



Server-Side Languages

Todd Smith
tbsmith@fullsail.com

Welcome to SSL Day 5!

Sessions, Hashing, and Salting

Day 5



Server-Side Languages

Sessions

A session is a method for managing user authentication. Files are created on the server-side that store user information.

A session is created upon successful login.

A session is destroyed upon logout or after a specified amount of time.



Server-Side Languages

Sessions

In PHP, we will use the built-in sessions package:

<http://www.php.net/manual/en/book.session.php>

In Python, we will wait for ASL to use a framework such as Web.py or Django

Day 5



Server-Side Languages

PHP Sessions

The `session_start()` method should be at the top of the index file, which all urls are mapped to.

```
<?php  
session_start();
```

Then use `$_SESSION` to get and store information.



Server-Side Languages

Protector

```
<?php

if (    empty($_SESSION)
    || empty($_SESSION['isLoggedIn'])
    || $_SESSION['isLoggedIn'] != True ) {

    // User is logged out
    header('Location: /user/logout');

}

// Else the user is logged
// in, so do nothing

?>
```

Include this on any pages that
require a login

```
<?php include "models/protector.php"; ?>

Aliens shot JFK!
```



Server-Side Languages

Hashes

A hash is the result of a one-way mathematical algorithm applied to plain-text.

The plain-text is variable length and the hash is of fixed length (32 characters).

Day 5



Server-Side Languages

Some hash algorithms are:
MD5, SHA-1, SHA-2

These are some MD5 hashes:

“dog”

06d80eb0c50b49a509b49f2424e8c805

"SSL is the most awesome class ever PHP is cool and **P**ython is cool too"

7894ff5c182503c159e0abe05696f56f

"SSL is the most awesome class ever PHP is cool and **p**ython is cool too"

a85ac7187c8292f1ea76f6cb84c30ed8

Day 5



Server-Side Languages

Hashes are kept in the database

userId	username	passwordHash	email
1	admin	e16ee4c36d92734e62cbe901d905fbc7	admin@example.com
2	joe	4017f8a42762bd17d7cd87a5c1b1894e	joe@example.com
3	sally	4b3e92f329ab31517bff77cac7b5862c	sally@example.com

When a user logs in, the typed password is hashed and compared to the hash in the database.



Server-Side Languages

The MD5 function in PHP

```
<?php  
  
$a = "Hello World";  
  
echo md5($a);  
  
?>
```

```
b10a8db164e0754105b7a99be72e3fe5
```

Day 5



Server-Side Languages

The MD5 function in Python

```
#!/usr/bin/python

import hashlib
m = hashlib.md5()
m.update("Hello World")
print m.hexdigest()
```

```
b10a8db164e0754105b7a99be72e3fe5
```



Server-Side Languages

Salt

Salt is an extra random string that is added to the user's password before it is hashed.

It helps to prevent brute-force attacks on the hash.



Server-Side Languages

Salt

Each user has a secret salt generated during the creation of his user account.

saltId	userId	salt
1	1	McJ5Z[l?/ns*BmllJw@
2	2	R7)%p5Dd2BLLZ2~?mGYJ
3	3	`F`%VfoHfs]&z#JY(,"?

Random chracters

Day 5



Server-Side Languages

Lab 5

Incorporate registration, login, and sessions into your PHP website.

Make a screencast tour of your code.

Day 5