PHP Sample XSS Vulnerability Fix

Downloading the newest available Sample Forms will have this fix already implemented as of May 25, 2010.

The following changes need to be made to the PHP Sample Contact Upload/Signup Forms, as well as the Sample Campaign Forms in order to fix a cross-site scripting security hole. This document is intended to provide steps to implement the security fix for those who do not wish to download the new PHP Samples.

Please Note: The line numbers used in this document are assuming that no changes have been made to the sample form since downloading it. If you have modified the sample forms in any way, these line numbers will likely not correspond to your own. For more detailed information of the exact changes made, please see the appendix of this document.

Sample Contact Upload/Signup Form

add_contact.php

1. Add:

```
header('Content-Type: text/html; charset=UTF-8');
```

to the top of the document, under the opening `<?php` tag.

2. Change line 76 from:

```
$message = "Contact ".$_POST["email_address"]." Added.";
```

to:

```
$message = "Contact ".htmlspecialchars($postFields["email_address"],
ENT_QUOTES, 'UTF-8')." Added.";
```

* 3. Change the value of each form text input from the format:

```
<?php  echo $_POST['VARIABLE_NAME'] ?>
```

To:

```
<?php  echo htmlspecialchars($_POST['VARIABLE_NAME'], ENT_QUOTES, 'UTF-8')
?>
```

This must be done on lines: 126, 132, 134, 138, 140, 145, 146, 147, 152, 174, 176, 180, 222, 224, 228, 236, 237, 242, 244, 248, 250, 254, 256, 260, 262, 266, 268, 272, 274, 278, 285. ****See Appendix for details.***

edit_contact_step1.php

1. Add:

```
header('Content-Type: text/html; charset=UTF-8');
```

to the top of the document, under the opening <?php tag.

2. Change line 10 from:

```
header('Location: simple_form.php?email='.urlencode($_POST['src_mail']));
```

to:

```
header('Location:
simple_form.php?email='.urlencode(htmlspecialchars($_POST['src_mail'],
ENT_QUOTES, 'UTF-8')));
```

3. Change line 13 from:

```
header('Location: edit_contact.php?email='.urlencode($_POST['src_mail']));
```

to:

```
header('Location:
edit_contact.php?email='.urlencode(htmlspecialchars($_POST['src_mail'],
ENT_QUOTES, 'UTF-8')));
```

list_contacts.php

1. Add:

```
header('Content-Type: text/html; charset=UTF-8');
```

to the top of the document, under the opening <?php tag.

simple_form.php

1. Add:

```
header('Content-Type: text/html; charset=UTF-8');
```

to the top of the document, under the opening <?php tag.

2. Change line 69 from:

```
$message = "Contact ".$_POST["email_address"]." Added.";
```

to:

```
$message = "Contact ".htmlspecialchars($postFields["email_address"],
ENT_QUOTES, 'UTF-8')." Added.";
```

*3. Change the value of each form text input from the format:

```
<?php  echo $_POST['VARIABLE_NAME'] ?>
```

To:

```
<?php  echo htmlspecialchars($_POST['VARIABLE_NAME'], ENT_QUOTES, 'UTF-8')
?>
```

This must be done on lines: 118, 124, 126, 130, 132, 137, 138, 139, 144, 166, 168, 172. ***See Appendix for details.***

cc_class.php (createContactXML function)

1. Change line 449 from:

```
$xml_string = "<entry xmlns='http://www.w3.org/2005/Atom'></entry>";
```

to:

```
$xml_string = "<?xml version=\"1.0\" encoding=\"UTF-8\"?><entry
xmlns='http://www.w3.org/2005/Atom'></entry>";
```

*2. All lines that make use of the htmlspecialchars function must have their format changed from:

```
$example_node = $xml_object->addChild("example",
htmlspecialchars("ExampleNode"));
```

to:

```
$example_node = $xml_object->addChild("example",
htmlspecialchars(("ExampleNode"), ENT_QUOTES, 'UTF-8'));
```

This must be done on lines: 451, 452, 454, 455, 456, 460, 462-467, 474-486, 490. ***See Appendix for details.***

Sample Campaign Form

edit_campaign.php

1. Add:

```
header('Content-Type: text/html; charset=UTF-8');
```

to the top of the document, under the opening <?php tag.

cc_class.php (createCampaignXML function)

* 1. All lines that make use of a variable from a text input must be modified from the format:

```
$example_node = $xml_object->addChild("example",
htmlentities($params['param_name']));
```

to:

```
$example_node = $xml_object->addChild("example",
htmlspecialchars($params['param_name'], ENT_QUOTES, 'UTF-8'));
```

This must be done on lines: 897, 907, 912, 913, 918, 921, 924, 927-932, 952, 956, 961, 966, 969, 970, 972. ***See Appendix for details.***

Appendix

Sample Signup Form

This section contains an exact before and after shot of every line modified in the Sample Forms in order to make the modifications necessary to implement the XSS vulnerability fix. Please note this only contains the line updates for the sections marked with "***See Appendix for details***".

add_contact.php

Before:

```
76  $message = "Contact ".$_POST["email_address"]." Added.";

126 <td align="left"><input type="text" name="email_address" value="<?php
    echo $_POST['email_address'] ?>" maxLength="100" /></td>

132 <td align="left"><input type="text" name="first_name" maxLength="100"
    value="<?php  echo $_POST['first_name'] ?>" /></td>

134 <td align="left"><input type="text" name="last_name" maxLength="100"
    value="<?php  echo $_POST['last_name'] ?>" /></td>

138 <td align="left"><input type="text" name="middle_name" maxLength="100"
    value="<?php  echo $_POST['middle_name'] ?>" /></td>

140 <td align="left"><input type="text" name="home_num" maxLength="100"
    value="<?php  echo $_POST['home_num'] ?>" /></td>

145 <input type="text" name="adr_1" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_1'] ?>" /><br/>
```

```
146 <input type="text" name="adr_2" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_2'] ?>" /><br/>

147 <input type="text" name="adr_3" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_3'] ?>" /><br/>

152 <td align="left"><input type="text" name="city" maxLength="100"
    value="<?php  echo $_POST['city'] ?>" /></td>

172 <td align="left"><input type="text" name="postal_code" maxLength="100"
    value="<?php  echo $_POST['postal_code'] ?>"/></td>

176 <td align="left"><input type="text" name="state_name" maxLength="100"
    value="<?php  echo $_POST['state_name'] ?>"/></td>

180 <td align="left"><input type="text" name="sub_postal" maxLength="100"
    value="<?php  echo $_POST['sub_postal'] ?>"/></td>

222 <td align="left"><input type="text" name="company_name" maxLength="100"
    value="<?php  echo $_POST['company_name'] ?>" /></td>

224 <td align="left"><input type="text" name="job_title" maxLength="100"
    value="<?php  echo $_POST['job_title'] ?>" /></td>

228 <td align="left"><input type="text" name="wrk_num" maxLength="100"
    value="<?php  echo $_POST['wrk_num'] ?>" /></td>

236 <td align="left"><input type="text" name="custom_field_1" maxLength="100"
    value="<?php  echo $_POST['custom_field_1'] ?>" /></td>

237 <td align="left"><input type="text" name="custom_field_2" maxLength="100"
    value="<?php  echo $_POST['custom_field_2'] ?>" /></td>

242 <td align="left"><input type="text" name="custom_field_3" maxLength="100"
    value="<?php  echo $_POST['custom_field_3'] ?>" /></td>

244 <td align="left"><input type="text" name="custom_field_4" maxLength="100"
    value="<?php  echo $_POST['custom_field_4'] ?>" /></td>

248 <td align="left"><input type="text" name="custom_field_5" maxLength="100"
    value="<?php  echo $_POST['custom_field_5'] ?>" /></td>

250 <td align="left"><input type="text" name="custom_field_6" maxLength="100"
    value="<?php  echo $_POST['custom_field_6'] ?>" /></td>

254 <td align="left"><input type="text" name="custom_field_7" maxLength="100"
    value="<?php  echo $_POST['custom_field_7'] ?>" /></td>

256 <td align="left"><input type="text" name="custom_field_8" maxLength="100"
    value="<?php  echo $_POST['custom_field_8'] ?>" /></td>

260 <td align="left"><input type="text" name="custom_field_9" maxLength="100"
    value="<?php  echo $_POST['custom_field_9'] ?>" /></td>

262 align="left"><input type="text" name="custom_field_10" maxLength="100"
    value="<?php  echo $_POST['custom_field_10'] ?>" /></td>
```

```
266 <td align="left"><input type="text" name="custom_field_11" maxLength="100"
    value="<?php  echo $_POST['custom_field_11'] ?>" /></td>

268 <td align="left"><input type="text" name="custom_field_12" maxLength="100"
    value="<?php  echo $_POST['custom_field_12'] ?>" /></td>

272 <td align="left"><input type="text" name="custom_field_13" maxLength="100"
    value="<?php  echo $_POST['custom_field_13'] ?>" /></td>

274 <td align="left"><input type="text" name="custom_field_14" maxLength="100"
    value="<?php  echo $_POST['custom_field_14'] ?>" /></td>

278 <td align="left"><input type="text" name="custom_field_15" maxLength="100"
    value="<?php  echo $_POST['custom_field_15'] ?>" /></td>

285 <textarea rows="8" cols="50" name="notes"><?php  echo
    htmlspecialchars($_POST['notes']) ?></textarea>
```

After:

```
76  $message = "Contact ".htmlspecialchars($postFields["email_address"],
    ENT_QUOTES, 'UTF-8')." Added.";

126 <td align="left"><input type="text" name="email_address" value="<?php
    echo htmlspecialchars($_POST['email_address'], ENT_QUOTES, 'UTF-8') ?>"
    maxLength="50" /></td>

132 <td align="left"><input type="text" name="first_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['first_name'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

134 <td align="left"><input type="text" name="last_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['last_name'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

138 <td align="left"><input type="text" name="middle_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['middle_name'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

140 <td align="left"><input type="text" name="home_num" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['home_num'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

145 <input type="text" name="adr_1" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_1'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>

146 <input type="text" name="adr_2" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_2'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>

147 <input type="text" name="adr_3" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_3'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>
```

```
152 <td align="left"><input type="text" name="city" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['city'], ENT_QUOTES, 'UTF-8')
    ?>" /></td>

174 <td align="left"><input type="text" name="postal_code" maxLength="25"
    value="<?php  echo htmlspecialchars($_POST['postal_code'], ENT_QUOTES,
    'UTF-8') ?>"/></td>

176 <td align="left"><input type="text" name="state_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['state_name'], ENT_QUOTES,
    'UTF-8') ?>"/></td>

180 <td align="left"><input type="text" name="sub_postal" maxLength="25"
    value="<?php  echo htmlspecialchars($_POST['sub_postal'], ENT_QUOTES,
    'UTF-8') ?>"/></td>

222 <td align="left"><input type="text" name="company_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['company_name'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

224 <td align="left"><input type="text" name="job_title" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['job_title'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

228 <td align="left"><input type="text" name="wrk_num" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['wrk_num'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

236 <td align="left"><input type="text" name="custom_field_1" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_1'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

237 <td align="left"><input type="text" name="custom_field_2" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_2'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

242 <td align="left"><input type="text" name="custom_field_3" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_3'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

244 <td align="left"><input type="text" name="custom_field_4" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_4'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

248 <td align="left"><input type="text" name="custom_field_5" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_5'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

250 <td align="left"><input type="text" name="custom_field_6" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_6'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

254 <td align="left"><input type="text" name="custom_field_7" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_7'], ENT_QUOTES,
    'UTF-8') ?>" /></td>
```

```
256 <td align="left"><input type="text" name="custom_field_8" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_8'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

260 <td align="left"><input type="text" name="custom_field_9" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_9'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

262 <td align="left"><input type="text" name="custom_field_10" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_10'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

266 <td align="left"><input type="text" name="custom_field_11" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_11'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

268 <td align="left"><input type="text" name="custom_field_12" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_12'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

272 <td align="left"><input type="text" name="custom_field_13" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_13'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

274 <td align="left"><input type="text" name="custom_field_14" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_14'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

278 <td align="left"><input type="text" name="custom_field_15" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['custom_field_15'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

285 <textarea rows="8" cols="50" name="notes"><?php  echo
    htmlspecialchars($_POST['notes'], ENT_QUOTES, 'UTF-8') ?></textarea>
```

simple_form.php

Before:

```
69  $message = "Contact ".$_POST["email_address"]." Added.";

118 <td align="left"><input type="text" name="email_address" value="<?php
    echo $_POST['email_address'] ?>" maxLength="100" /></td>

124 <td align="left"><input type="text" name="first_name" maxLength="100"
    value="<?php  echo $_POST['first_name'] ?>" /></td>

126 <td align="left"><input type="text" name="last_name" maxLength="100"
    value="<?php  echo $_POST['last_name'] ?>" /></td>

130 <td align="left"><input type="text" name="middle_name" maxLength="100"
    value="<?php  echo $_POST['middle_name'] ?>" /></td>

132 <td align="left"><input type="text" name="home_num" maxLength="100"
    value="<?php  echo $_POST['home_num'] ?>" /></td>
```

```
137 <input type="text" name="adr_1" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_1'] ?>" /><br/>

138 <input type="text" name="adr_2" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_2'] ?>" /><br/>

139 <input type="text" name="adr_3" maxLength="100" style="width: 440px"
    value="<?php  echo $_POST['adr_3'] ?>" /><br/>

144 <td align="left"><input type="text" name="city" maxLength="100"
    value="<?php  echo $_POST['city'] ?>" /></td>

166 <td align="left"><input type="text" name="postal_code" maxLength="100"
    value="<?php  echo $_POST['postal_code'] ?>"/></td>

168 <td align="left"><input type="text" name="state_name" maxLength="100"
    value="<?php  echo $_POST['state_name'] ?>"/></td>
172 <td align="left"><input type="text" name="sub_postal" maxLength="100"
    value="<?php  echo $_POST['sub_postal'] ?>"/></td>
```

After:

```
69  $message = "Contact ".htmlspecialchars($postFields["email_address"],
    ENT_QUOTES, 'UTF-8')." Added.";

118 <td align="left"><input type="text" name="email_address" value="<?php
    echo htmlspecialchars($_POST['email_address'], ENT_QUOTES, 'UTF-8') ?>"
    maxLength="50" /></td>

124 <td align="left"><input type="text" name="first_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['first_name'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

126 <td align="left"><input type="text" name="last_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['last_name'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

130 <td align="left"><input type="text" name="middle_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['middle_name'], ENT_QUOTES,
    'UTF-8') ?>" /></td>

132 <td align="left"><input type="text" name="home_num" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['home_num'], ENT_QUOTES, 'UTF-
    8') ?>" /></td>

137 <input type="text" name="adr_1" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_1'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>

138 <input type="text" name="adr_2" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_2'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>
```

```
139 <input type="text" name="adr_3" maxLength="50" style="width: 440px"
    value="<?php  echo htmlspecialchars($_POST['adr_3'], ENT_QUOTES, 'UTF-8')
    ?>" /><br/>

144 <td align="left"><input type="text" name="city" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['city'], ENT_QUOTES, 'UTF-8')
    ?>" /></td>

166 <td align="left"><input type="text" name="postal_code" maxLength="25"
    value="<?php  echo htmlspecialchars($_POST['postal_code'], ENT_QUOTES,
    'UTF-8') ?>"/></td>

168 <td align="left"><input type="text" name="state_name" maxLength="50"
    value="<?php  echo htmlspecialchars($_POST['state_name'], ENT_QUOTES,
    'UTF-8') ?>"/></td>

172 <td align="left"><input type="text" name="sub_postal" maxLength="25"
    value="<?php  echo htmlspecialchars($_POST['sub_postal'], ENT_QUOTES,
    'UTF-8') ?>"/></td>
```

cc_class.php (createContactXML Function)

Before:

```
451 $title_node = $xml_object->addChild("title",
    htmlspecialchars("TitleNode"));

452 $updated_node = $xml_object->addChild("updated",
    htmlspecialchars($update_date));


454 $author_name = $author_node->addChild("name", htmlspecialchars("CTCT
    Samples"));

455 $id_node = $xml_object->addChild("id", $id);

456 $summary_node = $xml_object->addChild("summary",
    htmlspecialchars("Customer document"));

460 $contact_node = $content_node->addChild("Contact",
    htmlspecialchars("Customer document"));

462 $email_node = $contact_node->addChild("EmailAddress",
    htmlspecialchars($params['email_address']));

463 $fname_node = $contact_node->addChild("FirstName",
    urldecode(htmlspecialchars($params['first_name'])));

464 $lname_node = $contact_node->addChild("LastName",
    urldecode(htmlspecialchars($params['last_name'])));

465 $lname_node = $contact_node->addChild("MiddleName",
    urldecode(htmlspecialchars($params['middle_name'])));
```

```
466 $lname_node = $contact_node->addChild("CompanyName",
    urldecode(htmlspecialchars($params['company_name'])));

467 $lname_node = $contact_node->addChild("JobTitle",
    urldecode(htmlspecialchars($params['job_title'])));

474 $hn_node = $contact_node->addChild("HomePhone",
    htmlspecialchars($params['home_number']));

475 $wn_node = $contact_node->addChild("WorkPhone",
    htmlspecialchars($params['work_number']));

476 $ad1_node = $contact_node->addChild("Addr1",
    htmlspecialchars($params['address_line_1']));

477 $ad2_node = $contact_node->addChild("Addr2",
    htmlspecialchars($params['address_line_2']));

478 $ad3_node = $contact_node->addChild("Addr3",
    htmlspecialchars($params['address_line_3']));

479 $city_node = $contact_node->addChild("City",
    htmlspecialchars($params['city_name']));

480 $state_node = $contact_node->addChild("StateCode",
    htmlspecialchars($params['state_code']));
481 $state_name = $contact_node->addChild("StateName",
    htmlspecialchars($params['state_name']));

482 $ctry_node = $contact_node->addChild("CountryCode",
    htmlspecialchars($params['country_code']));

483 $zip_node = $contact_node->addChild("PostalCode",
    htmlspecialchars($params['zip_code']));

484 $subzip_node = $contact_node->addChild("SubPostalCode",
    htmlspecialchars($params['sub_zip_code']));

485 $note_node = $contact_node->addChild("Note",
    htmlspecialchars($params['notes']));

486 $emailtype_node = $contact_node->addChild("EmailType",
    htmlspecialchars($params['mail_type']));

490 $contact_node->addChild("CustomField".$k, htmlspecialchars($v));
```

After:

```
451 $title_node = $xml_object->addChild("title",
    htmlspecialchars(("TitleNode"), ENT_QUOTES, 'UTF-8'));

452 $updated_node = $xml_object->addChild("updated",
    htmlspecialchars(($update_date), ENT_QUOTES, 'UTF-8'));

454 $author_name = $author_node->addChild("name", ("CTCT Samples"));
```

```
455 $id_node = $xml_object->addChild("id", htmlspecialchars(($id),ENT_QUOTES,
    'UTF-8'));

456 $summary_node = $xml_object->addChild("summary",
    htmlspecialchars(("Customer document"),ENT_QUOTES, 'UTF-8'));

460 $contact_node = $content_node->addChild("Contact",
    htmlspecialchars(("Customer document"), ENT_QUOTES, 'UTF-8'));

462 $email_node = $contact_node->addChild("EmailAddress",
    htmlspecialchars(($params['email_address']), ENT_QUOTES, 'UTF-8'));

463 $fname_node = $contact_node->addChild("FirstName",
    urldecode(htmlspecialchars(($params['first_name']), ENT_QUOTES, 'UTF-
    8')));

464 $lname_node = $contact_node->addChild("LastName",
    urldecode(htmlspecialchars(($params['last_name']), ENT_QUOTES, 'UTF-8')));

465 $lname_node = $contact_node->addChild("MiddleName",
    urldecode(htmlspecialchars(($params['middle_name']), ENT_QUOTES, 'UTF-
    8')));

466 $lname_node = $contact_node->addChild("CompanyName",
    urldecode(htmlspecialchars(($params['company_name']), ENT_QUOTES, 'UTF-
    8')));

467 $lname_node = $contact_node->addChild("JobTitle",
    urldecode(htmlspecialchars(($params['job_title']), ENT_QUOTES, 'UTF-8')));

474 $hn_node = $contact_node->addChild("HomePhone",
    htmlspecialchars($params['home_number'], ENT_QUOTES, 'UTF-8'));

475 $wn_node = $contact_node->addChild("WorkPhone",
    htmlspecialchars($params['work_number'], ENT_QUOTES, 'UTF-8'));

476 $ad1_node = $contact_node->addChild("Addr1",
    htmlspecialchars($params['address_line_1'], ENT_QUOTES, 'UTF-8'));

477 $ad2_node = $contact_node->addChild("Addr2",
    htmlspecialchars($params['address_line_2'], ENT_QUOTES, 'UTF-8'));

478 $ad3_node = $contact_node->addChild("Addr3",
    htmlspecialchars($params['address_line_3'], ENT_QUOTES, 'UTF-8'));

479 $city_node = $contact_node->addChild("City",
    htmlspecialchars($params['city_name'], ENT_QUOTES, 'UTF-8'));

480 $state_node = $contact_node->addChild("StateCode",
    htmlspecialchars($params['state_code'], ENT_QUOTES, 'UTF-8'));

481 $state_name = $contact_node->addChild("StateName",
    htmlspecialchars($params['state_name'], ENT_QUOTES, 'UTF-8'));

482 $ctry_node = $contact_node->addChild("CountryCode",
    htmlspecialchars($params['country_code'], ENT_QUOTES, 'UTF-8'));
```

```
483 $zip_node = $contact_node->addChild("PostalCode",
    htmlspecialchars($params['zip_code'], ENT_QUOTES, 'UTF-8'));

484 $subzip_node = $contact_node->addChild("SubPostalCode",
    htmlspecialchars($params['sub_zip_code'], ENT_QUOTES, 'UTF-8'));

485 $note_node = $contact_node->addChild("Note",
    htmlspecialchars($params['notes'], ENT_QUOTES, 'UTF-8'));

486 $emailtype_node = $contact_node->addChild("EmailType",
    htmlspecialchars($params['mail_type'], ENT_QUOTES, 'UTF-8'));

490 $contact_node->addChild("CustomField".$k, htmlspecialchars(($v),
    ENT_QUOTES, 'UTF-8'));
```

Sample Campaign Form

cc_class.php (createCampaignXML Function)

Before:

```
897 $title_node = $xml_object->addChild("title",
    htmlentities($params['cmp_name']));

907 $name_node = $campaign_node->addChild("Name",
    urldecode(htmlentities($params['cmp_name'])));

912 $subj_node = $campaign_node->addChild("Subject",
    urldecode(htmlentities($params['cmp_subject'])));

913 $from_name_node = $campaign_node->addChild("FromName",
    urldecode(htmlentities($params['cmp_from_name'])));

918 $as_weblink_node = $campaign_node->addChild("ViewAsWebpageLinkText",
    urldecode(htmlentities($as_web_lnk_txt)));

921 $as_webtxt_node = $campaign_node->addChild("ViewAsWebpageText",
    urldecode(htmlentities($as_web_txt)));

924 $text_reminder_node = $campaign_node->addChild("PermissionReminderText",
    urldecode(htmlentities($permission_reminder_text)));

927 $grt_str_node = $campaign_node->addChild("GreetingString",
    htmlentities($params['cmp_grt_str']));

928 $org_name_node = $campaign_node->addChild("OrganizationName",
    htmlentities($params['cmp_org_name']));

929 $org_addr1_node = $campaign_node->addChild("OrganizationAddress1",
    htmlentities($params['cmp_org_addr1']));

930 $org_addr2_node = $campaign_node->addChild("OrganizationAddress2",
    htmlentities($params['cmp_org_addr2']));

931 $org_addr3_node = $campaign_node->addChild("OrganizationAddress3",
    htmlentities($params['cmp_org_addr3']));
```

```
932 $org_city_node = $campaign_node->addChild("OrganizationCity",
    htmlentities($params['cmp_org_city']));

952 $international_state = $params['org_state'];

956 $org_zip_node = $campaign_node->addChild("OrganizationPostalCode",
    htmlentities($params['org_zip']));

961 $fwd_email_node = $campaign_node->addChild("ForwardEmailLinkText",
    htmlentities($fwd_txt));

966 $sub_link_node = $campaign_node->addChild("SubscribeLinkText",
    htmlentities($sub_txt));

969 $html_body_node = $campaign_node->addChild("EmailContent",
    htmlentities($params['cmp_html_body']));

970 $text_body_node = $campaign_node->addChild("EmailTextContent",
    "<Text>".strip_tags($params['cmp_text_body'])."</Text>");

972 $style_sheet_node = $campaign_node->addChild("StyleSheet",
    $campaign_style_sheet);
```

After:

```
897 $title_node = $xml_object->addChild("title",
    htmlspecialchars($params['cmp_name'], ENT_QUOTES, 'UTF-8'));

907 $name_node = $campaign_node->addChild("Name",
    urldecode(htmlspecialchars($params['cmp_name'], ENT_QUOTES, 'UTF-8')));

912 $subj_node = $campaign_node->addChild("Subject",
    urldecode(htmlspecialchars($params['cmp_subject'], ENT_QUOTES, 'UTF-8')));

913 $from_name_node = $campaign_node->addChild("FromName",
    urldecode(htmlspecialchars($params['cmp_from_name'], ENT_QUOTES, 'UTF-
    8')));

918 $as_weblink_node = $campaign_node->addChild("ViewAsWebpageLinkText",
    urldecode(htmlspecialchars(($as_web_lnk_txt), ENT_QUOTES, 'UTF-8')));

921 $as_webtxt_node = $campaign_node->addChild("ViewAsWebpageText",
    urldecode(htmlspecialchars(($as_web_txt), ENT_QUOTES, 'UTF-8')));

924 $text_reminder_node = $campaign_node->addChild("PermissionReminderText",
    urldecode(htmlspecialchars(($permission_reminder_text), ENT_QUOTES, 'UTF-
    8')));

927 $grt_str_node = $campaign_node->addChild("GreetingString",
    htmlspecialchars($params['cmp_grt_str'], ENT_QUOTES, 'UTF-8'));

928 $org_name_node = $campaign_node->addChild("OrganizationName",
    htmlspecialchars($params['cmp_org_name'], ENT_QUOTES, 'UTF-8'));
```

```
929 $org_addr1_node = $campaign_node->addChild("OrganizationAddress1",
    htmlspecialchars($params['cmp_org_addr1'], ENT_QUOTES, 'UTF-8'));

930 $org_addr2_node = $campaign_node->addChild("OrganizationAddress2",
    htmlspecialchars($params['cmp_org_addr2'], ENT_QUOTES, 'UTF-8'));

931 $org_addr3_node = $campaign_node->addChild("OrganizationAddress3",
    htmlspecialchars($params['cmp_org_addr3'], ENT_QUOTES, 'UTF-8'));

932 $org_city_node = $campaign_node->addChild("OrganizationCity",
    htmlspecialchars($params['cmp_org_city'], ENT_QUOTES, 'UTF-8'));

952 $international_state = htmlspecialchars($params['org_state'], ENT_QUOTES,
    'UTF-8');

956 $org_zip_node = $campaign_node->addChild("OrganizationPostalCode",
    htmlspecialchars($params['org_zip'], ENT_QUOTES, 'UTF-8'));

961 $fwd_email_node = $campaign_node->addChild("ForwardEmailLinkText",
    htmlspecialchars(($fwd_txt), ENT_QUOTES, 'UTF-8'));

966 $sub_link_node = $campaign_node->addChild("SubscribeLinkText",
    htmlspecialchars(($sub_txt), ENT_QUOTES, 'UTF-8'));

969 $html_body_node = $campaign_node->addChild("EmailContent",
    htmlspecialchars($params['cmp_html_body'], ENT_QUOTES, 'UTF-8'));

970 $text_body_node = $campaign_node->addChild("EmailTextContent",
    "<Text>".htmlspecialchars(strip_tags($params['cmp_text_body']),
    ENT_QUOTES, 'UTF-8')."</Text>");

972 $style_sheet_node = $campaign_node->addChild("StyleSheet",
    htmlspecialchars($campaign_style_sheet, ENT_QUOTES, 'UTF-8'));
```