Vulnerability Assessment & Penetration Testing

A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of system's security policy or, in other words, the possibility for intruders (hackers) to get unauthorized access.

What is Vulnerability Assessment?

Vulnerability Assessment is a software testing technique performed to evaluate the sudden increase of risks involved in the system in order to reduce the probability of the event.

It depends on two mechanisms:-

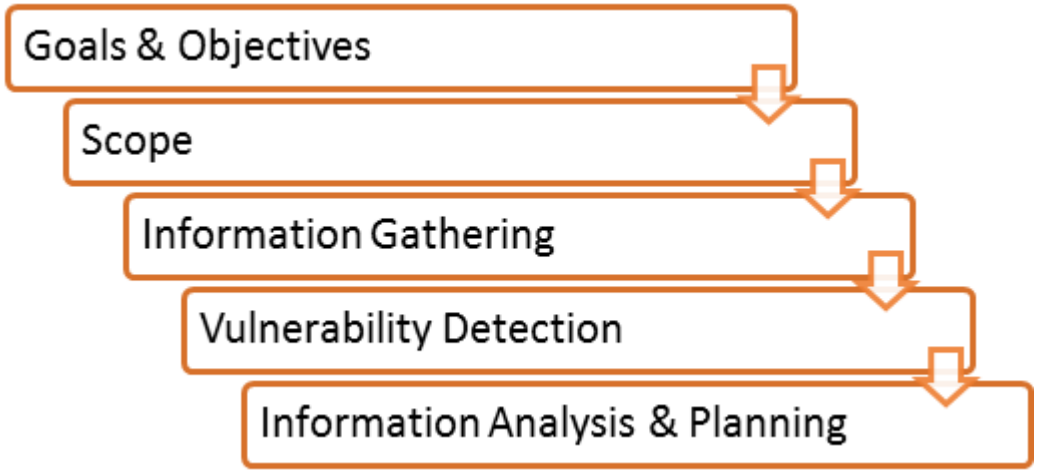
1. Vulnerability Assessment

2. Penetration Testing

Why do Vulnerability Assessment

- It is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

The process of Vulnerability Assessment



1. **Goals& Objectives: -** Defines goals and objectives of Vulnerability Analysis

2. **Scope**: - While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.

The following are the three possible scopes exist:

- Black Box Testing: - Testing from an external network with no prior knowledge of the internal network and systems.
- Grey Box Testing: - Testing from either external or internal networks, with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- White Box Testing: - Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

3. **Information Gathering**: - Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing, and White Box Testing

4. **Vulnerability Detection**: -In this process, vulnerability scanners are used, it will scan the IT environment and will identify the vulnerabilities.

5. **Information Analysis and Planning**: - It will analyze the identified vulnerabilities, to devise a plan for penetrating into the network and systems.

Vulnerability Methodologies

1. **Setup:**

- Begin Documentation
- Secure Permission
- Update Tools
- Configure Tools

2. **Test Execution:**

- Run the Tools
- Run the captured data packet (A packet is the unit of data that is routed between an origin and the destination. When any file (e-mail message, HTML file, Uniform Resource Locator(URL) request, etc. ..) is sent from one place to another on the internet, the TCP layer of TCP/IP divides the file into a number of "chunks" for efficient routing, and each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packet. When they have all arrived, they will be reassembled into the original file by the TCP layer at the receiving end. , while running the assessment tools

3. **Vulnerability Analysis:**

- Defining and classifying network or System resources.
- Assigning priority to the resource(Ex: - High, Medium, Low)
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritize problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

5. **Reporting**

6. **Remediation:**

- The process of fixing the vulnerabilities.
- For every vulnerability

Types of a vulnerability scanner

1. **Host Based**

- Identifies the issues in the host or the system.
- The process is carried out by using host-based scanners and diagnose the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.

2. **Network-Based**

- It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners.

3. **Database-Based**

- It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: - Injecting SQL statements into the database by the malicious users, which can read the sensitive data's from the database and can update the data in the Database.)

Vulnerability Testing Methods

Active Testing

- Inactive Testing, a tester introduces new test data and analyzes the results.

- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.
- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive Testing

- Passive testing, monitoring the result of running software under test without introducing new test cases or data

Network Testing

- Network Testing is the process of measuring and recording the current state of network operation over a period of time.
- Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.
- We need to Test the following Network Characteristics:-

1. Utilization levels

2. Number of Users

3. Application Utilization

Distributed Testing

- Distributed Tests are applied for testing distributed applications, which means, the applications that are working with multiple clients simultaneously. Basically, testing a distributed application means testing its client and server parts separately, but by using the distributed testing method, we can test them all together.
- The test parts will interact with each other during the Test Run. This makes them synchronized in an appropriate manner. Synchronization is one of the most crucial points in distributed testing.

Web Application Testing

I always love to share practical knowledge, which in a case can be useful to several users in their career life. This is quite a lengthy article, so sit back and get relaxed to get the most out of it.

Web testing checklists

1) Functionality Testing
2) Usability testing
3) Interface testing
4) Compatibility testing
5) Performance testing
6) Security testing

#1) Functionality Testing
Test for – all the links in web pages, database connection, forms used for submitting or getting information from the user in the web pages, Cookie testing etc.

Check all the links:

- Test the outgoing links from all the pages to the specific domain under test.
- Test all internal links.
- Test links jumping on the same pages.
- Test links used to send email to admin or other users from web pages.
- Test to check if there are any orphan pages.
- Finally, link checking includes, check for broken links in all above-mentioned links.

Test forms on all pages:
Forms are an integral part of any website. Forms are used for receiving information from users and to interact with them. So what should be checked in these forms?

- First, check all the validations on each field.
- Check for default values of the fields.
- Wrong inputs in the forms to the fields in the forms.
- Options to create forms if any, form delete, view or modify the forms.

Let’s take an example of the search engine project currently I am working on, in this project we have advertiser and affiliate signup steps. Each sign-up step is different but its dependent on the other steps.

So sign up flow should get executed correctly. There are different field validations like email Ids, User financial info validations etc. All these validations should get checked in manual or automated web testing.

Cookies Testing:
Cookies are small files stored on the user machine. These are basically used to maintain the session- mainly the login sessions. Test the application by enabling or disabling the cookies in your browser options.

Test if the cookies are encrypted before writing to the user machine. If you are testing the session cookies (i.e. cookies that expire after the session ends) check for login sessions and user stats after the session ends. Check effect on application security by deleting the cookies. (I will soon write a separate article on cookie testing as well)

Validate your HTML/CSS:
If you are optimizing your site for Search engines then HTML/CSS validation is the most important one. Mainly validate the site for HTML syntax errors. Check if the site is crawlable to different search engines.

Database testing:
Data consistency is also very important in a web application. Check for data integrity and errors while you edit, delete, modify the forms or do any DB related functionality.

Check if all the database queries are executing correctly, data is retrieved and also updated correctly. More on database testing could be a load on DB, we will address this in web load or performance testing below.

In testing the functionality of the websites the following should be tested:
Links
i. Internal Links
ii. External Links
iii. Mail Links
iv. Broken Links
Forms
i. Field validation
ii. Error message for wrong input
iii. Optional and Mandatory fields
Database
Testing will be done on the database integrity.

#2) Usability Testing
Usability testing is the process by which the human-computer interaction characteristics of a system are measured, and weaknesses are identified for correction.

- Ease of learning
- Navigation
- Subjective user satisfaction
- General appearance

Test for navigation:
Navigation means how a user surfs the web pages, different controls like buttons, boxes or how the user uses the links on the pages to surf different pages.

Usability testing includes the following:

- The website should be easy to use.
- Instructions provided should be very clear.
- Check if the instructions provided are perfect to satisfy its purpose.
- The main menu should be provided on each page.
- It should be consistent enough.

Content checking:

Content should be logical and easy to understand. Check for spelling errors. Usage of dark colors annoys the users and should not be used in the site theme.

You can follow some standard colors that are used for web page and content building. These are the commonly accepted standards like what I mentioned above about annoying colors, fonts, frames etc.

Content should be meaningful. All the anchor text links should be working properly. Images should be placed properly with proper sizes.

These are some of the basic important standards that should be followed in web development. Your task is to validate all for UI testing.

Other user information for user help:

Like search option, sitemap also helps files etc. The sitemap should be present with all the links in websites with a proper tree view of navigation. Check for all links on the sitemap.

“Search on the site” option will help users to find content pages that they are looking for easily and quickly. These are all optional items and if present they should be validated.

#3) Interface Testing

In web testing, the server side interface should be tested. This is done by verifying that communication is done properly. Compatibility of the server with software, hardware, network, and the database should be tested.

The main interfaces are:

- Web server and application server interface
- Application server and Database server interface.

Check if all the interactions between these servers are executed and errors are handled properly. If database or web server returns an error message for any query by application server then application server should catch and display these error messages appropriately to the users.

Check what happens if the user interrupts any transaction in-between? Check what happens if the connection to the web server is reset in between?

#4) Compatibility Testing

Compatibility of your website is a very important testing aspect. See which compatibility test to be executed:

- Browser compatibility
- Operating system compatibility
- Mobile browsing
- Printing options

Browser compatibility:
In my web-testing career, I have experienced this as the most influencing part of web site testing.
Some applications are very dependent on browsers. Different browsers have different configurations and settings that your web page should be compatible with.
Your website coding should be a cross-browser platform compatible. If you are using java scripts or AJAX calls for UI functionality, performing security checks or validations then give more stress on browser compatibility testing of your web application.

Test web application on different browsers like Internet Explorer, Firefox, Netscape Navigator, AOL, Safari, Opera browsers with different versions.

OS compatibility:
Some functionality in your web application is that it may not be compatible with all operating systems. All new technologies used in web development like graphic designs, interface calls like different API's may not be available in all Operating Systems.

Hence test your web application on different operating systems like Windows, Unix, MAC, Linux, Solaris with different OS flavors.

Mobile browsing:
We are in the new technology era. So in future Mobile browsing will rock. Test your web pages on mobile browsers. Compatibility issues may be there on mobile devices as well.

Printing options:
If you are giving page-printing options then make sure fonts, page alignment, page graphics etc., are getting printed properly. Pages should fit the paper size or as per the size mentioned in the printing option.

#5) Performance testing
The web application should sustain to heavy load. Web performance testing should include:

- Web Load Testing
- Web Stress Testing

Test application performance on different internet connection speed.

Web **load testing**: You need to test if many users are accessing or requesting the same page. Can system sustain in peak load times? The site should handle many simultaneous user requests, large input data from users, simultaneous connection to DB, heavy load on specific pages etc.
Web Stress testing: Generally stress means stretching the system beyond its specified limits. Web stress testing is performed to break the site by giving stress and its checked as for how the system reacts to stress and how it recovers from crashes. Stress is generally given on input fields, login and sign up areas.
In web performance, testing website functionality on different operating systems and different hardware platforms is checked for software and hardware memory leakage errors.

Performance testing can be applied to understand the web site's scalability or to benchmark the performance in the environment of third-party products such as servers and middleware for potential purchase.

Connection Speed
Tested on various networks like Dial-Up, ISDN etc.
Load
i. What is the no. of users per time?
ii. Check for peak loads and how the system behaves
iii. A large amount of data accessed by the user
Stress
i. Continuous Load
ii. Performance of memory, CPU, file handling etc..

#6) Security Testing
Following are some of the test cases for web security testing:

- Test for TOP 10 OWASP
- Test by pasting internal URL directly into the browser address bar without login. Internal pages should not open.
- If you are logged in using username and password and browsing internal pages then try changing URL options directly. I.e. If you are checking some publisher site statistics with publisher site ID= 123. Try directly changing the URL site ID parameter to different site ID which is not related to the logged in user. Access should be denied for this user to view others stats.
- Try some invalid inputs in input fields like login username, password, input text boxes etc. Check the system's reaction to all invalid inputs.
- Web directories or files should not be accessed directly unless they are given download option.
- Test the CAPTCHA for automating script logins.
- Test if SSL is used for security measures. If it is used, the proper message should get displayed when user switch from non-secure HTTP:// pages to secure HTTPS:// pages and vice versa.
- All transactions, error messages, security breach attempts should get logged in log files somewhere on the web server.

The primary reason for testing the security of a web is to identify potential vulnerabilities and subsequently repair them.

• Network Scanning
• Vulnerability Scanning
• Password Cracking
• Log Review
• Integrity Checkers
• Virus Detection

Conclusion

Vulnerability Testing depends on two mechanisms namely Vulnerability Assessment and Penetration Testing. Both these tests differ from each other in strength and the tasks that they perform. However, to achieve a comprehensive report on Vulnerability Testing, the combination of both procedures is recommended.