Client side cross-site scripting

Name: Client side cross-site scripting

Description: Writing user input directly to the DOM allows for a cross-site scripting vulnerability.

ID: js/xss

Kind: path-problem

Severity: error

Precision: high

Directly writing user input (for example, a URL query parameter) to a webpage without properly sanitizing the input first, allows for a cross-site scripting vulnerability.

This kind of vulnerability is also called *DOM-based* cross-site scripting, to distinguish it from other types of cross-site scripting.

Recommendation

To guard against cross-site scripting, consider using contextual output encoding/escaping before writing user input to the page, or one of the other solutions that are mentioned in the references.

Example

The following example shows part of the page URL being written directly to the document, leaving the website vulnerable to cross-site scripting.

```
1 function setLanguageOptions() {
2     var href = document.location.href,
3         deflt = href.substring(href.indexOf("default=")+8);
4     document.write("<OPTION value=1>"+deflt+"</OPTION>");
5     document.write("<OPTION value=2>English</OPTION>");
6 }
```

References

- OWASP: DOM based XSS Prevention Cheat Sheet.
- OWASP: XSS (Cross Site Scripting) Prevention Cheat Sheet.
- OWASP DOM Based XSS.
- OWASP Types of Cross-Site Scripting.
- Wikipedia: Cross-site scripting.
- Common Weakness Enumeration: CWE-79.
- Common Weakness Enumeration: CWE-116.