Security Testing: Assignments #7-8

Due on Friday, April 19, 2013

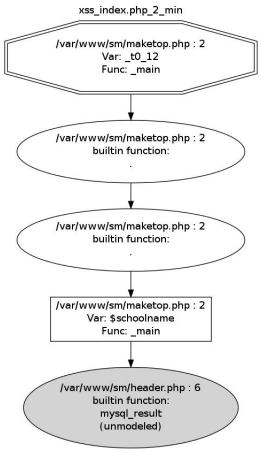
Jones 13:30am

Fabrizio Zeni

Contents

Vulnerabilities 2,3,4,6,10,53

Brief Analysis



Files: maketop.php,header.php

VARIABLE	RESULT
schoolname	false positive

Explanation

Explanation

```
1  $query = mysql_query("select schoolname from schoolinfo")
       or die("Unable to retrieve school name: " . mysql_error());
3
   $schoolname = mysql_result($query,0);
```

/var/www/sm/header.php

As we can see from the query, the field that can be the source of the vulnerability is *schoolname*, so we have to check if and where a injection can be made over that field.

```
$query = mysql_query("UPDATE schoolinfo SET schoolname = \"".htmlspecialchars($_POST["
    schoolname"])."\", address = '$_POST[schooladdress]', phonenumber = '$_POST[
    schoolphone]', sitetext = '$_POST[sitetext]', sitemessage = '$_POST[sitemessage]',
    numsemesters = '$_POST[numsemesters]', numperiods = '$_POST[numperiods]', apoint = '
    $_POST[apoint]', bpoint = '$_POST[bpoint]', cpoint = '$_POST[cpoint]', dpoint = '
    $_POST[dpoint]', fpoint = '$_POST[fpoint]' where schoolname = '$schoolname' LIMIT 1 ")
    ;
```

/var/www/sm/header.php

Inside the application we have only one *UPDATE* statement, which is contained in header.php. However we can notice that the input for schoolname is sanitizied through the **htmlspecialchars()** function call. So no injection is possible and then the vulnerability can be classified as a false positive.

Vulnerabilities(*)

Brief Analysis

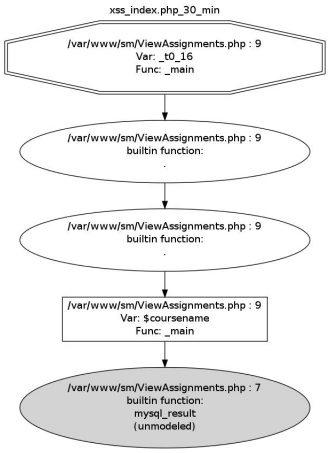
VARIABLE	AFFECTED PAGES(*)	RESULT
page	all	false positive
page2	all	false positive
selectclass	11,37,76,87,89,165,180,181,183,194,200,201,309,316	false positive
student	13,142,194	false positive
semester	13	false positive
delete	37,41,44,76,85,111,115,149,161	false positive
assignment	76	false positive
onpage	146,183,257,260,268,273,283,288,293,309,320	false positive

(*) 11: AddAssignment.php — 13: AddAttendance.php —16: AddAnnouncements.php — 18: AddUser.php — 19: AddTerm.php — 37: EditAssignment.php — 41: EditAnnouncements.php — 44: EditTerms.php — 63: AddTeacher.php — 70: AddStudent.php — 71: AddSemester.php — 76: EditGrade.php — 85: EditSemester.php — 87/88: ViewClassSettings.php — 90: ViewStudents.php — 93: AddParent.php — 111: EditTeacher.php — 115: EditStudent.php — 126: ViewCourses.php — 138: StudentViewCourses.php — 141: AddClass.php — 142: ParentViewCourses.php — 146/147/148: ViewAnnoucements.php — 149: EditUser.php — 161: EditParent.php — 165: StudentMain.php — 180: TeacherMain.php — 181: ViewStudents.php — 183/184: ViewAssignments.php — 186/241: AdminMain.php — 191: DeficiencyReport.php — 194: ParentMain.php — 200/201: ViewGrades.php — 212: PointsReport.php — 130: VisualizeClasses.php — 238: VisualizeRegistration.php — 239: EditClasses.php — ManageAnnouncements.php — 260: ManageTerms.php — 268. ManageTerms.php — 272: ManageAttendance.php — 273: ManageTeachers.php — ManageUsers.php — 288: ManageParents.php — 293: ManageStudents.php — 299: Registration.php — 309: ManageAssignments.php — 316: ManageGrades.php — 320: ManageClasses.php

Explanation

Vulnerabilities 30,31,207

Brief Analysis



Files: ViewAssignmets.php,ManageAssignments.php

VARIABLE	RESULT
coursename	positive

Explanation

```
1  $query = mysql_query("INSERT INTO courses VALUES('', '$_POST[semester]', '$termid', '
       $_POST[title]', '$_POST[teacher]', '$_POST[sectionnum]', '$_POST[roomnum]', '$_POST[
       periodnum]','','','','','','','','','','$dotw','$_POST[substitute]','')")
   or die("ManageClasses.php: Unable to insert new class - " . mysql_error());
```

/var/www/sm/ManageClasses.php

```
     $query = mysql_query("INSERT INTO courses VALUES('', '$_POST[semester]', '$termid', '
         $_POST[title]', '$_POST[teacher]', '$_POST[sectionnum]', '$_POST[roomnum]', '$_POST[
         periodnum]','','','','','','','','','','$dotw','$_POST[substitute]', '')")
2  or die("ManageClasses.php: Unable to insert new class - " . mysql_error());
```

/var/www/sm/ManageClasses.php

```
     $query = mysql_query("INSERT INTO courses VALUES('', '$_POST[semester2]', '$termid', '
         $_POST[title]', '$_POST[teacher]', '$_POST[sectionnum]', '$_POST[roomnum]', '$_POST[
         periodnum]','','','','','','','','','','$dotw','$_POST[substitute]', '')")
2  or die("ManageClasses.php: Unable to insert new class - " . mysql_error());
```

/var/www/sm/ManageClasses.php

```
1  $query = mysql_query("UPDATE `courses` SET `coursename`='$_POST[title]', `teacherid`='
       $_POST[teacher]', `semesterid`='$_POST[semester]', `sectionnum`='$_POST[sectionnum]',
       `roomnum`='$_POST[roomnum]', `periodnum`='$_POST[periodnum]', `dotw`='$dotw', `
       substituteid`='$_POST[substitute]' WHERE `courseid`='$_POST[courseid]' LIMIT 1")
   or die("ManageClasses.php: Unable to update the class information - ".mysql_error());
```

/var/www/sm/ManageClasses.php

Vulnerability 54

Brief Analysis

File: Login.php

VARIABLE	RESULT
text	positive

Explanation

```
$query = mysql_query("select sitetext from schoolinfo");
$text  = mysql_result($query,0);
```

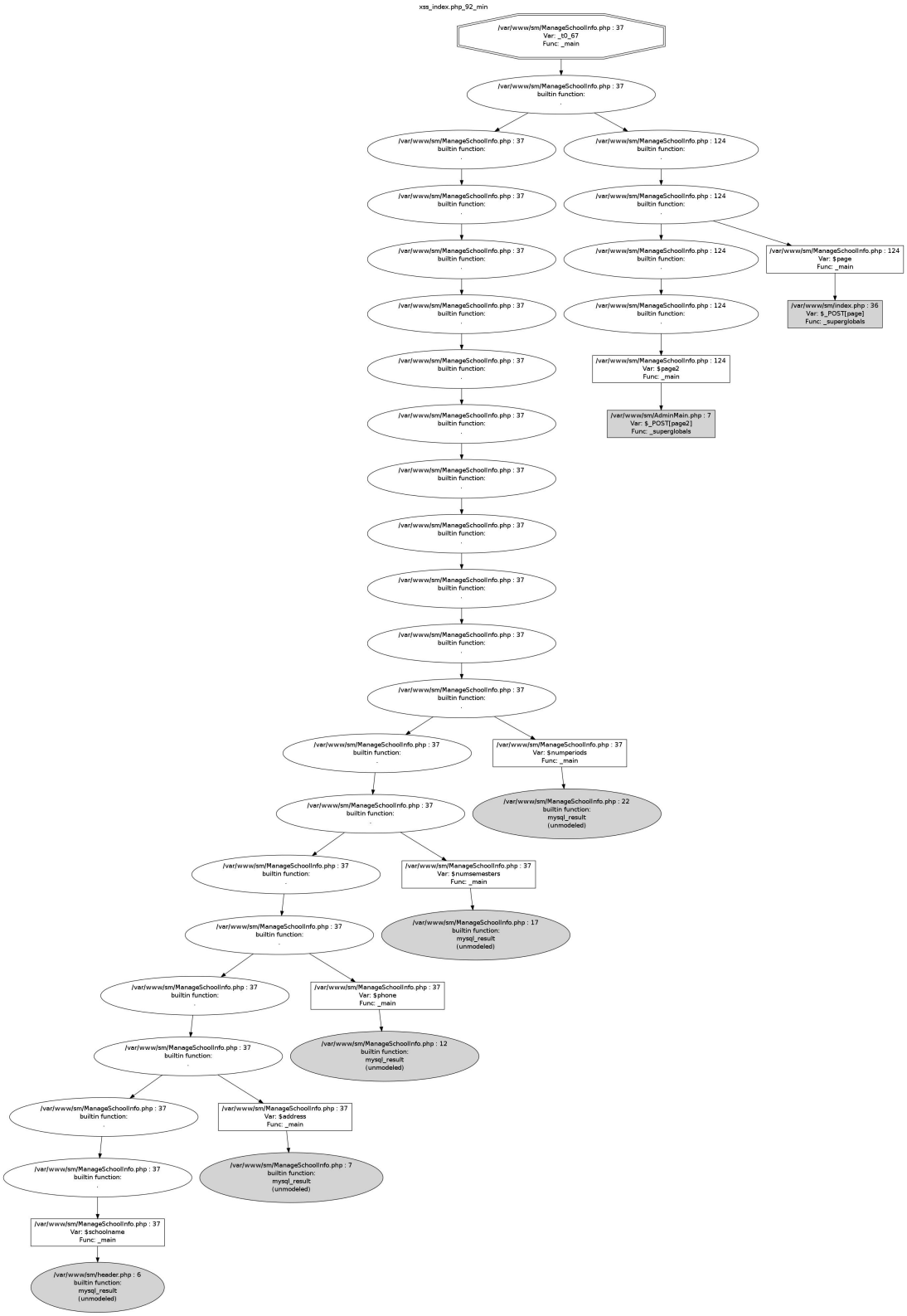
/var/www/sm/Login.php

```
$query = mysql_query("UPDATE schoolinfo SET schoolname = \"".htmlspecialchars($_POST["
    schoolname"])."\", address = '$_POST[schooladdress]', phonenumber = '$_POST[
    schoolphone]', sitetext = '$_POST[sitetext]', sitemessage = '$_POST[sitemessage]',
    numsemesters = '$_POST[numsemesters]', numperiods = '$_POST[numperiods]', apoint = '
    $_POST[apoint]', bpoint = '$_POST[bpoint]', cpoint = '$_POST[cpoint]', dpoint = '
    $_POST[dpoint]', fpoint = '$_POST[fpoint]' where schoolname = '$schoolname' LIMIT 1 ")
    ;
```

/var/www/sm/header.php

Vulnerability 92

Brief Analysis



File: ManageSchoolInfo.php

VARIABLE	RESULT
page	false positive
page2	false positive
numperiods	positive
numsemesters	positive
phone	positive
address	positive
schoolname	false positive

Explanation

The analysis of the section *Vulnerabilities*$^{(*)}$ can also fit for *page* and *page2*. Moreover, *Vulnerabilities 2,3,4,6,10,53* explains the result over *schoolname*.

numperiods,numsemesters,phone,address

```
1  $query = mysql_query("SELECT address FROM schoolinfo")
       or die("ManageSchoolInfo.php: Unable to retrieve School Address " . mysql_error());
3
   $address = mysql_result($query,0);
5
   $query = mysql_query("SELECT phonenumber FROM schoolinfo")
7      or die("ManageSchoolInfo.php: Unable to retrieve PhoneNumber " . mysql_error());

9  $phone = mysql_result($query,0);

11 $query = mysql_query("SELECT numsemesters FROM schoolinfo")
       or die("ManageSchoolInfo.php: Unable to retrieve NumSemesters " . mysql_error());
13
   $numsemesters = mysql_result($query,0);
15
   $query = mysql_query("SELECT numperiods FROM schoolinfo")
17     or die("ManageSchoolInfo.php: Unable to retrieve NumPeriods " . mysql_error());

19 $numperiods = mysql_result($query,0);
```

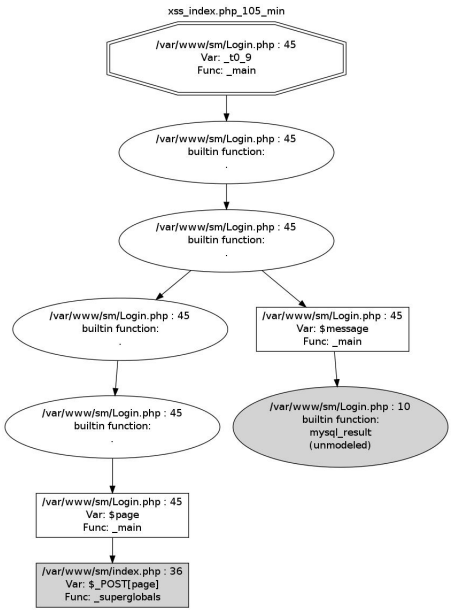
/var/www/sm/ManageSchoolInfo.php

```
$query = mysql_query("UPDATE schoolinfo SET schoolname = \"".htmlspecialchars($_POST["
    schoolname"])."\", address = '$_POST[schooladdress]', phonenumber = '$_POST[
    schoolphone]', sitetext = '$_POST[sitetext]', sitemessage = '$_POST[sitemessage]',
    numsemesters = '$_POST[numsemesters]', numperiods = '$_POST[numperiods]', apoint = '
    $_POST[apoint]', bpoint = '$_POST[bpoint]', cpoint = '$_POST[cpoint]', dpoint = '
    $_POST[dpoint]', fpoint = '$_POST[fpoint]' where schoolname = '$schoolname' LIMIT 1 ")
    ;
```

/var/www/sm/header.php

Vulnerability 105

Brief Analysis



File: Login.php

VARIABLE	RESULT
message	positive
page	false positive

Explanation

The analysis of the section *Vulnerabilities*$^{(*)}$ can also fit for *page*.

message

```
1 $query = mysql_query("select sitemessage from schoolinfo");

3 $message = mysql_result($query,0);
```

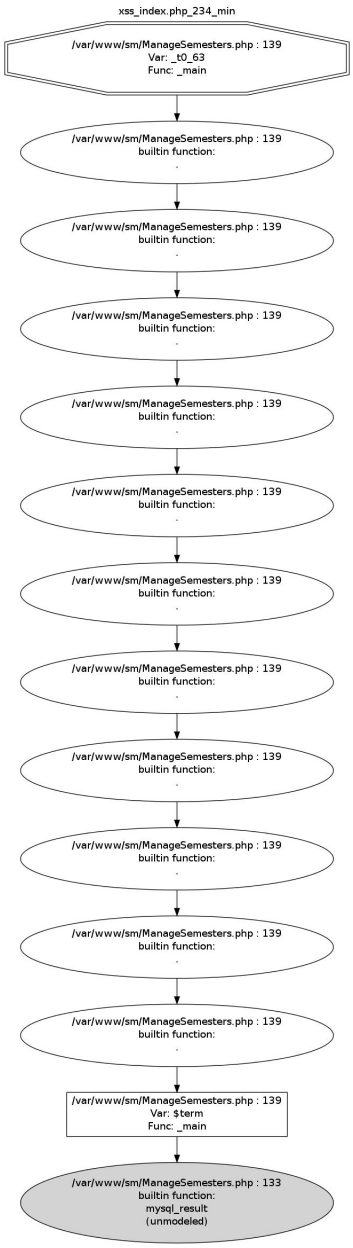
/var/www/sm/Login.php

```
$query = mysql_query("UPDATE schoolinfo SET schoolname = \"".htmlspecialchars($_POST["
    schoolname"])."\", address = '$_POST[schooladdress]', phonenumber = '$_POST[
    schoolphone]', sitetext = '$_POST[sitetext]', sitemessage = '$_POST[sitemessage]',
    numsemesters = '$_POST[numsemesters]', numperiods = '$_POST[numperiods]', apoint = '
    $_POST[apoint]', bpoint = '$_POST[bpoint]', cpoint = '$_POST[cpoint]', dpoint = '
    $_POST[dpoint]', fpoint = '$_POST[fpoint]' where schoolname = '$schoolname' LIMIT 1 ")
    ;
```

/var/www/sm/header.php

Vulnerability 234

Brief Analysis



File: ManageSemesters.php

VARIABLE	RESULT
term	positive

Explanation

```
1  $query2 = mysql_query("SELECT title FROM terms WHERE termid='$smstr[1]'");
   $term = mysql_result($query2,0);
```

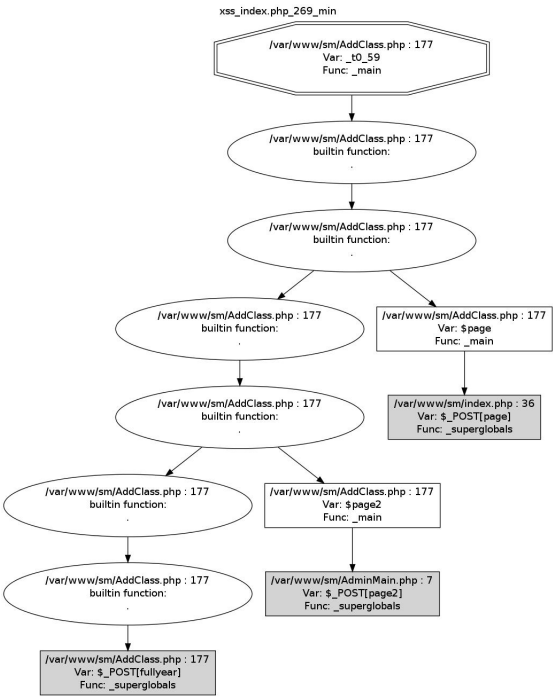
/var/www/sm/ManageSemesters.php

```
1  $query = mysql_query("UPDATE `terms` SET `title`='$_POST[title]', `startdate`='$_POST[
       startdate]', `enddate`='$_POST[enddate]' WHERE `termid`='$_POST[termid]' LIMIT 1")
   or die("ManageTerms.php: Unable to update the term information - ".mysql_error());
```

/var/www/sm/ManageTerms.php

Vulnerability 269

Brief Analysis



File: AddClass.php

VARIABLE	RESULT
page	false positive
page2	false positive
fullyear	false positive

Explanation

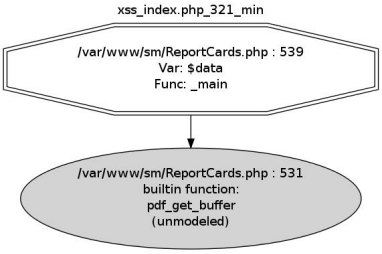
The analysis of the section *Vulnerabilities*$^{(*)}$ can also fit for *page* and *page2*.

fullyear

The parameter is just used to display a different form of insertion of the class, so no xss is possible here.

Vulnerability 321

Brief Analysis



File: ReportCards.php

VARIABLE	RESULT
data	positive

Explanation

```
$sql = mysql_query("SELECT coursename, q1points, q2points, totalpoints, aperc, bperc, cperc
    , dperc, fperc, secondcourseid, semesterid FROM courses WHERE courseid = $cid[0]
    $clause");
while($class = @mysql_fetch_row($sql))
{
```

/var/www/sm/ReportCards.php

```
pdf_show_xy($pdf, "$class[0]", 55, $start);
```

/var/www/sm/ReportCards.php

As long as seen at *Vulnerabilities 30,31,207*, *coursename* can be a injected with malicious strings which can lead to an xss vulnerability. In this case the pdf generated can contain such malicious string.