes or vulnerabilities in web applications and corporate websites. Due to these vulnerabilities, websites are left open for exploitation.

2. DIFFERENT TYPES OF PENETRATION TESTING

Pen-testers are usually categorized as White Box Pentest, Black Box Pentest, and Grey Box Pentest, depending upon the amount of information made accessible to the Pen-testers.

2.1 White box penetration testing:

In this testing the pen-testers are fully informed about the internal makeup of their target software system.

2.2 Black box penetration testing:

In this testing the pen-testers operate with no internal knowledge of the target.

2.3 Grey box approach to penetration testing:

In this approach, it is a combination of white box and black box where the pen-testers are provided with limited information about the target.

The penetration testing phases that we will discuss here are relevant for all of these approaches.

3. WEB APPLICATION PENETRATION TESTING

Web application penetration testing involves a methodological series of steps aimed at gathering information about the target system, finding vulnerabilities or faults in them,

- Remediation and On-going Support

4. PHASES OF PENETRATION TESTING WEB APPLICATION

4.1 Phase I: Pre-engagement phase of Pen- testing

This is the stage where the logistics and the rules of engagement of the test are discussed. The VAPT providers and the target organization can discuss the legal implications of the exercise. The objective of the test is determined, and the goals of the pen- test are aligned with the specific requirements of a business. You may want to keep certain areas off limits for the pen-testing team; this is the phase to clarify all of that.

This is also the time when the scope of the penetration test is defined.
Determining the scope of the penetration test ensures that both the target and the tester know what to expect from the test. There are certain assets that the pen-testers are allowed to test, those are within the scope of the pen-test, others are not. Similarly, the target organization's security posture is tested for a predetermined set of vulnerabilities, anything out of that set is out of scope for the pen-test. The scope of the pen-test greatly influences all the subsequent penetration testing phases.

4.2 Phase II: Reconnaissance

To simulate a cyber-attack on an application or a network, the pen-tester needs access to information about the target. They gather this information in the reconnaissance stage.
Whether a hacker wants to target an entire network or a single web application, they need to know as much as they can. That is exactly how a pen-tester too approaches the target. The scoping done in the previous phase helps the pen-tester narrow down the recon to increase efficiency.

researching for exploits that will succeed against those faults or vulnerabilities and compromise the web application.

Web Pen Test Steps and Methods

- Information Gathering
- Research and Exploitation
- Reporting and Recommendations

There are two kinds of reconnaissance:

- **Active reconnaissance:** The pen-testers engage directly with the target system to gather information. While this is a more accurate approach to reconnaissance, it makes more noise since the intruder interacts with the system.
- **Passive reconnaissance:** In this mode, the intruder does not interact with the target system and applies different passive strategies instead to gather information. They can try to eavesdrop on network traffic, trace OS foot printing, or internet foot printing.

When it comes to attacking a web application, mapping is an important part of the recon operation. This step helps the attacker to look at all the pieces of application at one place and form an

understanding of how the app works.
An application has many implemented functionalities and understanding them is crucial for the success of the subsequent penetration testing phases.

4.3 Phase III: Discovery

The discovery phase can be divided into two parts:

- Further information gathering
- Vulnerability scan

The first part involves gathering more information about the target network using a bunch of different techniques. Let us talk about a few of them.
Hackers can uncover hostnames and IP information using techniques like DNS interrogation, Inter NIC queries, and network sniffing. Banner grabbing can be used to uncover application and service information.
During an internal test, the tester can uncover system information such as names and shares using NetBIOS enumeration.
The second part consists of testing the

application or the operating system for known vulnerabilities. You can get an automated scan where the system is tested against a vulnerability database. Or you can go for a manual scan where security engineers manually scan the systems. The latter is more suitable for uncovering new and hidden vulnerabilities whereas the former is faster.

4.4 Phase IV: Vulnerability Analysis

You will discover various threat sources during a security scan. It is important to tie each of those threat sources to a vulnerability and then prioritize it depending on the risk it poses to the system.

You need a well-defined and consistent process of analyzing the vulnerabilities in terms of severity and risk. It is the job of a VAPT provider to analyses the vulnerabilities and create a clear picture for you to understand and act upon.

While it is difficult to assign an exact number to a vulnerability, a lot of VAPT companies use a semi quantitative method of rating the vulnerabilities.

The Common Vulnerability Scoring System (CVSS) is a globally accepted method of producing a numerical score based on the severity of vulnerability. The CVSS score helps you rate vulnerability as low, medium, or high in terms of severity. You can prioritize one vulnerability over others depending on these factors, when it comes to remediation, the last one of the Penetrationtesting phases.

The assessment of vulnerabilities is usually performed in line with various security and risk assessment standards such as the Risk Assessment Guide for Information Technology Systems by the National Institute of Standards and Technology (NIST), ISO 27001, HIPAA, and more.

4.5 Phase V: Exploitation and Post Exploitation

The previous phases prepare the stage for the exploitation phase. The goal here is establishing access to a system using the loopholes uncovered in the earlier phases of

Penetration testing. The pen-tester tries to identify an entry point and then look for assets that can be accessed through that.

The pen-testers have to be very careful while conducting this phase to ensure that the business functionalities are not compromised or hindered. Nevertheless, system crashes during penetration testing are very rare.

The post exploitation phase is after the pen-tester has exploited a vulnerability and identified an entry point to the system the next job is to determine the value of that entry point. The questions they ponder upon are

- How much access does the entry point yield?
- How easy is it to maintain access?
- How much time may pass before the breach is spotted?
- What is the degree of harm that the vulnerability may cause?

The exploitation and post exploitation phases help the tester gain access, locate sensitive data, identify communication channels, etc. They can also try and exploit the connection between different systems within the network and expand the breach.

The extent to which a pen-tester may exploit a certain vulnerability is determined by the rules of engagement agreed upon in the pre-engagement stage.

4.6 Phase VI: Reporting and Recommendations

All the previous penetration testing phases contribute to these phases where a VAPT report is created and shared with the client. In the reporting phase, the pen-testers provide detailed information about the vulnerabilities such as,

- The description of the vulnerabilities.
- Ratings according to a common vulnerability scoring system.
- Severity and impact of vulnerability.
- Risk assessment report.
- Video POCs.
- Recommendations for fixing the vulnerabilities.

The quality of a VAPT report determines how quickly and how efficiently you will reproduce and remove the vulnerabilities from your system.

4.7 Remediation and Rescan

The VAPT report consists of step-by-step recommendations for fixing the vulnerabilities. Your developers can follow those recommendations to close the gaps in

your application security. The VAPT company you are partnering with for the security testing should help you at every step of this process.
An ideal remediation phase looks something like this:

- Vulnerabilities are reported with detailed remediation steps.
- There is video based assistance from the security engineers.
- Developers get on a call to discuss the remediation steps when needed.
- Once the vulnerabilities are fixed, the VAPT company should offer rescans to
- identify any security loopholes that might have been left unattended.
-

5. OWASP TOP 10 WEB APPLICATION SECURITY RISKS

5.1 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

5.2 Cryptographic Failures

Many web applications and APIs do not properly protect sensitive data with strong encryption. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data must be encryption at rest and in transit, using a modern (and correctly configured) encryption algorithm.

5.3 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Insecure Design

Pre-coding activities are critical for the design of secure software. The design phase of your development lifecycle should gather security requirements and model threats, and development time should be budgeted to allow for these requirements to be met. As software changes, your team should test assumptions and conditions for expected and
failure flows, ensuring they are still accurate and desirable. Failure to do so will let slip critical information to attackers and fail to anticipate novel attack vectors.

5.4 Security Misconfiguration

Your software is only as secure as you configure it to be. Using ad hoc configuration standards can lead to default accounts being left in place, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

5.5 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

5.6 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

5.7 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure deployment pipeline can introduce the potential for unauthorized access, malicious code, or system compromise.

Lastly, many applications now include auto-

update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations.

5.8 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

5.10. Server-Side Request Forgery

Server-Side Request Forgery (SSRF) flaws occur whenever a web application fetches a remote resource without validating the user- supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

6. DIFFERENT TYPES OF WEB APPLICATION PENETRATION TESTING TOOLS

6.1 Astra's Pentest

Astra Security has been driven by the urge to simplify web application security for users. Astra's Pentest has taken this philosophy home. This web application penetration testing tool comes with great advantages. For instance, you can integrate CI/CD tools with Astra's pentest suite, so whenever there is a code update, it launches an automated scan.
Moreover, you can integrate it with say, Jira or Slack, which means you can assign pentest and remediation-related tasks to your team members without them having access to the suite. Of course, the pentest suite itself allows you to connect with developers and security experts. It is like having an in-house security team, without actually having one.

6.2 NMAP

NMAP is short for Network Mapper. It is an open-source tool that helps you map a network by scanning ports, discovering operating systems, and creating an inventory of devices and the services running on them. It sends differently structured packets for different transport layer protocols which return with IP addresses and other information. You can use this information for Metasploit currently includes nearly 1677 exploits along with almost 500 payloads that include

- Command shell payloads
- Dynamic payloads
- Meterpreter payloads
- Static payloads

The framework also includes listeners, encoders, post-exploitation code, and whatnot.

- Host discovery
- OS fingerprinting
- Service discovery
- Security auditing

You can use the tool for a large network with thousands of devices and ports.

6.3 WireShark

WireShark is another famous open-source tool that you can use for protocol analysis. It allows you to monitor network activities at a microscopic level. It is a growing platform with thousands of developers contributing from across the world.

With WireShark you can perform

- Live capture and offline analysis
- Inspection of hundreds of different protocols
- Browse captured data via GUI
- Decrypt protocols
- Read live data from Ethernet, and a number of other mediums
- Export output to XML, PostScript, CSV, or plain text

WireShark is the industry standard for protocol analysis in many different sectors. If you know what you are doing, it is a great tool to use.

6.4 Metasploit

Metasploit is a Ruby-based open-source framework, used by both ethical hackers and malicious actors to probe systematic vulnerabilities on networks and servers. The Metasploit framework also contains portions of fuzzing, anti-forensic, and evasion tools. It is easy to install and can work on a wide range of platforms regardless of the languages they run on. The popularity and the wide availability of Metasploit among professional hackers make it an important tool for Penetration Testers as well.

6.5 Burp Suite

Burp Suite is a set of penetration testing tools by Portswigger Web Security. It is used by ethical hackers, pen-testers, and security engineers. It is like a one-stop-shop for bug bounty hunters and security researchers. Let us take a look at a few tools included in Burp Suite.

- Spider: It is a web crawler. You can use it to map the target application. It lets you create an inventory of all the endpoints, monitor their functionalities, and look for vulnerabilities.
- Proxy: As explained earlier, a proxy sits between the browser and the internet to monitor, and modify the requests and responses in transit.
- Intruder: It runs a set of values through an input point and lets you analyze the output for success, failure and content length.

These aside the suite includes Repeater, Sequencer, Decoder, Extender, and some other add-on tools.

8. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber-crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber-crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

1. https://portswigger.net/
2. https://tryhackme.com/
3. https://www.hackerone.com/
4. https://medium.com/
5. https://mobile-security.gitbook.io/mobile-security-testing-guide/overview/0x03-verview
6. https://book.hacktricks.xyz/
7. https://www.udemy.com/course/postman-masterclass-and-rest-api-testing/