

## Bus Pass Management System v1.0 | Stored XSS

**Vulnerability name:** Stored Cross-Site Scripting.

**Vulnerability Description:** The application does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

**Impact:** The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes. Stored cross-site scripting flaws are typically more serious than reflected vulnerabilities because they do not require a separate delivery mechanism in order to reach target users, and are not hindered by web browsers' XSS filters.

**CWE:** 79

**OWASP-2017:** A7

**Mitigation:** Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.

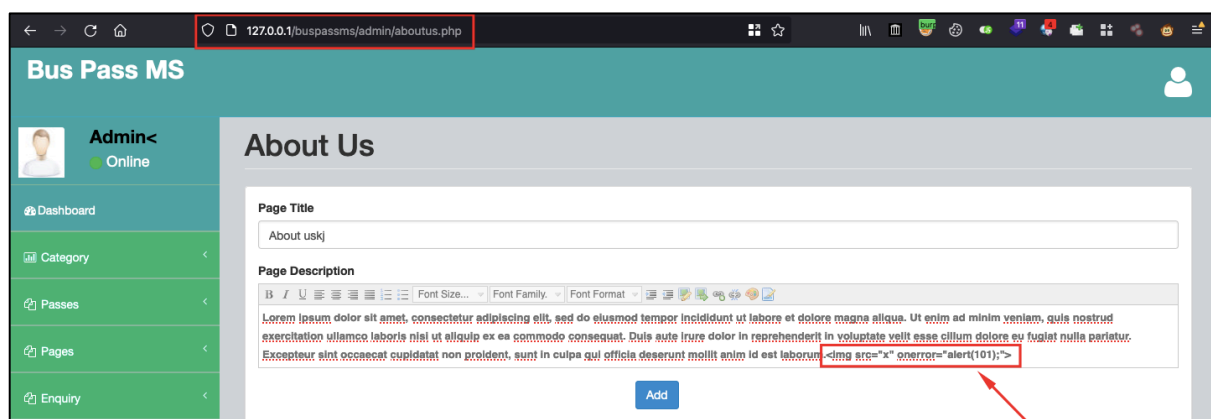
User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including `<` `>` `"` `'` and `=`, should be replaced with the corresponding HTML entities (`&lt;` `&gt;` etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax.

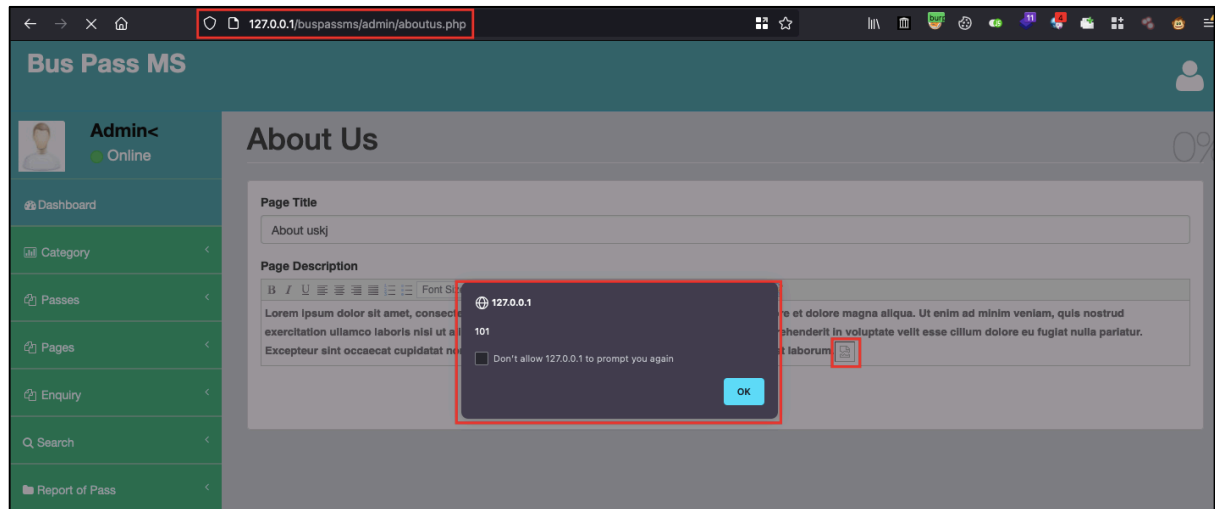
### Proof of Concepts

**Step-1:** Open the URL “<http://127.0.0.1/buspassms/admin/aboutus.php>” and enter the payload as shown below:

**Payload:** ``



**Step-2:** Save the page by clicking on “Add”, you will see that the payload is saved successfully as shown below:



**Step-3:** Open the public URL: “<http://127.0.0.1/buspassms/about.php>” and you will see here that payload is getting executed successfully:

