**Cross-Site Scripting (Reflected XSS) Vulnerability in blackcatcms\_v1.3\_**

Hi,

I found a Cross-site Scripting vulnerability(Reflected XSS) in blackcatcms\_v1.3\_

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

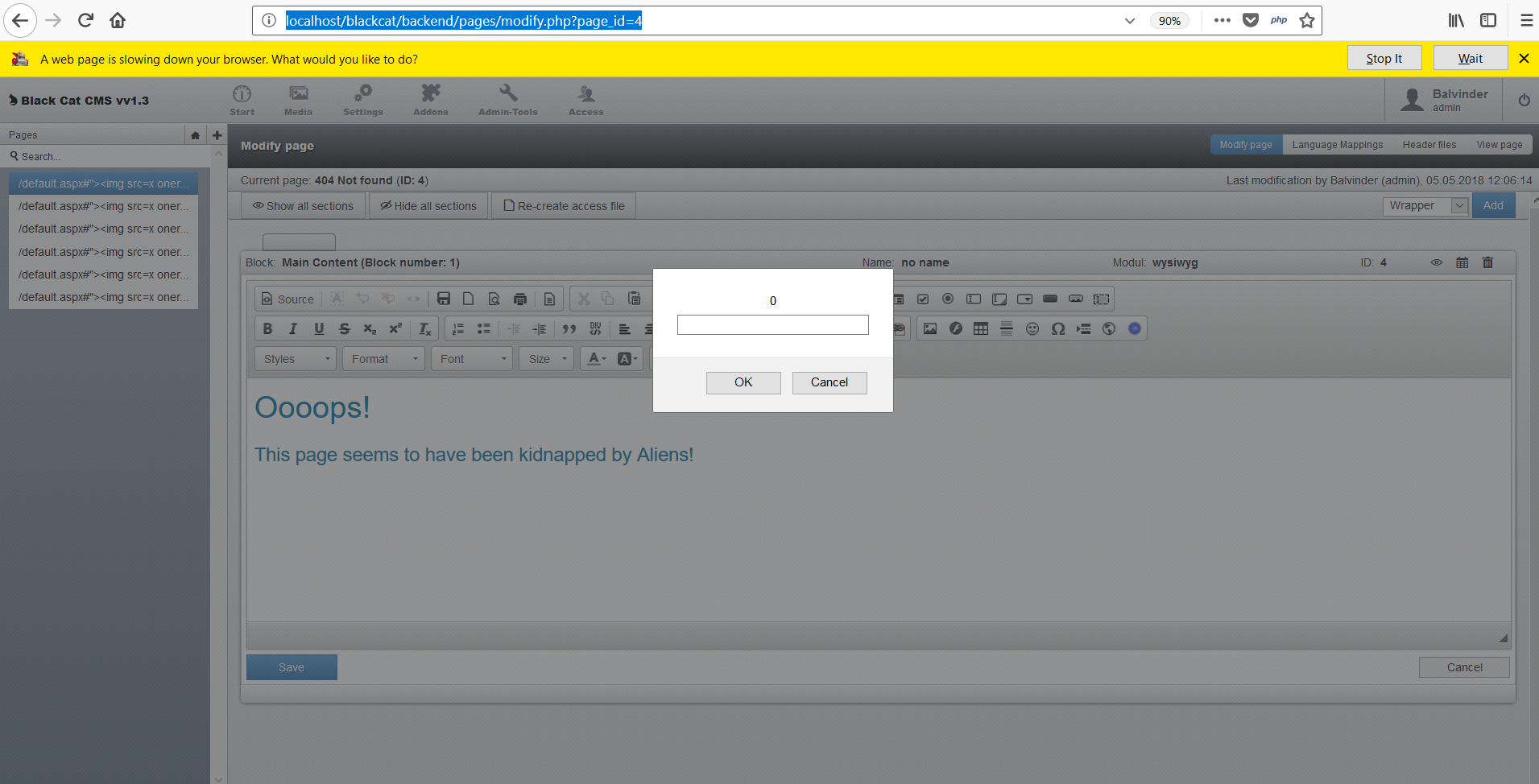
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Reflected XSS Attacks  
Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other web site. When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user’s browser. The browser then executes the code because it came from a "trusted" server. Reflected XSS is also sometimes referred to as Non-Persistent or Type-II XSS.

Vulnerability Name: Cross-Site Scripting (Reflected XSS)  
Vulnerable URL: <http://localhost/blackcat/backend/pages/modify.php?page_id=4>

Steps to Reproduce:  
Step - 1: Logged In as a Admin Role  
Step - 2: On Search panel with /default.aspx#"><img src=x onerror=prompt('0');>  
Step - 3: It will store the search content as javascript code and it will execute cross-site scripting.

Vulnerable field is search panel.



Additional information

->blackcatcms\_v1.3\_  
->DB type and version: MySQL - 10.1.9-MariaDB  
->HTTP server type and version: PHP/5.6.15