FORMS

By Hafiza Alia

PHP Form Handling

- The PHP superglobals $_GET and $_POST are used to collect form-data.

What is the $_SERVER["PHP_SELF"] variable?

- The $_SERVER["PHP_SELF"] is a super global variable that returns the filename of the currently executing script.
- So, the $_SERVER["PHP_SELF"] sends the submitted form data to the page itself, instead of jumping to a different page.

PHP Form Security

- The $_SERVER["PHP_SELF"] variable can be used by hackers!
- If PHP_SELF is used in your page, then a user can enter a slash (/) and then some Cross Site Scripting (XSS) commands to execute.
- `http://www.example.com/test_form.php/%22%3E%3Cscript%3Ealert('hacked')%3C/script%3E`
- In this case, the above code will be translated to:
  - `<form method="post" action="test_form.php/"><script>alert('hacked')</script>`

What is the htmlspecialchars() function?

- The htmlspecialchars() function converts special characters to HTML entities. This means that it will replace HTML characters like < and > with &lt; and &gt;. This prevents attackers from exploiting the code by injecting HTML or Javascript code (Cross-site Scripting attacks) in forms.

How To Avoid $_SERVER["PHP_SELF"] Exploits?

-
  ```
  <form method="post" action="<?php echo htmlspecialchars($_SERVER["PHP_SELF"]);?>">
  ```

- The htmlspecialchars() function converts special characters to HTML entities. Now if the user tries to exploit the PHP_SELF variable, it will result in the following output:

-
  ```
  <form method="post" action="test_form.php/&quot;&gt;&lt;script&gt;alert('hacked')&lt;/script&gt;">
  ```

Data Validation

1. Strip unnecessary characters (extra space, tab, newline) from the user input data (with the PHP trim() function)
2. Remove backslashes (\) from the user input data (with the PHP stripslashes() function)

- 3. The htmlspecialchars() function converts special characters to HTML entities.

Data Validation

```
function test_input($data) {
  $data = trim($data);
  $data = stripslashes($data);
  $data = htmlspecialchars($data);
  return $data;
}
```