TABLE OF CONTENTS

INTRODUCTION TO CYBER SECURITY

WHAT IS CYBER SECURITY: -

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide

cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

WHY WE NEED CYBER SECURITY EXPERTS: -

A cybersecurity expert is a professional whose primary goal is to mitigate the risk of cyber-attacks and protect individuals and organizations from unauthorized access. In addition, cyber specialists ensure that networks, applications, software systems, and data centres are secure during development. India had a total of 11,58,208 cyber security incidents in 2020-21. Cyber security attacks increased to 12,13,784 till October

2021.That is the main reason why we need more skilled cyber security experts in india.

INTRODUCTION TO ETHICAL HACKING

➢What is Ethical Hacking?

Ethical Hacking is performed by White Hat Hackers to find the security vulnerabilities of the system and prevent the Black Hat hackers from illegally infiltrating and stealing data from any system. The big organizations perform ethical hacking to test the cybersecurity level and identify the weak points. Ethical hacking is performed as per the rules and regulations set by the legal authorities. Generally, the device owners or the organizations on which the ethical hacking is performed knows about the hacking being performed on them.

➢What is Unethical Hacking?

Unethical Hacking or Black Hat hacking is performed by cybercriminals with the false intention of stealing sensitive data, money, and access the restricted networks and systems. Such type of hacking is practiced to disrupt official website networks and infiltrate communication between two or more parties. Generally, the targets on which black hat hacking is performed do not know about the infiltration as it is done quietly in the background.

THERE ARE MAINLY THREE TYPES OF HACKERS:

1. White Hat Hackers.
2. Black Hat Hackers.
3. Gray Hat Hackers.

WHITE HAT HACKERS: -

A white hat is an ethical security hacker. Ethical hacking is a term meant to imply a broader category than just penetration testing. Under the owner's consent, white hat hackers aim to identify any vulnerabilities the current system has.

BLACK HAT HACKERS: -

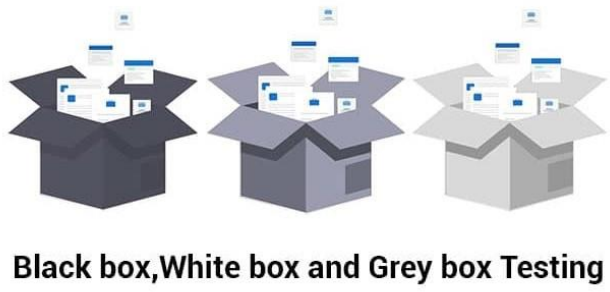
Black Hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

GRAY HAT HACKERS: -

A grey hat is a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but usually does not have the malicious intent typical of a black hat hacker. The term came into use in the late 1990s, derived from the concepts of "white hat" and "black hat" hackers.

INTRODUCTION OF INFORMATION SECURITY AND COMPUTER NETWORKING

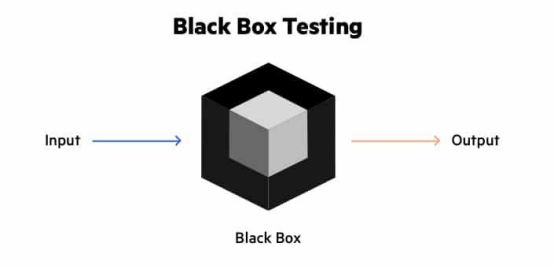
THERE ARE THREE TYPES OF TESTING TECHNIQUE: -



Black box,White box and Grey box Testing

- BLACK BOX TESTING
- WHITE BOX TESTING
- GREY BOX TESTING

BLACK BOX TESTING: - Black box testing assesses a system solely from the outside, without the operator or tester knowing what is happening within the system to g

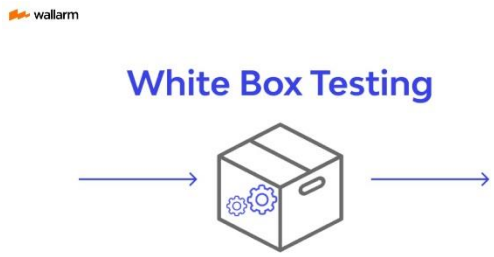


enerate responses to test actions. A black box refers to a system whose

behaviour has to be observed entirely by inputs and outputs.

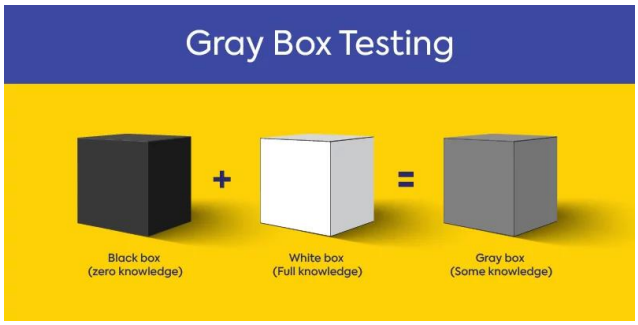
WHITE BOX TESTING: -

white box testing which also known as glass box is testing, structural testing, clear box testing, open box testing and transparent box testing.



It tests internal coding and infrastructure of a software focus on checking of predefined inputs against expected and desired outputs. It is based on inner workings of an application and revolves around internal structure testing. In this type of testing programming skills are required to design test cases. The primary goal of white box testing is to focus on the flow of inputs and outputs through the software and strengthening the security of the software

GREY BOX TESTING: -



Grey box testing is a software testing method to test the software application with partial knowledge of the internal working structure. It is a combination of black box and white box testing because it involves access to internal coding to design test cases as white box testing and testing practices are done at functionality level as black box testing.

INFORMATION GATHERING AND BASICS OF WEB DEVELOPMENT

WHAT IS DIGITAL FOOTPRINT: -

A digital footprint is data that is left behind when users have been online. There are two types of digital footprints which are passive and active. A passive footprint is made when information is collected from the user without the person knowing this is happening.

WHAT IS XAMPP: -

XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages.

WHAT IS GOOGLE DORKING: -

Google hacking, also named Google dorking, is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using.

INTRODUCTION TO VAPT, OWASP, AND SQL INJECTIONS

WHAT IS VAPT: -

Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot.

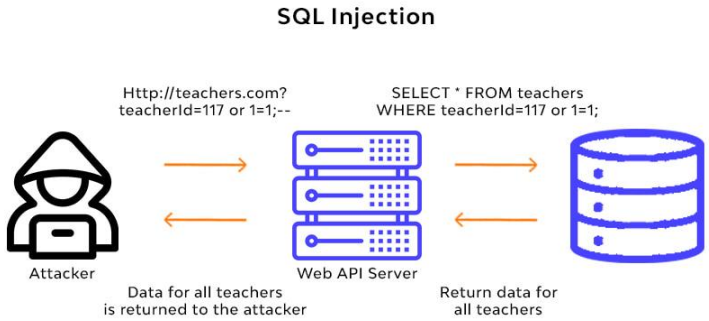
WHAT IS OWASP: -

The Open Web Application Security Project (OWASP) is a non-profit foundation dedicated to improving software security. It operates under an "open community" model, which means that anyone can participate in and contribute to OWASP-related online chats, projects, and more.

OWASP
Open Web Application Security Project

WHAT IS SQL INJECTION: -

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

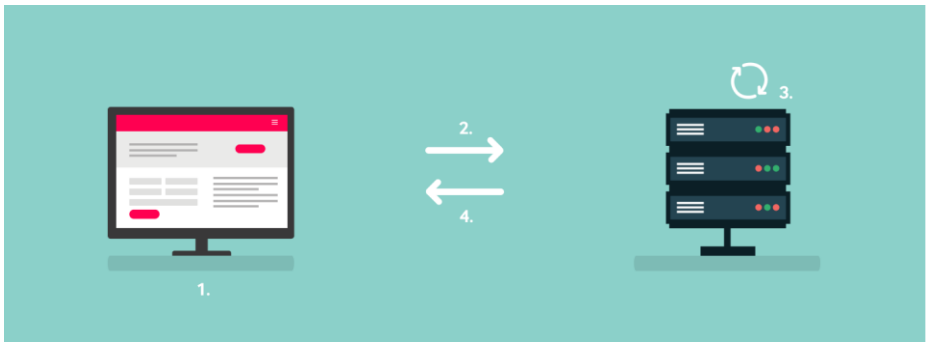


ADVANCE WEB APPLICATION ATTACKS

WHAT IS CLINT SIDE FILTERS BYPASS: -

Many websites lack client-side filter checks, so it becomes easy to bypass that. But our bypass will only be successful if there is no server-side filter check either.

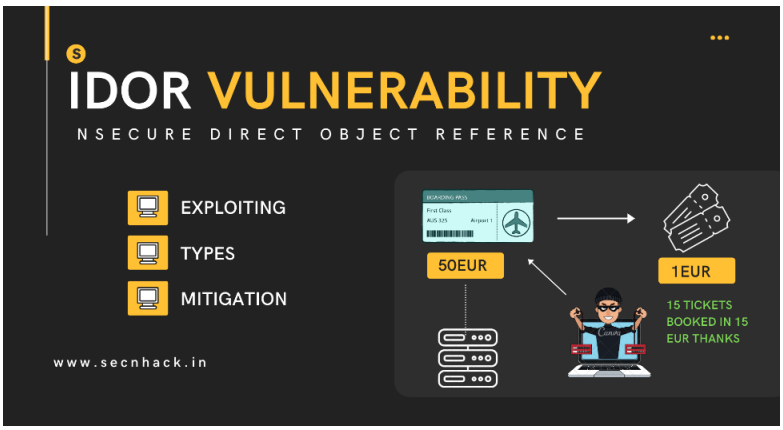
These filters ensure that the input given by the user is in the correct format.



Basically, this filter validates the input, and then it is forwarded to the server-side. For example: If you don't put '@' in

your email id, or if u don't click on terms and conditions if you insert alphabets in phone no. field, you are prompted to enter valid inputs.

WHAT IS IDOR: -

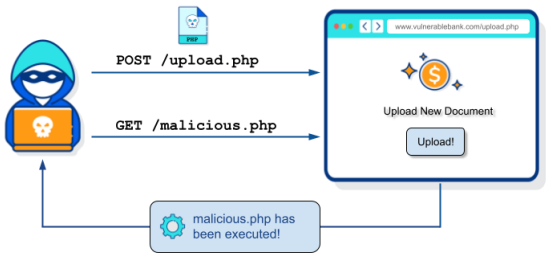


An insecure direct object reference (IDOR) is an access control vulnerability where unvalidated user input can be used for unauthorized access to resources or operations. IDORs can have serious consequences for cybersecurity and be hard to find yet easy to exploit.

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. The term IDOR was popularized by its appearance in the OWASP 2007 Top Ten.

ARBITRARY FILE UPLOAD VULNERABILITIES: -

An arbitrary file upload vulnerability is a type of security flaw that allows an attacker to upload malicious files onto a server. This can be done by exploiting a vulnerability in a web application that doesn't properly validate the file type or by tricking the user into uploading a malicious file. Once uploaded, these files can be used to compromise the server or perform other malicious actions.



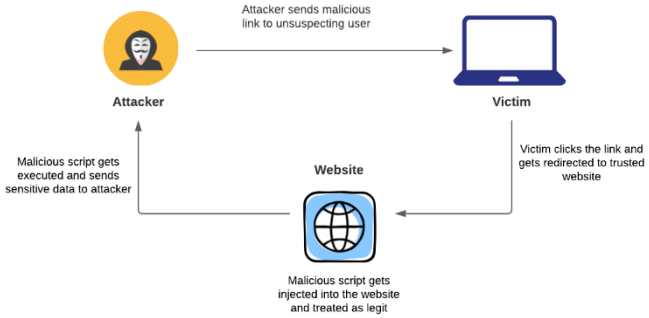
Arbitrary file upload vulnerabilities are often used in attacks known as "web shell" attacks. In these attacks, the attacker uploads a malicious PHP script onto the server. This script can then be used to execute

arbitrary commands on the server, allowing the attacker to gain full control of it.

CLIENT-SIDE ATTACKS

WHAT IS CROSS SITE SCRIPTING (XSS): -

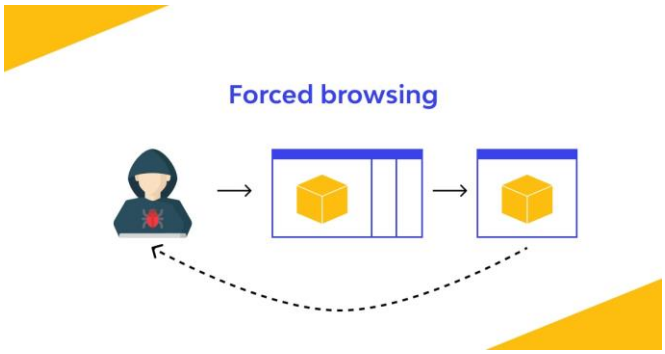
Cross site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it. If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system. As a result, the attacker can steal the user's active session cookie.



Examples of reflected cross-site scripting attacks include when an attacker stores malicious script in the data sent from a website's search or contact form. A typical example of reflected cross-site scripting is a search form, where visitors send their search query to the server, and only they see the result.

UNDERSTANDING FORCED BROWSING: -

A Forced browsing attack is a vulnerability in which an unauthorized user has access to the contents of an authorized user. Forced browsing is an attack when a Web application has more than one user privilege level for the same user. Thus, an attacker gets sensitive information which should otherwise not be accessible to him/her. The attacker can use a brute force approach to get common directories, files, or information of user accounts present on the website. Forced browsing is named so because we are forcefully browsing the URL which only an authorized user is supposed to browse. Also, using forceful browsing, a hacker can get access to common files that may contain important data. Forced browsing attacks can also be performed using hit and trial method where application index pages and directories are based on predictable values. Due to its severity, it's ranked in OWASP Top 10 vulnerability list.

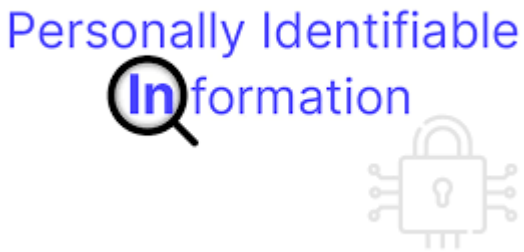


EXAMPLE: -

Let's assume a user logs on to his account and the URL is-www.gfg.com/info/user1.php. Now, he copies this URL and pastes it in the incognito mode tab.If the same page opens, it means the website isn't checking for authentication. The user can modify the URL by a hit and trial or brute force approach like this-www.gfg.com/info/user2.php and load the page. He will get information of user2 present on that website without asking for password or email ID or any sort of identity verification to access the account of user2.Similarly, if the user gets the URL of the admin somehow, he will be able to get admin privileges without any authentication. So, this vulnerability is critical.

PERSONALLY IDENTIFIABLE INFORMATION (PII) LEAKAGE: -

Personally identifiable information leakage vulnerability is a vulnerability where the information gives specific details about a specific individual, that in turns help to distinguish that particular individual from the rest of other individual.



IDENTIFYING SECURITY MISCONFIGURATION AND EXPLOITING OUTDATED WEB APPLICATIONS

WHAT IS SECURITY MISCONFIGURATIONS: -

Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

SOME COMMON MISCONFIGURATION: -

- Unpatched systems
- Default usernames and passwords
- Unencrypted files
- Old and out of date web applications
- Unsecured devices
- Web application and cloud misconfiguration

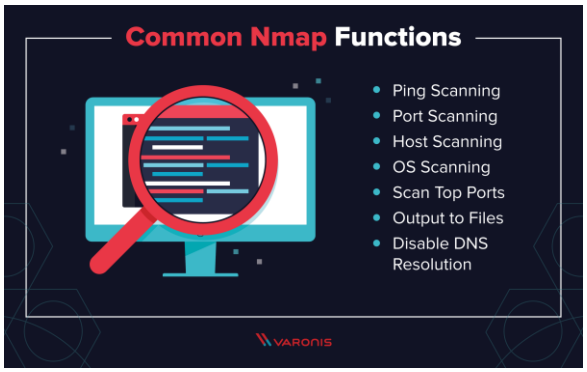
- Insufficient firewall protection

WHAT IS PUBLIC EXPLOIT: -

An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations

AUTOMATING VAPT AND SECURE CODE DEVELOPMENT

WHAT IS NMAP: -



Nmap, the acronym for Network Mapper, is an open-source security auditing and network scanning software designed by Gordon Lyon. It is developed in such a way that it can quickly analyze massive networks as well as single hosts.

WHAT IS NIKTO: -

The Nikto web server scanner is a security tool that will test a web site for thousands of possible security issues. Including dangerous files, mis-configured services, vulnerable scripts and other issues. It is open source and structured with plugins that extend the capabilities.

WHAT IS BURPSUIT PRO: - Burp Suite Professional is the web security tester's toolkit of choice. Use it to automate repetitive testing tasks - then dig deeper with its expert-designed manual and semi-automated security testing tools. Burp Suite Professional is one of the most popular penetration testing and vulnerability finder tools, and is often used for checking web application security. "Burp," as it is commonly known, is a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing.

DOCUMENTING AND REPORTING VULNERABILITIES

THERE ARE TWO TYPES OF VULANERABLITY REPORT: -

1. DETAILED DEVELOPER REPORT
2. HIGH LEVEL MANAGEMENT SUMMARY

1.DETAILED DEVELOPER REPORT: -

In detailed developer report it contains technical stuff like, how did I found the bug, where I found the bug, what are tools I used for the find and exploit the bugs, procedure for finding and exploiting the bug, ways to patch the bug, any other references from where developer can read more about the bugs. So, we can also say that it's a technical developer report and this report specifically made for developers.

2.HIGH LEVEL MANAGEMENT SUMMARY: -

In high level management summary report security incharge wants to know impact of the bugs so this report will become less technical and more technical based .so the person needs to know: -

- Security status of the organization.
- Business impact of the vulnerability found
- Proof of concept