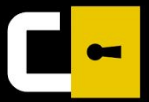
Web e XSS

Palestra 1 - 05/04

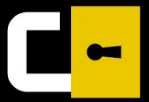
IMEsec

http://bit.do/ecN9m

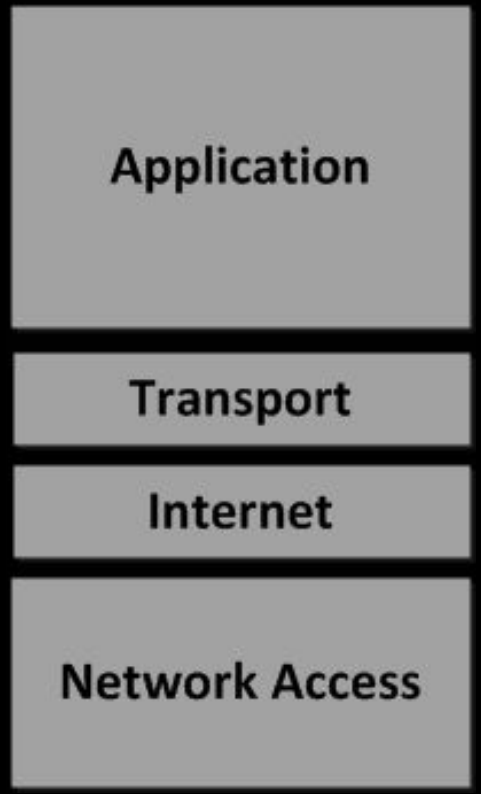
Internet x Web



Internet x Web



TCP/IP Stack



Domínios:
www.google.com

HTTP, SMTP, FTP, SSH, DNS, ...

porta: :80, :443...

TCP, UDP

Endereço de IP:
103.204.80.23

IP, ICMP, ...

Ethernet, 802.11 (Wi-fi)...

Demo: Servidor de tempo em 10 linhas em ruby

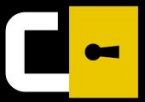
http://

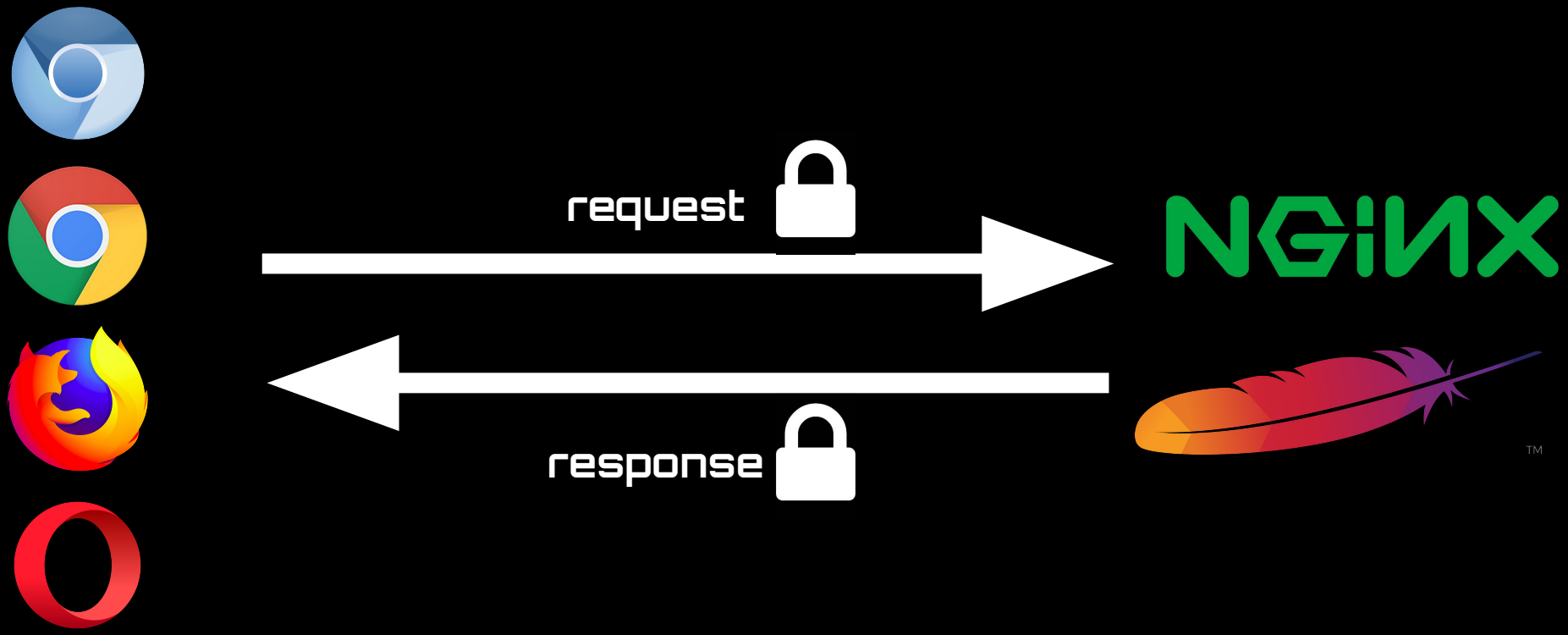
(e https://)

request

response

NGINX




request
response
NGINX
TM

Request:

```
GET /user?id=3 HTTP/1.1
Host: www.simplesite.com
```

Response:

```
HTTP/1.1 200 OK
Host: www.simplesite.com
Content-type: text/html; charset=UTF-8
Connection: close

<html><body><p>Hello World!</p></body></html>
```

DEMO:

```
curl -v http://www.google.com.br/
```

Um pouco mais sobre HTML

```
<html>
    <head>
        <title>Some Site</title>
        <script>console.log('example javascript!')</script>
    </head>
    <body>
        <h1>Hello World!</h1>
        <p>This is an example site.</p>
    </body>
</html>
```

Um pouco mais sobre HTML

```
<html>
    <head>
        <title>Some Site</title>
        <script>console.log('example javascript!')</script>
    </head>
    <body>
        <h1>Hello World!</h1>
        <p>This is an example site.</p>
    </body>
</html>
```

HTML não é uma linguagem de programação completa.

Solução? JavaScript!

```
<script>run_js()</script>

<script src=http://xss.rocks/xss.js></script>

<body onload=run_js() />

<img src='javascript:run_js()' />

<img onmouseover=run_js() />

<img src='/idontexist.jpg' onerror=run_js() />
```

Não há nada de errado ter vários métodos de invocar javascript.

...só quando as pessoas programam seus sites errado.

XSS: Cross site scripting

Programas mal feitos não escapam input do usuário

(nunca confie no usuário!)

Case 1:

```
<form action="<?php $_PHP_SELF ?>" method="POST">
  Name: <input type="text" name="name" />
  Age: <input type="text" name="age" />
  <input type="submit" />
</form>
<p>
  <?php
  if( $_REQUEST["name"] || $_REQUEST["age"] ) {
    echo "Welcome ". $_REQUEST['name']. "<br />";
    echo "You are ". $_REQUEST['age']. " years old.";
  }
  ?>
</p>
```

```
<form action="<?php $_PHP_SELF ?>" method="POST">
  Name: <input type="text" name="name" />
  Age: <input type="text" name="age" />
  <input type="submit" />
</form>
<p>
  <?php
  if( $_REQUEST["name"] || $_REQUEST["age"] ) {
    echo "Welcome ". $_REQUEST['name']. "<br />";
    echo "You are ". $_REQUEST['age']. " years old.";
  }
  ?>
</p>
```

como está:

```
echo "Welcome ". $_REQUEST['name']. "<br />";
```

como deveria ser:

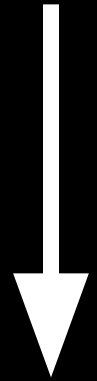
```
echo "Welcome ".htmlspecialchars($_REQUEST['name'], ENT_QUOTES, 'UTF-8');
."<br />";
```

Demo:

http://linux.ime.usp.br/~razgrizone/sandbox/xss.php

Case 2:

www.ms.gov.br/?s=abacate

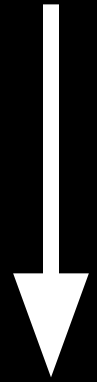


```
<input type="text" name="s" value="abacate" placeholder="Digite um termo
para pesquisar...">
```

www.ms.gov.br/?s=">

```
<input type="text" name="s" value="&quot;&gt;" placeholder="Digite um termo
                                para pesquisar...">
```

www.ms.gov.br/?s=">

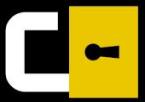


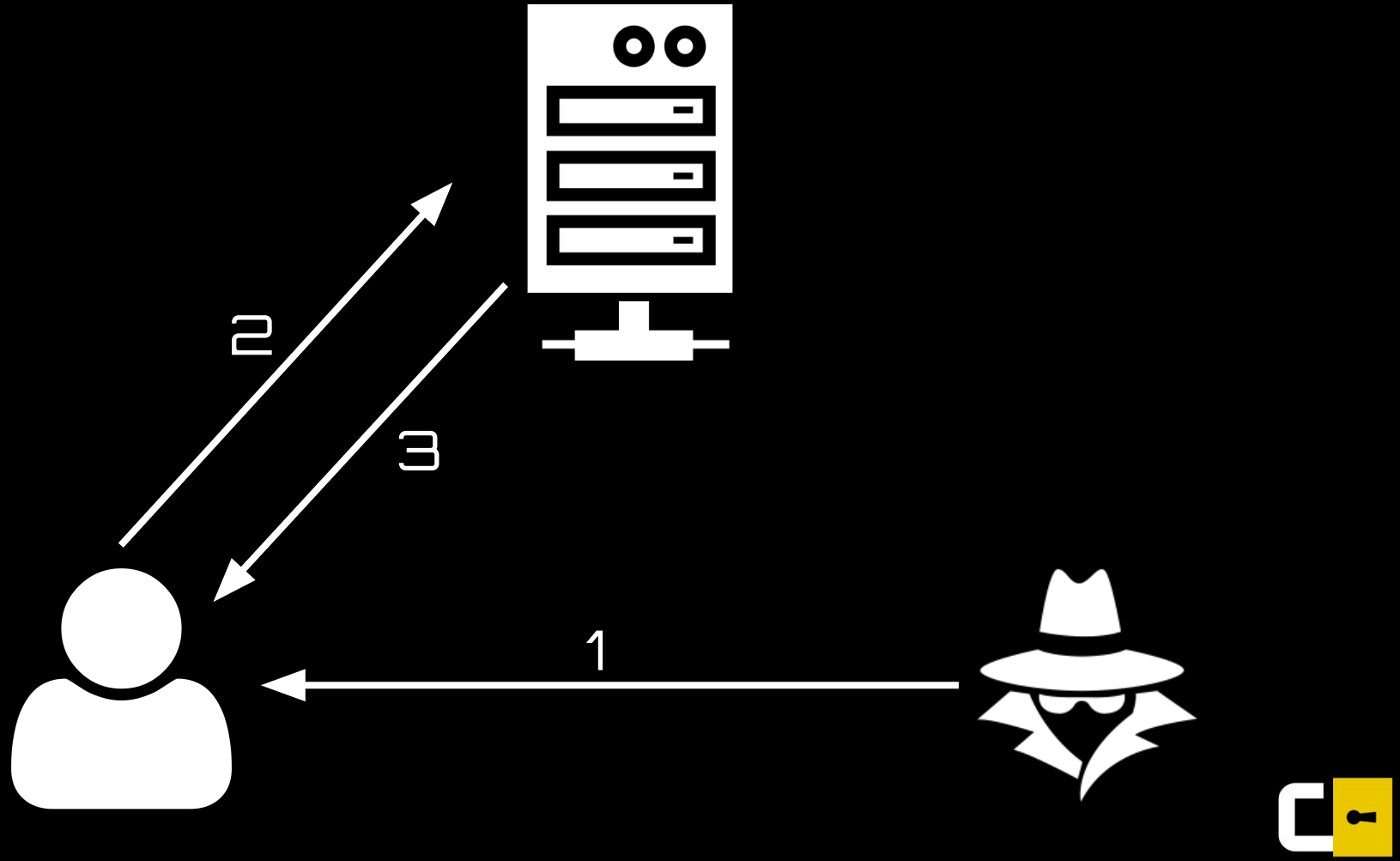
```
<input type="text" name="s" value=""> " placeholder="Digite um termo para
pesquisar...">
```

Reflected XSS

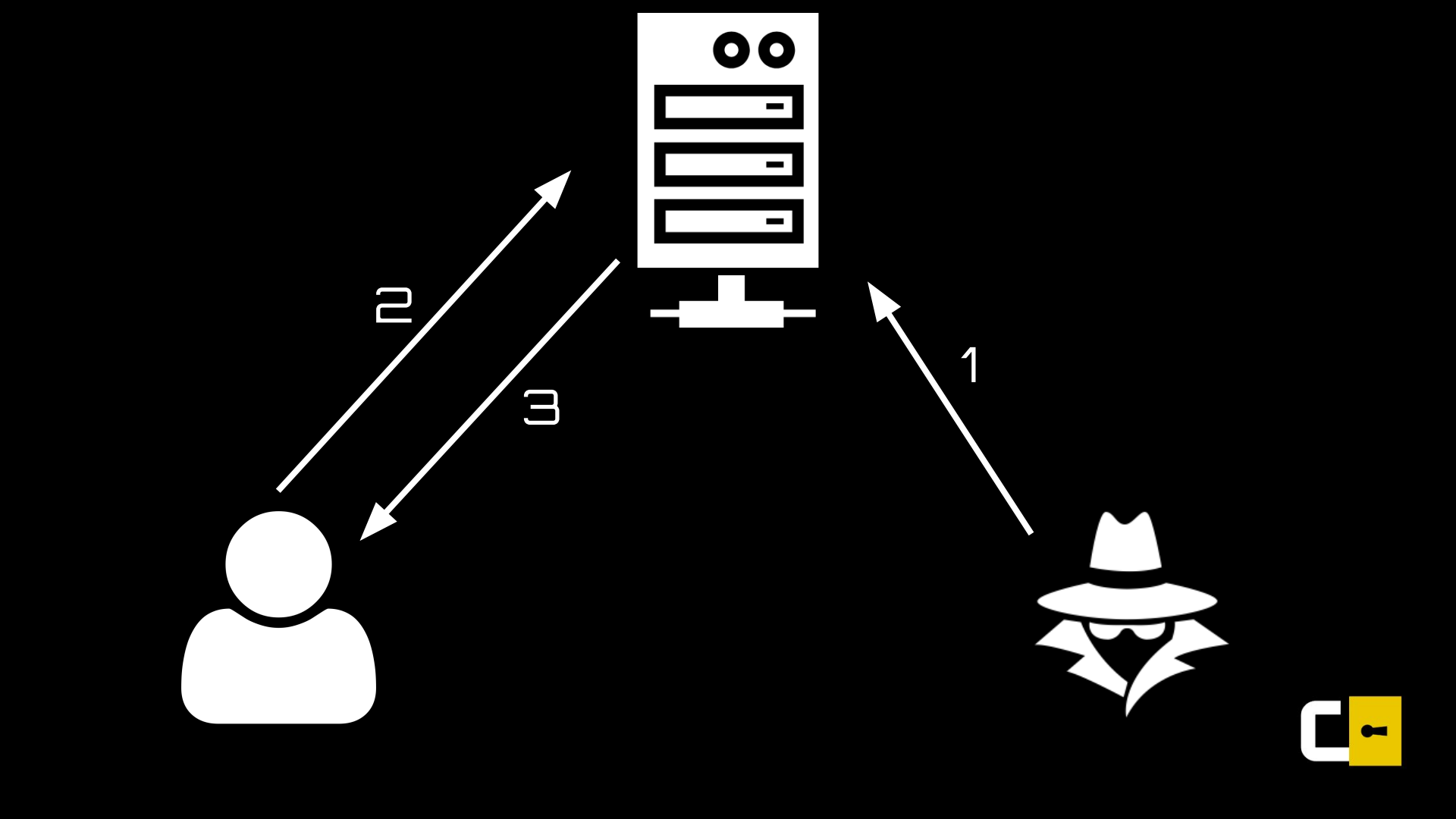
pedido malicioso

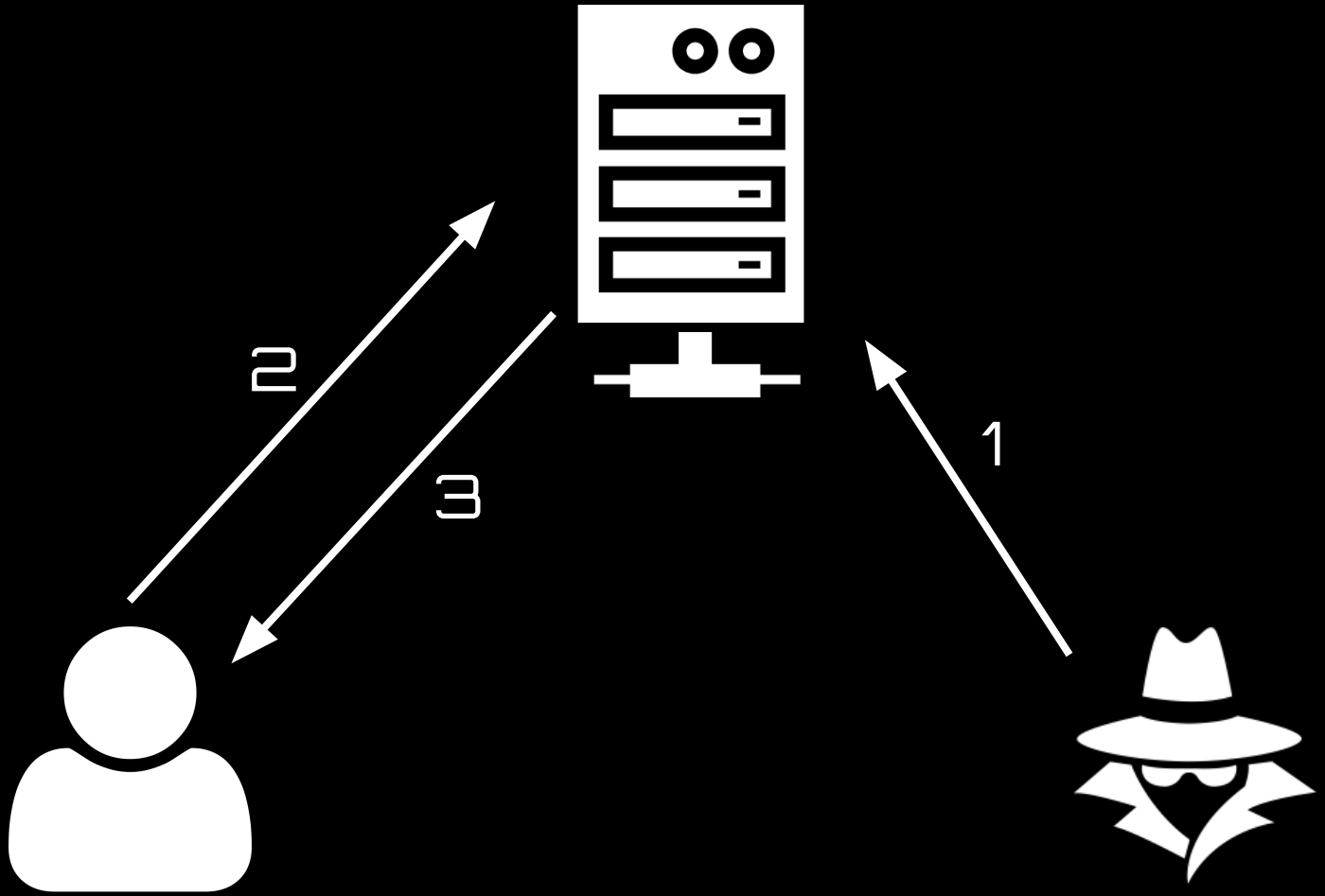
resposta quebrada




2
3
1

Stored XSS


2
3
1



O servidor armazena o XSS!


Paca
ENGLISH (EN)
Pedro Pereira < img onerror=alert('xss in paca'); src='/>
Pedro Pereira < img onerror=alert('xss in paca'); src='/>
Customise this page
COURSE OVERVIEW
Timeline
Courses
In progress
Future
Past
MAC0219/5742 Introdução à Programação Concorrente, Paralela e Distribuída
Curso de computação paralela e distribuída
MAC0350 Desenvolvimento de Sistemas Computacionais
O principal objetivo desta disciplina é prover técnicas de bancos de dados e engenharia de software de modo a viabilizar o ...
MY ENROLLED COURSES
MAC0350 Desenvolvimento de Sistemas de Computação
MAC0350 Desenvolvimento de Sistemas Computacionais
Show/Hide courses
LATEST BADGES
You have no badges to display

Case 3: Tweetdeck

Case 4: MySpace


MySpace.com | Home
The Web
MySpace
Search
Help | Sign
classmates.com
I graduated in:
State: MD
Year: 90
GO!
Springfield High (1084)
Martin Luther King High (676)
Trinity High School (328)
NEW! YOUR High School (820)
Home | Browse | Search | Invite | Rank | Mail | Blog | Favorites | Forum | Groups | Events | Games | Music | Classifieds
KICK A$$
Mail Center
Friend Request Manager
I RULE
Approve or Deny Your Friend Requests Here [he
Inbox
Saved
Sent
Trash
Bulletin
Friend Requests
Pending Requests
Event Invites
Listing 1-10 of 919664
1 2 3 4 5 >> of 91967
Next
Date:
From:
Confirmation:
PLEASE DON'T PRESS CHARGES
Oct 4, 2005 10:22 PM
Online Now!
Lulu the Loveable Freak wants to be your friend!
Approve
Deny
Send Message

Conclusão

Nunca confie no input do usuário.

Obrigado!