Cross-Site Scripting (XSS)

Reflected Cross-Site Scripting

Malicious codes are added into the end of the URL of a webpage as

```
http://example.com/page.php?user=<script> codes
</script>
```

To capture this from the server-side

```
<?php

if (!empty($_GET[users])) {

    $log = fogen ("data.txt", "at"):

    fwrite($log, $_GET["user"]);

    fclose($log);

}

?>
```

Persistent Cross-Site Scripting:

This happens on a site that lets users post content that other users see, such as a comments forum or social media sites.

Example:
"Hello, my name is sofia, I like coding.

<hacking <script> malicious codes here </script>"

Mitigation:
Proper code validation and sanitization wherever user-generated contents are used.