Class 7

Security

BY:

BRUNO ANGELO MEDEIROS
bruno.medeiros@sc.senai.br

SQL INJECTION

PDO not only provides methods that make parameterized queries easy to use, but also makes code more portable and is easier to read. Instead of being vulnerable to SQL injection without making use of parameterized SQL queries, PDO with parameterized statements fixes the SQL injection vulnerability.

In short, we can formulate two simple rules:

Even dynamically created, SQL query have to consist of 2 possible kinds of data only:

- constant parts hardcoded in the script
- placeholders for the every dynamical value

When followed, these rules will guarantee 100% protection.

CROSS-SITE SCRIPTING (XSS)

Basically XSS occurs when a user is capable of injecting a script, often Javascript. So to prevent that from happening we need to use some functions in PHP to avoid the attack.

The simplest and most effective way to prevent XSS attacks is to escape any character that can affect the structure of your document using PHP function:

- htmlspecialchars

Note: For best result, it's import to create a function that you can reuse when necessary.

How it works:

```
1.  echo htmlspecialchars('<Byl kogda-to>.');
2.  // Output: &lt;Byl kogda-to&gt;.
```

HTACCESS

With htaccess you can configure many things, but for WorldSkills only a few are worth it.

One of them is to block the access to files.

```
1.  # Block access to specific file
2.  <files myfile.doc>
3.      Order allow, deny
4.      Deny from all
5.  </files>
6.
7.  # Block access to multiple file types
8.  <FilesMatch "\.(htaccess|htpasswd|ini|psd|log|sh)$">
9.      Order allow, deny
10.     Deny from all
11. </FilesMatch>
12.
13. # Block list of files
14. Options -Indexes
```