Web Security: Active Defense

Luciano Arango ‘16

seguratec

saving | your | digital | life

Harvard SEAS

Information Security Office

WARNING

- We haven’t seen some of this material yet

- I’ll fly through it but I promise you’ll see it

Stay Ethical/Legal

Don’t try this at home

– Unless you own it, then definitely try

– Cops don’t like jokes

Head over to

http://www.hcs.harvard.edu/hrak/

XSS (Cross-Site Scripting)

XSS Javascript

- Javascript is run on the clients web browser
- Inject malicious Javascript
  - Persistent
  - Non-persistent

Example

- `alert()`

- How could this be malicious?

Preventing XSS

- Sanitizing user input
- NOT just looking for <script>
- `htmlspecialchars()`

SQL Injection

SQL

Special programming language designed for managing data held in databases

```
"SELECT * FROM users WHERE name =   '$username’ ";
```

SQL Injection

Insert malicious code to steal data or cause damage

What if $username = ' or '1'='1

```
"SELECT * FROM users WHERE name =   '$username’ ":

"SELECT * FROM users WHERE name =   '' or '1'='1' ";
```

Then it will always be true

SQL Injection

```
"SELECT * FROM users WHERE name =   '$username’";
```

What if $username = ';DROP TABLE users;--

```
"SELECT * FROM users WHERE name ='';DROP TABLE
users;--’";
```

Good bye tables!

Example

- Use #

Prevent SQLi

```
$sth = $dbh>prepare('SELECT name, colour, calories
FROM fruit WHERE calories < ? AND colour = ?');

$sth->execute(array(150, 'red'));

$red = $sth->fetchAll();

$sth->execute(array(175, 'yellow'));

$yellow = $sth->fetchAll();
```

Relying On Others

- Are you using frameworks?
- Bootstrap?
- Wordpress?
- Make sure you keep updated and in the loop

Passwords and PII

Passwords

- Don’t store passwords in Plain Text
- One way hash
  - `sha1($password)`
  - Not really good

Hash

- Salting is better
  - sha1('thisismyveryfirstsalt' . $pw)
  - They don’t know your salt
  - Harder to compute
- Think of rand(), we know what it generats now
- Random salts are better

Hash

- `crypt()` is the best
- Hashes and salts for you many times

Personal Identificable Data

- Examples:
  - Social Security
  - Credit Card
  - Sometimes Name with DOB
- Be careful with it
- Don't get sued

Shell Injection

Shell Injection

- Intruder gets to run code on your server

- Hacker ☺
- You ☹

Example

- Try it!

- `".system('uname%20-a')%3B%23"`

Prevent Shell Injection

- Don't use eval

- Don't use system

- Don't allow file uploads

Prevent Shell Injection

- Don't use eval
- Don't use system
- Don't allow file uploads

Tools

- Security Compass Firefox add ons
  - –SQL Inject Me
  - –XSS Me

Principles

- Never trust the user
- Sanitize everything
- Always be updated

Thanks to

- PentestLabs
  - https://www.pentesterlab.com/

- Carl Jackson ’13 2011 Web Security Seminar
  - Go watch it

- Questions? Comments?
  - lucianoarango@college.harvard.edu
  - lucianoa@seas.harvard.edu