



# **(PHP) Sessions, Cookies, & Authentication**

**Gerard Sychay**

**#tek11**

**05/26/2011**



0.

## Introduction



**Gerard Sychay.**

**Zipscenemobile.com**

**Cincy Coworks**

0.

Introduction

# This is Henry



# 0.

## Introduction

**facebaby**

Email

Password

☒ Keep me logged in

[Forgot your password?](#)

Login



**Sign Up**  
It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am: 

Select Sex:

Birthday: 

Month:

Day:

Year:

Why do I need to provide this?

Sign Up

Create a Page for a celebrity, band or business.

# 0.

Introduction

**1. Sessions**

**2. Authentication**

**3. Keep Me Logged In**

**4. Security**



# 1.

## Sessions

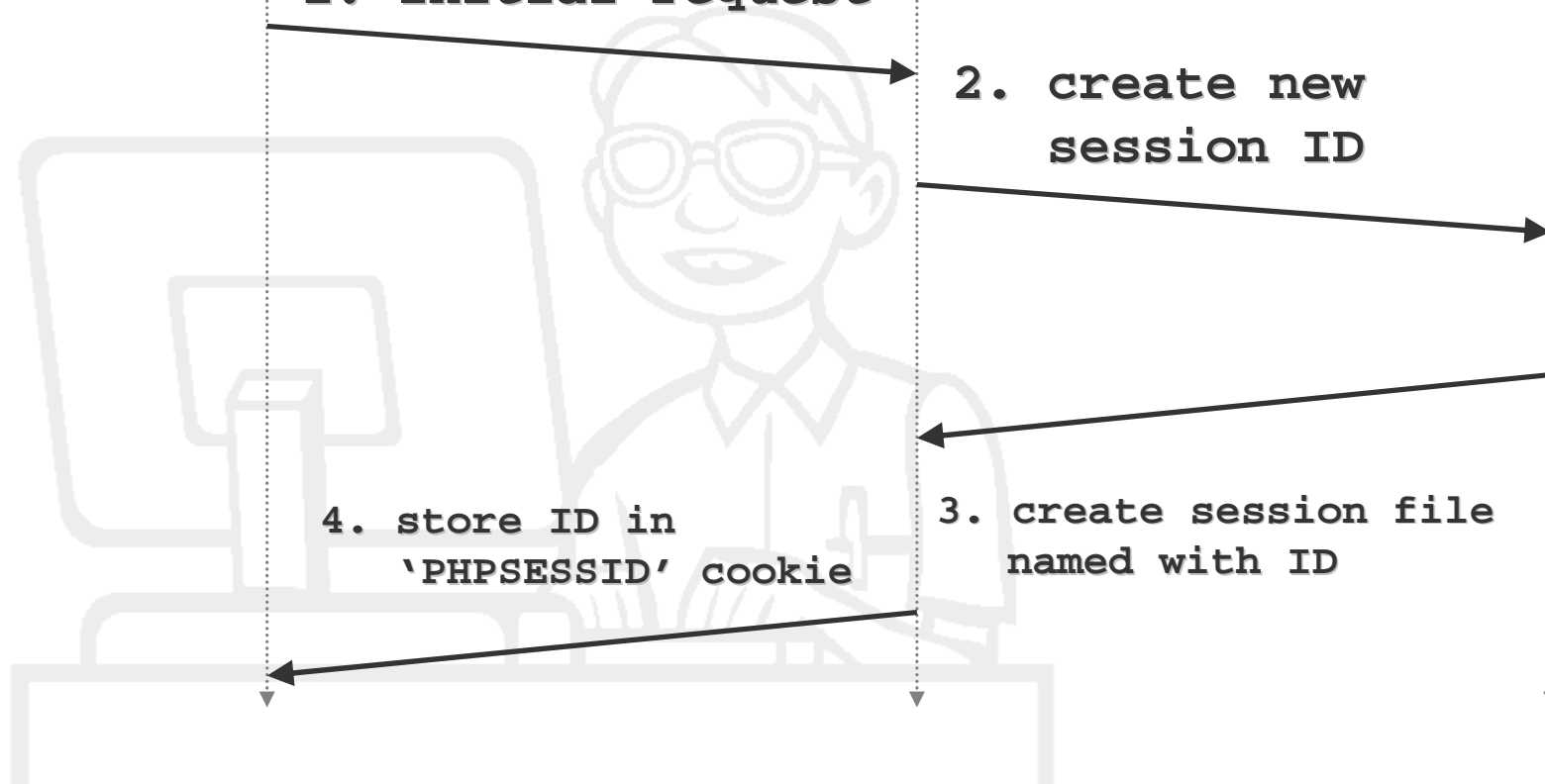


1. initial request

2. create new  
session ID

4. store ID in  
'PHPSESSID' cookie

3. create session file  
named with ID



# 1.

## Sessions

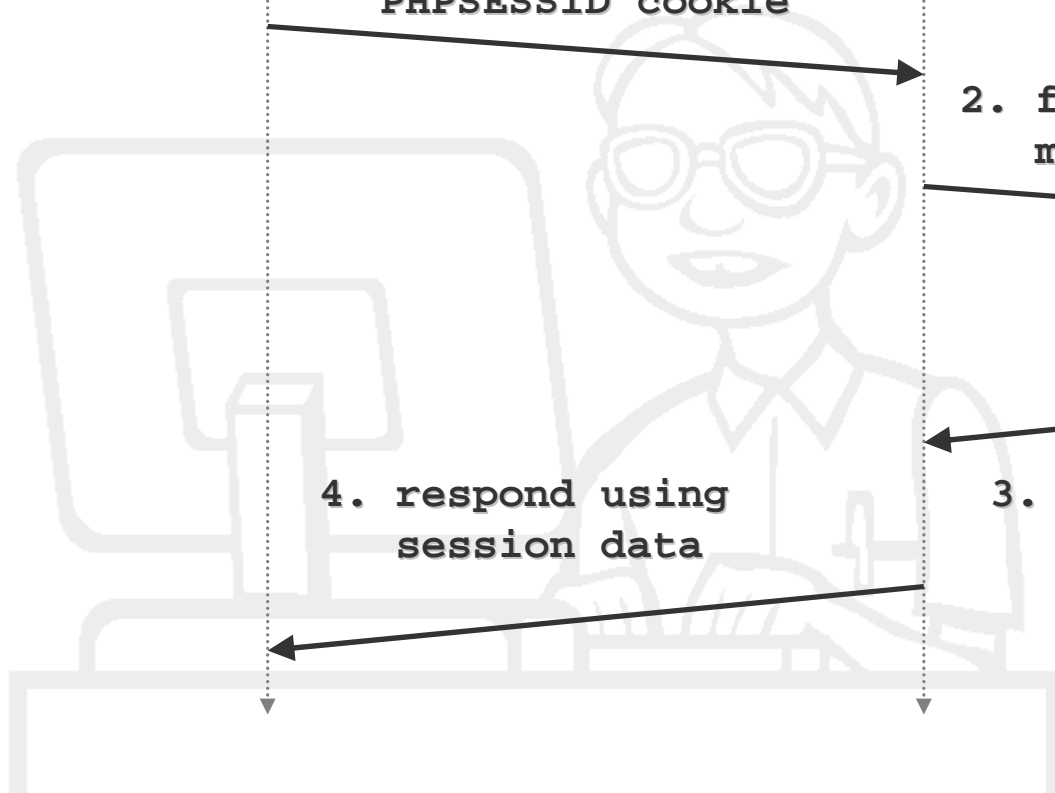


1. read session ID from  
PHPSESSID cookie

2. find file with name  
matching session ID

3. read session data  
from session file

4. respond using  
session data



# 1.

## Sessions

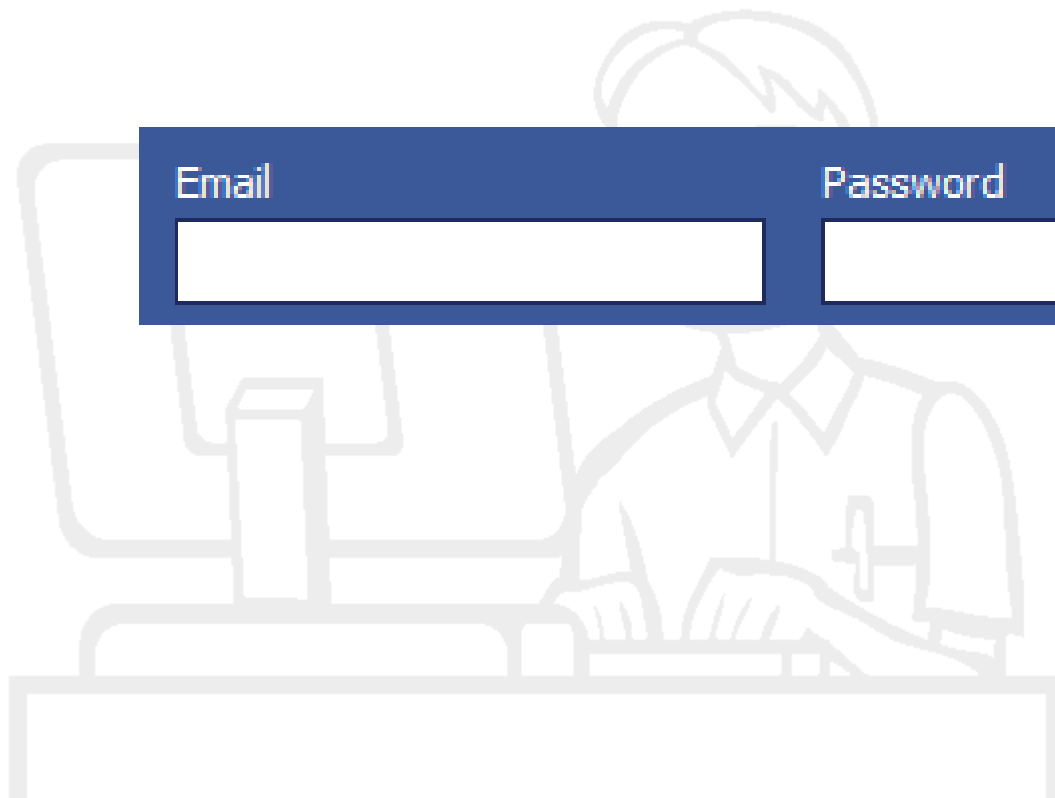




# 2.

## Authentication

**Sessions... what are they good for?**



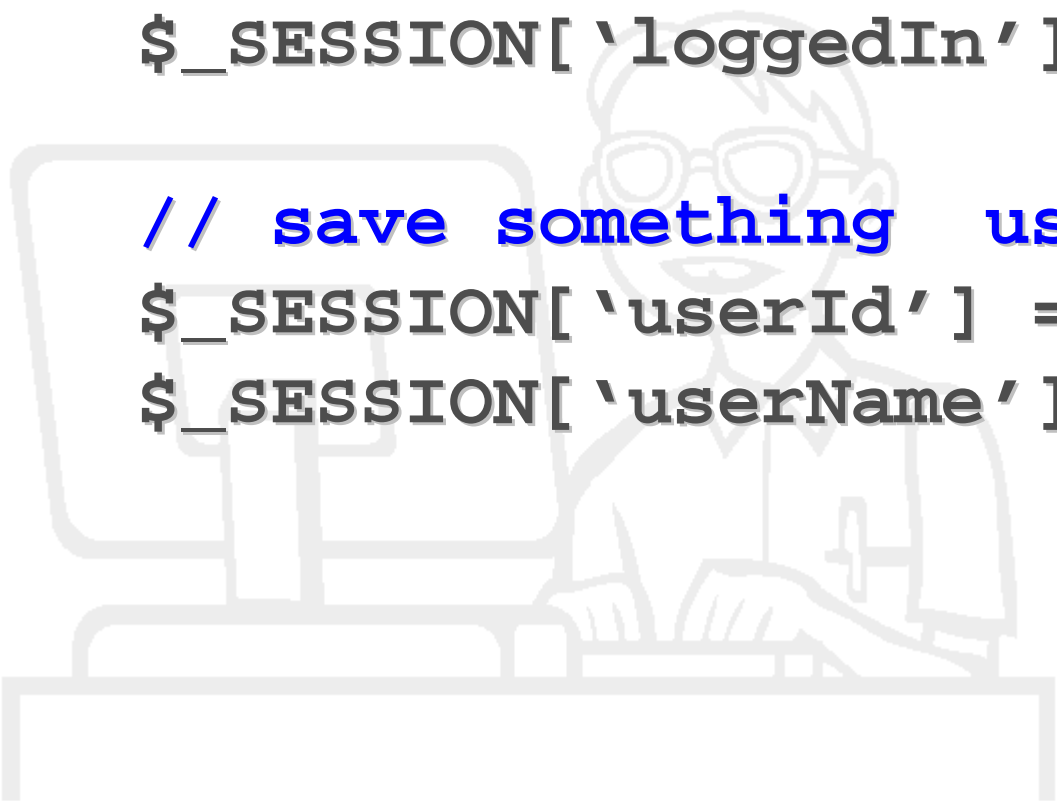
Email	Password	Login
<input type="text"/>	<input type="text"/>	

# 2.

## Authentication

```
// set a flag
$_SESSION['authenticated'] = true;
$_SESSION['loggedIn'] = true;

// save something useful
$_SESSION['userId'] = 123;
$_SESSION['userName'] = 'jsmith';
```



# 2.

## Authentication



# 2.

## Authentication

A login form with a blue background. It contains two input fields: 'Email' and 'Password'. Below the 'Email' field is a checkbox labeled 'Keep me logged in' which is checked. To the right of the checkbox is a link that says 'Forgot your password?'. To the right of the 'Password' field is a button labeled 'Login'. A red oval is drawn around the 'Keep me logged in' checkbox and its label.

**“You know that thing  
that they have?”**

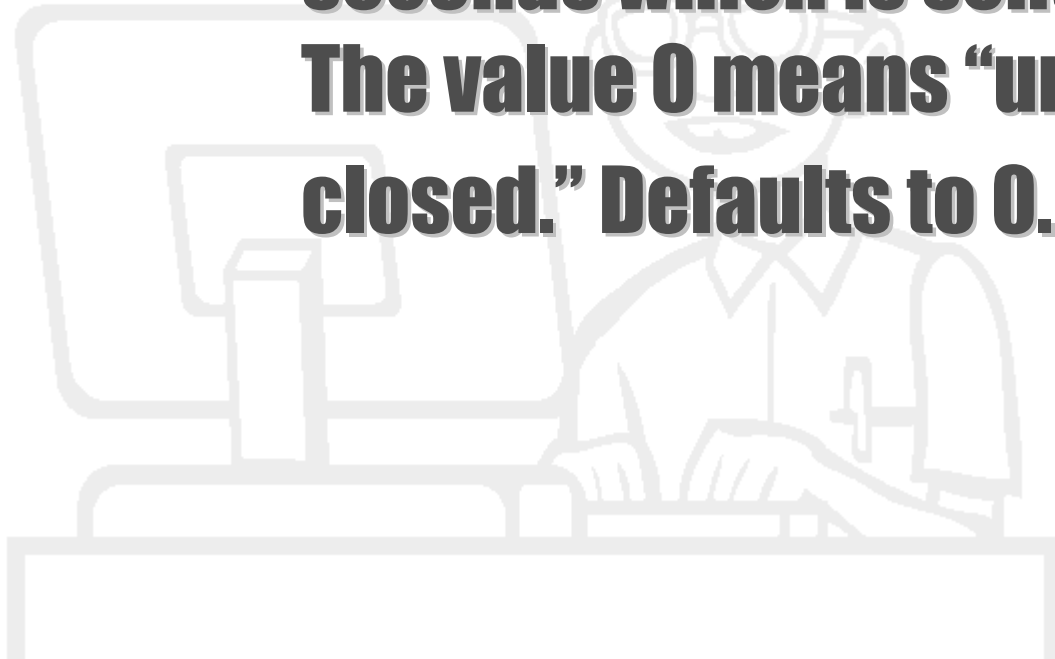
# 2.

## Authentication

*session.cookie\_lifetime*

”

**Specifies the lifetime of the cookie in seconds which is sent to the browser. The value 0 means “until the browser is closed.” Defaults to 0.**



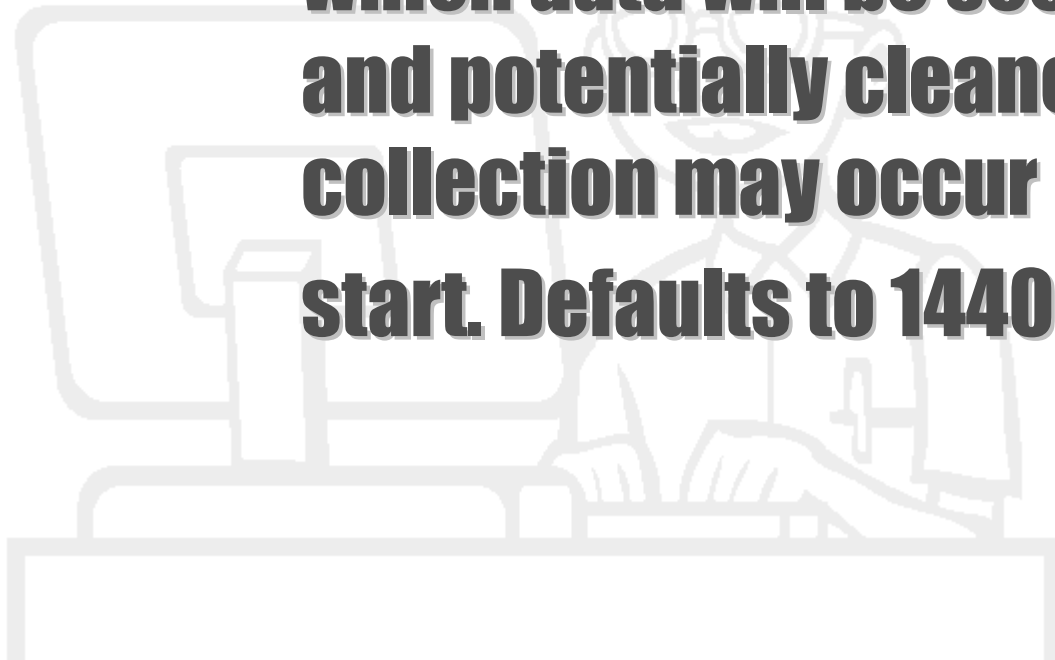
# 2.

## Authentication

*session.gc\_maxlifetime*



**Specifies the number of seconds after which data will be seen as ‘garbage’ and potentially cleaned up. Garbage collection may occur during session start. Defaults to 1440 seconds.**



# 2.

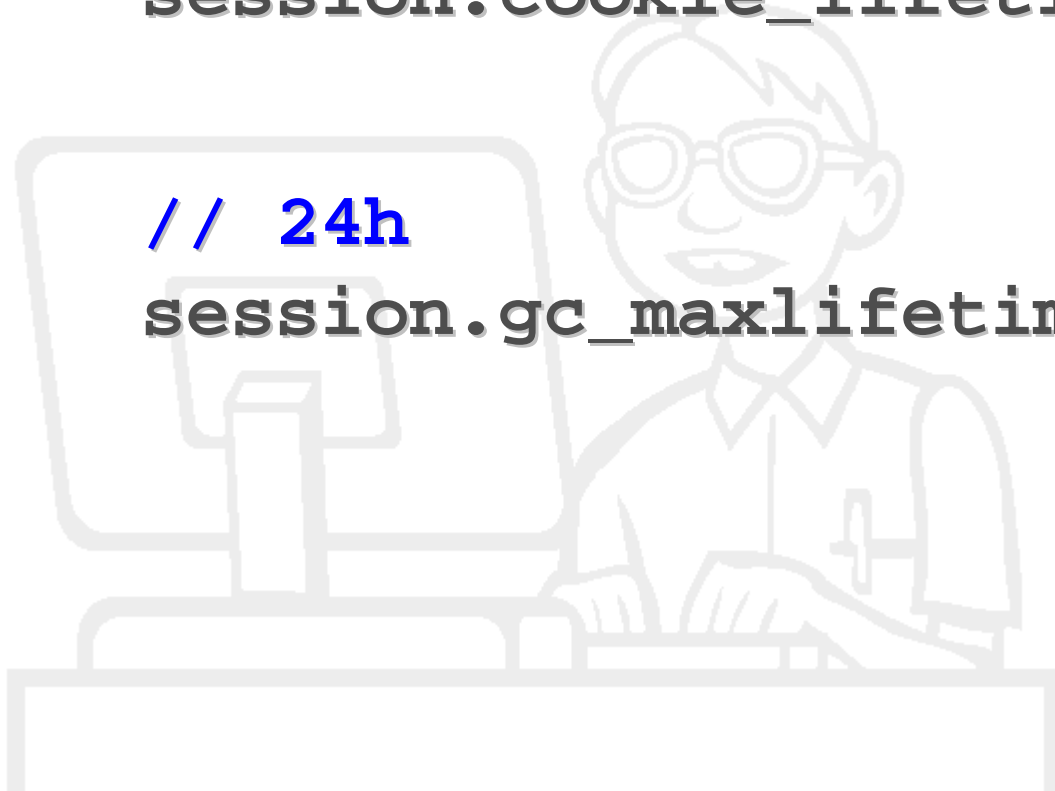
## Authentication

```
// 24h
```

```
session.cookie_lifetime = 86400;
```

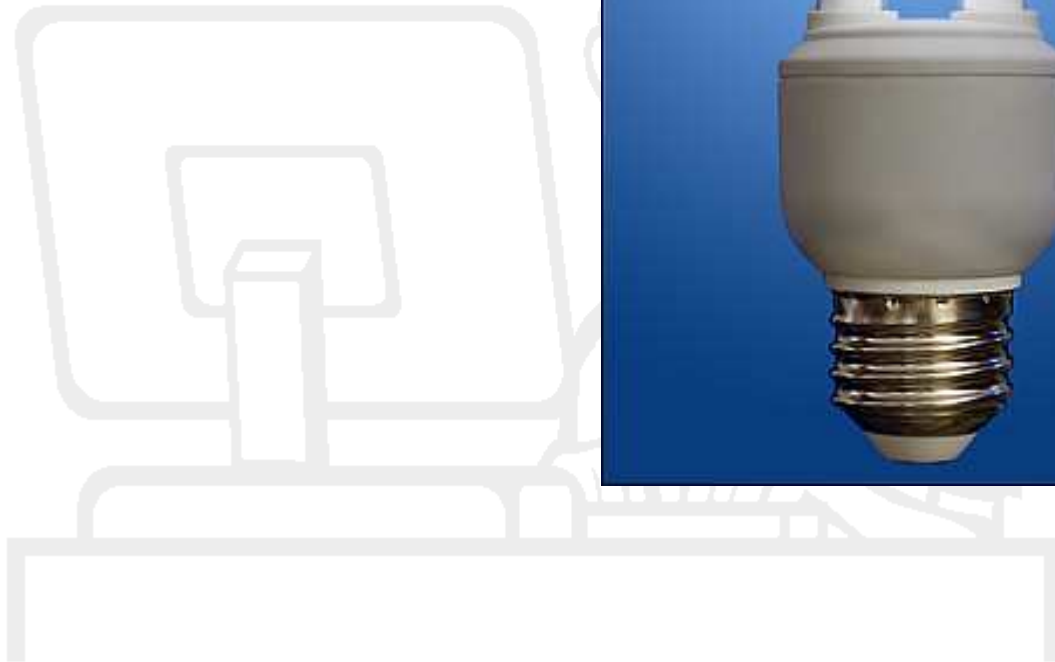
```
// 24h
```

```
session.gc_maxlifetime = 86400;
```



# 2.

## Authentication

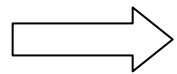




# 2.

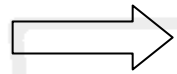
## Authentication

`session.cookie_lifetime`



***Absolute* expiration time**

`session.gc_maxlifetime`



**Maximum *idletime***



# 2.

## Authentication

### Example

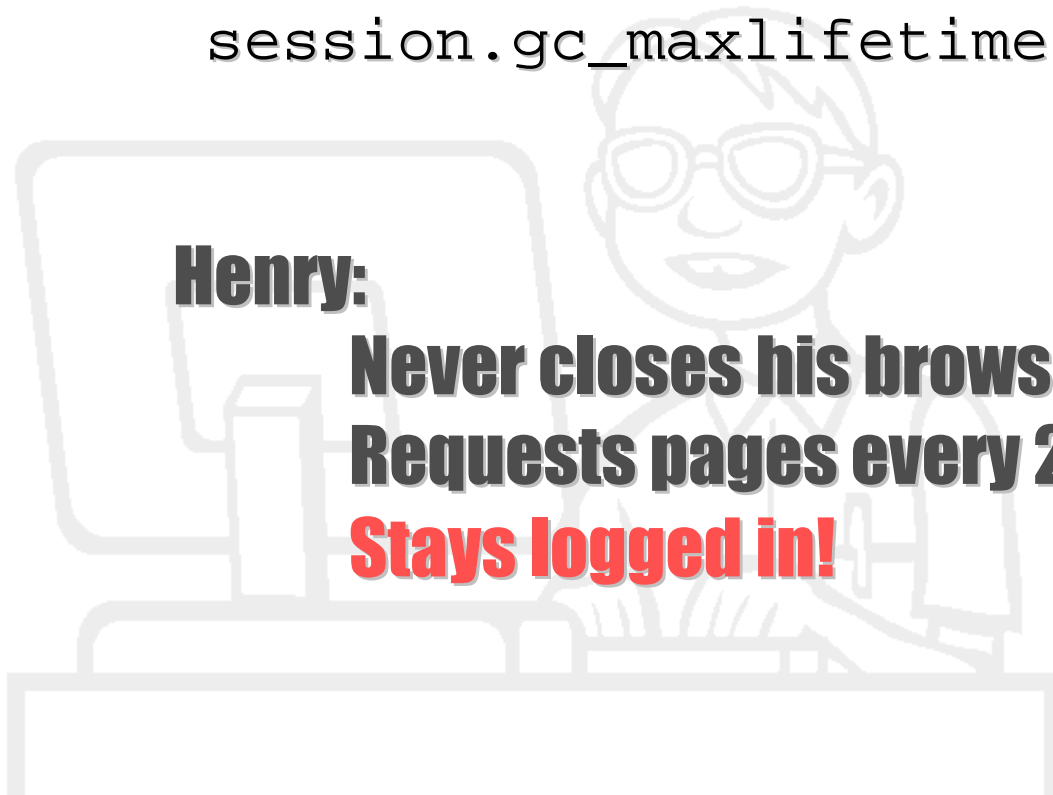
```
session.cookie_lifetime = 0; // default  
session.gc_maxlifetime = 1440; // default
```

**Henry:**

**Never closes his browser**

**Requests pages every 20 minutes or so.**

**Stays logged in!**



# 2.

## Authentication

### Example

```
session.cookie_lifetime = 0; // default  
session.gc_maxlifetime = 1440; // default
```

**Henry:**

**Leaves his browser open**

**Takes a 30 min. snack break**

**Session garbage collected – logged out!**



# 2.

## Authentication

### Example

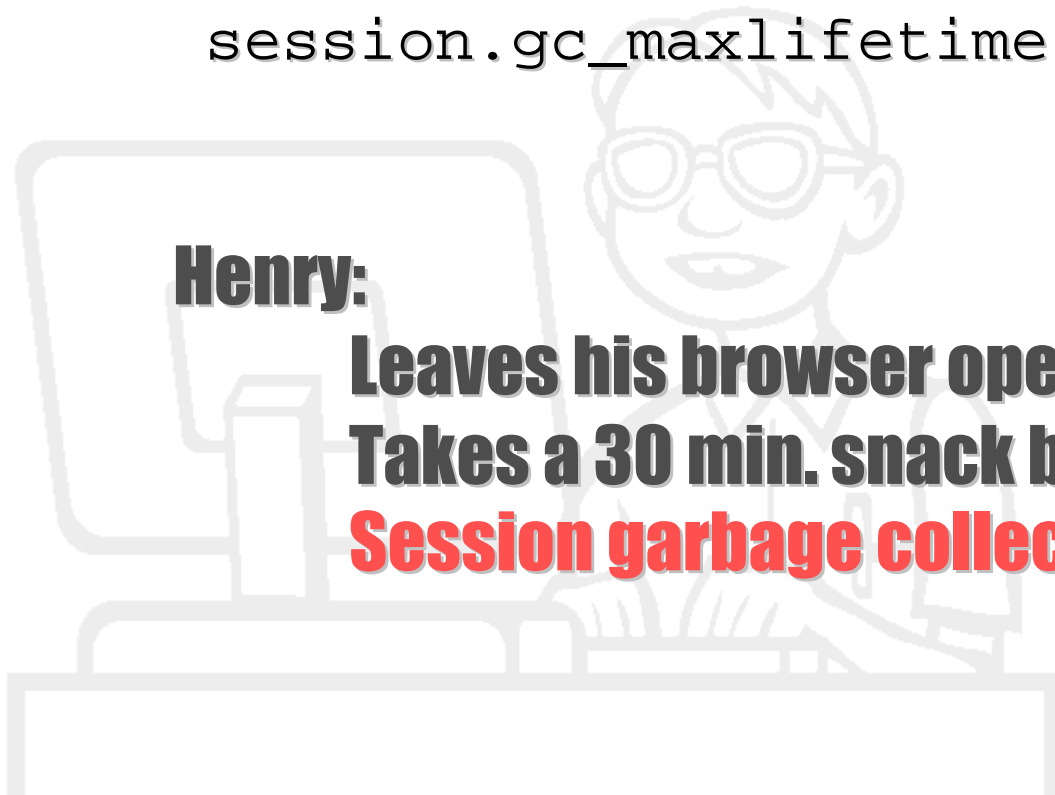
```
session.cookie_lifetime = 3600; // 1 hr  
session.gc_maxlifetime = 1440; // default
```

**Henry:**

**Leaves his browser open**

**Takes a 30 min. snack break**

**Session garbage collected – logged out!**



# 2.

## Authentication

### Example

```
session.cookie_lifetime = 3600; // 1 hr  
session.gc_maxlifetime = 3600; // 1 hr
```

**Henry:**

**Leaves his browser open**

**Takes a 45 min. snack break**

**Works for 30 mins.**

**Session cookie expires – logged out!**

# 2.

## Authentication

**Oh yeah, what was I trying to do?**



Email	Password	Login
<input type="text"/>	<input type="password"/>	
<input checked="" type="checkbox"/> Keep me logged in		Forgot your password?

# 2.

## Authentication



3.

Keep Me Logged In

**What would**

twitter

**do?**





# 3.

## Keep Me Logged In

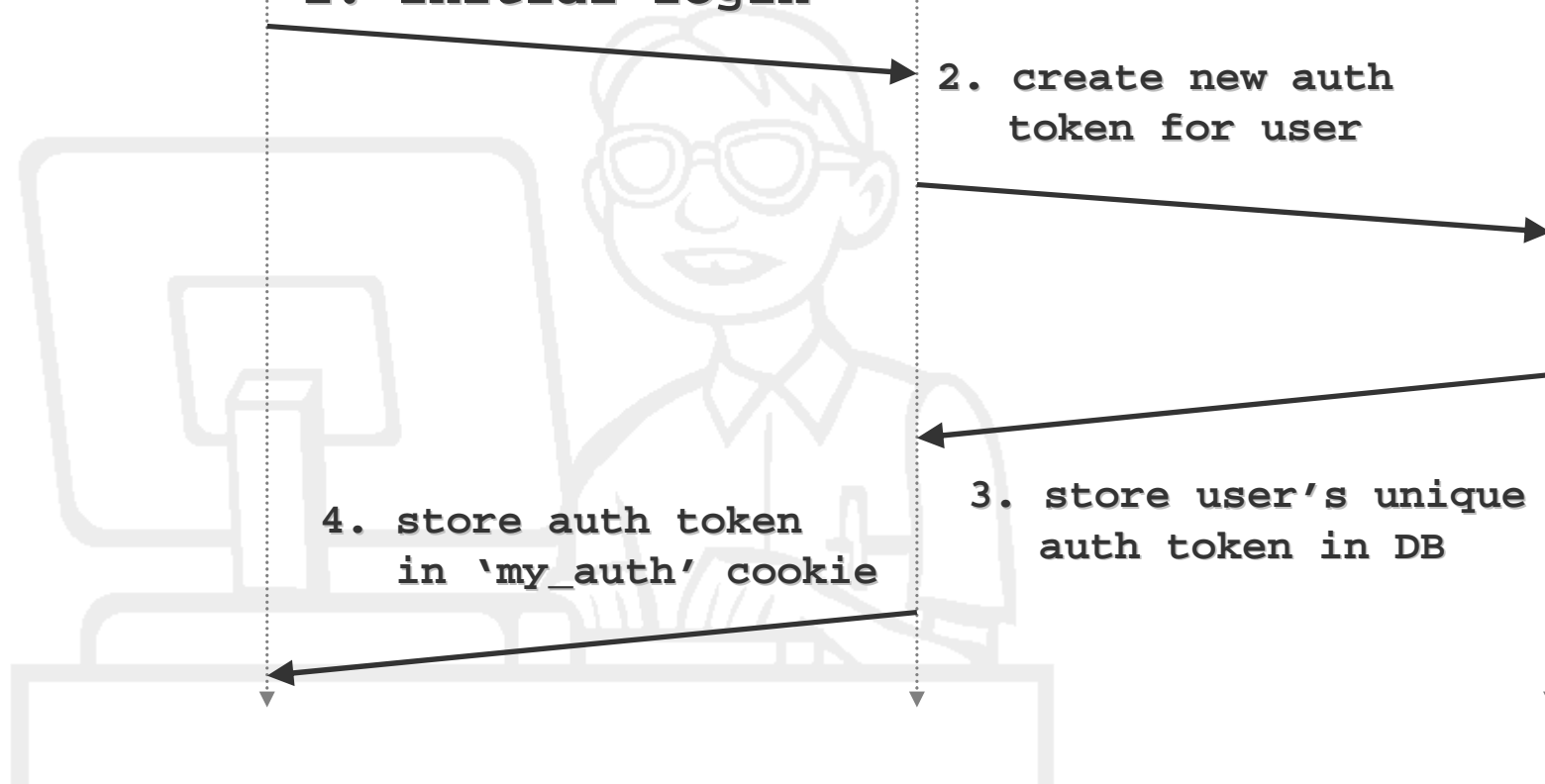


1. initial login

2. create new auth token for user

3. store user's unique auth token in DB

4. store auth token in 'my\_auth' cookie



# 3.

## Keep Me Logged In

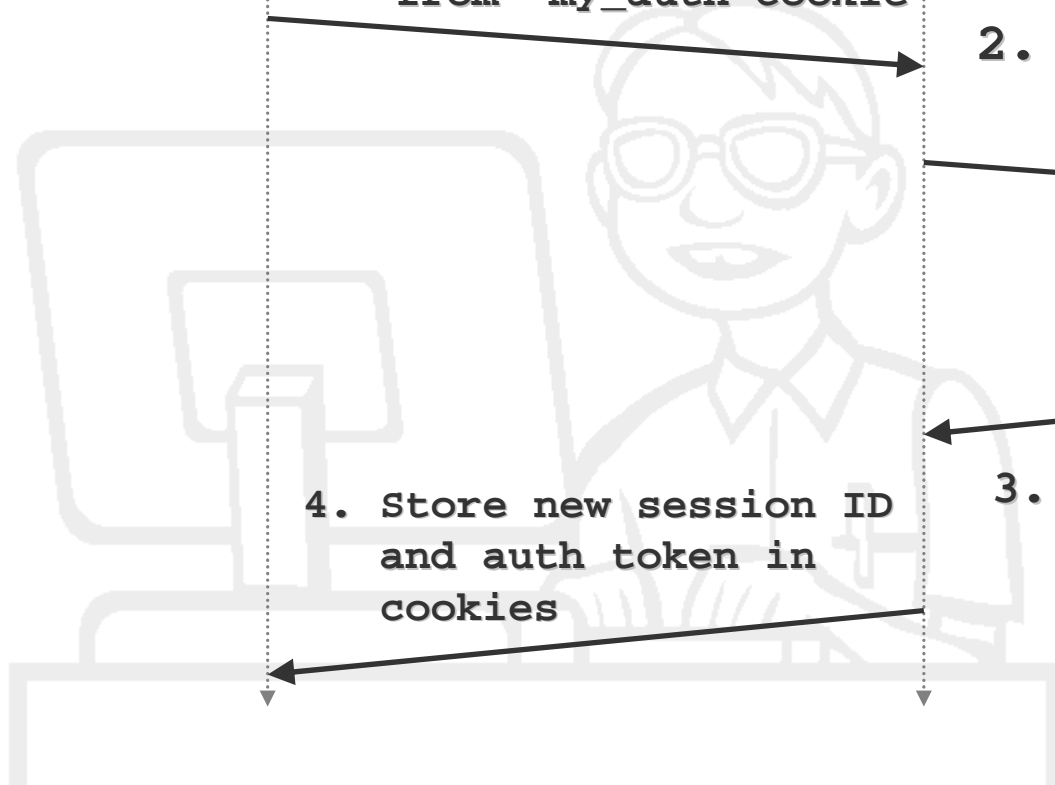


1. read auth token  
from 'my\_auth' cookie

2. lookup auth  
token in DB

3. if valid token,  
log user in

4. Store new session ID  
and auth token in  
cookies



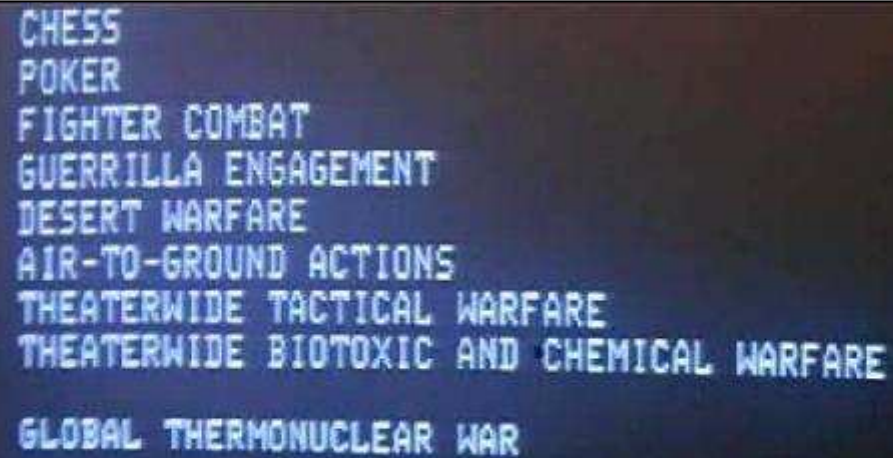
# 3.

**Keep Me Logged In**



# 4.

## Security



CHESS  
POKER  
FIGHTER COMBAT  
GUERRILLA ENGAGEMENT  
DESERT WARFARE  
AIR-TO-GROUND ACTIONS  
THEATERWIDE TACTICAL WARFARE  
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE  
GLOBAL THERMONUCLEAR WAR



**What about security?**

# 4.

## Security



4.

Security



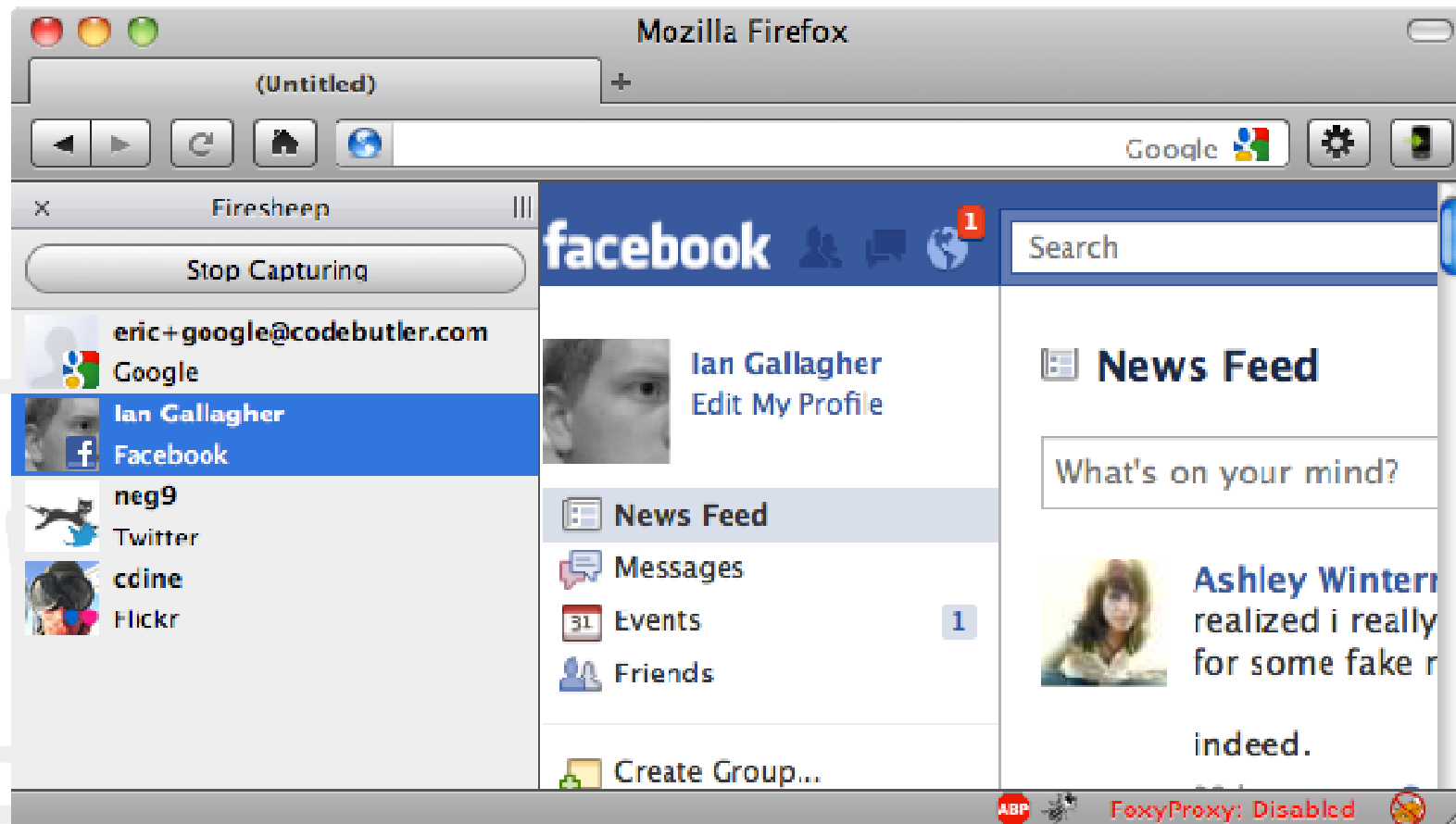
WOMPWORLD.COM

**Firesheep**



# 4.

## Security



# 4.

Security

## I CAN HAZ SSL?

HTTPS Only



Always use HTTPS

Use a secure connection where possible to encrypt your account information.

twitter

facebook®



4.

Security

**Re-authenticate!**

**Linked** 

**amazon.com<sup>®</sup>**  


# 4.

## Security



5.

Thanks!

**Enjoy the wi-fi!**

**@hellogerard**

**<http://straylightrun.net>**

**<http://github.com/hellogerard/tek11>**

**© 2011. Some rights reserved.**

