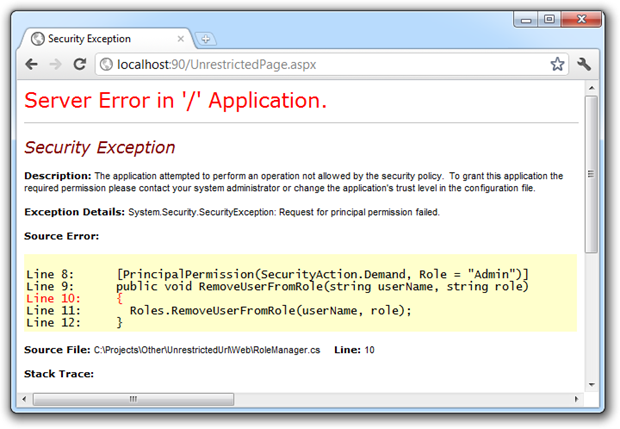
TASK-4

Understand any vulnerabilities except for OWASP Top 10

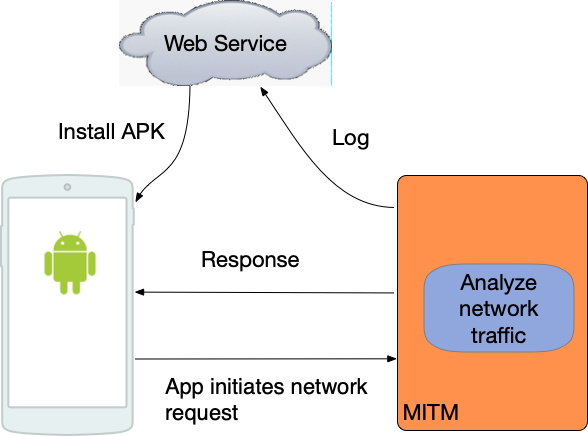
1.Failure to restrict URL attack

A "failure to restrict URL attack" happens when a website or web application doesn't properly control which parts of the website users can access. This can allow unauthorized people to access things they shouldn't be able to, like private information or administrative tools. Attackers can do this by manipulating the website's addresses (URLs) in a way that lets them get to these sensitive parts. To prevent this, websites need to have strong security measures in place to check who is allowed to see and use different parts of the site.



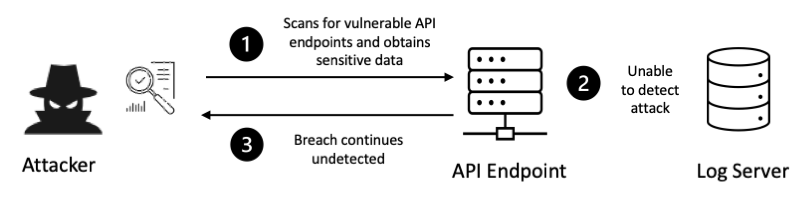
2.Improper Certification validation

Improper certificate validation refers to a security issue where a computer program or system fails to correctly verify the authenticity and legitimacy of digital certificates. Digital certificates are used to establish secure communication over the internet, ensuring that the website or service you're interacting with is indeed who they claim to be.



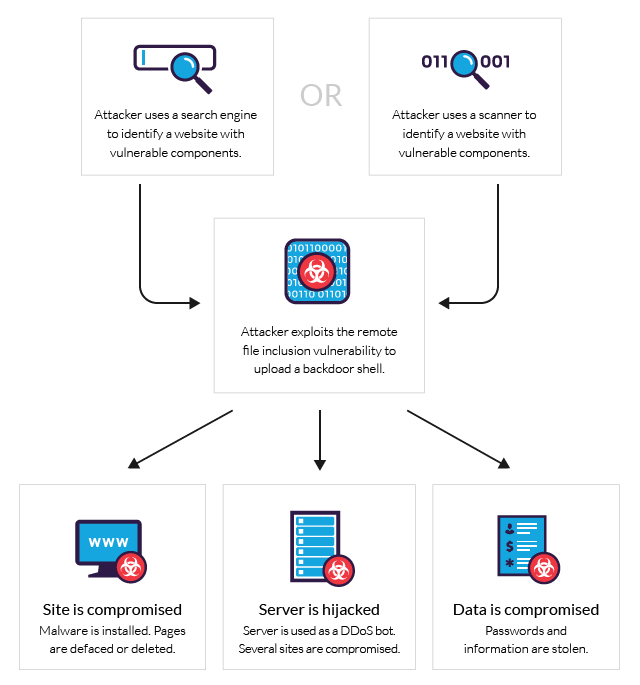
3. Insufficient logging and monitoring

Insufficient logging and monitoring refers to a cybersecurity weakness where an organization's systems and applications don't have adequate mechanisms in place to record and track events, incidents, and activities. This lack of comprehensive logging and monitoring makes it difficult to detect and respond to security breaches or other malicious activities effectively.



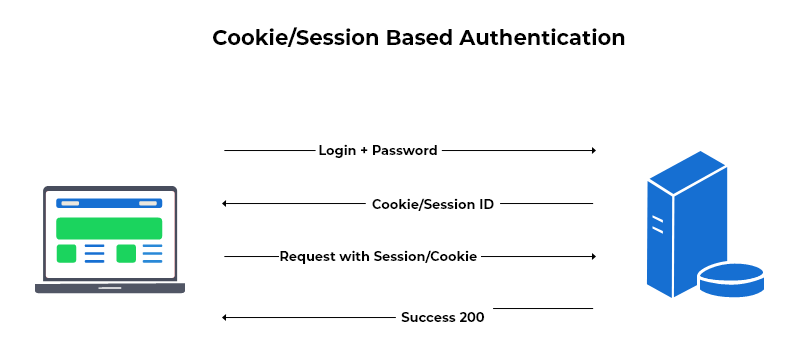
4.Remote file inclusion

Remote File Inclusion (RFI) is a type of cybersecurity vulnerability that occurs when a web application allows an attacker to include remote files on a server. This can lead to the execution of malicious code or unauthorized access to sensitive files and data on the server. RFI is often found in web applications that do not properly validate or sanitize user input, allowing attackers to manipulate the application's behavior.

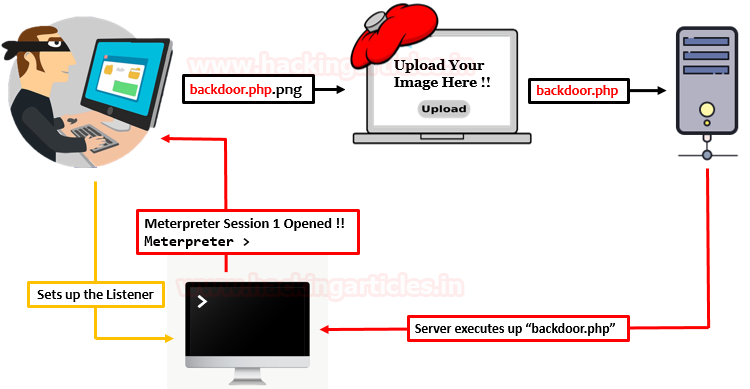


5. Session ID leakage

Session ID leakage, also known as session fixation, is a security vulnerability that occurs when an attacker is able to obtain or manipulate a valid user's session ID. Session IDs are tokens that are used to identify a user's session and maintain their authentication state as they interact with a web application. If an attacker gains control over a user's session ID, they can impersonate that user and potentially gain unauthorized access to their account and data

6. Unrestricted File Upload

Unrestricted file upload is a cybersecurity vulnerability that occurs when a web application allows users to upload files without implementing proper security measures. Attackers can exploit this vulnerability by uploading malicious files (such as scripts or malware) to the server, which can then be executed or accessed by other users. This can lead to a range of security risks and potential compromises.



7.Encapsulation

It refers to the practice of enclosing data and functionalities within a well-defined boundary, such as a class or module, to control access and interactions. Encapsulation helps enhance security by limiting direct access to sensitive data and ensuring that interactions with that data are controlled through defined methods and interfaces.

8.Missing PT\_DENY\_ATTACH

PT\_DENY\_ATTACH is a process control flag used in macOS systems to prevent the debugging of a process. It's typically used to enhance the security of sensitive applications and prevent attackers from attaching a debugger to the application's process, which could aid in reverse engineering or exploitation.

9.Race condition

A race condition in web security happens when a web application doesn't handle multiple actions happening at the same time correctly. Imagine a situation where two or more users are trying to do something on a website, like updating their profile or making a purchase, all at once. If the website doesn't manage these actions properly, their actions might "race" against each other, leading to unexpected and potentially harmful results.

10.Senesitive data exposure

Sensitive data exposure happens when confidential information, like personal details or financial records, is accidentally made accessible to people who shouldn't have access. This can occur due to security weaknesses in systems or applications. When sensitive data gets into the wrong hands, it can lead to identity theft, financial loss, and privacy violations. Preventing exposure involves strong security practices, like encryption and access controls, to keep sensitive information safe.