

## Transcrição

Os problemas de injeção de código, conforme vimos, são muito comuns. A OWASP é uma empresa sem fins lucrativos, que desenvolveu o projeto que estamos utilizando e também criou um ranking das maiores vulnerabilidades que existem na internet. O ranking está disponível na página da Owasp, clicando aqui:

The screenshot shows the 'Top 10 2013-Top 10' page of the OWASP website. At the top, there are navigation links for 'Page', 'Discussion', 'Read', 'View source', 'View history', and a search bar. Below the header, the title 'Top 10 2013-Top 10' is displayed. To the left, there are back and forward navigation arrows labeled 'Risk'. In the center, there are four green boxes representing the top four vulnerabilities: 'A1-Injection', 'A2-Broken Authentication and Session Management', 'A3-Cross-Site Scripting (XSS)', and 'A4-Insecure Direct Object References'. Each box contains a brief description of the vulnerability. At the top right, there is a link 'A1-Injection →'.

Rank	Vulnerability	Description
1	A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2	A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
3	A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
4	A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Essas informações são baseadas em dados que a OWASP recolhe de diversas empresas!

Repare que *A1-Injection* ocupa a primeira posição no quesito de problemas de vulnerabilidade. Clicando nela, abre-se uma nova página com mais referências sobre essa vulnerabilidade. Mais abaixo nesse novo link podemos verificar textos que trazem histórias de ataques comumente realizados e também dicas de como podemos nos prevenir!