

#PEN20250002: XSS in Test Shop (Fixed)

Asset	CWE	Status	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vector
Test Shop	CWE-79	Fixed	High (7.1)	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N

Description

A *Cross-Site Scripting* vulnerability has been identified.

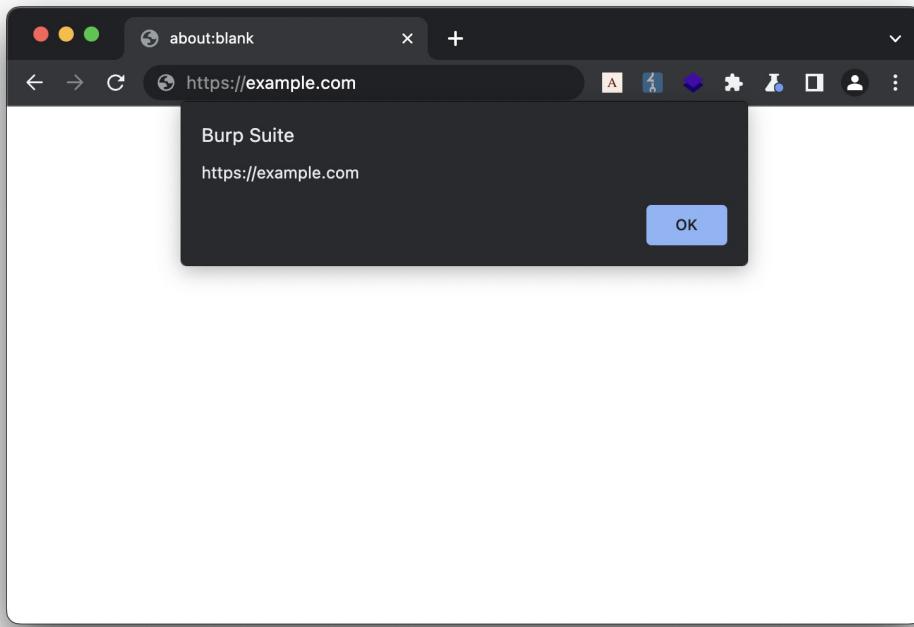
This type of vulnerability arises, if an application uses user-controlled inputs to generate dynamic outputs in an insecure manner.

Exemplary Payload:

```
<s>test</s>
```

JavaScript:

```
3      [...]
4      function demo() {
5          alert(1);
6      }
```



Recommendation

It is recommended to consider all input to the application as potentially dangerous. If user-controlled contents are embedded within the application, they need to be encoded and/or filtered in a *context aware* manner. If the contents are for instance reflected within the JavaScript Context, a different encoding and sanitization needs to be performed than for the HTML context. Further guidance can be found within OWASP's [Cross Site Scripting Prevention Cheat Sheet](#).

References

- [OWASP: Cross-Site Scripting \(XSS\)](#)

