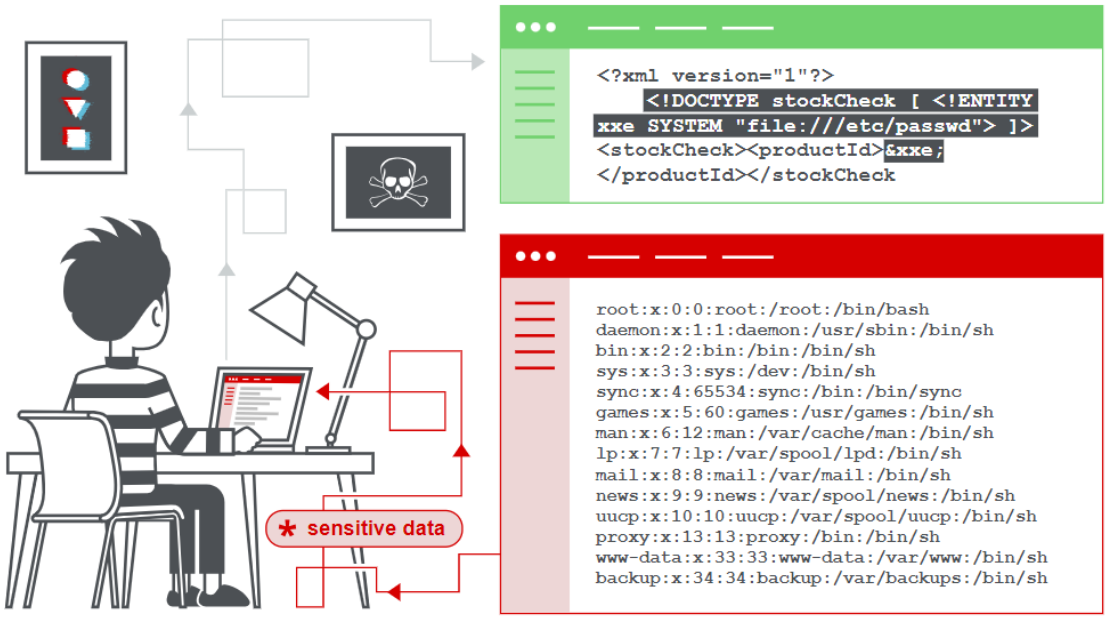
Web Vulnerability Attacks

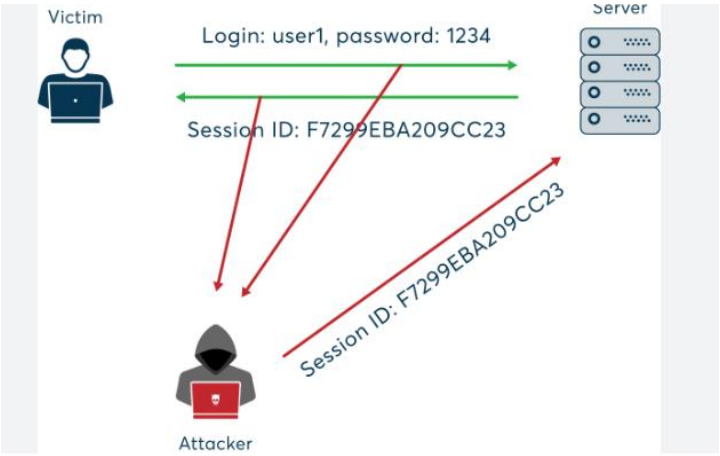
Other than top 10 web vulnerabilities

1. XML External Entities



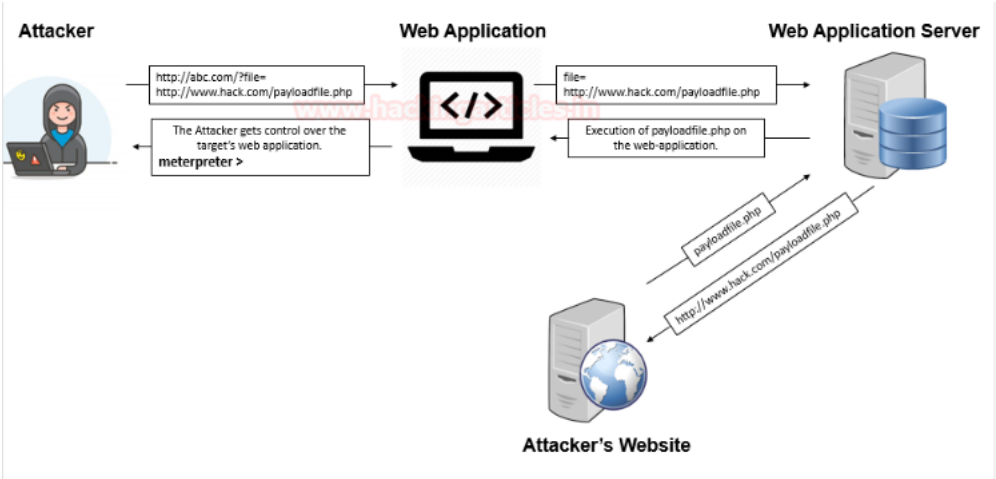
XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

2. Session id leakage



To perform session hijacking, an attacker needs to know the victim's session ID (session key). This can be obtained by stealing the session cookie or persuading the user to click a malicious link containing a prepared session ID. In both cases, after the user is authenticated on the server, the attacker can take over (hijack) the session by using the same session ID for their own browser session. The server is then fooled into treating the attacker's connection as the original user's valid session.

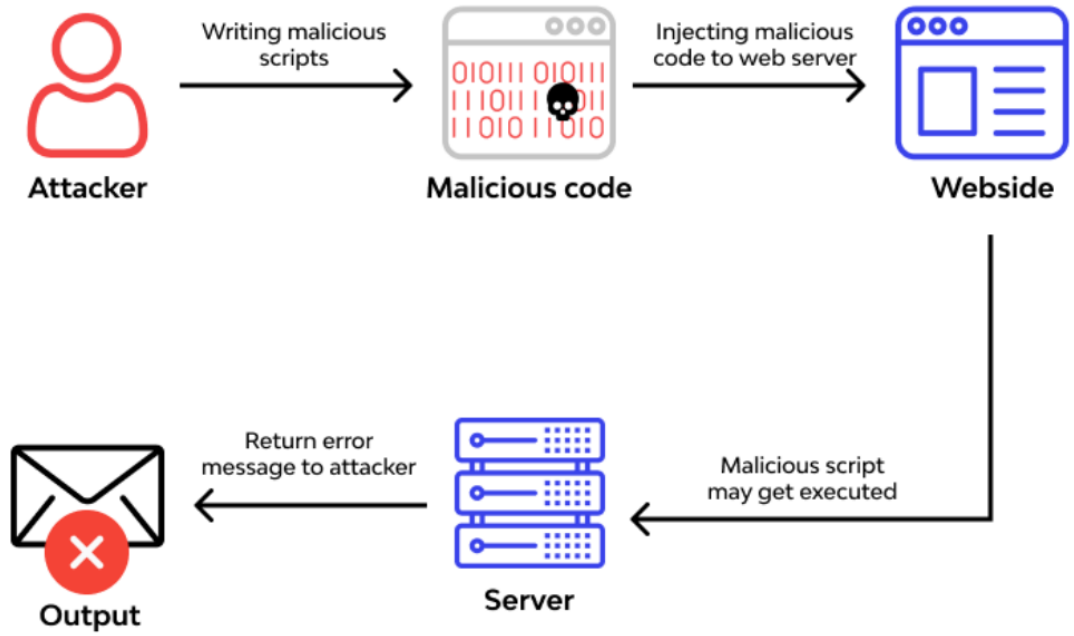
3. **Remote file inclusion**



Remote File inclusion is another variant to the **File Inclusion vulnerability,** which arises when the **URI of a file** is **located on a different server** and is **passed to as a parameter** to the PHP functions either "include", "include_once", "require", or "require_once".

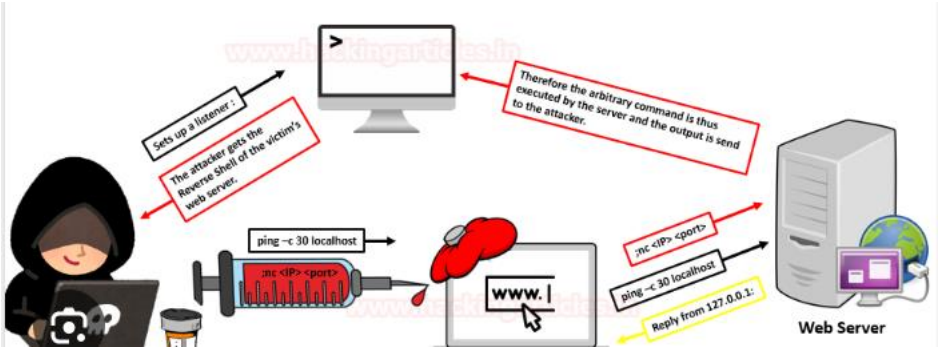
The Remote File Inclusion vulnerabilities are easier to exploit but are less common say **in 1 of the 10 web-applications.** Here thus, instead of accessing a file on a local server, the attacker could simply inject his/her vulnerable PHP scripts which are **hosted on his remote web-application into the unsanitized web application's URL**,

4. **Remote code execution**



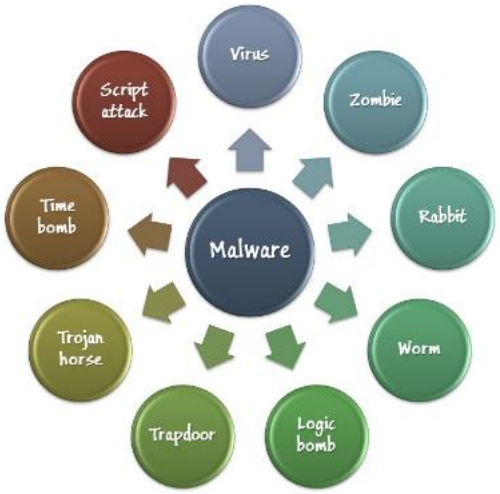
Remote Code Execution is used to expose a form of vulnerability that can be exploited when user input is injected into a file or string and the entire package is run on the parser of the programming language. This is not the type of behavior that is exhibited by the developer of the web application. A Remote Code Execution Attack can lead to a full-scale attack that would compromise an entire web application and the webserver. RCE could lead also into privilege escalation, network pivoting and establishing persistence. This is why RCE is always having HIGH/CRITICAL severity. You should also note that virtually all programming languages have different code evaluation functions.

5. Operating system command injection



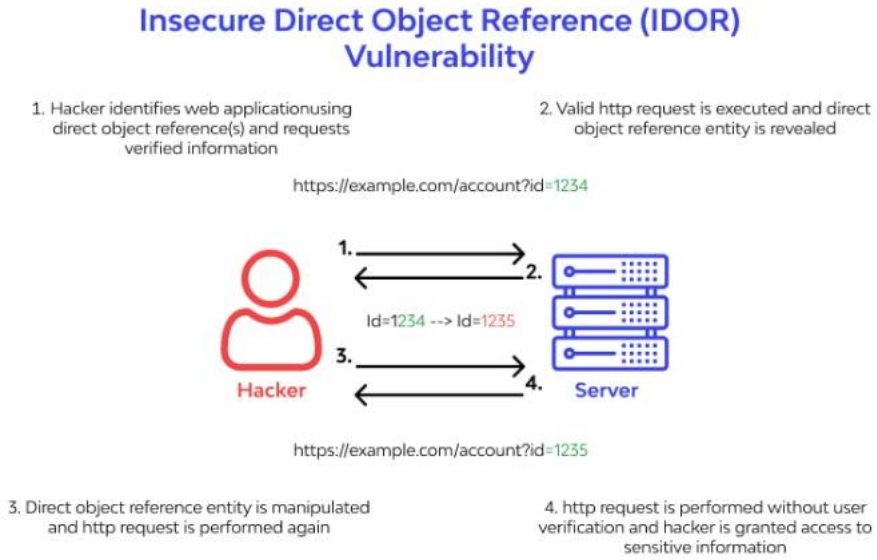
Command Injection also referred to as Shell Injection or OS Injection. It arises when an attacker tries to perform system-level commands directly through a vulnerable application in order to retrieve information of the webserver or try to make unauthorized access into the server. Such an attack is possible only when the user-supplied data is not properly validated before passing to the server. This user data could be in any form such as forms, cookies, HTTP headers, etc.

6. **Malicious code**



Malicious code is a term for code — whether it be part of a script or embedded in a software system — designed to cause damage, security breaches or other threats to application security. An important part of this definition is intent. Non-malicious attacks do happen and are often accidental or due to negligence.

7. **Insecure direct object references**



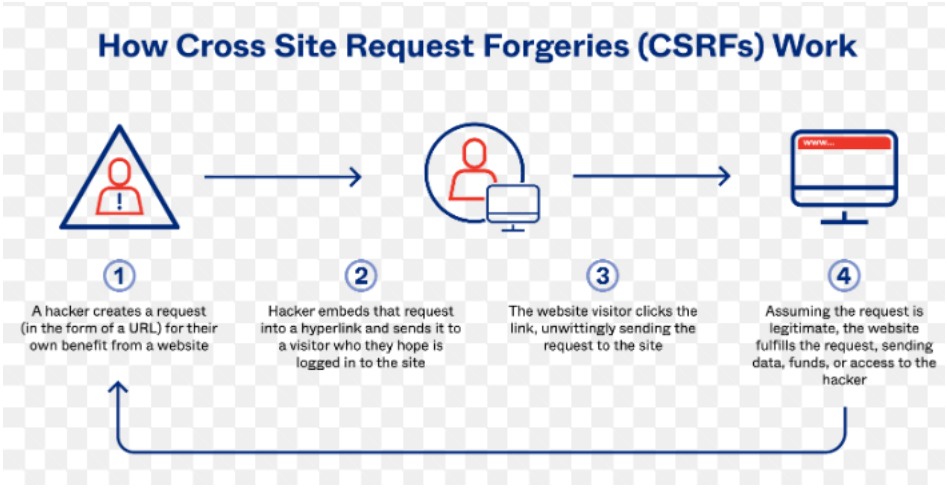
It takes place when authorized user input is used by any other unauthorized entity to gain access to a specific application/resource/software/operation. If not tackled promptly, a well-planned IDOR attack leads to serious dangers.

At times, Insecure Direct Object Reference (IDOR) is not a direct threat. But, using this type of access control attack, skilled hackers/threat actors can create a threat-conducive environment for a bigger and damage-causing attack.

8. Improper certificate validation

The SSL Certificate Details provide information about the certificate associated with the HTTPS server. This information describes important attributes of the certificate and should be reviewed for the correctness of the contact information, whether it is self-signed, and how soon it will expire. The Supported Ciphers provides information about each available encryption scheme available for each of the possible SSL/TLS protocols.

9. Cross site request forgery



A Cross-Site Request Forgery attack, also known as a CSRF attack, tricks an authenticated user into performing unintended actions by submitting malicious requests without them realizing it.

10. Carriage return and line feed injection