Riscos de segurança em aplicações web

Redes e Segurança Informática

2º semestre > 1º ano

Carlos Guerra

Cofinanciado por: NORTE 2020 Programa Regional do Norte | PORTUGAL 2030 | Cofinanciado pela União Europeia

Index

- Configuração Insegura
- Injeção de SQL
- Cross site scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Clickjacking
- Entidades externas XML
- Outras vulnerabilidades

Configuração Insegura

- Contas por omissão com senhas por omissão
- Listagem de pastas e ficheiros (directory listing)
- Permissões indevidas de pastas e ficheiros
- Gestão remota
- Certificados SSL com problemas
- Instalação de remendos
- Mensagens de erro com informação confidencial e/ou desnecessária

Injeção de SQL

- As vulnerabilidades de injeção de SQL estão presentes em aplicações que constroem comandos SQL a partir de entradas fornecidas pelo utilizador. Dado que a linguagem SQL utiliza vários metacarateres, um atacante poderá fornecer entradas maliciosas com uma mistura inteligente de carateres e metacarateres, de forma a alterar a lógica do comando SQL onde as entradas são inseridas.

Cross site scripting (XSS)

- O Cross Site Scripting (tipicamente identificado pela sigla XSS), permite a um atacante executar um script no navegador da vítima, contornando mecanismos de controlo de acesso como a política da mesma origem (same-origin policy).
- A política de mesma origem está implementada em todos os navegadores modernos, tendo como principal objetivo garantir que um determinado script apenas acede a informações e/ou executa operações no mesmo sítio web em que está alojado.

Cross Site Request Forgery (CSRF)

- Um sítio web tem uma vulnerabilidade deste tipo quando autentica os seus utilizadores com base numa credencial constante, submetida de forma automática (por exemplo, identificador de sessão armazenado num cookie).
- Isto poderá fazer com que um atacante consiga conduzir a vítima a executar ações não desejadas num sítio web vulnerável em que esteja autenticada.

Clickjacking (UI redressing)

- Clickjacking is a type of attack where a malicious site wraps another site in a frame. This attack can result in an unsuspecting user being tricked into performing unintended actions on the target site.

Riscos de segurança em ficheiros XML

- Entidades externas XML / XML eXternal Entity injection (XXE)
  - An XXE attack occurs when untrusted XML input with a reference to an external entity is processed by a weakly configured XML parser - “OWASP”
- Outros.

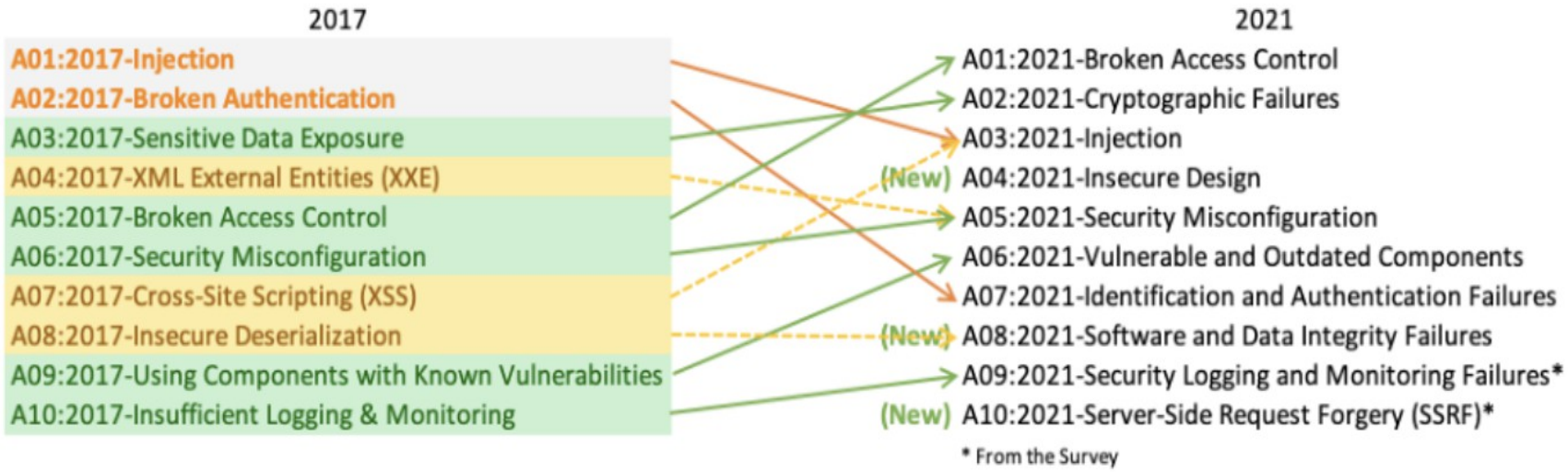
Outras vulnerabilidades

- Configuração por omissão
- Atualizações de segurança
- Dados armazenados em claro

OWASP Top 10

- The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

  https://owasp.org/Top10/



Referências Bibliográficas

- elearning
- Bibliografia

  - ZÚQUETE, André. **"Segurança em redes informáticas"**, 6ª Edição, FCA, 2021
  - STALLINGS, William. **"Network Security Essentials: Applications and Standards"**, 6th Edition, Pearson, 2017
  - CORREIA, Miguel; SOUSA, Paulo. **"Segurança no Software"**, 2ª Edição, FCA, 2017
  - STALLINGS, William. **"Cryptography and Network Security: Principles and Practice"**, 7th Edition, Pearson, 2016
  - STALLINGS, William; BROWN, Lawrie. **"Computer Security: Principles and Practice"**, 4th Edition, Pearson, 2018
  - BARRET, Daniel J; SILVERMAN, Richard E.; BYRNES, Robert G. **"SSH, The Secure Shell: The Definitive Guide"**, 2nd Edition, O'Reilly Media, Inc. , 2005
  - CRIST, Eric F; KEIJSER, Jan Just. **"Mastering OpenVPN"**, Packt Publishing, 2015