A2 Autenticação quebrada e Gerenciamento de Sessões

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ameaça**  **Agentes** | **Vetores de Ataque** | **Segurança**  **Fraquezas** | **Impactos Tecnicos** | **Impactos no negócio** |
| **Especificação da aplicação** | **Exploração**  **MÉDIA** | **Prevalência**  **COMUM // Média de Detecção** | **Impactos Severos** | **Aplicação /**  **Específico de Negócios** |
| Considerar ataques  anônimo  externos,  assim como  Usuários autorizados,  Quem pode tentar  Roubar contas  de outros. Além disso  Considerar intrusos  Querendo disfarçar  Suas ações dentro da organização. | Os atacantes usam vazamentos  Ou falhas na  Autenticação ou  Gestão das  Sessões    (Por exemplo,  Contas expostas,  Senhas, sessão  IDs) para temporariamente  Ou permanentemente, “ (index.of passwd.txt) | Os desenvolvedores costumam criar  Autenticação e esquemas de gerenciamento de sessão  mas construí-los corretamente é  Difícil. Como resultado, esses esquemas personalizados  Freqüentemente possuem falhas em áreas como  Logout, criar conta, alterar senha,  Esqueci minha senha, timeouts, lembre-se  Me, pergunta secreta, atualização da conta, etc.  Encontrar essas falhas às vezes pode ser  Difícil, uma vez que cada uma implementação é unica. | Tais falhas podem Permitir que alguns ou mesmo Todas as contas sejam atacadas. Uma vez com Sucesso, o  atacante pode fazer Qualquer coisa a vítima, ganhar Privilegios do Alvo são freqüente | Considere o Valor de negócio dos dados afetados  E aplicação funções.    Considere também o Impacto nas empresas  como a Exposição pública da vulnerabilidade. |

**Sou Vulnerável ao hijacking?**

Os recursos de gerenciamento de sessão são como credenciais

IDs de sessão devidamente protegidos? Você pode estar vulnerável se:

1. As credenciais de autenticação do usuário não estão devidamente protegidas

Quando armazenado usando hash ou criptografia. Ver 2017-A6.

2. As credenciais podem ser adivinhadas ou substituídas por

Funções de gerenciamento de contas (por exemplo, criação de contas,

Alterar senha, recuperar senha, IDs de sessão fraca).

3. IDs de sessão são expostos na URL (por exemplo, reescrita de URL).

4. IDs de sessão são vulneráveis a ataques de fixação de sessão.

5. IDs de sessão não timeout, ou sessões de usuário ou

Tokens de autenticação (particularmente o single sign-on (SSO)

Tokens) não são devidamente invalidados durante logout.

6. Os IDs de sessão não são rodados após o login bem-sucedido.

7. Senhas, IDs de sessão e outras credenciais são enviadas

Sobre conexões não criptografadas. Ver 2017-A6.

Veja as áreas de requisitos ASVS V2 e V3 para mais detalhes

**Como posso evitar isso?**

A principal recomendação para uma organização é fazer

Disponíveis para desenvolvedores:

1. Um único conjunto de autenticação forte e sessão

Controlos de gestão. Esses controles devem se esforçar para:

A) cumprir todos os requisitos de autenticação e

Requisitos de gestão definidos na OWASP

Padrão de verificação de segurança de aplicativos (ASVS)

Áreas V2 (Autenticação) e V3 (Sessão

Gestão).

B) ter uma interface simples para desenvolvedores. Considere o

ESAPI Authenticator e User APIs como bons exemplos

Para emular, usar ou construir sobre o assunto.

2. Devem também ser envidados esforços enérgicos para evitar falhas XSS

Que pode ser usado para roubar IDs de sessão. Ver 2017-A3.

**Exemplo de cenários de ataque**

Cenário # 1:

Um aplicativo de reservas de viagem suporta URL

Reescrever, colocando IDs de sessão no URL:

http://example.com/sale/saleitems;jsessionid=

2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii

Um usuário autenticado do site quer deixar seus amigos

Saber sobre a venda. O usuário e-mails o link acima sem

Sabendo que eles também estão dando o seu ID de sessão. Quando

Os amigos usam o link que usam sessão do usuário e cartão de crédito.

Cenário # 2:

Os tempos limite do aplicativo não estão definidos corretamente. O utilizador

Usa um computador público para acessar o site. Em vez de selecionar

"Logout" o usuário simplesmente fecha a guia do navegador e caminha

longe. Um invasor usa o mesmo navegador uma hora depois e

Esse navegador ainda está autenticado.

Cenário # 3:

Um intruso ou atacante externo ganha acesso ao banco de dados de senhas do sistema. Senhas de usuário não são Corretamente cifrados em hash e salt expondo a senha de cada usuário.

Referências da OWASP

Para obter um conjunto mais completo de requisitos e Evitar nesta área, ver as áreas de requisitos [ASVS para Autenticação (V2) e Gerenciamento de Sessão (V3) da comunidade.](https://www.owasp.org/index.php/ASVS)

• [Ficha de autenticação OWASP](https://www.owasp.org/index.php/Authentication_Cheat_Sheet)

• [OWASP Esqueceu sua senha?](https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet)

• [OWASP Password Storage Cheat Sheet](https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)

• [OWASP Session Management Cheat Sheet](https://www.owasp.org/index.php/Session_Management_Cheat_Sheet)

• [Guia de Teste OWASP: Capítulo sobre Autenticação](https://www.owasp.org/index.php/Testing_for_authentication)

Externo

• [Entrada CWE 287 sobre autenticação imprópria](http://cwe.mitre.org/data/definitions/287.html)

• [Entrada CWE 384 sobre Fixação de Sessão](http://cwe.mitre.org/data/definitions/384.html)