-------------------------------------------------------------------------------------------An Overview of Penetration Testing

------------------------------------------------------------------------------------------------------------------------------------------

Now a day’s every organization is using the web application and vulnerabilities is also increasing rapidly so By taking advantage attackers and cyber criminals can exploit vulnerabilities and can steal confidential data which will lead to loss of organization confidential data and reputation. Vulnerability Assessment and penetration testing Helps to identify and exploit the vulnerabilities in webaplication and it helps to analyze the effectiveness of security measures impose on system and also helps to get security weakness available in the system. In this process we have to understand and use the different tools that are being using by the attackers. This paper will provide information about vulnerability and pen testing, different steps in VAPT, different free and open source tools available for VAPT process and Over view of vulnerabilities like SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion and Cross Site Request Forgery in web application with remediation

------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Introduction**

Iudgvfj

In purpose of little deeper in the vulnerability assessment and penetration in this paper We have analyzed overview of the penetration

testing process and its limitations and includes various tools which are helpful to conduct VAPT process of these high-risk vulnerabilities like sqlinjection,Local file inclusion, remote file inclusion, cross site request forgery, cross site scription with it remediation.

------------------------------------------------------------------------------------------------------------------------------------------------

Ever since the inception of computers, information security has been a major concern for most organizations. Web application attacks in particular, represent the biggest threats in the organization’s security [1–3]. Verizon [2], reported that in 2016 web application attacks is the main source of data breaches, ranked number 1 with an estimate of over 40 percent of all the data breaches. White Hack Security [6], also reported that web application attacks represent over 40 percent of all the total data breaches in 2015. Web application Usage grew tremendously in the last few decades and it has brought great benefits to the people, however, these benefits are associated with some challenges and one of the most important challenges is that of security. Security in web application refers to the threat which occurs due to flaws in software design, coding, testing and implementation. Web application services are more prone to cyber attacks due to their public access. And web applications are increasingly used to deliver security critical services so they become a valuable target for security attacks. Many web applications interact with back-end database systems, which may store sensitive information (e.g., financial, health), the compromise of web applications would result in breaching an enormous amount of information, leading to severe economical losses, ethical and legal consequences [5,6].

The Web platform is a complex ecosystem composed of large number of components and technologies, including HTTP protocol, web server and server-side application development technologies (e.g., CGI, PHP, ASP), web browser and client-side technologies (e.g., JavaScript, Flash). Web application built and hosted upon such a complex framework faces characteristic challenges postured by the highlights of those components and innovations and the irregularities among them. For developers with insufficient security vulnerabilities knowledge or awareness results in a high rate of web applications sent on the Web is uncovered to security vulnerabilities. According to a report by the Internet Application Security Consortium, around 49% of the internet applications being looked into contain vulnerabilities of tall hazard level and more than 13% of the websites can be compromised totally naturally [4]. A later report [3] uncovers that over 80% of the websites on the Web have had at least one serious Vulnerability.

In purpose of little deeper in the vulnerability assessment and penetration in this paper We have analyzed overview of the penetration testing process and its limitations and includes various tools which are helpful to conduct VAPT process of these high-risk vulnerabilities like sqlinjection,Local file inclusion, remote file inclusion, cross site request forgery, cross site scripting with it remediation.

Penetration testing is different from security functional testing. The security functional testing helps to analyze the correct behavior of the system’s controls while penetration testing determines the different security loopholes and vulnerabilities

This paper is organized as follows: Section

------------------------------------------------------------------------------------------------------------------------------------------

**Related Work (or) Literature Survey**

There has been a lot of research in the field of security testing of web applications.

**Studies carried out in Literature Survey**

Wang Linzhang et al. (2007) [17] focuses on threat model driven approach for security testing. They identify threat as a condition that enables attacker to violate the security policy. Threats are behaviors that an attacker may pose to the system and violate security properties such as authentication, authorization, confidentiality and privacy.

Turpe Sven et al. (2008) [6] mentions about various issues like path traversal, command injection, cross site scripting, content spoofing, SQL injection, LDAP injection.

Avancini Andrea et al. (2011) [1] mentions about the content injection, file injection and cross site scripting attack.

Avancini Andrea et al. (2012) [10] mentions about the issues like cross site scripting vulnerabilities, missing or inadequate validation of input data, disclosure of any sensitive information or hijacking of user session.

Andrea Avancini et al. (2012) [18] discusses about cross site scripting and SQLi vulnerabilities involved with many of the web applications build in java.

Buchler Matthias et al. (2012) [11] mentions about the most critical issue related with the security testing of web applications i.e. cross site scripting attack.

Aileen G. Bacudio.(2011)[12] discuss about the penentration testing of web application and its type

Arunima Jaiswal.(2014)[13] has been dissussed about the challenges and issues in the secure testing of web application

Researcher considers that SQL Injection, Cross Site Scripting, Remote File Inclusion and Local file inclusion are the high-risk vulnerabilities ( Dimitris Mitropoulos; Panagiotis Louridas; Michalis Polychronakis; Angelos D. Keromytis, 2017, ). OWASP also included these threats in Top 10 High Risk of web application. These technical vulnerabilities occurred when the web application processes data without proper filtration or validation.

Reference Links

[1] Security Testing of Web Applications: a Search Based Approach for Cross-Site Scripting Vulnerabilities, Andrea Avancini, Mariano Ceccato , 2011- 11th IEEE International Working Conference on Source Code Analysis and Manipulation.

[6] SUPPORTING SECURITY TESTERS IN DISCOVERING INJECTION FLAWS. Sven T¨urpe, Andreas Poller, Jan Trukenm¨uller, J¨urgen Repp and Christian Bornmann, Fraunhofer-Institute for Secure Information Technology SIT, Rheinstrasse 75,64295 Darmstadt, Germany, 2008 IEEE,Testing: Academic & Industrial Conference - Practice and Research Techniques.

[10] Security Testing of Web Applications: A Research Plan by Andrea Avancini,Fondazione Bruno Kessler, 2012 IEEE,ICSE 2012, Zurich, Switzerland , Doctoral Symposium.

[11] Semi-Automatic Security Testing of Web Applications from a Secure Model by Matthias Buchler,Johan Oudinet,Alexander Pretschner, Karlsruhe Institute of Technology, 2012 IEEE Sixth International Conference on Software Security and Reliability.

[17] A Threat Model Driven Approach for Security Testing. Linzhang Wang, Department of Computer Science, Nanjing University, Eric Wong, Department of Computer Science, University of Texas at Dallas, Dianxiang Xu, Department of Computer Science, North Dakota State University. Third International Workshop on Software Engineering for Secure Systems (SESS'07). 2007 IEEE.

[18] Grammar Based Oracle for Security Testing of Web Applications by Andrea Avancini and Mariano Ceccato, Fondazione Bruno Kessler, Trento, Italy. 2012 IEEE,AST 2012, Zurich, Switzerland.

[12] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones. (2011). AN OVERVIEW OF PENETRATION TESTING., International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[13] Arunima Jaiswal ,Gaurav Raj ,Dheerendra Singh (2014),Security Testing of Web Applications: Issues and Challenges , International Journal of Computer Applications (0975 – 8887) Volume 88 – No.3, February 2014

------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------

Penentration testing

A **penetration test**, is also familiar with **pen test** or **ethical hacking**, It is a type of authorized cyber attack performed on system to evaluate security poster of system which helps to trace out both vulnerabilities and back boors that helps attacker and malicious users to gain un authorized access to system .the different security issues revealed during the penetration test should be reported to system administrators or developers with impact of vulnerability and countermeasure to reduce risk. Penetration testing is a core tool for analysing the security of IT systems.

For penetration testing different standards and methodologies exist which includes the open Web Application Security Project(OWASP) Testing Guide ,the Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), the NIST Special Publication 800-115, the Information System Security Assessment Framework (ISSAF).

The Vulnerabilities in system can incur due to multiple reasons like Flaws in the design of hardware and software, using of less secure network, human errors, network misconfigurations, using unpathed software or operating system etc.so by using the vulnerability assessment the vulnerabilities can be traced out and can be improved in order to secure the system

The goals of a penetration test vary depending on the type of approved activity for any given engagement with the primary goal focused on finding vulnerabilities that could be exploited by a nefarious actor and informing the client of those vulnerabilities along with recommended mitigation strategies[10] and after any modification in the system the penetration testing should to performed.

--------------------------------------------------------------------------------------------------------

[10] Patrick Engebretson, The basics of hacking and penetration testing, Elsevier, 2013

--------------------------------

With cyber attacks becoming the norm, it is more important than ever before to undertake regular [vulnerability scans and penetration testing](http://www.itgovernance.co.uk/penetration-testing-packages.aspx) to identify vulnerabilities and ensure on a regular basis that the cyber controls are working.

--------------------------------

In the present world the

---------------------------  
   
Geraint Williams, Senior Consultant at cyber security experts [IT Governance,](http://www.itgovernance.co.uk/) explains: “Vulnerability scanning examines the exposed assets (network, server, applications) for vulnerabilities – the down side of a vulnerability scan is that false positives are frequently reported. False positives may be a sign that an existing control is not fully effective, i.e. sanitising of application input and output, especially on web applications.”  
   
Penetration testing looks at vulnerabilities and will try and exploit them. The testing is often stopped when the objective is achieved, i.e. when an access to a network has been gained - this means there can be other exploitable vulnerabilities not tested.”  
   
Organisations need to conduct regular testing of their systems for the following key reasons:

* To determine the weakness in the infrastructure (hardware), application (software) and people in order to develop controls
* To ensure controls have been implemented and are effective – this provides assurance to information security and senior management
* To test applications that are often the avenues of attack (Applications are built by people who can make mistakes despite best practices in software development)
* To discover new bugs in existing software (patches and updates can fix existing vulnerabilities, but they can also introduce new vulnerabilities)

Geraint adds: “If people are attacked through social engineering this bypasses the stronger perimeter controls and exposes less protected internal assets.  
   
The worst situation is to have an exploitable vulnerability within infrastructure, application or people that you are not aware of, as the attackers will be probing your assets even if you are not. Breaches, unless publicised by the attackers, can go undetected for months.”  
   
[Vulnerability scanning and penetration testing](http://www.itgovernance.co.uk/penetration-testing-packages.aspx) can also test an organisations ability to detect intrusions and breaches. Organisations need to scan the external available infrastructure and applications to protect against external threats. They also need to scan internally to protect against insider threat and compromised individuals. Internal testing needs to include the controls between different security zones (DMZ, Cardholder data environment, SCADA environment etc.) to ensure these are correctly configured.

Cybersecurity is of utmost importance, especially in today’s world. Our world is connected through a fragile network that deals with internet banking and government infrastructure as DoS attacks, website defacement, and other cyber-attacks are on the rise.

Global cybercrime costs saw an increase of approximately 27.4% in the last year alone. Of late, 85% of the companies in the UK and the U.S. have fallen victim to phishing attacks (9 out of 10 phishing emails carried malicious ransomware). The number of newly evolved ransomware attacks in 2017 is over 4 times more than in 2016. An organization is hit with a ransomware attack every 40 seconds; at least 71% of these attacks are successful. The time taken, on an average, for a company to resolve even one of these attacks is 23 days.

**Why Are Penetration Tests Important?**

1. They can give security personnel real experience in dealing with an intrusion. A penetration test should be done without informing staff, and will allow an organisation to test whether its security policies are truly effective. A penetration test can be imagined much like a fire drill.
2. It can uncover aspects of security policy that are lacking. For example, many security policies give a lot of focus to preventing and detecting an attack on an organisation's systems, but neglect the process of evicting an attacker. You may uncover during a penetration test that whilst your organisation detected attacks, that security personnel could not effectively remove the attacker from the system in an efficient way before they caused damage.
3. They provide feedback on the most at risk routes into your company or application. Penetration testers think outside of the box, and will try to get into your system by any means possible, like a real world attacker would. This could reveal lots of major vulnerabilities your security or development team never considered. The reports generated by penetration tests provide you with feedback on prioritising any future security investment.
4. Penetration testing reports can be used to help train developers to make fewer mistakes. If developers can see how an outside attacker broke into an application or part of an application they helped develop, they will be more motivated to improve their security education, and avoid making similar errors in the future.

## Uncover Hidden System Vulnerabilities Before the Criminals Do

The most surefire way to measure your security level is by studying how it can be hacked. A penetration test offers an ability to safely test your system’s resistance to external hacking attempts. It models the actions of a potential intruder by trying to exploit the vulnerabilities caused by code mistakes, software bugs, insecure settings, service configuration errors and/or operational weaknesses.

The major difference between a penetration test and a real hacking experience rests in its safe and controlled manner. It simulates a real attack scenario and exploits the vulnerabilities only to showcase the potential harm of a malicious hacking attempt. Moreover, the client company can pre-define the scope and timing of a penetration test and is informed beforehand about any active exploitation of vulnerabilities in its IT infrastructure.

Organizations usually conduct penetration tests right after the deployment of new infrastructure and applications or after the introduction of major changes to their infrastructure (e.g. changes in firewall rules, firmware updates, patches and software upgrades). This service can help them identify and validate potential security loopholes in their IT systems before cybercriminals can make use of them and successfully bring new products to the market.

## Save Remediation Costs and Reduces Network Downtime

The process of recovering from a security breach can cost your business thousands or even millions of dollars including expenditures on customer protection programs, regulatory fines and loss of business operability. A [recent study](https://safeatlast.co/blog/data-breach-statistics/) found that the average cost of a data breach globally in 2018 is **$3.86 million**, which is 6.4% more compared to the last year’s result. Therefore, getting everything back on track and running will require substantial investments, advanced security measures and weeks to recover.

A penetration test is a proactive solution for identifying the biggest areas of weakness in your IT systems and for preventing your business from serious financial and reputational losses. However, to ensure your business continuity, you need to conduct regular penetration tests at least once or twice a year.

Professional security analysts can advise you on the minimum frequency of penetration tests required for your specific business domain and IT infrastructure. Additionally, they can advise on the necessary procedures and investments aimed at building a more secure environment within your organization.

## Develop Efficient Security Measures

The summarized results of a penetration test are essential for assessing the current security level of your IT systems. They can provide your company’s top management with insightful information about identified security gaps, their actuality and their potential impact on the system’s functioning and performance. An experienced penetration tester will also present you with a list of recommendations for their timely remediation as well as help you develop a reliable information security system and prioritize your future cybersecurity investments.

However, before ordering a pentest, make sure the company uses world-leading methodologies, such as **ISECOM OSSTMM3**, [**NIST**](https://www.tripwire.com/solutions/solutions-by-industry/government/) **SP800-115, PTES** and **OWASP,**and that its specialists are certified and competent. Even though a penetration test may involve the use of automated tools, the focus is still on the manual skills, professional knowledge and experience of penetration testers.

## Enable Compliance with Security Regulations

Undoubtedly, penetration testing plays a crucial role in terms of protecting your business and its valuable assets from potential intruders. However, the benefits of a pentest extend far beyond network and data security.

Regular pentests can help you comply with security regulations dictated by the leading security standards, such as [**PCI**](https://www.tripwire.com/solutions/compliance-solutions/pci-dss-compliance/)**,** [**HIPAA**](https://www.tripwire.com/solutions/compliance-solutions/hipaa-compliance/)and **ISO 27001,**and avoid the heavy fines associated with non-compliance. These standards require company managers and system owners to conduct regular penetration tests and security audits with the help of professional security analysts.

For instance, the [PCI DSS](https://www.tripwire.com/solutions/compliance-solutions/pci-dss-compliance/) (Payment Card Industry Data Security) standard requires organizations that handle large volumes of transactions to conduct both annual and regular penetration testing (after any system changes). What’s more, the detailed reports generated from penetration tests can help organizations enhance their [security controls](https://www.tripwire.com/products/tripwire-file-integrity-monitoring/) and illustrate ongoing due diligence to assessors.

## Preserve Company’s Image and Customer Loyalty

Security attacks may compromise your sensitive data, which leads to the loss of trusted customers and serious reputational damages. Penetration testing can help you avoid costly security breaches that put your organization’s reputation and customers’ loyalty at stake. Moreover, a pen test may grow in time and complexity if the system requires additional scope. It may be also conducted in combination with [vulnerability scanning](https://www.tripwire.com/products/tripwire-ip360/) to provide even more meaningful insights on vulnerabilities and potential breach points in your IT infrastructure.

Overall, only penetration testing can make a realistic assessment of your company’s “health” and its resistance to cyber attacks. A pen test can showcase how successful or unsuccessful a malicious attack on your company’s IT infrastructure can be. Moreover, it can help you prioritize your security investments, comply with industry regulations and develop efficient defensive mechanisms so that your business will be protected from intruders in the long run.

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Types of pentesting

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Penetration Testing Strategies**

* **Black box tests** are performed with [no prior knowledge](https://biztechmagazine.com/article/2018/08/top-penetration-testing-tools-and-types-safeguard-against-cybersecurity-threats-perfcon) of the tested network ecosystem. A black box test is an objective assessment of security as seen from outside the network by third parties. It’s a test of software security operations, versus a white box test (which is structural).  
    
  Examples of black box testing include functional testing, non-functional testing, and [regression testing](https://smartbear.com/learn/automated-testing/what-is-regression-testing/). However, a standard black box test likely wouldn’t involve a tactic like a denial-of-service (DoS) attack, which could cause severe damage to the network.
* **White box tests** are performed with full knowledge of the internal design and structure of the tested ecosystem.  
    
  White box testing is used to logic test software for gaps in code and security, instead of behavior testing against malicious outside agents. Path testing, loop testing, and condition testing are all white box.
* **Grey box tests** combine aspects of white and black box testing into one. For this variety of test, experts will assess the level of software security seen by a legitimate user with an account.

## Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

### Advantages of Black Box Penetration Testing

It has the following advantages −

* Tester need not necessarily be an expert, as it does not demand specific language knowledge
* Tester verifies contradictions in the actual system and the specifications
* Test is generally conducted with the perspective of a user, not the designer

### Disadvantages of Black Box Penetration Testing

Its disadvantages are −

* Particularly, these kinds of test cases are difficult to design.
* Possibly, it is not worth, incase designer has already conducted a test case.
* It does not conduct everything.

## White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

### Advantages of White Box Penetration Testing

It carries the following advantages −

* It ensures that all independent paths of a module have been exercised.
* It ensures that all logical decisions have been verified along with their true and false value.
* It discovers the typographical errors and does syntax checking.
* It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

## Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

### Advantages of Grey Box Penetration Testing

It has the following advantages −

* As the tester does not require the access of source code, it is non-intrusive and unbiased
* As there is clear difference between a developer and a tester, so there is least risk of personal conflict
* You don’t need to provide the internal information about the program functions and other operations

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Stages in pen testing

### Scoping

### Reconnaissance

[**Threat Modeling & Vulnerability Identification**](https://cyberx.tech/penetration-testing-phases#numthree)

[**Exploitation**](https://cyberx.tech/penetration-testing-phases#numfour)

[**Post-Exploitation**](https://cyberx.tech/penetration-testing-phases#numfive)

[**Reporting**](https://cyberx.tech/penetration-testing-phases#numsix)

[**Resolution & Re-Testing**](https://cyberx.tech/penetration-testing-phases/#numseven)

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Web penetration pen test**

**Pentesting is the most commonly used methodology for web application. The different standards available for web application pretesting are** [OWASP](https://www.owasp.org/index.php/Main_Page)**(Open Web Application Security Project),**[OSSTMM](http://www.isecom.org/research/)**(Open Source Security Testing Methodology Manual),**PTF**(Penetration Testing Framework),**[ISSAF](http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf)**(Information Systems Security Assessment Framework),**[PCIDSS](https://www.pcisecuritystandards.org/pci_security/)**(Payment Card Industry Data Security Standard)etc.Owasp is the the mainly used standard for testing the web application.Owasp is the open source community which will provide the testing guidelines and checklist for testing the web application.the owasp 2017 top 10 vunlerabiites areshown in table 1**

|  |
| --- |
| OWASP TOP 10 |
| A1:2017-injection |
| A2:2017-Broken Authentication |
| A3:2017-Sensitive Data Exposure |
| A4:2017-Xml External Entities(XXE) |
| A5:2017-Broken Access control |
| A6:2017-Security misconfiguration |
| A7:2017-Cross-site Scripting |
| A8:2017-Insecure Deserialization |
| A9:2017-Using components with known Vulnerabilities |
| A10:2017-Insufficient logging and Monitoring |

**Table1.** OWASP Top Ten Vulnerability 2017 [10]

Injection

Broken Authentication

Sensitive Data Exposure

Xml External Entities(XXE)

Broken Access control

Security misconfigurations

Cross-site Scripting

Insecure Deserialization

Using components with known Vulnerabilities

Insufficient logging and Monitoring

[10] The Open Web Application Security Project: The Ten Most Critical Web Application Security Vulnerabilities, “https://www.owasp.org/index.php/Main\_Page:OWASP\_Top\_Ten\_Project”

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Major Web application vulnerabilities with remediation

Sql injection

Cross site Scripting

Local File inclusion

Remote File Inclusion

Cross Site Request Forgery

Broken Access Control

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Web application pen testing tools

Burpsuite

Nmap

Zenmap

Sqlmap

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Conclusion

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

references

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------