

Transcrição

Os ataques referenciando problemas de autenticação são muito comuns nos sistemas web, por isso o site **OWASP** disponibilizou um ranking com as dez maiores vulnerabilidades em sistemas.

O ranking foi divulgado na publicação "Top 10 2013-Top 10":

Page Discussion Read View source View history Search

Top 10 2013-Top 10

[← Risk](#) [2013 Table of Contents](#) [2013 Top 10 List](#) [A1-Injection →](#)

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.
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.
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.
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.

Clicando no segundo item da lista, o *A2-Broken Authentication and Session Manager*, seremos redirecionados para a seguinte página:

<h3>Example Attack Scenarios</h3> <p>Scenario #1: Airline reservations application supports URL rewriting, putting session IDs in the URL:</p> <pre>http://example.com/sale/saleitems?sessionid=268544541&dest=Hawaii</pre> <p>An authenticated user of the site wants to let his friends know about the sale. He e-mails the above link without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.</p> <p>Scenario #2: Application's timeouts aren't set properly. User uses a public computer to access site. Instead of selecting "logout" the user simply closes the browser tab and walks away. Attacker uses the same browser an hour later, and that browser is still authenticated.</p> <p>Scenario #3: Insider or external attacker gains access to the system's password database. User passwords are not properly hashed, exposing every users' password to the attacker.</p>	<h3>References</h3> <p>OWASP</p> <p>For a more complete set of requirements and problems to avoid in this area, see the ASVS requirements areas for Authentication (V2) and Session Management (V3).</p> <ul style="list-style-type: none"> • OWASP Authentication Cheat Sheet • OWASP Forgot Password Cheat Sheet • OWASP Session Management Cheat Sheet • OWASP Development Guide: Chapter on Authentication • OWASP Testing Guide: Chapter on Authentication <p>External</p> <ul style="list-style-type: none"> • CWE Entry 287 on Improper Authentication • CWE Entry 384 on Session Fixation
--	--

Essa página traz uma descrição desse ataque, maneiras de prevenção e outros itens. O interessante é que também podemos encontrar alguns links de referência para proteção.

Cada um desses sites traz dicas diversas para evitar invasões, por exemplo, o uso de senhas mais complexas para dificultar os possíveis ataques.

