Input sanitisation

Why its needed and how to do it

Xss – Cross site scripting

- Trusted websites infested with code
- Usually javascript
- Malicious intent

SQL Injection attack

- Equifax told is about their attack 2017
- Less secure webapp
- SQL injection to access unauthorised data

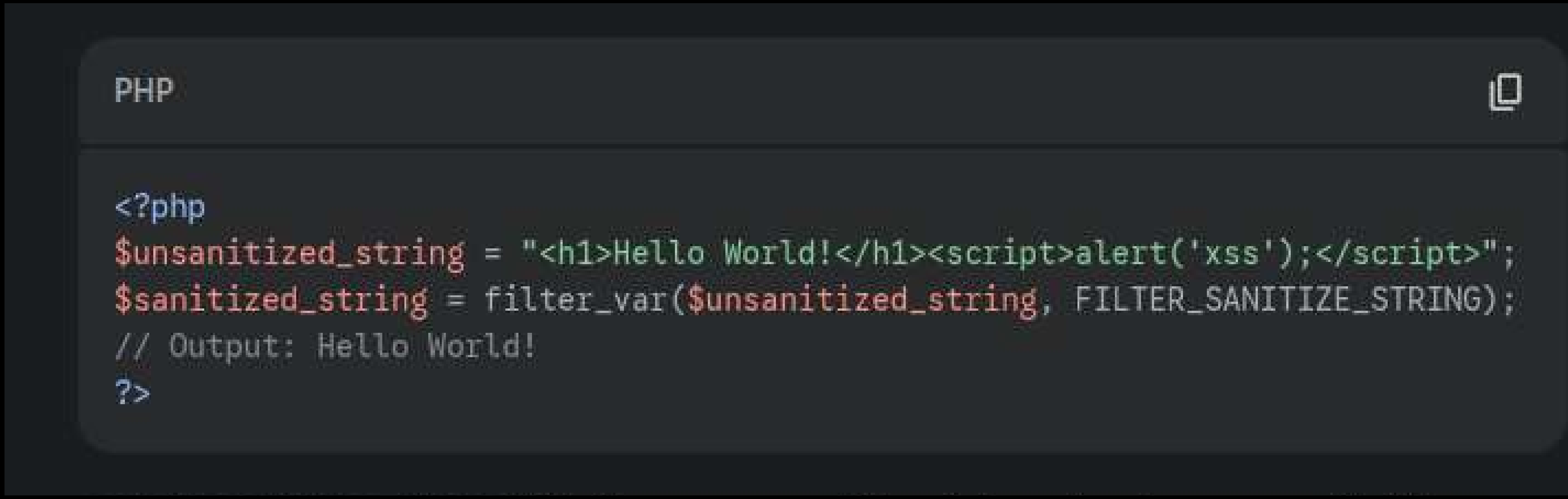
filter_var()

- Built in feature of PHP

- Sub routine that is called, it cleans out input and RETURNS a clean value.

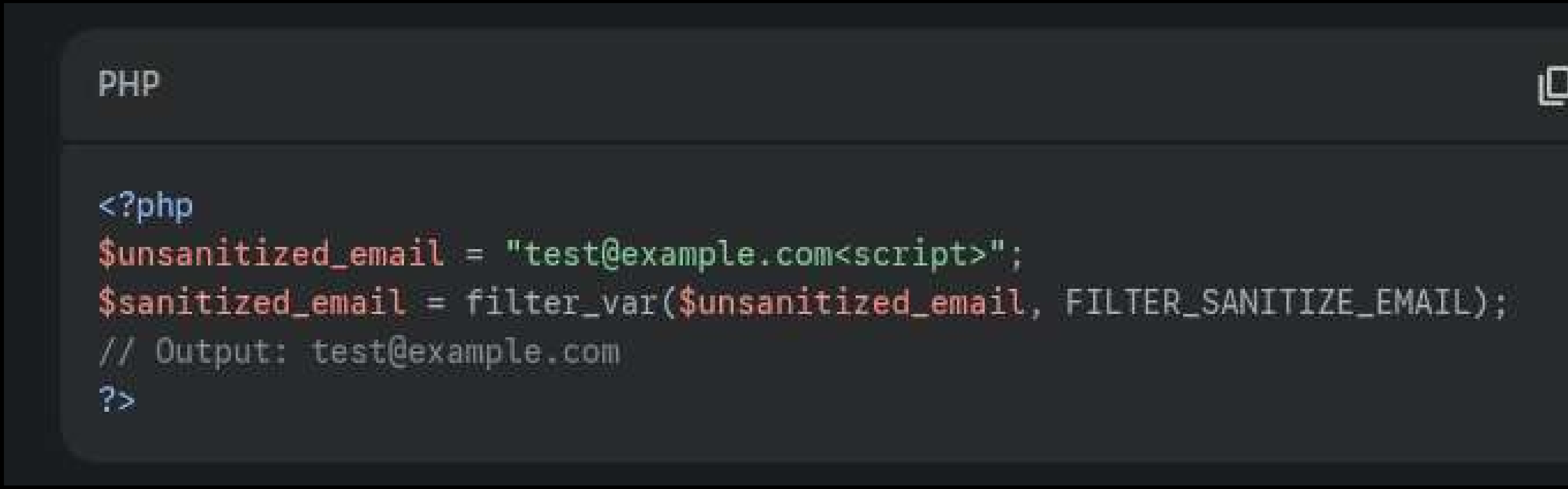
- Make sure to capture the returned value

FILTER_SANITIZE_STRING


PHP

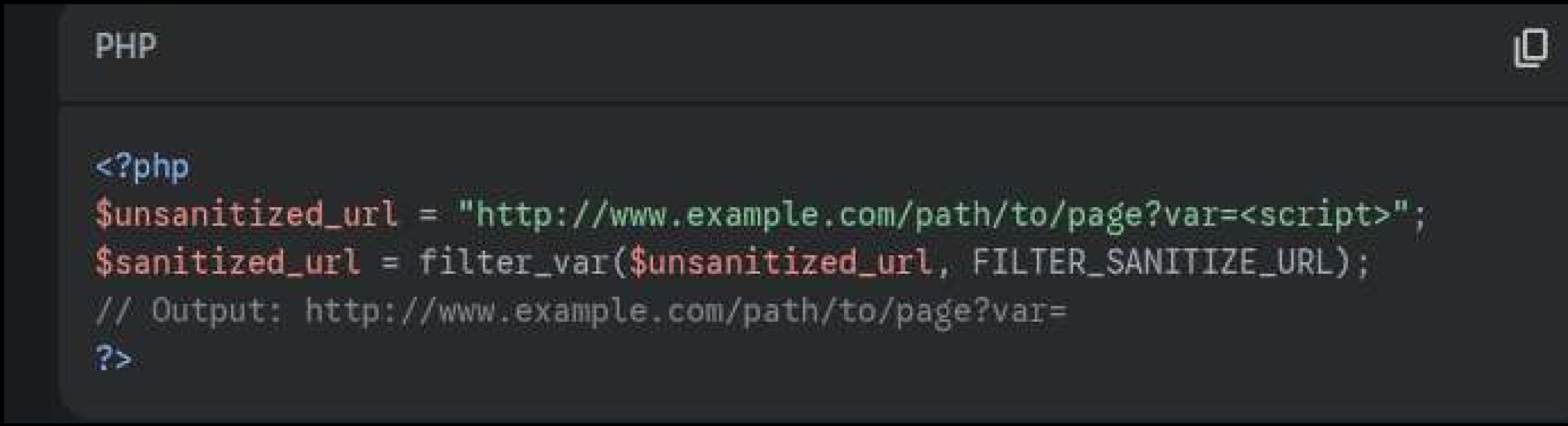
```php
<?php
$unsanitized_string = "<h1>Hello World!</h1><script>alert('xss');</script>";
$sanitized_string = filter_var($unsanitized_string, FILTER_SANITIZE_STRING);
// Output: Hello World!
?>
```

FILTER_SANITIZE_EMAIL


PHP

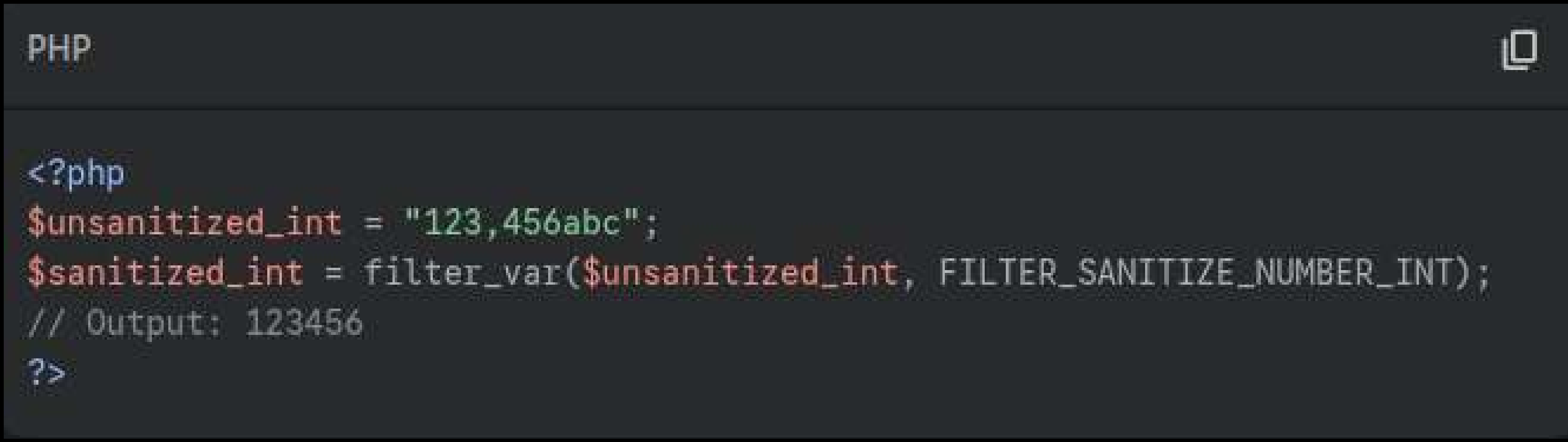
```php
<?php
$unsanitized_email = "test@example.com<script>";
$sanitized_email = filter_var($unsanitized_email, FILTER_SANITIZE_EMAIL);
// Output: test@example.com
?>
```

FILTER_SANITIZE_URL


PHP

```php
<?php
$unsanitized_url = "http://www.example.com/path/to/page?var=<script>";
$sanitized_url = filter_var($unsanitized_url, FILTER_SANITIZE_URL);
// Output: http://www.example.com/path/to/page?var=
?>
```

FILTER_SANITIZE_NUMBER_INT


PHP

```php
<?php
$unsanitized_int = "123,456abc";
$sanitized_int = filter_var($unsanitized_int, FILTER_SANITIZE_NUMBER_INT);
// Output: 123456
?>
```

FILTER_SANITIZE_NUMBER_FLOAT

- <?php
- $unsanitized_float = "123.456,789";
- $sanitized_float = filter_var($unsanitized_float, FILTER_SANITIZE_NUMBER_FLOAT, FILTER_FLAG_ALLOW_FRACTION); // Output: 123.45

Task: Make a mini site called "sa

- Set up directory called: sani
- Create a form on the index page which takes in ea
  the types of input to sanitise
- Sanitise each output the result with a suitable mes