Ethical hacking

A Project Report for Summer Industrial Training

Submitted by

Mani Kant

in partial fulfillment for the award of the degree of

B.tech

In

Computer Science and Engineering

Heritage Institute Of Technology

At

INTERNSHALA

Index

Introduction:

Hacking is the art or technique of finding and exploiting a security loophole in an infrastructure like a website, a software, a computer, or even a human being, and the artist is called a hacker.
Vulnerability is a flaw in a system that leaves it open to attack. It is a security loopholes or weak entry point in the system. In technical terms, a loophole can be referred to a part of a system which is not properly defined or secured and hence can be exploited to cause unintended things in the system.

Unethical Hacking :

When a hacker uses his knowledge to steal from or cause damage to other people, it is known as Unethical Hacking. Like stealing, unethical hacking is also a crime and if caught, the thief will be arrested and would be tried in court.

Ethical Hacking :

When the hacker helps organisations or individuals with finding security loopholes and fixing them with their permission, it is referred to as ethical hacking. And this is legal because you take permission from the system owner and your motive is not to cause harm or steal, but to secure the system.

Types of Hacker :

i) White Hat
ii) Black Hat
iii) Grey Hat

Types of Security Testing : Peneteration Testing

White Box Testing

Black Box Testing

Grey Box Testing

Steps Involved by White Hackers :

1. Legal Documentation

MOU,Non-disclosure agreement,Financial agreement

2. Scope Assessment

What needs to be tested ?

Admin Dashboard, Test Accounts, Code Review

3. Information Assessment

Gather targeted information about an organisation or a person using the basic information .

- To check IP of domain : nslookup domain
- To check open ports : netstat -an|grep LISTEN
- To check registration information of IP or domain : WhoIs Information
- To check all the domains/websites hosted on a server : Reverse IpLookup
- To find technology being used in website/webserver : www.builtwith.com
- To check history of evolution of website : web.archive.org
- To find related subdomains of given domain : dnsdumpster.com
- Use of Dorks for more accurate search and GHDB(Google hacking Database).

Tools for Advanced Information Gathering :

- Fierce - python3 ./fierce/fierce.py - -domain __domain name____
- Dirbuster – to find out directory and file names.

4. Vulnerability Assessment & Peneteration Testing (VAPT)

Tools for Advanced VAPT :

i) Nmap (Linux) & Zenmap(GUI Version)

ii) Nikto which uses Active State Perl & Strawberry Perl

iii) Burp Suite Pro

5. Gaining Access

6. Privilege Escalation

7. Report Generation

8. Patch Assistance

9. Recommendations

VAPT in detail :

VA : The phase where a hacker/security expert tries to find all the vulnerabilities in a system.

PT : exploits a vulnerability and tests how much damage he can cause using that vulnerability.

OWASP top 10 list

S.No.	Vulnerability	Explanation
1	Injection	It allows hacker to inject server side codes or commands. These are the flaws that allows a hacker to inject his own codes/commands into the web server that can provide illegal access to the data.
2	Broken Authentication and Session Management	These flaws generally arise when application functions related to security and session management are not implemented properly, which allows hackers to bypass authentication mechanisms. For eg. Login
3	Cross Site Scripting (XSS)	This is one of the most common flaw in which hackers injects codes like HTML, JS directly into the web pages allowing them to deface websites and stealing data of the users who trust these websites.
4	Insecure Direct Object References (IDOR)	These are the flaws that may cause severe impact as with IDORs, the hackers get access to objects in the database that belong to other users, which allows them to steal or even edit critical data of other users on the website. They can either steal that information or even delete someone’s account.
5	Security Misconfigurations	These are again one of the most common flaws as the developers/administrators forget to securely seal an application before making it live. Common flaws under this vulnerability includes keeping default password, default pages etc.
6	Sensitive Data Exposure	These type of flaws occur when websites are unable to protect sensitive data like credit card information, passwords etc. which allows hackers to steal this information and may cause credit card fraud or identity theft.

7	Missing Function-Level Access Controls	These flaws occur when security implementation are not implemented properly in applications on both User interface and server i.e. front and back end respectively. This allows hackers to bypass security and gain restricted access.
8	Cross Site Request Forgery	This vulnerability allows a hacker to send forged requests on behalf of a trusted user, which allows the hacker to act on behalf of the user. For example, telling the bank server to transfer money from X to Y on the victim's behalf and the bank server accepting it.
9	Using Components with Known Vulnerabilities	There are certain applications or their components that are known to exhibit vulnerabilities. If anyone is using these applications, it becomes easy for hackers to exploit these vulnerabilities and steal user data for eg. using an older version of windows server can be exploited by using an exploit code which is available online.
10	Unvalidated Redirects and Forwards	This flaw redirects users from a trusted website to a malicious website, which allows hackers to steal sensitive user information. For eg. if a user visits website A which he trusts but is redirected to website X which has a malware. But as user trusts A, he ends up trusting X.

1. SQL Injections

These are the vulnerabilities through which attackers gains illegal access to the data. It allows attackers to directly insert their commands/codes into the web server.While performing SQL Injection, you will need to sometimes comment out rest of the query after the payload.

In case of input field:

You need to enter a space, then two hyphens and then again a space after the payload. For example: password' or '1'='1'--

In case of URL:

The plus sign (+) is the URL encoded form a space. so to comment out rest of the query in a URL, you have to type space, two hyphens and then a plus sign after the payload.

For example : something' or '1'='1' --+

I. GET based SQL Injection

Union Based SQL Injection is used to find the number of columns in database to be fetched using order by.

i) Select database(),database()... : to know the name of database.

ii) Select table_name FROM information_schema.tables where table_schema="....." : to know tables name in database.

iii) Select column_name FROM information_schema.columns where table_schema="....." AND table_name="....." : this selects columns name inside the table of that database.

II. POST based SQL Injection : Using BurpSuite – local proxy server

III. **ERROR based SQL Injection :** for instance – convert(int,db_name())

IV. BOOLEAN based Blind Injection :for instance- AND getfirst_character_of(Password)='a'--+

V. Time based Blind Injection : for instance sleep for 10 seconds if query executed successfully.

VI. Automating SQL Injection : Using SQL Map, a Python based tool to exploit http request.

i) python sqlmap.py -u".....URL...."

ii) python sqlmap.py -u"...URL..." --dbs

iii) python sqlmap.py -u"...URL..." D"....db_name.." --tables

2. Improper or Missing Server Side Validation Vulnerability : Enter correct details and intercept using BupsSuite and the send the intercepted one.

3. IDOR and Rate-limiting Issues : In Insecure Direct Object References there should be restrictions on number of attempts.

4. Arbitrary File Upload Vulnerability : It allows to upload any format of file. This can be done by installing Backdoor to the victim's system.

5. Cross Site Scripting : allows to insert malicious codes into the HTML code of the browser. It's of two types -

i) Temporary XSS- can be done by inserting tags in URL.Injected code is not stored within the Application.

i)Permanent XSS - can be exploited by using BurpSuite by putting special character in http request.Injected code is stored permanently.

6. CSRF : It works only if Referer Header is not checked otherwise Open Redirection is used be editing URL to exploit.

7. Brute forcing : It is of two types- Dictionary based Brute forcing & Logical Brute forcing.

8. Server Misconfiguration Flaws : this is because of descriptive error messages, default debug files, default/weak password vulnerabilities & components with known vulnerabilities used by server. Fuzzing is used to exploit it(feeding lots of input & analysing the response).

References :

Wpvulndb.com - used to search for vulnerabilities.

Exploit-db.com - database of codes used to misuse a vulnerability.

CVEdetails – database of vulnerabilities

Supporting Website- www.trainings.internshala.com

Acquisitions – www.crunchbase.com