Penetration Testing Project

Preparing Penetration Testing Project Plan for IT of E-commerce company “Easy buy online”.

Date- December,2020

Name-Deepak Rathour

Organization- 4N6

Project No.1

AIM: The aim of this project plan is to find weakness in computer and network Infrastructure. To achieve the desired results, we need to Include following activities:

- Vulnerability assessment.
- Policy Check.
- Security controls.
- Documentations
- Security Audits.

Scope: The very first thing is to get our target. We should know about our target. In our case its E-commerce company "Easy buy online".

The work is done following phases

- Planning Phase.
- Information Gathering and Analysis Phase.
- Conducting Assessment (Asset Value, Define Assets).
- Security Controls.
- Policies.
- Documentation and Review.
- Penetration testing Report writing.

Planning Phase: Its one of the important phases while preparing. Beginning of plan what are going to do is important.

In our case its E-commerce company "Easy buy online". We need to know the environment of company plan certain things. what operation we going to perform. Tools used everything need to plan first according to environment and Infrastructure used.

Information Gathering and Analysis Phase: In this phase we will do some field work. Get to know about company. Its assets, working style, getting to know about infrastructure. We design a blueprint of scenario, from endpoint user to the servers of company, Network topology, Firewalls used, so we can define the weakness.

Conducting Assessment: This is the main phase of this process. Conducting Assessment is like conducting Vulnerability Assessment. To be short and to the point, vulnerability assessment is responsible for highlighting security weaknesses in computer systems, applications (web, mobile, etc.), and network infrastructures. It offers an organization a clearer understanding of their network environment and provides the information on the security flaws in it. The primary goal of network vulnerability assessment is to reduce the probability that cybercriminals will find the weaknesses in your network and exploit them, thus causing DDoS or stealing your sensitive data.

Network vulnerability assessment is carried out to superficially identify main problems due to which the organization would not be able, for example, to meet security standards (Health Insurance Portability and Accountability Act (HIPAA) if it concerns the healthcare industry,

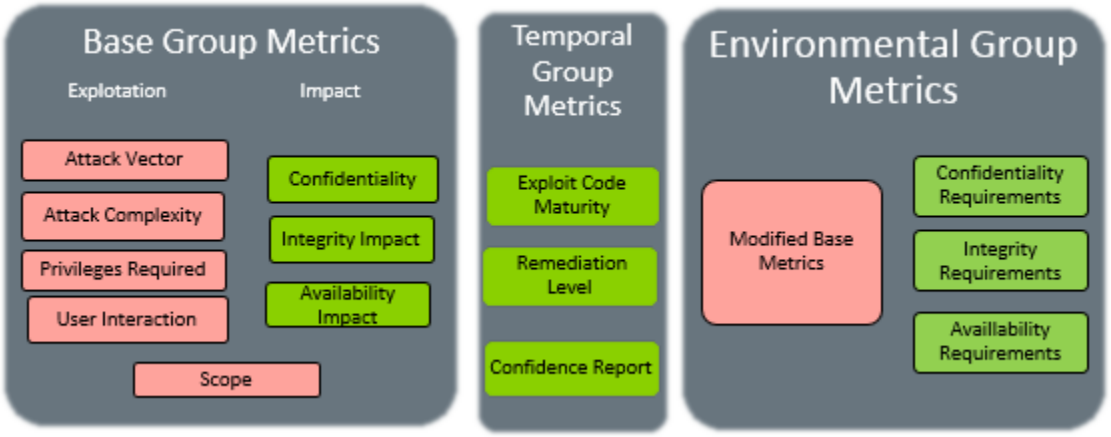
Payment Card Industry Data Security Standard (PCI DSS) if it concerns banking and finance) and carry out their business operations.

For E-commerce company both these standards are important. These standard makes work hard for attacker, and easy for defenders.

The tasks of vulnerability assessment are the following:

- Identification, quantification and ranking of vulnerabilities found in network infrastructure, software and hardware systems, applications.
- Explaining the consequences of a hypothetical scenario of the discovered security 'weakness 'holes', 'backdoors''.
- Developing a strategy to tackle the discovered threats.
- Providing recommendations to improve a company's security posture and help eliminate security risks.

CVSS: common vulnerability scoring system made work easy for vulnerability assessors. Its new latest version cvss3.1 has many features according to the vulnerabilities.



CVSS Score	Severity Level	ASV Scan Result	Guidance
7.0 through 10.0	High Severity	**Fail**	To achieve a passing ASV scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report(s) that shows a passing ASV scan).
4.0 through 6.9	Medium Severity	**Fail**	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical, until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	**Pass**	While passing ASV scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

According to the cvss score vulnerability is defined in three types according the nature of their impact: low, medium, high.

In our target 'Easy buy online' we must access and treat the vulnerability in the following above-mentioned criteria. High severity vulnerabilities must be treated on priority.

Security controls. In this phase we check whom has access to which resources, for example we check whether an employee has access to administrators account or whether an employee has permissions that does not need or require to give to normal employee.

1. The best practice method for security control is Least privilege i.e., Principle of Least privilege.
2. Multi Factor Authentication: Password, username, and Identity cards.
3. Biometrics Scans are the important security scan for organizations, whom has authority to access the resources.

Policies: In this phase we need to check whether the policies are applied according to the prospective of security or not and go through the documentations what are configuration and find loopholes to get weakness.

Documentation and Review. In this phase we need to write documentation of everything the process done, and the steps taken according to time interval.

For example: we access a system, what resources we used, and for what time interval all this need to be documented well. OS forensic triage software helps regarding this and during audits.

Penetration Testing Report writing: In this report we need to write a report on functions we performed, tools we used while pen testing, test cases used etc.

Key points to consider before writing a penetration testing –

- Identify and define the goals of penetration testing.
- Define the area for penetration testing.
- Understand plausible impacts.
- Draft the testing process and related techniques.

Following is the typical content of a penetration testing report −

Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows server information

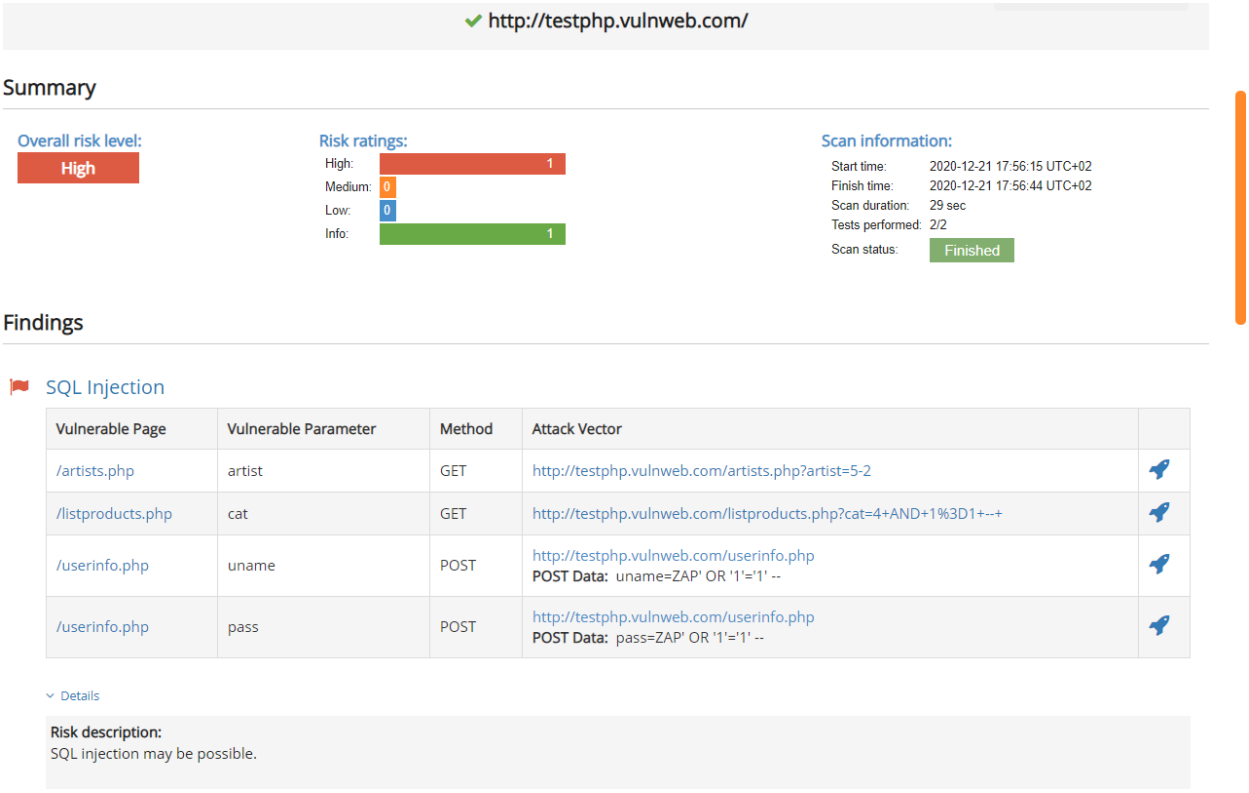
Penetration Testing Report

Phase 1: Information Gathering: In this step I find the website that is vulnerable to sql injection. I found the website that is vulnerable to sql injection: Site: http://testphp.vulnweb.com

I checked this website whether sql injection possible on this site or not.

I used online vulnerability tool

And its result are as follows:



As we can clearly Risk description: SQL Injection may be possible.

We also found which pages are vulnerable to attack.

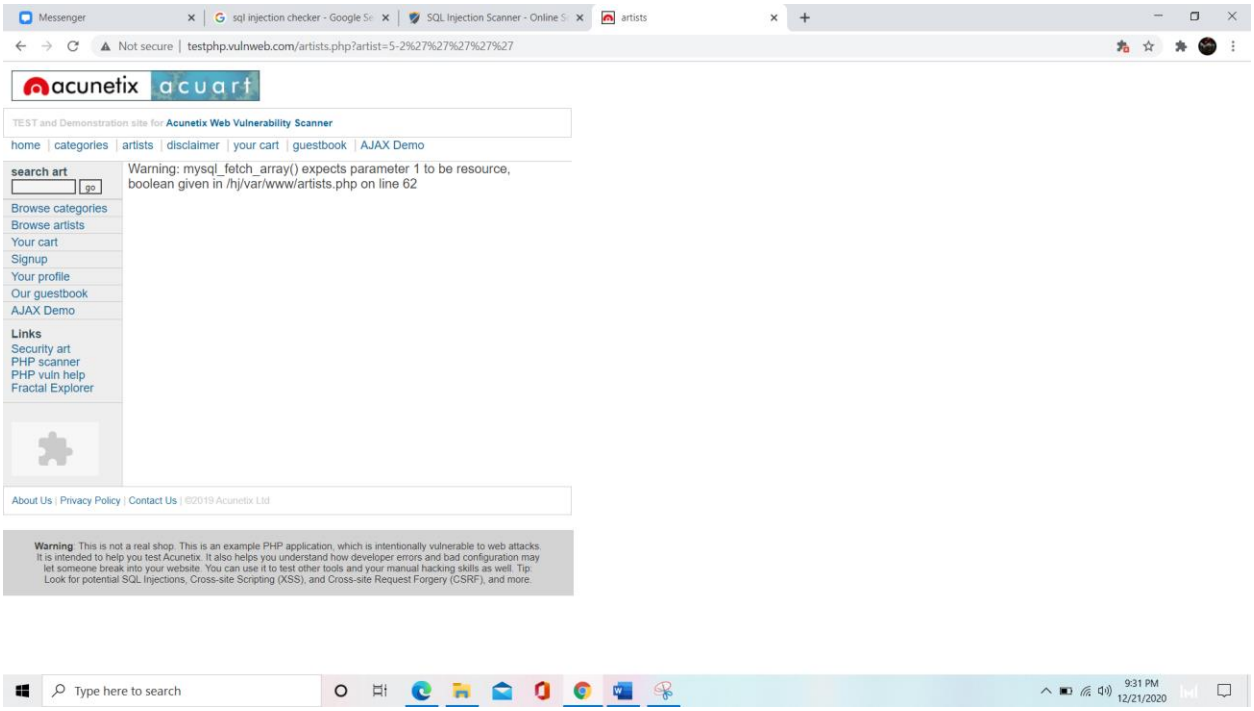
Next Step visiting to vulnerable page and finding error.

http://testphp.vulnweb.com/artists.php?artist=5-2

Here error means success

http://testphp.vulnweb.com/artists.php?artist=5-2%27%27%27%27%27

As we can see in Screenshot:



Vulnerability type: SQL injection.

Now we can easily exploit the database and find any credentials.

This type of Vulnerabilities is harmful for any organization.

Data I found using Light Scan are as follows:

Light spider results: 11 dynamic URLs of total 25 URLs crawled

METHOD	URL	PARAMS
GET	/listproducts.php	cat=2
GET	/listproducts.php	cat=3
GET	/listproducts.php	cat=4
POST	/userinfo.php	uname=ZAP&pass=ZAP
POST	/search.php?test=query	searchFor=ZAP&goButton=go
GET	/showimage.php	file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
POST	/guestbook.php	name=anonymous+user&text=&submit=add+message
GET	/artists.php	artist=3
GET	/artists.php	artist=2
GET	/listproducts.php	cat=1
GET	/artists.php	artist=1

Recommendation:

- Do not trust client-side input, even if there is client side validation in place.
- In general, type check all data on the server side.

1. If the application uses JDBC, use Prepared Statement or Callable Statement, with parameters passed by '?'
2. If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

- If database Stored Procedures can be used, use them.
- Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!
- Do not create dynamic SQL queries using simple string concatenation.
- Escape all data received from the client.
- Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.
- Apply the principle of least privilege by using the least privileged database user possible.
- Avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.
- Grant the minimum database access that is necessary for the application.