



Hack Night

Week 3: Web Security

But first...

Make sure you have signed in!

Grab some food :)




Hack Night chat: <https://hn-chat.csaw.io>

Sign up link: <https://goo.gl/rSpeI0>




Join our mailing list: <https://goo.gl/wRe0U5>

HTML

HyperText Markup Language used to render pages on browsers

 Preview File  Save File  Search Ln: 14 Col: 1

```
1  <!doctype html>
2  <html>
3    <head>
4      <meta charset="utf8" />
5      <title>Hello World</title>
6      <link rel="stylesheet"
7          type="text/css"
8          href="main.css" />
9    </head>
10   <body>
11     <h1>Hello, world!</h1>
12   </body>
13 </html>
14
```



Hello, world!

CSS

Style sheet language easier
way of styling web pages

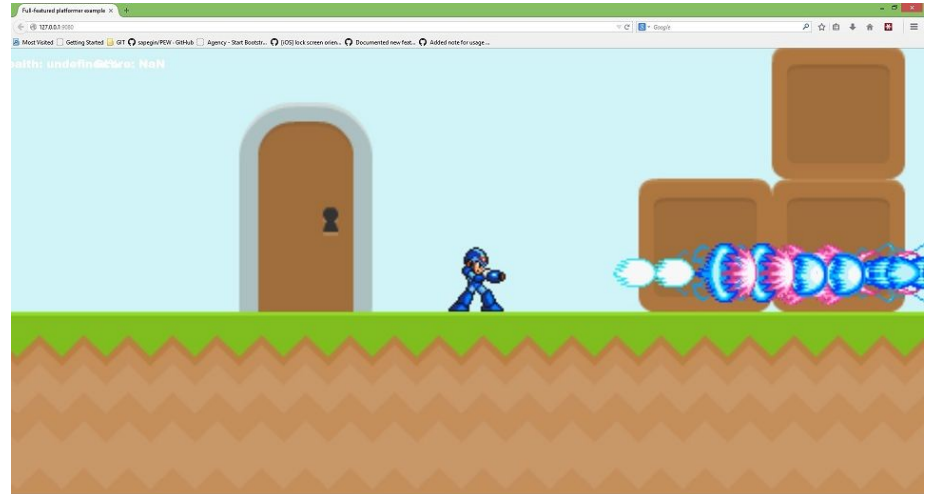
Very flexible and convenient

Anatomy of a CSS Rule



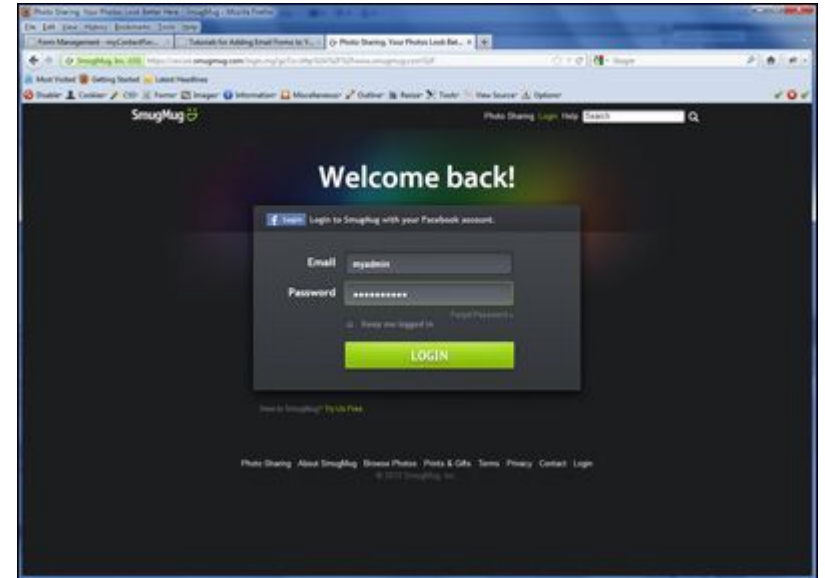
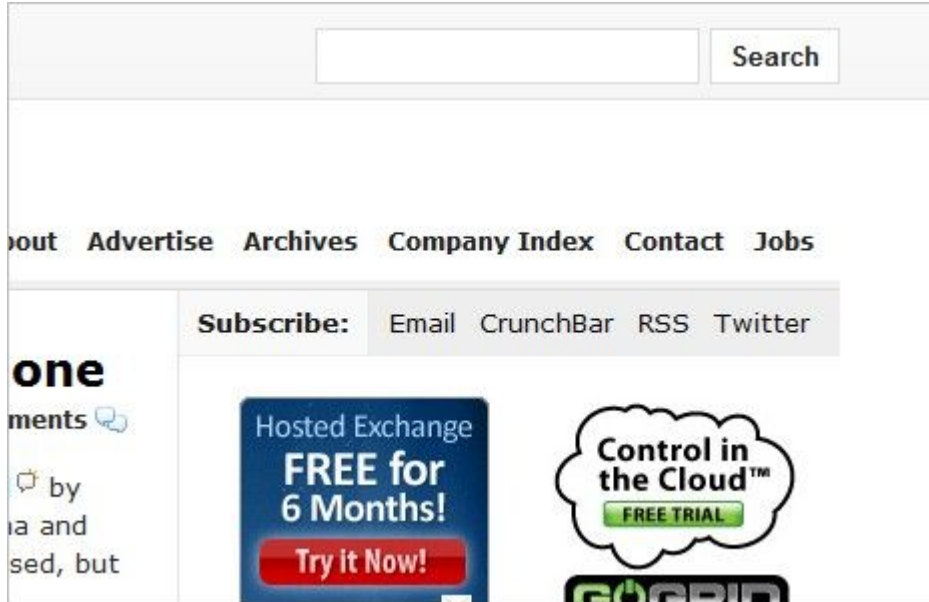
JavaScript

Client side programming language used to make web pages interactive or dynamic



PHP

Scripting language primarily used for server side operations



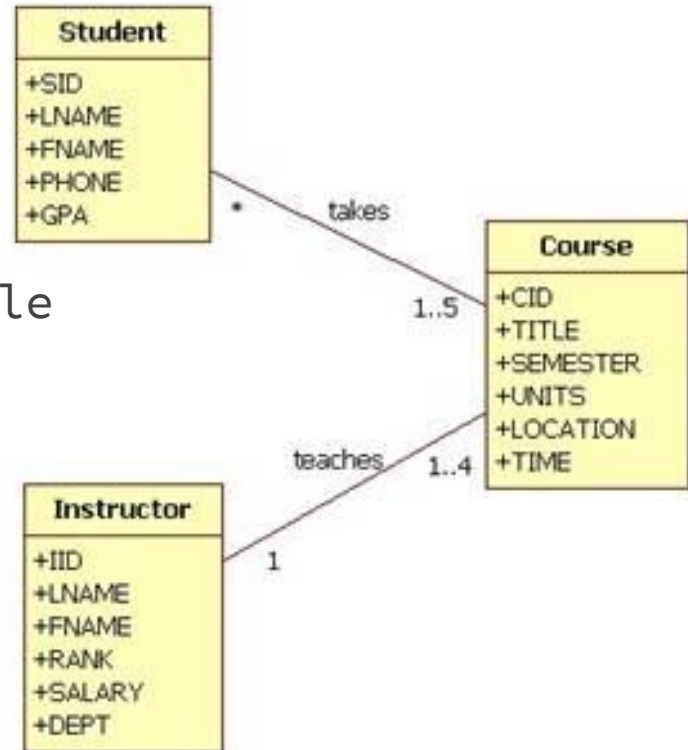
Databases

Insanely powerful spreadsheets

Searchable, programmable, restrictable

Students Records				
	Student #	First Name	Last Name	Gender
	255084	Gertrude	Monay	Female
	947225	Raymond	Kouma	Male
	735395	Alain	Paulson	Male
	293744	Robert	Bidoula	Male
	802481		Massimo	Unknown
✎	927950	Willie	Crows	Female
*				

Close



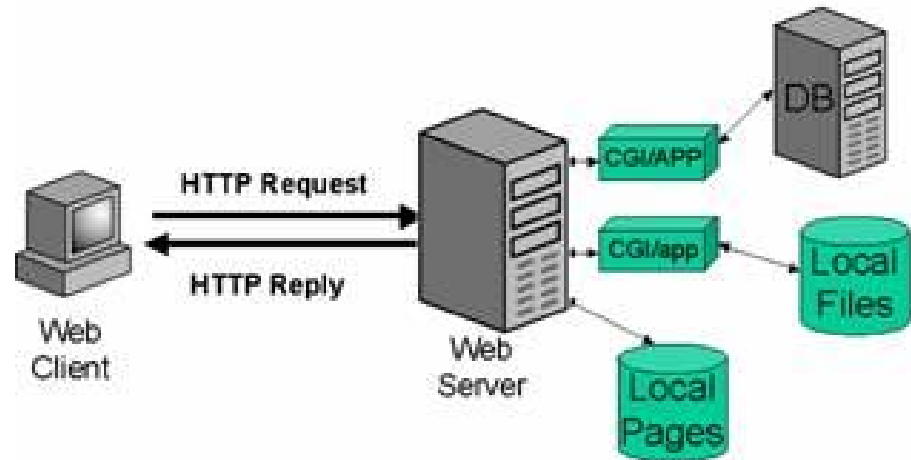
SQL

Structured Query Language

Used to interact with a database. Request, input, or delete information.

Simple and easy
understand

Web server Architecture



```
String SQLQuery ="SELECT Username, Password  
FROM users WHERE Username='" + Username +  
"' AND Password='" + Password + "'";
```

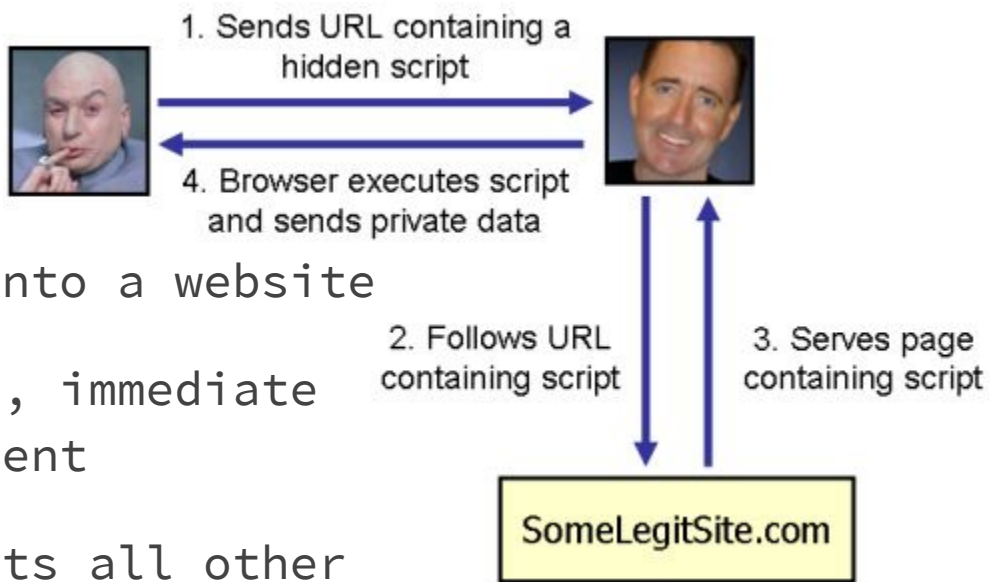

Cross Site Scripting (XSS)

Injecting unauthorized code into a website

Reflected XSS: Not persistent, immediate input only affects single client

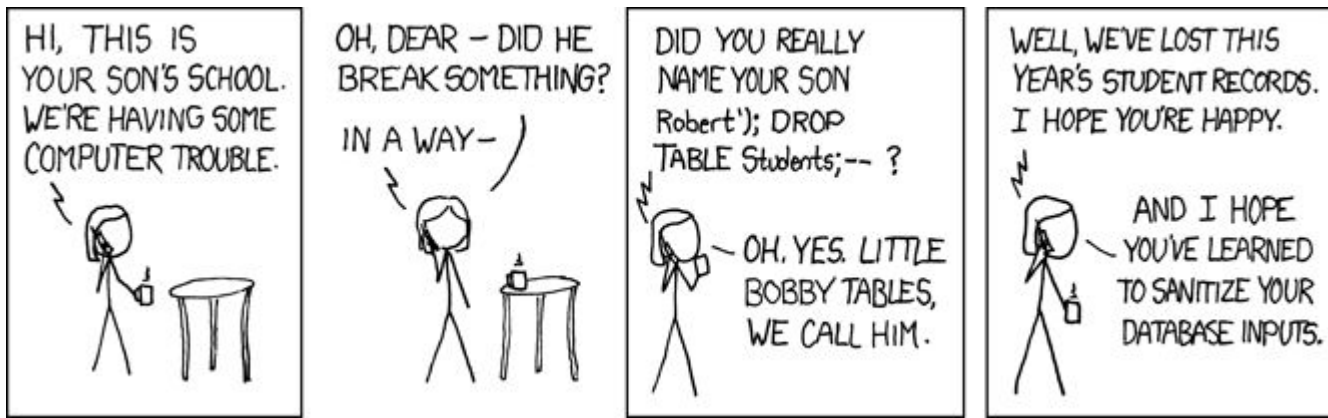
Stored XSS: Persistent, affects all other users on the site

DOM-based XSS: Executed as a result of modifying DOM environment



SQL Injection

Executing unauthorized queries to either retrieve or insert protected information



SQL Injection

When user input is not validated or sanitized attackers can get into the query string and manipulate it

SQL Injection.

User-Id:

Password:

`select * from Users where user_id= ' srinivas ' and password = ' mypassword '`

User-Id:

Password:

`select * from Users where user_id= ' ' OR 1 = 1; /* ' and password = ' */-- '`

Command Injection

— — —



Identifying places where
unsanitized user input is evaluated
as a command

Find a way to execute additional
commands using the existing command

Wargames

— — —

<http://prompt.ml>

<https://xss-game.appspot.com>

<http://overthewire.org/wargames/natas/>

<http://picoctf.com>

Let's try it out

Go to <https://hn.csaw.io>

Osiris wifi password:

deeeeeeeaaaaaadbeeeeeeeeeef