UNIVERSIDADE PORTUCALENSE

Cross Site Scripting

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

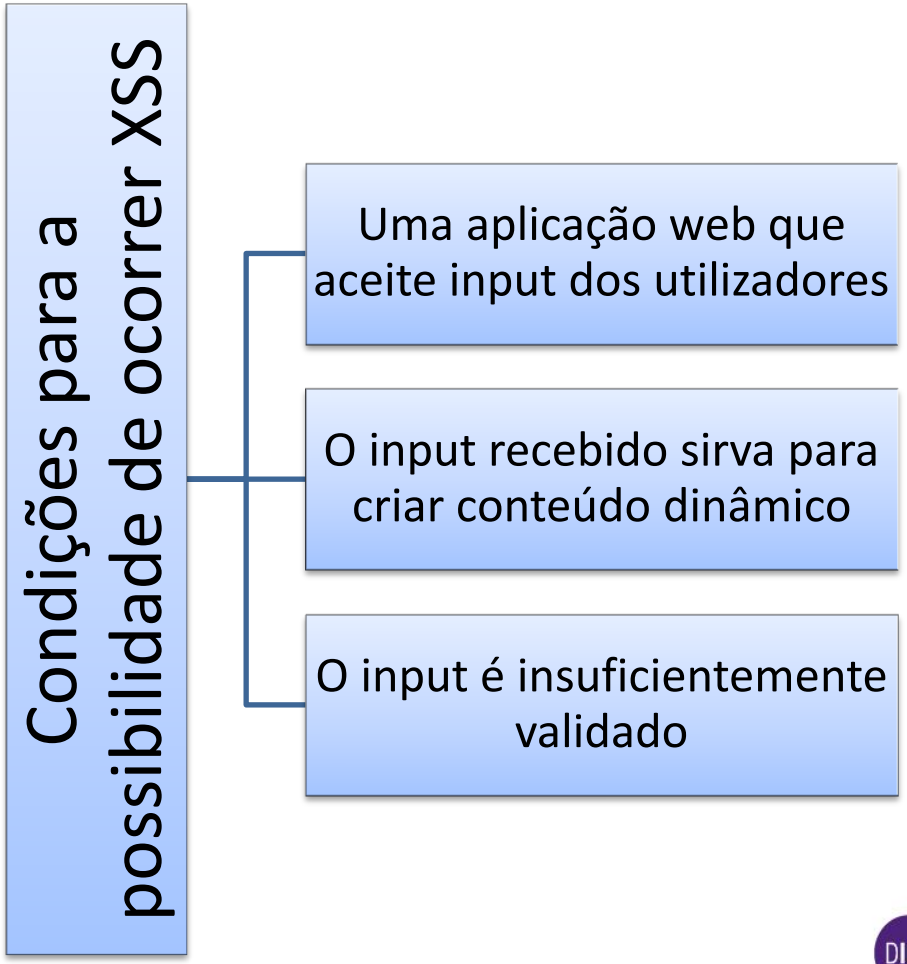
UNIVERSIDADE PORTUCALENSE

Definição

- Cross Site Scripting (XSS) é um problema de segurança que permite que sejam inseridos conteúdos numa zona sem privilégios para serem executados em zonas com privilégios.
- O site de confiança é utilizado para guardar, transportar e disseminar código malicioso para as vitimas
- A ideia é fazer com que o browser execute comandos maliciosos
- É causado por validação insuficiente dos valores de entrada

UNIVERSIDADE PORTUCALENSE

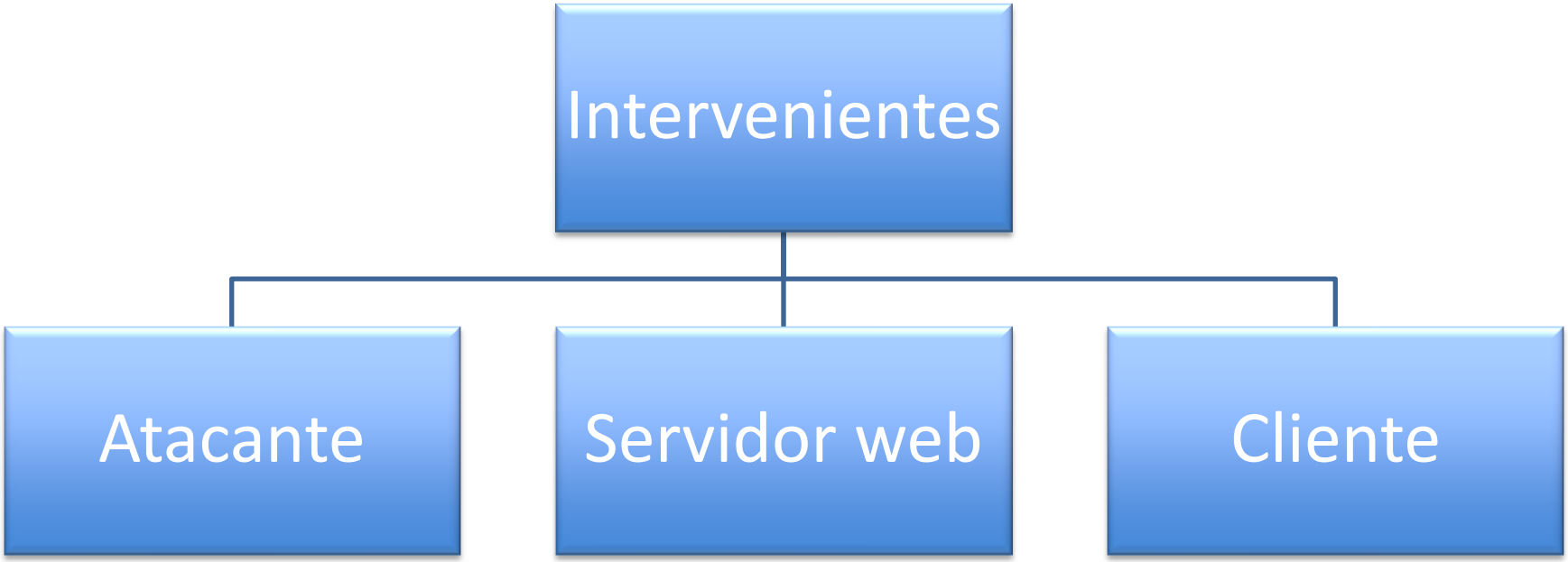
O que é o XSS



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

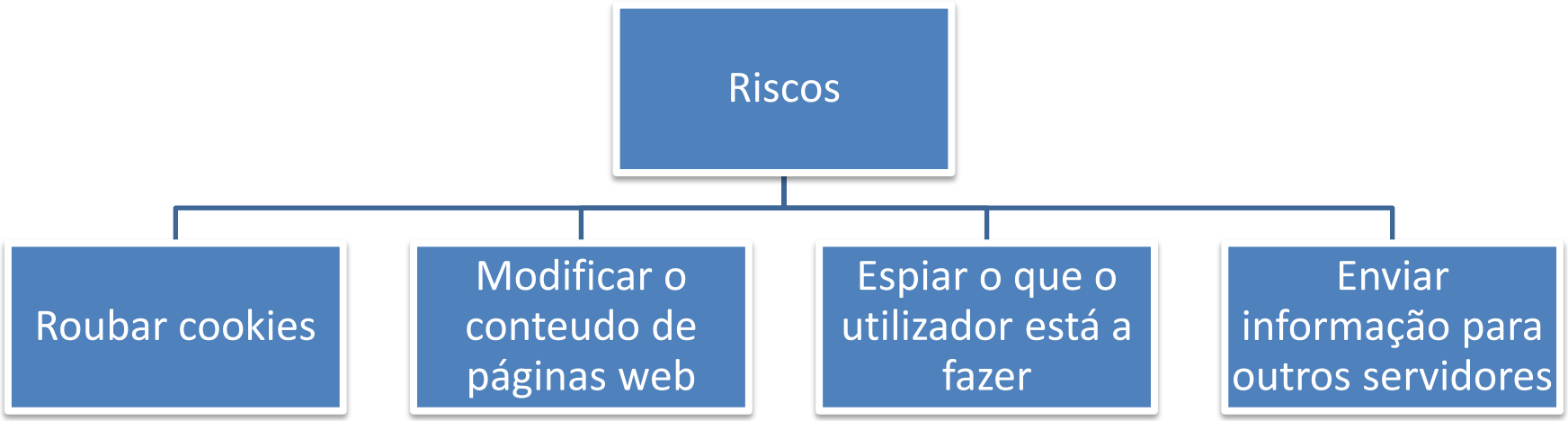
XSS



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

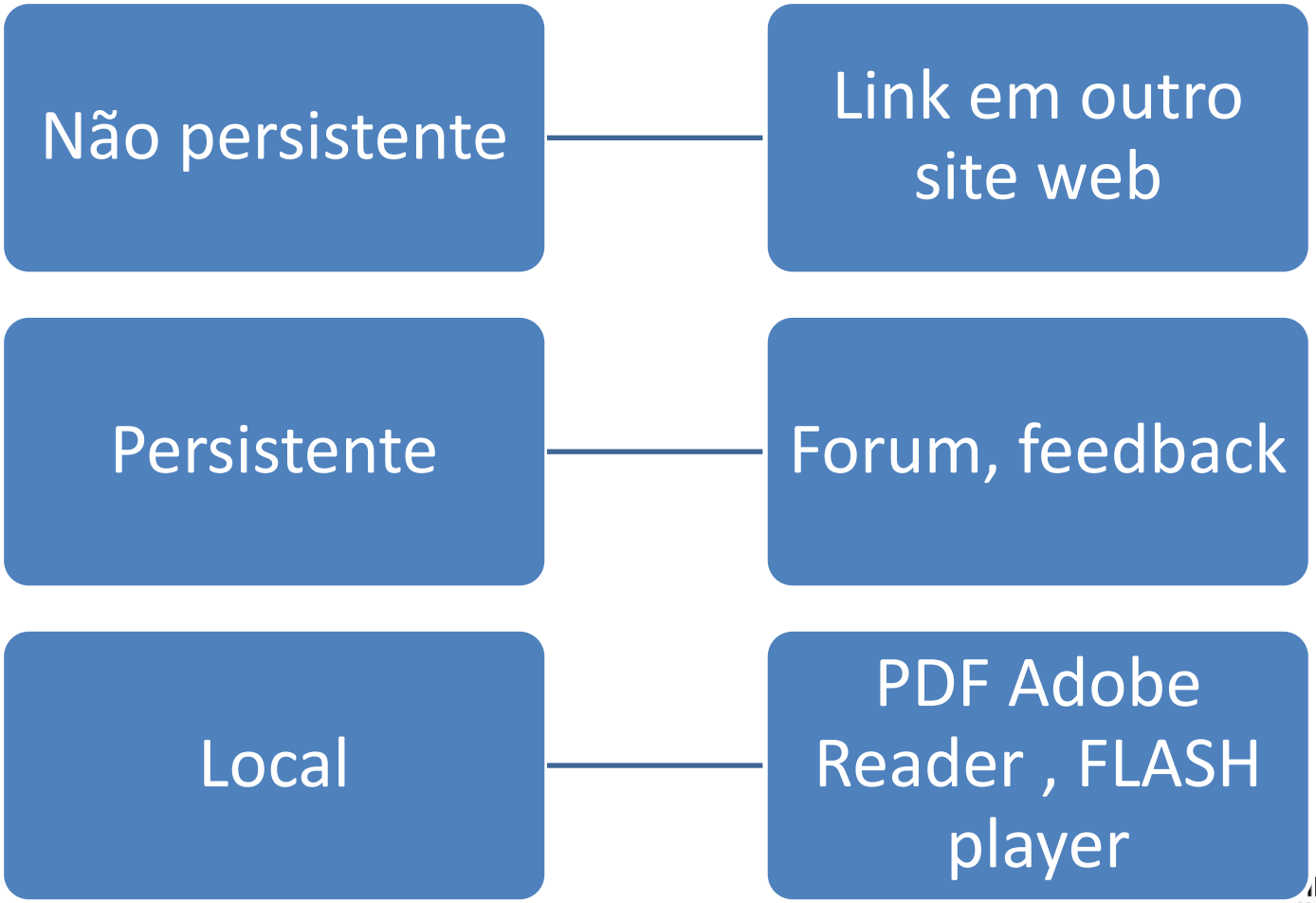
UNIVERSIDADE PORTUCALENSE

Riscos



UNIVERSIDADE PORTUCALENSE

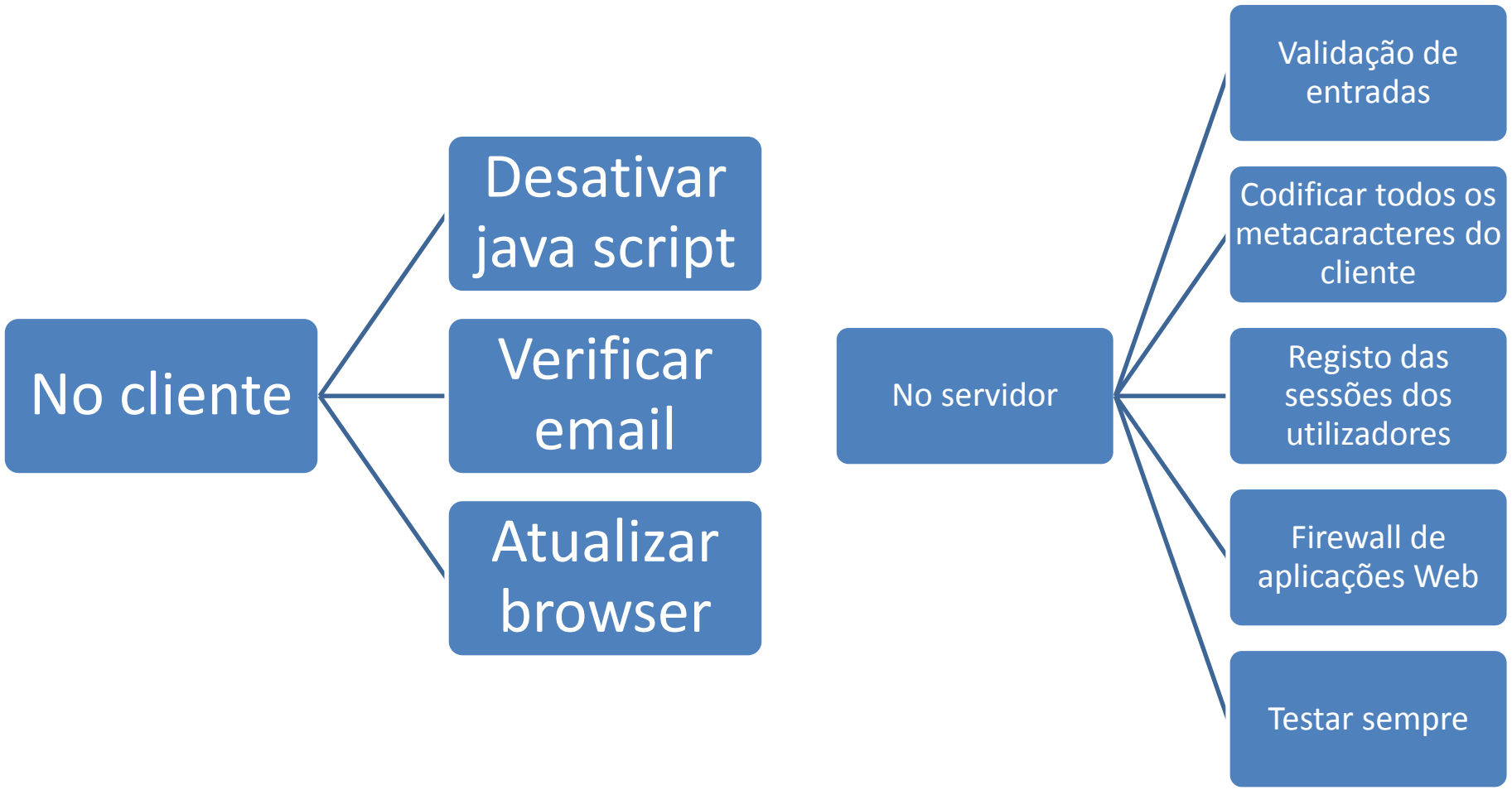
Tipos de XSS



INOVAÇÃO CIENCIA E TECNOLOGÍA

UNIVERSIDADE PORTUCALENSE

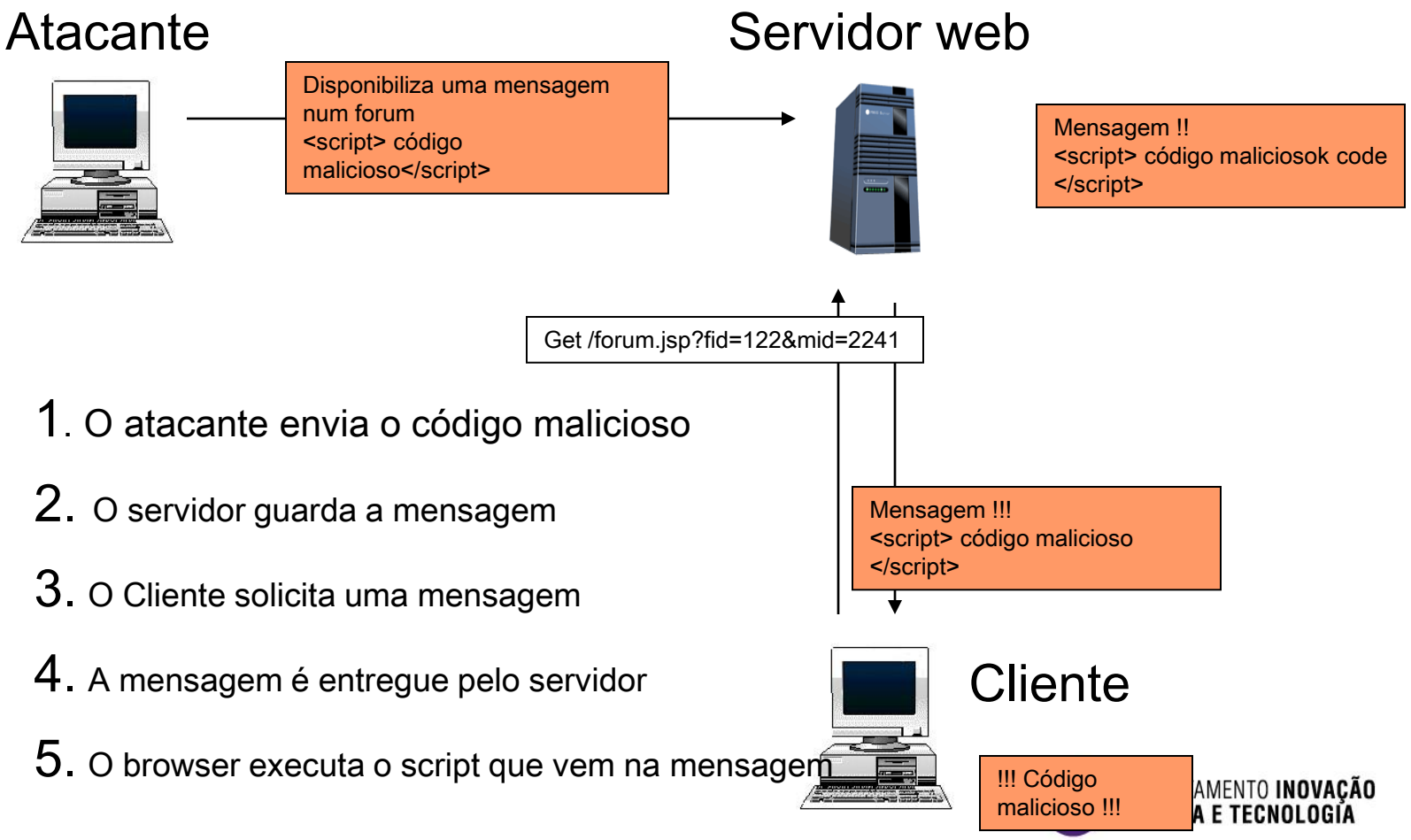
Proteção



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Como funciona um ataque

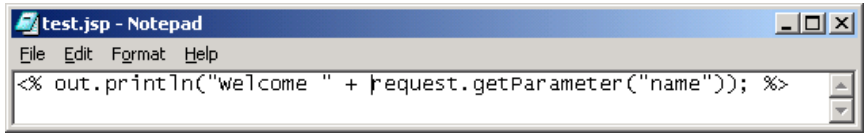


1. O atacante envia o código malicioso
2. O servidor guarda a mensagem
3. O Cliente solicita uma mensagem
4. A mensagem é entregue pelo servidor
5. O browser executa o script que vem na mensagem

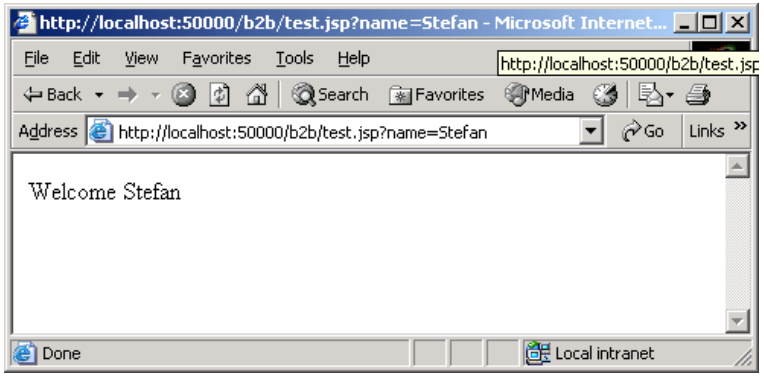
AMENTO INOVAÇÃO
A E TECNOLOGÍA

UNIVERSIDADE PORTUCALENSE

XSS ataque

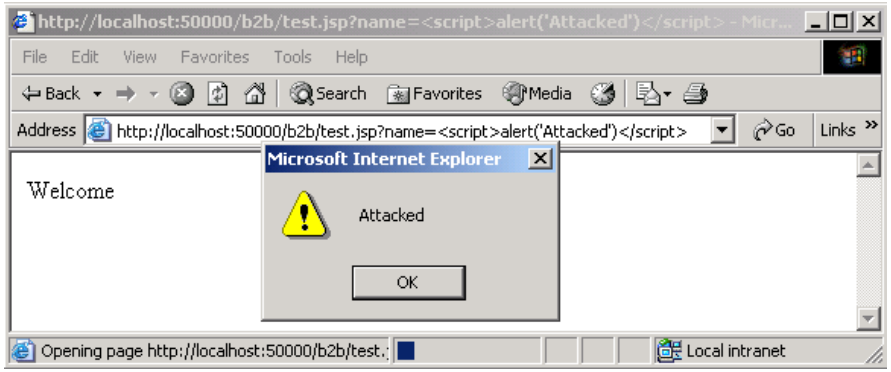


http://servidor.pt/test.jsp?name=Stefan




```
<HTML>
<Body>
Welcome Stefan
</Body>
</HTML>
```

http://servidor.pt/welcome.jsp?name=<script>alert("Attacked")</script>




```
<HTML>
<Body>
Welcome <script>alert("Attacked")</script>
</Body>
</HTML>
```

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Como validar os inputs

- Verificar se o input é o esperado
  - Não se deve verificar por inputs “errados”
- Testar recorrendo a black lists não é solução
  - Estas listas nunca são completas
- Deve-se testar recorrendo a white list
  - Só devem ser aceites os valores esperados
  - Utilizar expressões regulares

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

SQL injection

HTTP Request
POST /login?u=foo&p=bar

SQL Query
SELECT user, pwd FROM users WHERE u = ‘foo’

- O atacante submete um pedido de HTTP com um parâmetro malicioso que altera a query de SQL

UNIVERSIDADE PORTUCALENSE

SQL injection

HTTP Request
POST /login?u=‘+OR+1<2#&p=bar

SQL Query
SELECT user, pwd FROM users WHERE u = ‘’ OR 1<2#

- O atacante submete um pedido de HTTP com um parâmetro malicioso que altera a query de SQL

UNIVERSIDADE PORTUCALENSE

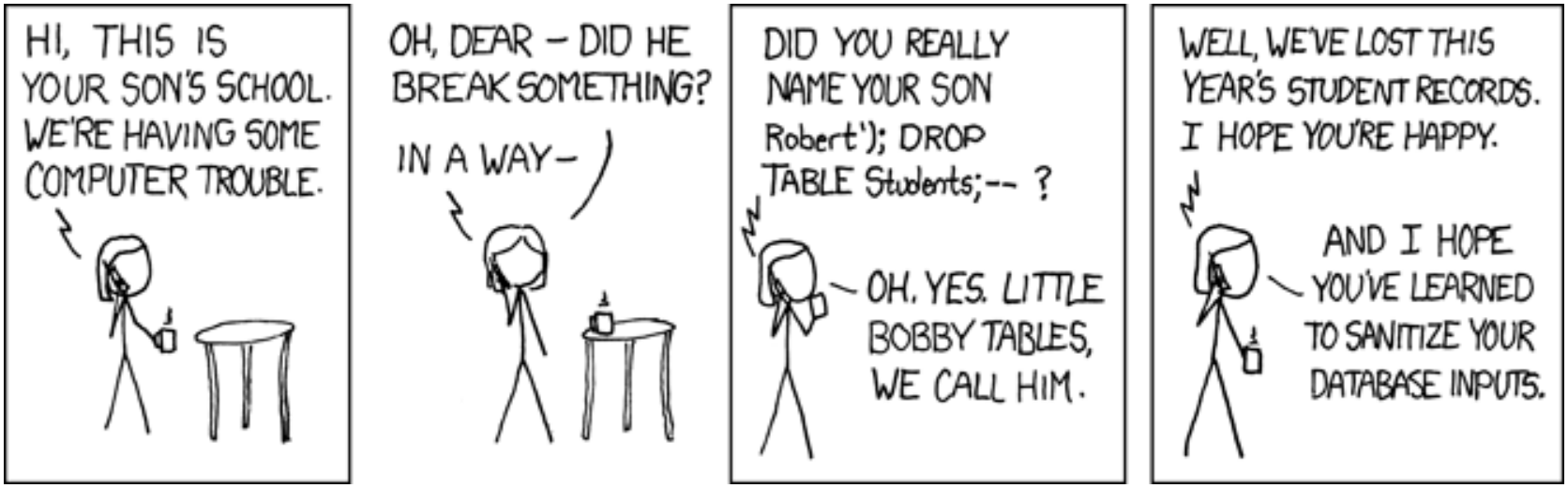
Exemplo de um ataque

Pesquisa: **ol‘ OR ‘x’ = ‘x**

- Este valor é colocado diretamente na query SQL da aplicação WEB
  - $query = “SELECT informacao FROM produtos WHERE nomeproduto = ‘” . $_POST[‘pesquisa’] . “’”;
- Gera o comando de SQL:
  - SELECT informacao FROM produtos WHERE nomeproduto = ‘**ol‘ OR ‘x’ = ‘x**’
- O atacante fica com acesso a toda a tabela.

UNIVERSIDADE PORTUCALENSE

SQL injection



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA