

KHBJ PHP Report

by Kai Bentley-Jennings

Submission date: 12-Dec-2022 02:57PM (UTC+0000)

Submission ID: 192026893

File name: 11982_Kai_Bentley-Jennings_KHBJ_PHP_Report_460452_1264480669.odt (34.62K)

Word count: 532

Character count: 2625

Databases & Application Development
Module Code: ACCA5026

Report Regarding Website Security

By Kai Hakkeem Bentley Jennings(1807048)

Threats To Websites

When it comes to making a website, it is imperative that the content on the website is safely protected against a range of security risks that remain plentiful as technology progresses. Any sensitive information that can be accessed without permission or through the proper chain of events can be disastrous, as it's likely that any intruder may also have the creative tools to alter or even delete entire databases as easily as they gained entry past measures. Shoring up defences for critical components is essential in beginning to safeguard valuable data.

A method of intrusive entry or vandalism is through SQL Injection. One of the more common ways to cause deliberate damage to a database-driven website. This commonly occurs when a Web Page asks for user input, such as when searching or entering in login details. If the input hasn't been properly sanitized in the background, then there is a very high risk that an intruder will gain access to information they should not know. This is all achieved by weaponizing SQL, as intrusion is usually done by inputting a dummy answer, followed by a more 'logical' one. For example:

"UserNo: 8261177 OR 1=1"

The above example is one of many ways to extract information from SQL Databases. The database is reading this as it might normally be inputted as code in the background. The employee number may not be as specified, but 1 is equal to 1. Depending on the output method, the intruder may now have every single bit of information to do with the Users table. And if not, they now know this area is vulnerable and may attempt to damage it using commands such as "DROP TABLE USERS" to cause as much havoc as possible. Below is an example of SQL Prepared Statements, which is used to prevent SQL Injection from occurring.

```
<?
echo "Weapon Search Results<br><br>";

$query="SELECT * FROM weapons, weapontype, placeoforigin WHERE weapons.wtype=weapontype.wtype AND weapons.worigin=placeoforigin.oid AND wtypename like ? OR weapons.wtype=weapontype.wtype";

$stmt=mysqli_stmt_init($link); //set up link
mysqli_stmt_prepare($stmt,$query); //prepare query without variables
mysqli_stmt_bind_param($stmt,"sss",$search,$search,$search); //connect variables
// ^^^ IF IT'S ONE VARIABLE BUT MULTIPLE QUERY REPEAT IT IN STMT ABOVE ^^^
mysqli_stmt_execute($stmt); //execute

$result = mysqli_stmt_get_result($stmt); //getrows

//print_r($result); //print array

$numrows=mysqli_num_rows($result);
echo "Records found: ".$numrows."<br><br>";
```

Figure 1: Prepared SQL Statement

The figure above has been implemented into the website to be seen in tandem with this document, as well as Login Session checks to ensure private pages for administrators aren't easy to access should the address be correctly guessed.

Improvement on Security Assignment Website

The website previously mentioned during SQL attacks is in need of further protection, a notable one being that it can create User Sessions to access CRUD features (although missing edit and remove), however cannot wipe sessions once the user is finished. If the website was live, this could mean that a User would need only be logged onto any computer once, and that device would keep the session saved when navigating to the specific URL. This can also mean user deletion is useless as a user would still be able to create, edit and delete valuable data when they would not be authorized to. User login is also not SQL statement prepared in contrast to the search function, and would also need applying. Unsure if inserting or editing records would also require SQL statements, but most likely will be the case. The website is also unprepared for other security threats out there, and would require further reading into.

KHBJ PHP Report

GRADEMARK REPORT

FINAL GRADE

58 / 100

GENERAL COMMENTS

Instructor

WEBSITE

Database structure and design - There are several tables presented although I think only 4 are in use (admincreds, weapons, placeoforigin, weaponstype). Suitable normalised, types and lengths selected are suitable 10 / 10

Range of PHP demonstrated - 30/50

Good use of populated pull-down menus on insert

Login is OK, but you need to manage it a bit better across your site - for example make sure that nobody except the person logging in can access pages such as insertweapon.php - it is possible to get to it via the URL.

Search is quite complex showing fairly extensive joining and searching more than one field - well done. Consider including some search fields where the user has more guidance on what to search for - I wouldn't have known I could search for countries if I hadn't seen them in your database.

Cannot find anything on edit/delete

Some validation of login fields. Needs validation on insert- allows you to insert a blank weapon.

Prepared statement used on search, could also be used on insert (see below)

Overall integration of website - Always use index.php or home.php as your first page, so that the website runs without needing to search for the correct file.

For usability, would be helpful not to see the Login form again once the user is logged in - this is confusing.

Layout is a bit basic. You could have used an include for the top and bottom styling of your site - this would make it easier to change the look of the site at a future point

5.5/10

REPORT

Investigation/analysis of two security issues - SQL Injection has been considered , but a second issues has not been. 6/15

Mitigation of security issues in your site - One prepared statement has been used. You don't seem sure where prepared statements would be needed - it is anywhere where user input is used to input to a database - so would include insert and edit. It is not always about malicious intent, it can be about preventing inadvertent errors (such as Mr O'Brien containing a single quote) No second issue considered 6/15

General Comments: All academic reports should be structured with an introduction and conclusion - a short one would be OK here given the low word count

TOTAL: 57.5/100

PAGE 1

PAGE 2

PAGE 3
