





OWASP Top 10 - 2013

Before we jump into the technicalities of the vulnerabilities listed in the OWASP Top 10 2013 list. Let’s quickly try to understand how these vulnerabilities work.

| **Vulnerability** | **Explanation** |
| --- | --- |
| 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. |
| 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 |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |

You can also check the list directly on the official OWASP website. Here’s the link:<https://www.owasp.org/index.php/Top_10_2013-Top_10>