Pixy graph #	File(s) involved	Type	Affected code	Explanation	Test file
2	header.php	FP		Both the query and the assignment to $schoolname are using htmlspecialchars to sanetize what comes from the POST	----
3	maketop.php header.php	FP		Same as 2	----
4	maketop.php header.php	FP		Same as 2	----
6	maketop.php header.php	FP		Same as 2	----
10	maketop.php header.php	FP		Same as 2	----
11.1	AddAssignment.php index.php	REFLECTED XSS	$page = $_POST["page"];	$page is printed in AddAssignment.php but when it's assigned no sanity check is performed in index.php	Test11
11.2	AddAssignment.php TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	$page2 is printed in AddAssignment.php but when it's assigned no sanity check is performed in TeacherMain.php	
11.3	AddAssignment.php TeacherMain.php	REFLECTED XSS	<input type='hidden' name='selectclass'value='$_POST[selectclass]' />	The selectclass parameters identifies the id (numeric) of a course. The value is directly taken from a post without any sanity or type checking.	
13.1	AddAttendance.php index.php	REFLECTED XSS	$page = $_POST["page"];	Same as 11.1	Test13
13.2	AddAttendance.php AdminMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 11.2	
13.3	AddAttendance.php	REFLECTED XSS	<input type='hidden' name='student' value='$_POST[student]' />	The value of the input is directly taken from the student POST wo any sanetization	
13.4	AddAttendance.php	REFLECTED XSS	<input type='hidden' name='semester' value='$_POST[semester]' />	Same as 13.3	
16.1	AddAnnouncement.php index.php	REFLECTED XSS	$page = $_POST["page"];	Same as 11.1	Test16
16.2	AddAnnouncement.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	$page2 is assigned in AdminMain wo any sanetization and used as value (see 11.2)	
18.1	AddUser.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	$page is assigned in index wo any sanetization and used as value (see 11.1)	Test18
18.2	AddUser.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
19.1	AddTerm.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test19
19.2	AddTerm.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
30	ViewAssignments.php	REFLECTED XSS	$coursename = mysql_result($query,0);	The query is built using directly $_POST [selectclass] wo any sanetization	Test30

31	ViewAssignments.php	REFLECTED XSS	$coursename = mysql_result($query,0);	Same as 30	Test31
37.1	EditAssignment.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test37
37.2	EditAssignment.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' />	The value of the input is directly taken from the selectclass POST wo any sanetization	
37.3	EditAssignment.php TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	$page2 is directly taken in TeacherMain wo any sanetization and used as input value in EditAssignment	
37.4	EditAssignment.php	REFLECTED XSS	$id = $_POST["delete"];	$id is assigned the POST of delete wo any sanetization and later used as value to be printed	
41.1	EditAnnouncment.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test41
41.2	EditAnnouncment.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
41.3	EditAnnouncment.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
44.1	EditTerm.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test44
44.2	EditTerm.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
44.3	EditTerm.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
53	header.php	FP		Same as 2	----
54	Login.php	STORED XSS	print("...$text...");	The result of the query is directly displayed in a div wo any sanetization when performing the update on the db	Test54
63.1	AddTeacher.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test63
63.2	AddTeacher.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
70.1	AddStudent.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test70
70.2	AddStudent.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
71.1	AddSemester.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test71
71.2	AddSemester.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
76.1	EditGrade.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test76
76.2	EditGrade.php TeacherMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
76.3	EditGrade.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' />	The POST value of selectclass is directly used as value in the input wo any sanetization	

76.4	EditGrade.php	REFLECTED XSS	<input type='hidden' name='assignment' value='$_POST[assignment]' />	The POST value of assignment is directly used as value in the input wo any sanetization	
76.5	EditGrade.php	REFLECTED XSS	$id = $_POST['delete'];	Same as 37.4	
85.1	EditSemester.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.1	Test85
85.2	EditSemester.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
85.3	EditSemester.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
87.1	ViewClassSettings.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 76.3	Test87
87.2	ViewClassSettings.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	
87.3	ViewClassSettings.php ParentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	$page2 is assigned in ParentMain wo any sanetization and used as value (see 11.2)	
88.1	ViewClassSettings.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 76.3	Test88
88.2	ViewClassSettings.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	
88.3	ViewClassSettings.php StudentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	$page2 is assigned in StudentMain wo any sanetization and used as value (see 11.2)	
89.1	ClassSettings.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 76.3	Test89
89.2	ClassSettings.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	
89.3	ClassSettings.php TeacherMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	$page2 is assigned in TeacherMain wo any sanetization and used as value (see 11.2)	
90.1	ViewStudents.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	Test90
90.2	ViewStudents.php ParentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 87.3	
92.1	ManageSchoolInfo.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	
92.2	ManageSchoolInfo.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
92.3	ManageSchoolInfo.php header.php	FP	$numperiods = mysql_result($query,0);	False positive, since the cast of $numperiods to an integer is done implicitly by the table schema on the database	
92.4	ManageSchoolInfo.php header.php	FP	$numsemesters = mysql_result($query,0);	False positive, since the cast of $numsemesters to an integer is done implicitly by the table schema on the database	

92.5	ManageSchoolInfo.php header.php	STORED XSS	$phone = mysql_result($query,0);	The result of the query is used as value in the input. Since $phone is assigned to the result of a "read" query, the vulterability is in the UPDATE query inside the header, where schoolinfo is updated using $_POST[schoolphone] wo any sanetization	Test92
92.6	ManageSchoolInfo.php header.php	STORED XSS	$address = mysql_result($query,0);	The result of the query is used as value in the input. Since $address is assigned to the result of a "read" query, the vulterability is in the UPDATE query inside the header, where schoolinfo is updated using $_POST[schooladdress] wo any sanetization	
92.7	ManageSchoolInfo.php header.php	FP		Same as 2	----
93.1	AddParent.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	Test93
93.2	AddParent.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
105.1	Login.php header.php	STORED XSS	$message = mysql_result($query,0);-	The result of the query is used as value in the input. Since $message is assigned to the result of a "read" query, the vulterability is in the UPDATE query inside the header, where schoolinfo is updated using $_POST[sitemessage] wo any sanetization	Test105
105.2	Login.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.1	
111.1	EditTeacher.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test111
111.2	EditTeacher.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
111.3	EditTeacher.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
115.1	EditStudent.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test115
115.2	EditStudent.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
115.3	EditTeacher.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
126.1	ViewCourses.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test126
126.2	ViewCourses.php TeacherMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 89.3	
138.1	StudentViewCourses.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test138
138.2	StudentViewCourses.php StudentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 88.3	

141.1	AddClass.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test141
141.2	AddClass.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
142.1	ParentViewCourses.php	REFLECTED XSS	$query = mysql_query("SELECT studentid, fname, lname FROM students WHERE studentid = $_POST[student]")	The query is built using directly $_POST[student] wo any sanetization and later the result is printed	Test142
142.2	ParentViewCourses.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	
142.3	ParentViewCourses.php ParentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 87.3	
146.1	ViewAnnouncements.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test164
146.2	ViewAnnouncements.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Direct handling of the post value. It is both used as value in an input tag and also controls the creation of some content in the page	
146.3	ViewAnnouncements.php ParentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 87.3	
147.1	ViewAnnouncements.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test147
147.2	ViewAnnouncements.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
147.3	ViewAnnouncements.php StudentMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 88.3	
148.1	ViewAnnouncements.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test148
148.2	ViewAnnouncements.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
148.3	ViewAnnouncements.php TeacherMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 89.3	
149.1	EditUser.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test149
149.2	EditUser.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
149.3	EditUser.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
161.1	EditParent.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	

161.2	EditParent.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	Test161
161.3	EditParent.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 149.3	
165.1	StudentMain.php	REFLECTED XSS	if($_POST['selectclass'] != "" && $page2 != 0) {} <input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 146.2	Test165
165.2	StudentMain.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	
165.3	StudentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	$page2 is used to display different elements in the page and is directly display itself wo any sanetization	
180.1	TeacherMain.php	REFLECTED XSS	if($_POST['selectclass'] != "" && $page2 != 0) {} <input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 146.2	Test180
180.2	TeacherMain.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	
180.3	TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
181.1	ViewStudents.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test181
181.2	ViewStudents.php TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
181.3	ViewStudents.php	REFLECTED XSS	if($_POST['selectclass'] != "" && $page2 != 0) {} <input type='hidden' name='selectclass' value='$_POST[selectclass]' />	Same as 146.2	
183.1	ViewAssignments.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test183
183.2	ViewAssignments.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	The POST value is used as input value and to build 2 queries wo any sanetization and then their result is displayed	
183.3	ViewAssignments.php	REFLECTED XSS	$_POST["onpage"]	Multiple usage of POST value to build the page structure and its directly displayed wo any sanetization (see 183.2)	
183.4	ViewAssignments.php ParentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
184.1	ViewAssignments.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test184
184.2	ViewAssignments.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	The POST value is used as input value and to build 2 queries wo any sanetizatio and then their result is displayed	

184.3	ViewAssignments.php	REFLECTED XSS	$_POST["onpage"]	Multiple usage of POST value to build the page structure and its directly displayed wo any sanetization (see 183.2)	
184.4	ViewAssignments.php StudentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
186.1	AdminMain.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.2	Test186
186.2	AdminMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
191.1	DeficiencyReport.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.2	Test191
191.2	DeficiencyReport.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
194.1	ParentMain.php	REFLECTED XSS	if($_POST['student'] != "" && $page2 != 0) {} <input type='hidden' name='student' value='$_POST[student]' />	Same as 146.2	Test194
194.2	ParentMain.php	REFLECTED XSS	if($_POST['selectclass'] != "" && $page2 != 5) {} <input type='hidden' name='selectclass' value='$_POST[selectclass]' />-	Same as 146.2	
194.3	ParentMain.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page'>	Same as 18.2	
194.4	ParentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];-	Same as 165.3	
200.1	ViewGrades.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test200
200.2	ViewGrades.php ParentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
200.3	ViewGrades.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	The POST value is used as input value and to build 2 queries wo any sanetizatio and then their result is displayed	
201.1	ViewGrades.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test201
201.2	ViewGrades.php StudentMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 165.3	
201.3	ViewGrades.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	The POST value is used as input value and to build 2 queries wo any sanetizatio and then their result is displayed	
207	ManageAssignments.php	REFLECTED XSS	$coursename = mysql_result($query,0);	The query is build concatenating POST parameters wo any sanetizationa and the result is then shown on the page	Test207

212.1	PointsReport.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test212
212.2	PointsReport.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
230.1	VisualizeClasses.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test230
230.2	VisualizeClasses.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
234	ManageSemesters.php	STORED XSS	$term = mysql_result($query2,0);	$term is computer using a query that reads from the DB. The DB can be filled with some attack vector in ManageSemesters, since the UPDATE query uses $_POST[semester] without any sanetization. Finally $term is displayed	Test234
238.1	VisualizeRegistration.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test238
238.2	VisualizeRegistration.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
239.1	EditClass.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test239
239.2	EditClass.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
239.3	EditClass.php	REFLECTED XSS	$id = $_POST["delete"];	Same as 37.4	
241.1	GradeReport.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test241
241.2	GradeReport.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
257.1	ManageAnnouncments.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test257
257.2	ManageAnnouncments.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
257.3	ManageAnnouncments.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
260.1	ManegeTerms.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test260
260.2	ManageTerms.php	REFLECTED XSS	if($_POST["onpage"] == "") {} <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
260.3	ManageTerms.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	

268.1	ManageSemesters.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test268
268.2	ManageSemesters.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
268.3	ManageSemesters.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
269.1	AddClass.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test269
269.2	AddClass.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
269.3	AddClass.php	REFLECTED XSS	if($_POST['fullyear']!=1) {} <input type='hidden' name='fullyear' value='$_POST[fullyear]' />	Same as 146.2	
272.1	ManageAttendance.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test272
272.2	ManageAttendance.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
273.1	ManageTeachers.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test273
273.2	ManageTeachers.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
273.3	ManageTeachers.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
283.1	ManageUsers.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test283
283.2	ManageUsers.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
283.3	ManageUsers.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
288.1	ManageParents.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test288
288.2	ManageParents.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
288.3	ManageParents.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	

293.1	ManageStudents.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test293
293.2	ManageStudents.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
293.3	ManageStudents.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
299.1	Registration.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test299
299.2	Registration.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
309.1	ManageAssignments.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test309
309.2	ManageAssignments.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	Same as 201.3	
309.3	ManageAssignments.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
309.4	ManageAssignments.php TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 11.2	
316.1	ManageGrades.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test316
316.2	ManageGrades.php TeacherMain.php	REFLECTED XSS	$page2 = $_POST["page2"];	Same as 11.2	
316.3	ManageGrades.php	REFLECTED XSS	<input type='hidden' name='selectclass' value='$_POST[selectclass]' /> $query = mysql_query(...)	Same as 201.3	
320.1	ManageClasses.php index.php	REFLECTED XSS	<input type='hidden' name='page' value='$page' />	Same as 18.2	Test320
320.2	ManageClasses.php	REFLECTED XSS	if($_POST["onpage"] == "") <input type='hidden' name='onpage' value='$_POST[onpage]'>	Same as 146.2	
320.3	ManageClasses.php AdminMain.php	REFLECTED XSS	<input type='hidden' name='page2' value='$page2'>	Same as 16.2	
321	ReportCards.php	FP		The library function *pdf_get_buffer* doesn't work so it' not possible to test it	----