| **Legend** | | |
|---|---|---|
| | ✓ | True positive |
| | ✗ | False positive |
| | ✔ | True positive not found by pixy |

| **User** | **Section** | **File** | **Vulnerabilities** | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | page | page2 | student | semester | fullyear | delete | onpage | selectclass | coursename | assignment | text | message(1) | numperiods | numsemesters | phone | address | schoolname | term | data | task | comment | message(2) | **Vulnerabilities count** |
| Admin | Add | AddAnnouncement | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddAttendance | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | 4 |
| | | AddClass | ✓ | ✓ | | | ✓ | | | | | | | | | | | | | | | | | | 3 |
| | | AddParent | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddSemester | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddStudent | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddTeacher | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddTerm | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | AddUser | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| | Edit | EditAnnouncement | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditClass | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditParent | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditSemester | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditStudent | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditTeacher | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditTerm | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | EditUser | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | | | | | | 3 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| | Manage | ManageAnnouncement | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | ✔ | 4 |
| | | ManageAttendance | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | ManageClass | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ManageParent | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ManageSchoolInfo | ✓ | ✓ | | | | | | | | | | | ✗ | ✗ | ✓ | ✓ | ✗ | | | | | | 4 |
| | | ManageSemester | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | ✓ | | | | | 4 |
| | | ManageStudent | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ManageTeacher | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ManageTerm | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ManageUser | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| | Other | AdminMain | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | Registration | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | VisualizeClasses | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | VisualizeRegistration | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| | Report | DeficiencyReport | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | GradeReport | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | PointsReport | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| Student | | StudentMain | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | StudentViewCourses | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | ViewAnnouncement | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | | 3 |
| | | ViewAssignment | ✓ | ✓ | | | | | ✓ | ✓ | ✓ | | | | | | | | | | | | | | 5 |
| | | ViewClassSettings | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | ViewGrades | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| Parent | | ParentMain | ✓ | ✓ | ✓ | | | | | ✓ | | | | | | | | | | | | | | | 4 |
| | | ParentViewCourses | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | 3 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| Teacher | | AddAssignment | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | ClassSettings | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | EditAssignment | ✓ | ✓ | | | | ✓ | | ✓ | | | | | | | | | | | | | | | 4 |
| | | EditGrade | ✓ | ✓ | | | | ✓ | | ✓ | | ✓ | | | | | | | | | | | ✔ | | 6 |
| | | ManageAssignment | ✓ | ✓ | | | | | ✓ | ✓ | ✓ | | | | | | | | | | | ✔ | | | 6 |
| | | ManageGrades | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | TeacherMain | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | ViewCourses | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | 2 |
| | | ViewStudents | ✓ | ✓ | | | | | | ✓ | | | | | | | | | | | | | | | 3 |
| | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| Misc | | Login | ✓ | | | | | | | | | | ✓ | ✓ | | | | | | | | | | | 3 |

| **Total** |
|---|
| 153 |

| Pattern | |
|---|---|
| 1 | ' /> <a href="http://unitn.it">Malicious Link</a><br ' |
| 2 | 1 -- ' /><a href="http://unitn.it">Malicious Link</a><br ' |
| 3 | 1)-- ' /><a href="http://unitn.it">Malicious Link</a><br ' |
| 4 | 1' -- '><a href="http://unitn.it">Malicious Link</a><br ' |

## Vulnerabilities found by pixy

| Variable Name | True Positive | Explanation | Proof of Concept | Pattern | Non-standard pattern |
|---|---|---|---|---|---|
| $page | yes | This variable is set in index.php through the POST method and it is used to determine the “user's section” eg. AdminMain,TeacherMain, StudentMain etc. It is printed into any page as an hidden field without any kind of sanitization. | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $page2 | yes | Similar to $page, this variable is set through POST method and used for page navigation. It is printed into any page as an hidden field without any kind of sanitization. | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $_POST['student'] | yes | As the name suggests this variable is used to specify the student. It is printed into an hidden field without any kind of sanitization | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $_POST['semester'] | yes | As the name suggests this variable is used to specify the semester. It is printed into an hidden field without any kind of sanitization | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $_POST['fullyear'] | yes | This variable is present only is AddClass.php. As usual the value is printed into an hidden field without sanitization | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $_POST['delete'] | yes | This variable is present in all the Edit*.php and it is printed into an hidden field without sanitization | The variable is used in an sql statement so I used the double dashes to make the query correct and inject a malicious link at the same time | 2 | Except for EditParent.java where pattern3 is used |
| $_POST['onpage'] | yes | This variable is printed into an hidden field without sanitization. | The injection is performed by concatenating a meaningful value with a malicious link | 1 | |
| $_POST['selectclass'] | yes | As the name suggests this variable is used to specify the class. It is printed into an hidden field without any kind of sanitization | The injection is performed by concatenating a meaningful value with a malicious link | 1 | Except for ManageGrades.java where pattern4 is used |
| $coursename | yes | The variable is the result of a mysql query. It is then printed in the page without validation | The injection is performed by exploiting $_POST['selectclass'] | - | ' union select concat(coursename,' <a href="http://www.unitn.it"> Evil</a>') from courses where courseid = '1 |
| $_POST['assignment'] | yes | The variable is printed on the page as an hidden field without any validation | The injection is performed by concatenating a meaningful value with a malicious link | 4 | |
| $text | yes | The variable is the result of a mysql query. It is then printed in the page without validation | This is the case of a stored XSS: it is sufficient to save a malicious link in “Text for Login page” in the page ManageSchoolInformation.php. This value will be retrieved by Login.php thus triggering the XSS. | | <a href="www.unitn.it">Evil</a> |
| $message | yes | The variable is the result of a mysql query. It is then printed in the page without validation | This is the case of a stored XSS: it is sufficient to save a malicious link in “Message for Login page” in the page ManageSchoolInformation.php. This value will be retrieved by Login.php thus triggering the XSS. | | <a href="www.unitn.it">Evil</a> |
| $_POST['numperiods'] | no | The variable is not sanitized but just a medium integer can be saved in the database | None | - | |
| $_POST['numsemesters]'] | no | The variable is not sanitized but just a medium integer can be saved in the database | None | - | |
| $_POST'[schooladdress'] | yes | The variable is not sanitized and the attacker has 50 characters maximum to inject an attack vector. | This injection is limited to the closure of a tag and the injection of a link | | "><a href=goo.gl>Mal</a> |
| $_POST['schoolphone'] | yes | The variable is not sanitized however just 14 characters can be stored in the database. Personally I think it is really hard to find an attack but still the vulnerability is present | This injection is limited to the closure of a tag and the injection of a link | | <a href=#>A |
| $_POST['schoolname'] | no | The variable is sanitized through “htmlspecialchars” | None | | |
| $term | yes | The variable is the result of a mysql query. It is then printed in the page without validation. Note that the injection is limited to 15 characters so again it is difficult to really exploit it. | The injection is limited to the injection of an empty link | - | <a href>T</a> |

## Additional vulnerabilities not found by Pixy

| | | | | | |
|---|---|---|---|---|---|
| $_POST['task'] | yes | This variable is saved in the database without sanitization. When it is then retrieved a stored XSS is triggered. | The injection consists of a malicious link | - | <a href="http://unitn.it">Evil Link</a> |
| $_POST['comment'] | yes | This variable is saved in the database without sanitization. When it is then retrieved a stored XSS is triggered. | The injection consists of a malicious link | - | <a href="http://unitn.it">Link to Malware</a> |
| $_POST['message'] | yes | This variable is saved in the database without sanitization. When it is then retrieved a stored XSS is triggered. | The injection consists of a malicious link | - | <a href="http://unitn.it">Drive by download</a> |