**Protection of e-commerce website from SQL injection**

**Rumnaz khan (151014063)**

**Zarin Tasnim momo (151014008)**

**Prapti Iffat audri (151014052)**

**Zakaria Hossain Saikat (151014071)**

**Department of computer science and engineering**

**University of Liberal Arts Bangladesh**

**Abstract:**

Existing vulnerabilities of Web system threaten the regular work of information systems. The most common Web system vulnerability is SQL injection. This technique gives unauthorized access to database by giving input which consists of malicious code included into the query. Malicious query is treated like valid query by the database and executed. Attacker may have different intensions for attacks. Attacker may want to identify inject able and weak parameter to attack. By the attacks he/she can modify data, change data and extract data. He/she can get the confidential and sensitive data from the storage of database. The aim of this project is to create an e-commerce website that prevents sql injection.

**Introduction:**

SQL injection attack is major issue and very serious so the anticipation of SQL injection attack is major challenge in day today life. This vulnerability exists when web applications do not have proper input validation and use not parameterized stored procedures. Poorly designed web applications are vulnerable to injection of malicious code to get database access by attacker. Proper input validation and use of parameterized procedures can be used to prevent SQL injection.

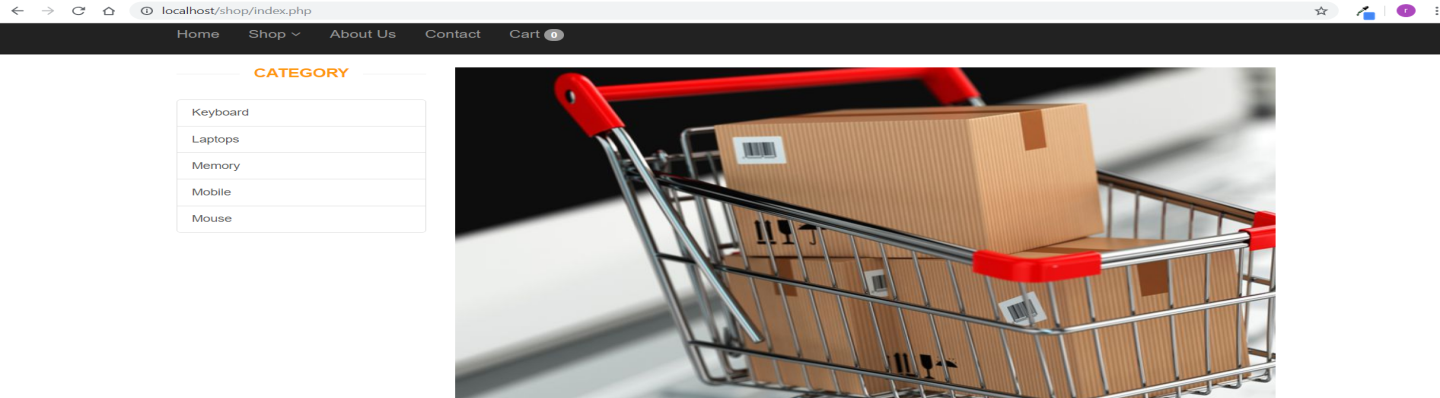
The main focus was to prevent various SQL injection attacks (version1.0) through input fields based on efficient attack detection strategies. To achieve this objective a lot of automatic tools were used which will be discussed in the later part of the report.

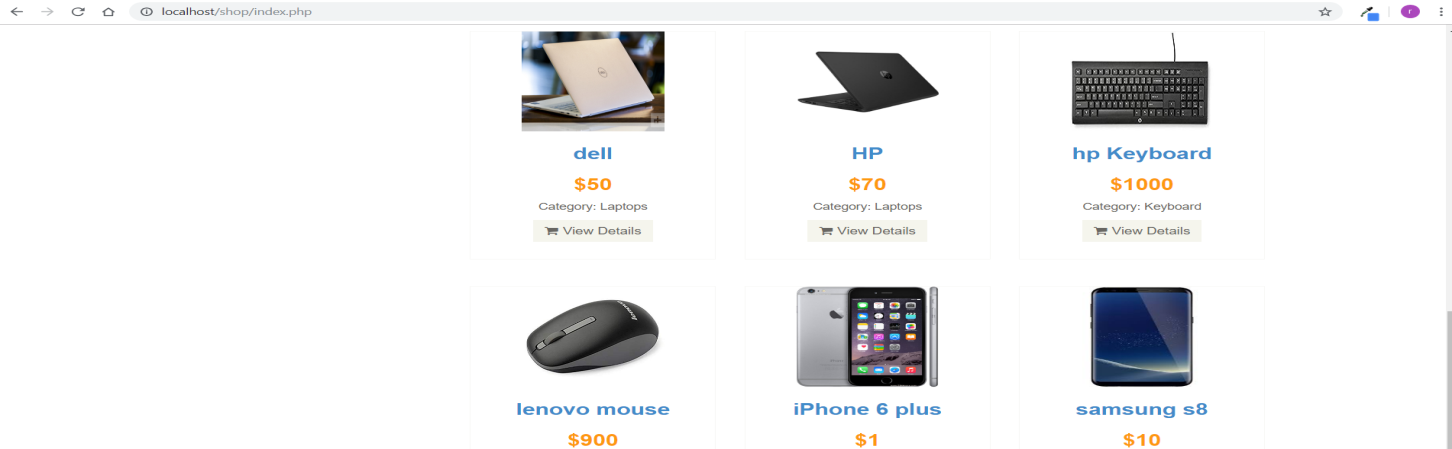
A notification system was created (version 2.0) that notifies the admin if a user is trying to attempt sql injection in the input field.

**website contents:**

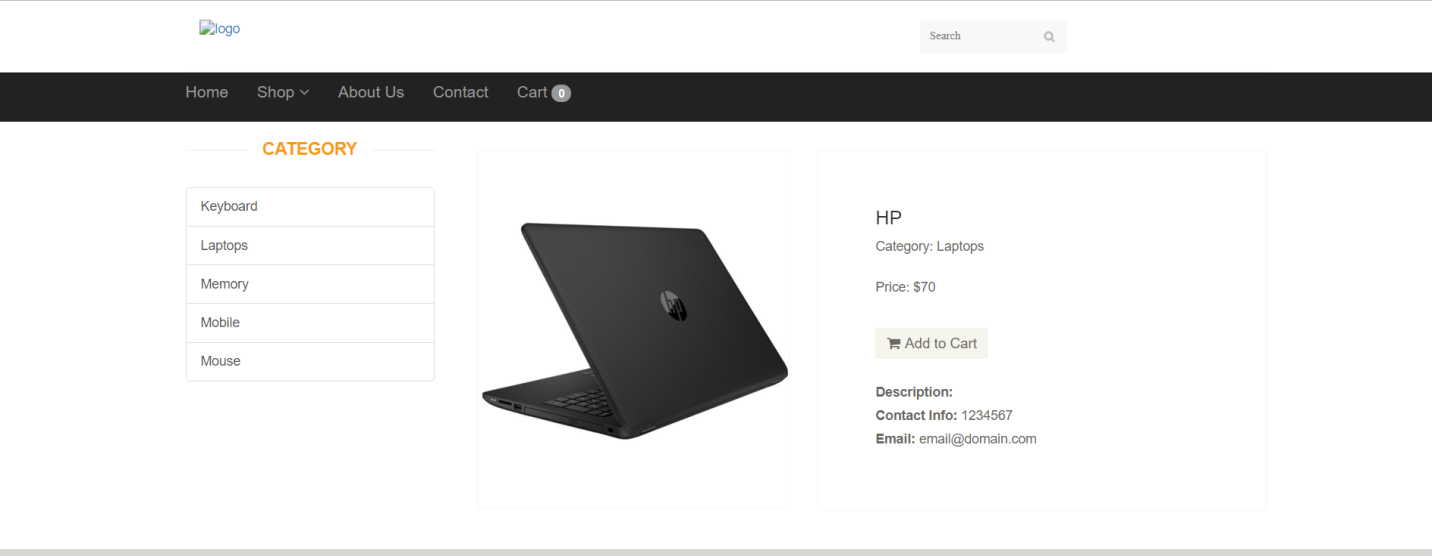
Our e-commerce website consists of all functions of a fully functional e-commerce website.

**Home page**

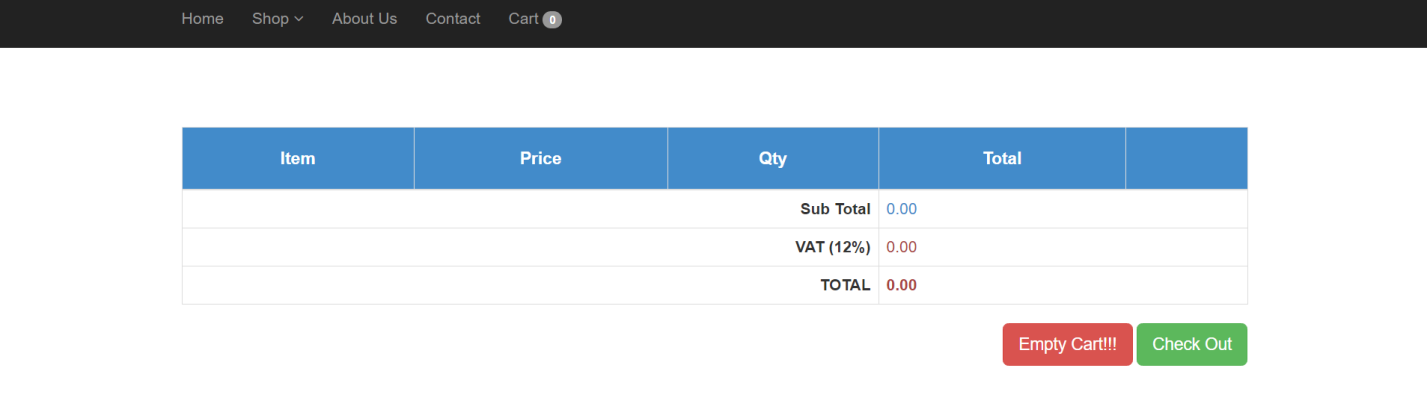




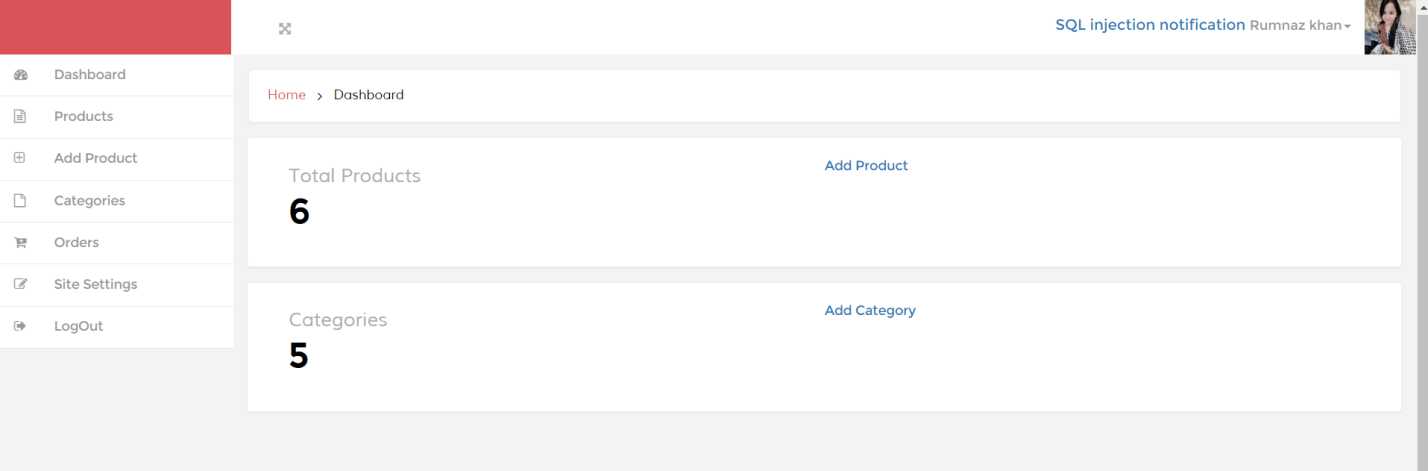
Details:



Cart:



Admin panel:

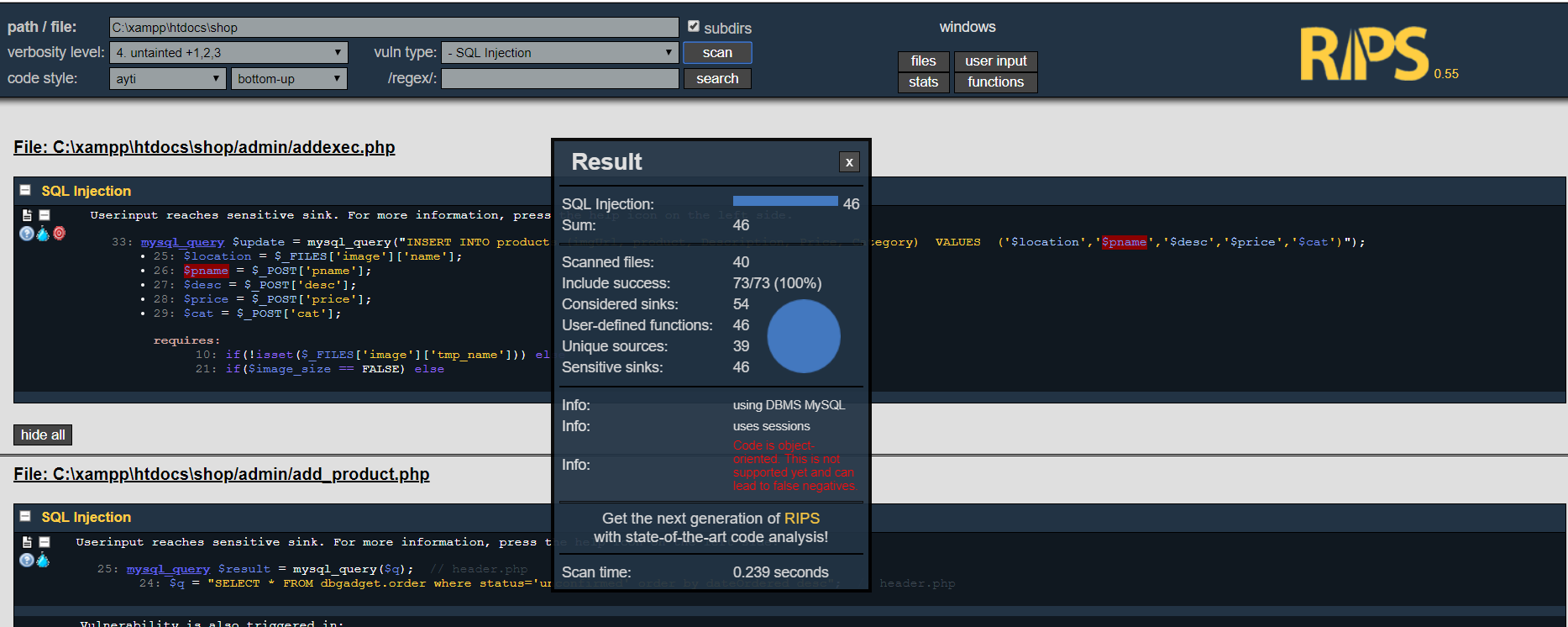


**Protection from sql injection:**

A number of ways were used for the prevention of sql injection

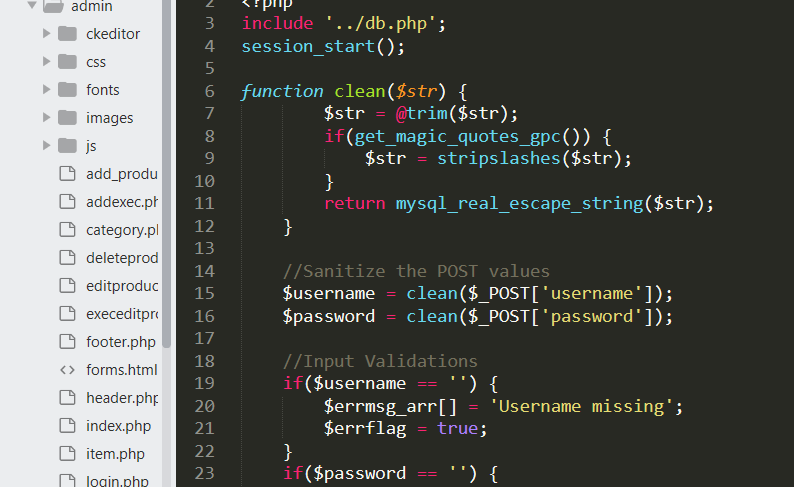
(In version 1.0)

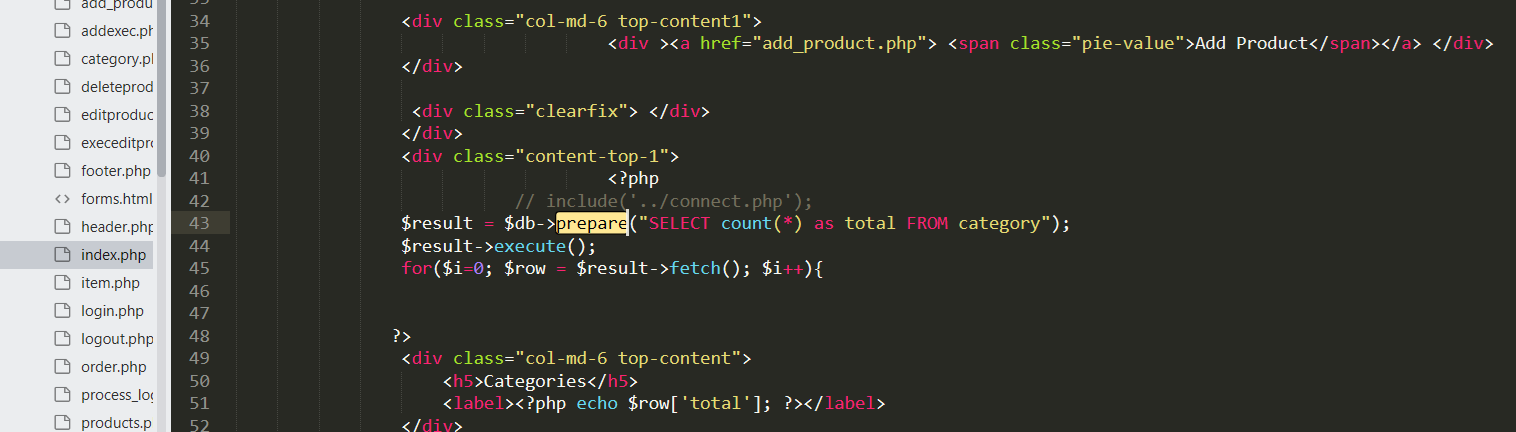
1. Firstly, RIPS was used for the detection of various vulnerabilities in the website. RIPS is the most popular static code analysis tool to automatically detect vulnerabilities in PHP applications. By tokenizing and parsing all source code files, RIPS is able to transform PHP source code into a program model and to detect sensitive sinks (potentially vulnerable functions) that can be tainted by user input (influenced by a malicious user) during the program flow.



Initially RIPS detected 46 vulnerable points in the website.

1. Next Prepared statements and mysql\_real\_escape\_string was used instead of normal sql queries.

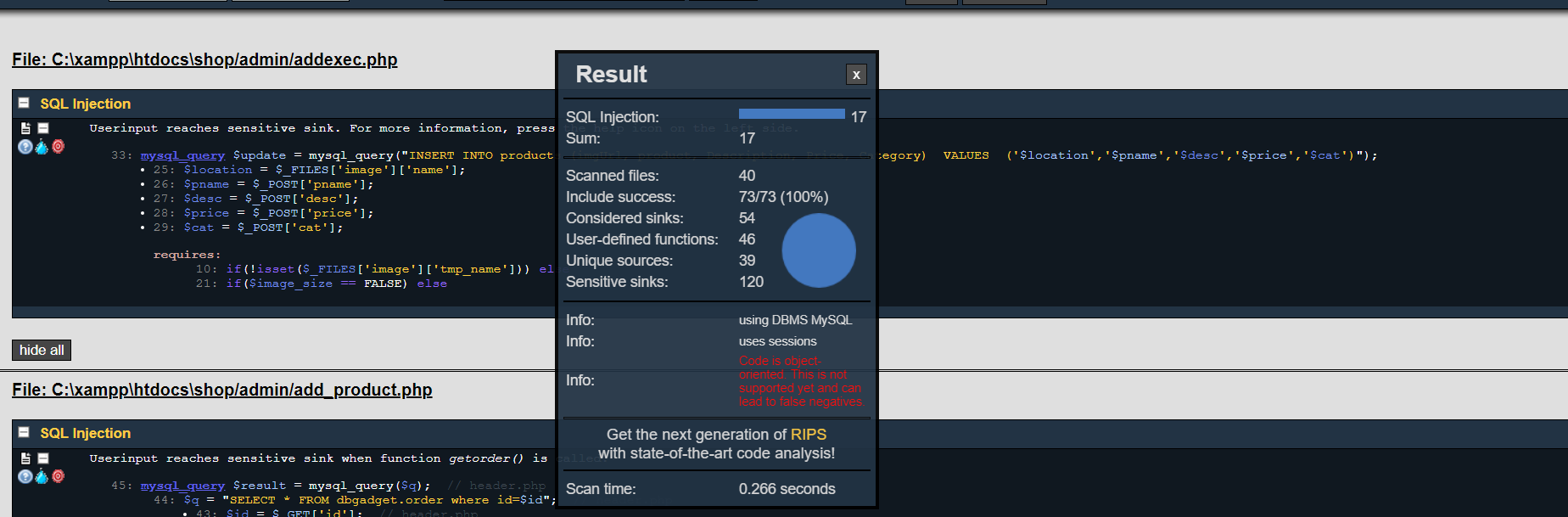






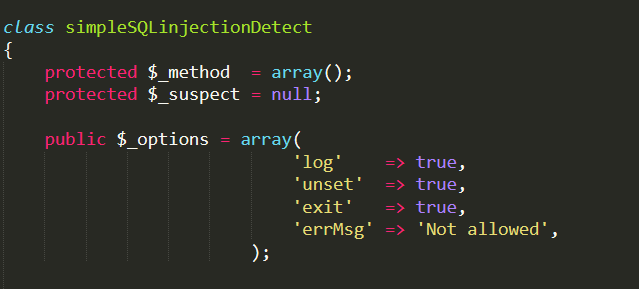


Prepared statements are resilient against SQL injection, because parameter values, which are transmitted later using a different protocol, need not be correctly escaped. If the original statement template is not derived from external input, SQL injection cannot occur. PHP provides mysql\_real\_escape\_string() to escape special characters in a string before sending a query to MySQL. This function was adopted by many to escape single quotes in strings and by the same occasion prevent SQL injection attacks. Thus vulnerabilities were brought down according to the report of RIPS:

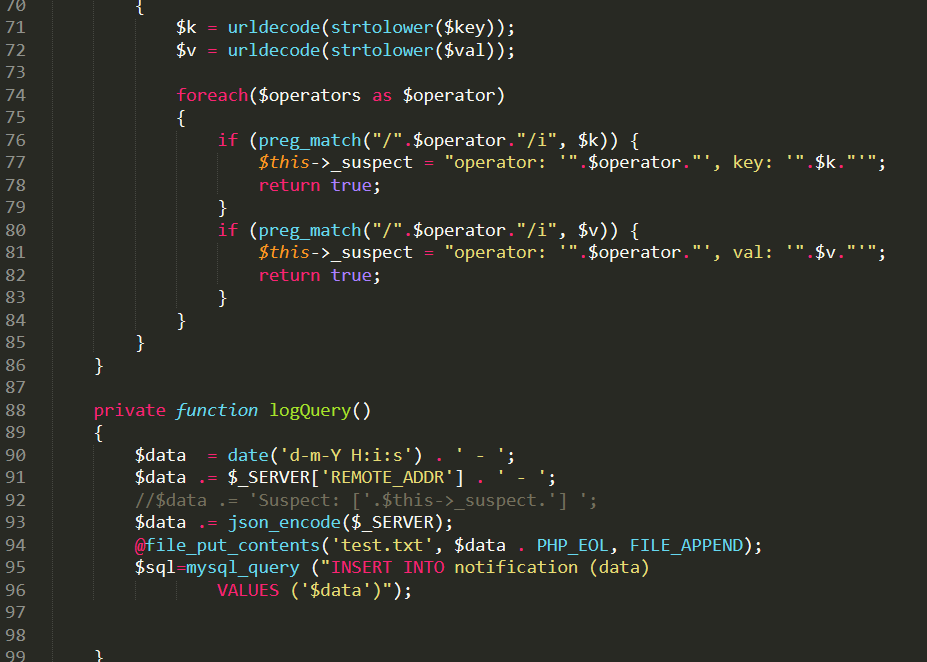


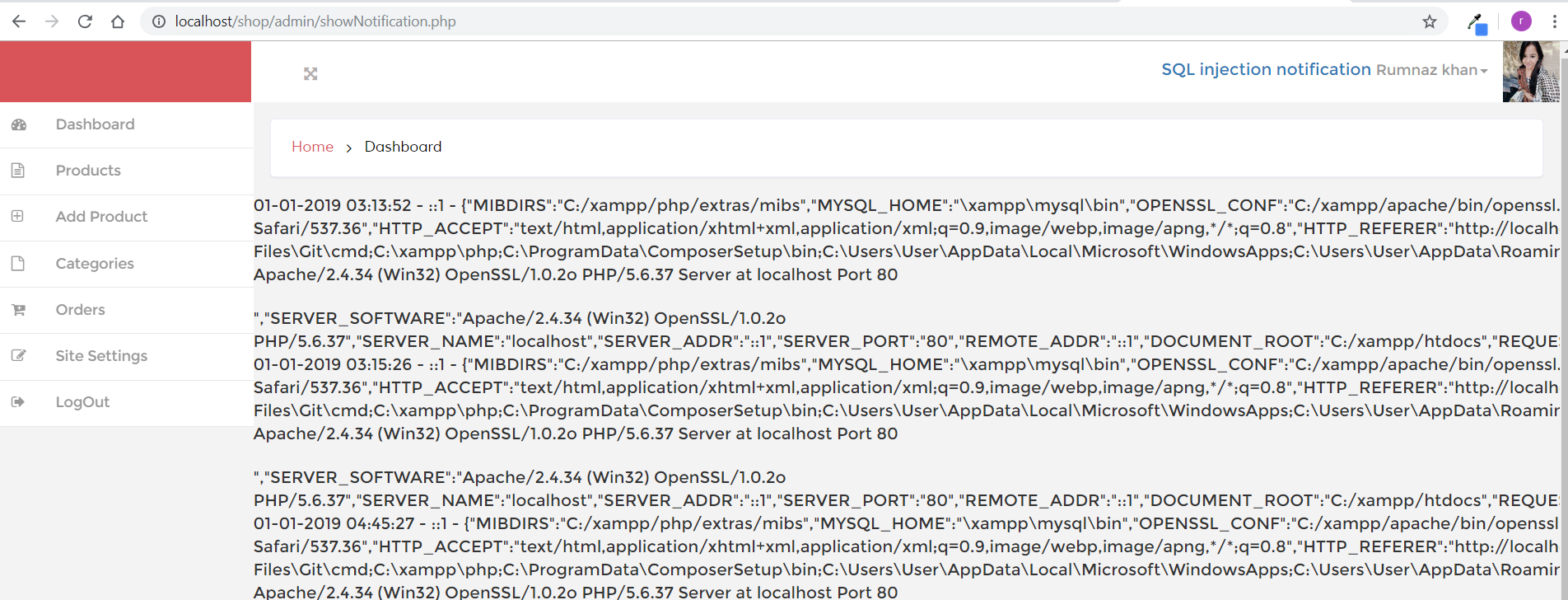
1. (Version 2.0)

A sql injection detection system is integrated within the e-commerce site that detects possible sql injection attempt. If someone is trying to put sql injection on the input field it creates a notification in the admin panel. This consists of information that when the sql injection attack was attempted and other log information. All the information are stored in the database If such an attempt is suspected the logging session dies.









**Conclusion:**

SQL Injection is most challenging threat to the web application and many solutions to these attacks have been proposed since the emerging of SQL injection. But no solution provides security to full extent. SQL Injection is a common technique that attacker use to attack on web applications. These attacks modify the SQL queries. The prevention system is mainly developed to work with MySQL, so it provides a budget, automated solution for protecting Web resources on SQL databases (and the sensitive data they hold).

In future, these detection tools can be used to detect SQL Injection attacks. These techniques can also provide as defense mechanisms for providing security against SQLIAs. In addition, more research is needed to improve analysis technique for providing better detection and prevention against strong SQLIAs.