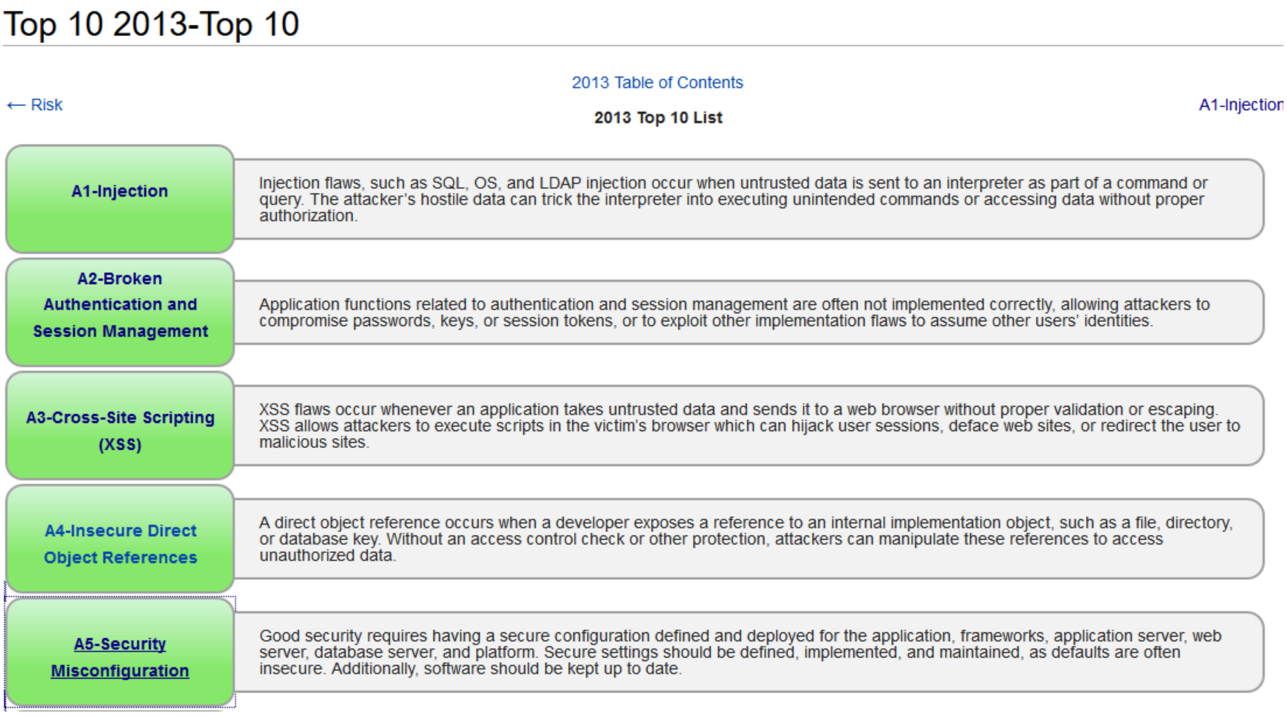
10

OWASP

Transcrição

Problemas de configuração que comprometem a segurança são recorrentes e por isso estão incluídos no **Ranking da OWASP**:



Top 10 2013-Top 10

← Risk

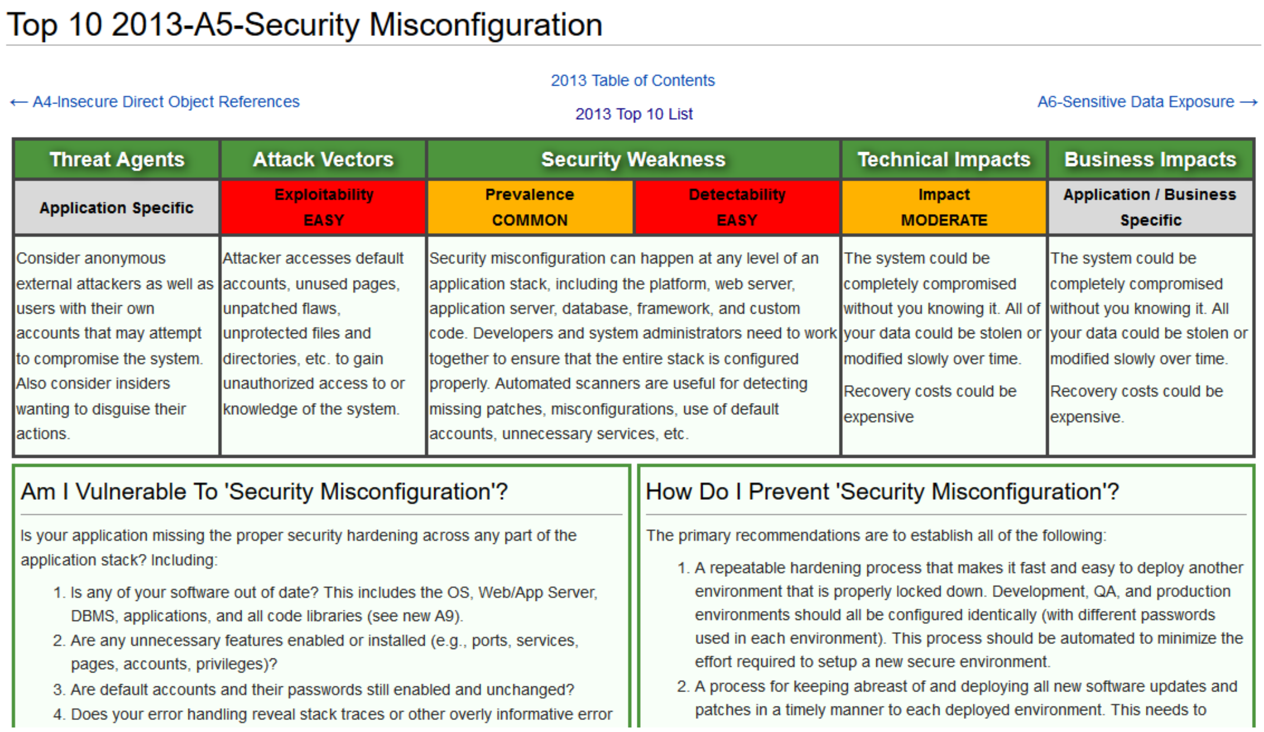
2013 Table of Contents

2013 Top 10 List

A1-Injectior

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.
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Esses problemas estão classificados na quinta posição como "*A5 - Security Misconfiguration*". Clicando nesse item somos redirecionados para a seguinte página:



Top 10 2013-A5-Security Misconfiguration

← A4-Insecure Direct Object References

2013 Table of Contents

2013 Top 10 List

A6-Sensitive Data Exposure →

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anonymous external attackers as well as users with their own accounts that may attempt to compromise the system. Also consider insiders wanting to disguise their actions.	Attacker accesses default accounts, unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.	Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, database, framework, and custom code. Developers and system administrators need to work together to ensure that the entire stack is configured properly. Automated scanners are useful for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc.		The system could be completely compromised without you knowing it. All of your data could be stolen or modified slowly over time. Recovery costs could be expensive	The system could be completely compromised without you knowing it. All your data could be stolen or modified slowly over time. Recovery costs could be expensive.

Am I Vulnerable To 'Security Misconfiguration'?

Is your application missing the proper security hardening across any part of the application stack? Including:

1. Is any of your software out of date? This includes the OS, Web/App Server, DBMS, applications, and all code libraries (see new A9).
2. Are any unnecessary features enabled or installed (e.g., ports, services, pages, accounts, privileges)?
3. Are default accounts and their passwords still enabled and unchanged?
4. Does your error handling reveal stack traces or other overly informative error

How Do I Prevent 'Security Misconfiguration'?

The primary recommendations are to establish all of the following:

1. A repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down. Development, QA, and production environments should all be configured identically (with different passwords used in each environment). This process should be automated to minimize the effort required to setup a new secure environment.
2. A process for keeping abreast of and deploying all new software updates and patches in a timely manner to each deployed environment. This needs to

Nela estão descritas algumas estratégias que usuários mal intencionados podem utilizar para ganhar acesso a um site e o impacto dessas práticas para o servidor. Além disso, no trecho "Referências", estão reunidos links com informações sobre prevenção, por exemplo, em páginas de acesso restrito devem ser colocadas maneiras de autenticação e devem existir tipos de certificação do *upload* de arquivos, ou seja, verificar o tipo de arquivo que está sendo enviado ao site.

Apesar de extensa, a documentação que a **OWASP** fornece é muito detalhada! Ler a documentação é uma maneira de obter informações valiosas para aplicar no projeto!