Excesso de Privilégios

Problemas de Segurança e Invasões em Banco de Dados

TOP 10 TIPOS DE FALHAS DE SEGURANÇA

Posição	2013 - Principais Ameaças	2015 - Principais Ameças
1	Privilégios excessivos ou esquecidos.	Privilégios excessivos ou esquecidos.
2	Abuso de privilégio	Abuso de privilégio
3	SQL Injection	Input Injection
4	Malware	Malware
5	Auditoria fraca	Auditoria fraca
6	Exposição de mídia de storage	Exposição de mídia de storage
7	Exploração de vulnerabilidades e configurações fracas de banco de dados	Exploração de vulnerabilidades e configurações fracas de banco de dados
8	Dados sensíveis sem politicas de segurança.	Dados sensíveis sem politicas de segurança.
9	DoS - Negação de Serviço	DoS - Negação de Serviço
10	Pouca experiência dos profissionais na área de segurança.	Pouca experiência dos profissionais na área de segurança.

Fonte: Perallis

Definição

Privilégios

Significado: Vantagem(ou direito) atribuída a uma pessoa e/ou grupo de pessoas em detrimento dos demais;

De acordo com os requisitos do sistema, cada usuário ou grupo de usuários irão possuir tipos diferenciados de acesso ao sistema. Ao que se dá o nome em Banco de Dados de “Controle de acesso”

Fonte: UAIPLACAS

Excesso de privilégios

Excesso de privilégios

Por definição, um usuário que possui maior abrangência no controle de acesso do sistema, do que o seu cargo na organização permite, caracteriza-se como excesso de privilégios.

Tendo acesso a informações sigilosas e que normalmente não teria acesso pelo seu cargo.

Fonte: giphy

Consequência da má gestão de privilégios

1. Perda financeira
2. Dano de reputação
3. Ações regulatórias de órgãos regulador/fiscalizador
4. Multas
5. e até a falência da organização.

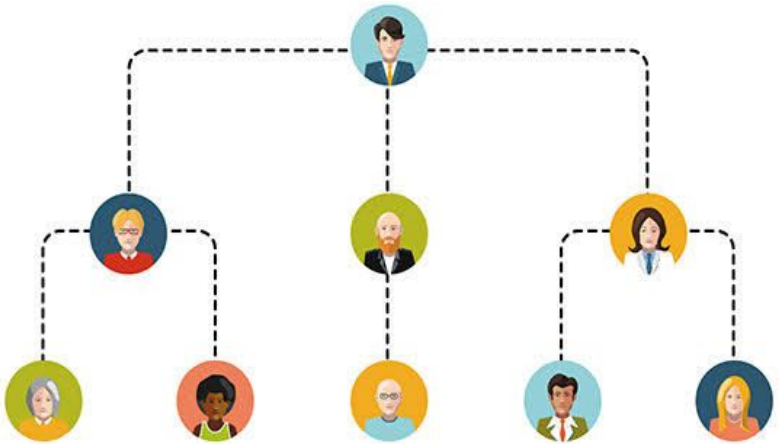
Prevenção

Papéis bem definidos na organização

O sistema tem que estar condizente com o mundo real, ou seja, qualquer alteração no mundo real tem que ser refletido no sistema.

Um dos princípios fundamentais da computação é “não informatizar o caos”. Logo, há situações em que o próprio processo de trabalho da organização possa gerar fragilidades no sistema a ser desenvolvido.

Portanto uma política de papéis bem definida e um processo de trabalho consistente diminui drasticamente o risco de vazamento de dados por **Excesso de privilégios.**



Fonte: JRM

Injeção de SQL

Problemas de Segurança e Invasões em Banco de Dados

Definição

Injeção de SQL

Ameaça de segurança que se baseia na manipulação de SQL.
Surge na falha de sistemas que interagem com o banco de dados, inserindo uma instrução dentro de uma consulta.

“É um ataque no qual um código mal-intencionado é inserido em cadeias de caracteres que são passadas posteriormente para uma instância do SQL”

(Microsoft, 2017)

COMO FUNCIONA

```
var BuscaNome;
BuscaNome = Request.form(“BuscaNome”);
var sql = “select * from Usuarios where Nome = ‘”+BuscaNome+”’”;
```

COMO FUNCIONA

```
SELECT * FROM Usuarios WHERE Nome = ‘Ana’
```

COMO FUNCIONA

```
SELECT * FROM Usuarios WHERE Nome = ‘Ana’
```

```
Ana’ DROP TABLE Usuarios --
```

COMO FUNCIONA

```
SELECT * FROM Usuarios WHERE Nome = ‘Ana’
```

```
Ana’; DROP TABLE Usuarios --
```

```
SELECT * FROM Usuarios WHERE Nome = ‘Ana’; DROP TABLE
Usuarios --
```

Prevenção

Valide todas as entradas

Valide a entrada do usuário testando:

- Tipo
- Comprimento
- Formato
- Intervalo

Fonte: giphy

Use parâmetros seguros

O SQL Server fornece o método “Parameters” que trata a entrada como um valor literal e não mais um código executável

```
SqlParameter parametro =
myCommand.SelectCommand.Parameters.Add("@valor",
      SqlDbType.VarChar);

parametro.Value = Login.Text;
```

Filtre a entrada

Remova caracteres de escape.
Sendo eles: ‘ ou “

```
private string SafeSqlLiteral(string
inputSQL)
{
   return inputSQL.Replace("'", "''");
}
```

Quebra de autenticação por força bruta

Problemas de Segurança e Invasões em Banco de Dados

Definição

AUTENTICAÇÃO POR FORÇA BRUTA

- O ataque de força bruta é um método de adivinhar senhas por meio de tentativas.

- Normalmente tem por objetivo o acesso a alguma área restrita do sistema ou servidor com os privilégios e liberações de acesso do usuário.

Fonte: InfoSafe

Como funciona

Como funciona

Na internet, 8 é geralmente o número padrão para o menor comprimento de uma senha.

Somando-se a quantidade de letras minúsculas(26) com letras maiúsculas(26) e números(10), têm-se um total de 62 caracteres possíveis para cada caractere da senha.

Para uma senha de 8 caracteres, será 62^8, o que representa 2.1834011×10^{14} de combinações possíveis.

Fonte:
How Stuff Works

Prevenção

Prevenção

- Tamanho da senha
- Limitar o número de tentativas falhas
- Complexidade da senha
- Uso de captchas
- Autenticação de dois fatores
- Limitar Login à uma range de IPs ou IP específico

Fonte: giphy

Manipulação de URL

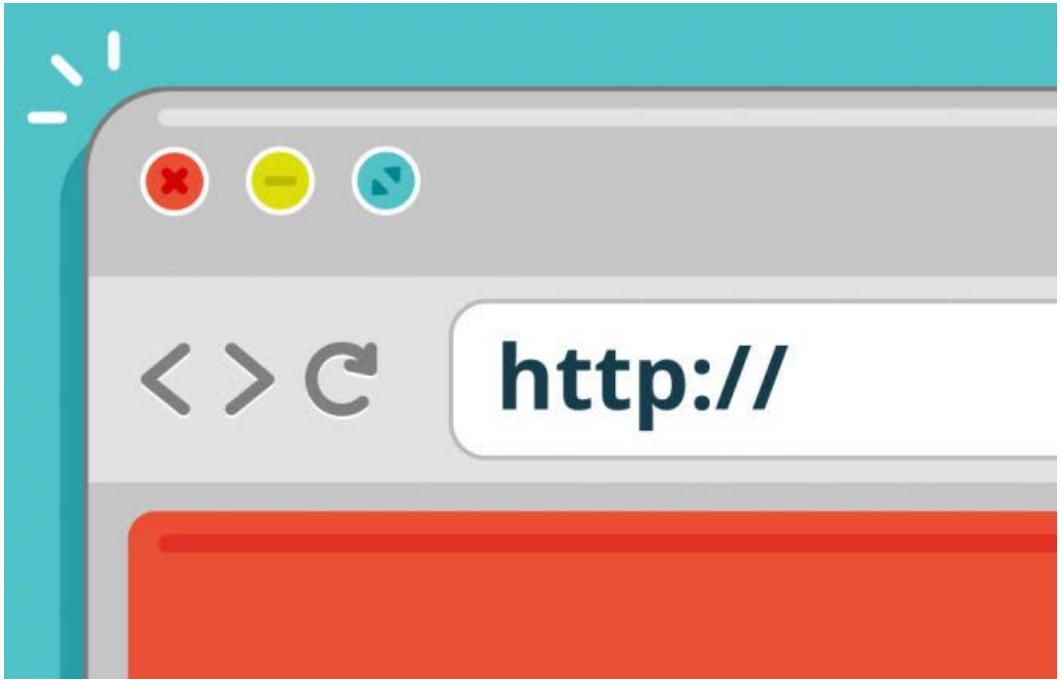
Problemas de Segurança e Invasões em Banco de Dados

Definição

URL (LOCALIZADOR UNIFORME DE RECURSOS)

URL: endereço de um recurso disponibilizado em uma rede, por exemplo, a rede de internet. A URL, nada mais é do que o caminho do recurso que usuário está buscando. Esse recurso pode ser uma página, arquivo, pasta e etc.

Manipulação de URL: a manipulação é geralmente feita por usuários com intenções maliciosas, afim de obter informações que normalmente não teriam acesso.



Fonte: Escola e Educação

Como funciona

Como funciona

Considere a seguinte url:

http://target/forum/index.php3?cat=1&page=2

A url acima representa uma página web para o grupo de usuários da categoria = 1 (Usuário comum)

Uma técnica possível de invasão seria alterar os parâmetros dinâmicos da url de modo que fosse possível visualizar dados de outra categoria de usuários

http://target/forum/?cat=2

Caso a categoria acima(2) fosse uma categoria de administrador e o desenvolvedor não tenha previsto tal evento, o invasor pode obter acesso em informações que não deveria.

Prevenção

CÓDIGOS AUTORIZADOS

Um meio de tornar o site imune é que o mesmo apenas carregue os nomes e códigos autorizados dentro do código.
Ou seja, que ele passe por um filtro no código-fonte.

Mapa de referência
Valor de Índice

Tem como objetivo prevenir ataques de manipulação de parâmetro.
Assim, o usuário que tentar buscar por um parâmetro, de modo malicioso, terá dificuldades em tentar acessar algum dado restrito

BLOQUEIO O ACESSO

Bloqueie o acesso a todos os tipos de arquivos que a aplicação não deve executar. Espera-se que isso venha bloquear qualquer tipo de tentativa de acesso a arquivos de log, XML, dentre outros que possam vulnerabilizar os dados do sistema

BIBLIOGRAFIA

MICROSOFT. Injeção SQL. 2017. Disponível em: <https://docs.microsoft.com/pt-br/sql/relational-databases/security/sql-injection?view=sql-server-ver15>. Acesso em: 17 nov. 2019.

INJEÇÃO de SQL. 2008. Disponível em: <https://www.php.net/manual/pt_BR/security.database.sql-injection.php>. Acesso em: 17 nov. 2019.

CANALTI. SQL Injection: Exemplo prático com PHP + MySQL. 2017. Disponível em: <https://www.canalti.com.br/banco-de-dados/sql-injection-exemplo-pratico-com-php-mysql/>. Acesso em: 10 nov. 2019.

As 10 vulnerabilidades de segurança mais críticas em aplicações WEB. São Paulo: Owasp Foundation, 2007. Disponível em: <https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf>. Acesso em: 17 nov. 2019.

Brute Force Attacks, 2018. Disponível em: <https://phoenixnap.com/kb/prevent-brute-force-attacks>. Acesso em: 17 nov. 2019.