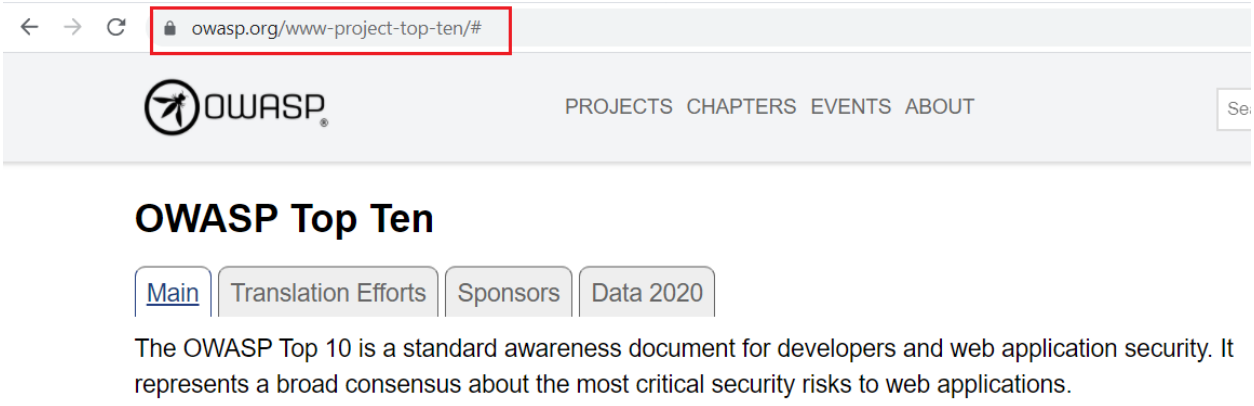
OWASP:

OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security. In short, OWASP is a repository of all things web-application-security, backed by the extensive knowledge and experience of its open community contributors.

OWASP Top 10:

OWASP Top 10 is the list of the 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures. OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks. Updated every three to four years, OWASP's top ten list is compiled and published every three to four years, highlighting the most critical security vulnerabilities. Additionally, the list includes examples of the weaknesses, how they can be exploited by attackers, and suggested methods that reduce or eliminate application exposure.

The Top 10 OWASP vulnerabilities in 2021 are: Injection, Broken Authentication, Sensitive Data exposure, XML external entities (XXE), Broken access control, Security Misconfigurations, Cross Site Scripting (XSS), Insecure Deserialization, Using Components with known Vulnerabilities and Insufficient Logging and Monitoring.



1-Injection:

A code injection happens when an attacker sends invalid data to the web application with the intention to make it do something that the application was not designed/programmed to do. Perhaps the most common example around this security vulnerability is the SQL query. Anything that accepts parameters as input can potentially be vulnerable to a code injection attack.

2-Broken Authentication:

f authentication and access restriction are not properly implemented, it's easy for attackers to take whatever they want. With broken access control flaws, unauthenticated or unauthorized users may have access to sensitive files and systems, or even user privilege settings. Websites with broken authentication vulnerabilities are very common on the web. Broken authentication usually refers to logic issues that occur on the application authentication's mechanism, like bad session management prone to username enumeration – when a malicious actor uses brute-force techniques to either guess or confirm valid users in a system.

3-Sensitive Data Exposure:

Sensitive data exposure is one of the most widespread vulnerabilities on the OWASP list. It consists of compromising data that should have been protected. Examples of Sensitive Data Some sensitive data that requires protection is: Credentials, Credit card numbers, Social Security Numbers, Medical information, Personally identifiable information (PII) and Other personal information

4-XML External Entities (XXE):

an XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. Most XML parsers are vulnerable to XXE attacks by default. That is why the responsibility of ensuring the application does not have this vulnerability lays mainly on the developer.

5-Broken Access Control:

In website security, access control means putting a limit on what sections or pages visitors can reach, depending on their needs. For example, if you own an ecommerce store, you probably need access to the admin panel in order to add new products or to set up a promotion for the upcoming holidays. However, hardly anybody else would need it. Allowing the rest of your website's visitors to reach your login page only opens up your ecommerce store to attacks.

And that's the problem with almost all major content management systems (CMS) these days. By default, they give worldwide access to the admin login page. Most of them also won't force you to establish a two-factor authentication method (2FA).

6-Security Misconfiguration.

Security misconfigurations are when design or configuration weaknesses result from a configuration error or shortcoming. Example is a default account and its original password are still enabled, making the system vulnerable to exploit.

7-Cross-Site Scripting (XSS).

XSS attacks occur when an application includes untrusted data on a webpage. Attackers inject client-side scripts into this webpage. Example is untrusted data in an application allow for an attacker to 'steal a user session' and gain access to the system.

8-Insecure Deserialization:

Deserialization, or retrieving data and objects that have been written to disks or otherwise saved, can be used to remotely execute code in your application or as a door to further attacks.

9-Using Components with Known Vulnerabilities.

It describes when applications are built and run using components that contain known vulnerabilities. Example is due to the volume of components used in development, a development team may not even know or understand the components used in their application. This can result in them being out-of-date and therefore vulnerable to attack.

10-Insufficient Logging and Monitoring.

Logging and monitoring are key to being able to detect what your site is doing at runtime. If you do not implement it correctly, you will be unable to detect when your system is under attack, and you are liable to get compromised without knowing it. Failure to adequately log and monitor a site leaves it vulnerable to more severe compromising activities. Example is events that can be audited, like logins, failed logins, and other important activities, are not logged, leading to a vulnerable application.