PHP Filter

A quick intro to PHP's filter functions

What is PHP Filter?

- Filter is a set of functions that allow you to easily validate or filter variables.
- A list of “filters” is at http://php.net/manual/en/intro.filter.php
- Pre-built into PHP 5.2; previous version available through PECL http://pecl.php.net/filter
- Can be setup via php.ini to auto-filter all input variables (but is not recommended usage)
- Remember Filter input, Escape output!!!

Example:

URL: /test.php?username=test<script>alert(document.cookie);</script>

<? echo $_GET['username']; ?>

test<script>alert(document.cookies);</script>

<? echo filter_input(INPUT_GET, 'username',
FILTER_SANITIZE_STRING); ?>

testalert(document.cookie);

<? echo filter_input(INPUT_GET, 'username',
FILTER_SANITIZE_SPECIAL_CHARS); ?>

test<script>alert(document.cookie);</script>

Careful:

/test.php?username=1 is < 2

1 is

Example 2:

```
<?
    if ( filter_var($data['email'], FILTER_VALIDATE_EMAIL) ) {
        $safe['email'] = filter_var($data['email'],
    FILTER_SANITIZE_EMAIL);
    }
    else {
        $errors[] = "Not a valid email address";
    }
?>
```

If you don't validate first, FILTER_SANITIZE_EMAIL turns michael@dom<script>alert(document.cookie);</script>ain.com into michael@domscriptalertxss/scriptain.com which is still a bad email.

Example 3:

- Use (filter_var_array) or filter_input_array()

  $filters = array('username' => FILTER_SANITIZE_STRING,
  'cost' => FILTER_SANITIZE_NUMBER_FLOAT,
  'email' => FILTER_SANITIZE_EMAIL);

  $safe = filter_var_array($input, $filters);

  $safe = filter_input_array(INPUT_POST, $filters);

- If you have your php.ini auto-filter, you can access the raw data via FILTER_UNSAFE_RAW and run your custom validation on the raw input

  $html_input = filter_input(INPUT_POST, 'forum_msg', FILTER_UNSAFE_RAW);

Closing

- Don't use the php.ini to set the filter type.
- Explicitly use filter_input rather than assuming _GET, _POST, _REQUEST, etc. are safe.
- Grep your code base for _GET, _POST, etc on a regular basis to ensure no one is using them directly.
- Remember Filter input, Escape output!!!
- Some people like it (Rasmus Leodorf http://toys.lerdorf.com/) and others don't (Stefan Esser http://blog.php-security.org/archives/64-Why-extfilter.html) so decide for yourself if it makes sense in your environment.

Credits/Hiring/Etc.

- http://php.net/filter
- http://pecl.php.net/filter
- http://php.net/security
- 35% off O'Reilly books. Code DSUG
- GameSpot is hiring Senior PHP Engineers: Contact Mike Tougeron (me) or Mariano Peterson for details

Code test_ex1.php

```
<?

if ( $_GET['username'] ) {
                        echo "Welcome " . $_GET['username'];
                        echo "\n<br/><hr><br/>\n";
                        echo "Welcome " . filter_input( INPUT_GET, 'username', FILTER_SANITIZE_STRING );
                        echo "\n<br/><hr><br/>\n";
                        echo "Welcome " . filter_input( INPUT_GET, 'username', FILTER_SANITIZE_SPECIAL_CHARS);
}
?>

<html>
<body bgcolor="Black" text="White">
<font size="+3">
<form action="" method="get">
<br />Enter your username:
<br /><textarea name="username" rows="10" cols="100">
test<script>alert(document.cookie);</script>
</textarea>
<br /><input type="submit">
</form>
</font>
<br /><a href="/meetup/test_ex1.php">reload</a>
<br /><a href="/meetup/index.php">home</a>

</body>
</html>
```

Code test_ex2.php

```
<?

	$data['email'] = $_GET['email'];

	if ( $data['email'] ) {
		if ( filter_var($data['email'], FILTER_VALIDATE_EMAIL) ) {
			$safe['email'] = filter_var($data['email'], FILTER_SANITIZE_EMAIL);
		}
		else {
			$errors[] = "Not a valid email address";
		}
	}

?>

<html>
<html>
<body bgcolor="Black" text="White">
<font size="+3">
<?
if ( $errors ) {
	foreach ( $errors as $error ) {
		echo "<br />$error<br />";
	}
}
```

Code test_ex2.php (cont.)

```
if ( $data['email'] ) {
        echo "<br />Your email address is: " . filter_var($data['email'], FILTER_SANITIZE_SPECIAL_CHARS);
}
?>
<form action="" method="get">
<br />Enter your email address:
<br /><textarea name="email" rows="10" cols="100">
michael@dom<script>alert(document.cookie);</script>ain.com
</textarea>
<br /><input type="submit">
</form>
</font>
<br /><a href="/meetup/test_ex2.php">reload</a>
<br /><a href="/meetup/index.php">home</a>

</body>
</html>
```

Code test_exp3.php

```
<?

        $filters = array( 'username' => FILTER_SANITIZE_STRING,
                                        'cost' => FILTER_SANITIZE_NUMBER_FLOAT,
                                        'email' => FILTER_SANITIZE_EMAIL );

        $data = filter_input_array(INPUT_GET, $filters);

        $filters = array( 'username' => FILTER_SANITIZE_STRING,
                                        'cost' => array('filter'    => FILTER_SANITIZE_NUMBER_FLOAT,
                'flags'     => FILTER_FLAG_ALLOW_THOUSAND | FILTER_FLAG_ALLOW_FRACTION,
                'options'   => array('decimal' => 2)
                ),
                                        'email' => FILTER_SANITIZE_EMAIL );

        $data2 = filter_input_array(INPUT_GET, $filters);

?>

<html>
<html>
<body bgcolor="Black" text="White">
<font size="+3">
<?
if ( $errors ) {
        foreach ( $errors as $error ) {
                echo "<br />$error<br />";
        }
}
```

Code test_ex3.php (cont.)

```
if ( $data['username'] ) {
        echo "<br />Your filtered username is: " . $data['username'];
}
if ( $data['cost'] ) {
        echo "<br />Your filtered cost is: " . $data['cost'];
}
if ( $data2['cost'] ) {
        echo "<br />Your filtered (</font>FILTER_FLAG_ALLOW_THOUSAND | FILTER_FLAG_ALLOW_FRACTION)<font size=\"+3\"> cost is: " . $data2['cost'];
}
if ( $data['email'] ) {
        echo "<br />Your filtered email address is: " . $data['email'];
}
?>
<form action="" method="get">
<br />Enter your username:
<br /><textarea name="username" rows="10" cols="100">
test<script>alert(document.cookie);</script>
</textarea>
<br />Enter your email address:
<br /><textarea name="email" rows="10" cols="100">
michael@dom<script>alert(document.cookie);</script>ain.com
</textarea>'
<br />Enter the cost:
<br /><textarea name="cost" rows="10" cols="100">123,154</textarea>
<br /><input type="submit">
</form>
</font>
<br /><a href="/meetup/test_ex3.php">reload</a>
<br /><a href="/meetup/index.php">home</a>
</body>
</html>
```