New issue

Jump to bottom

Reflected XSS attack with navigate-quickse parameter and affect many modules in NavigateCMS 2.9 #24

Closed **hydrasky-team** opened this issue on Jun 22, 2021 · 1 comment

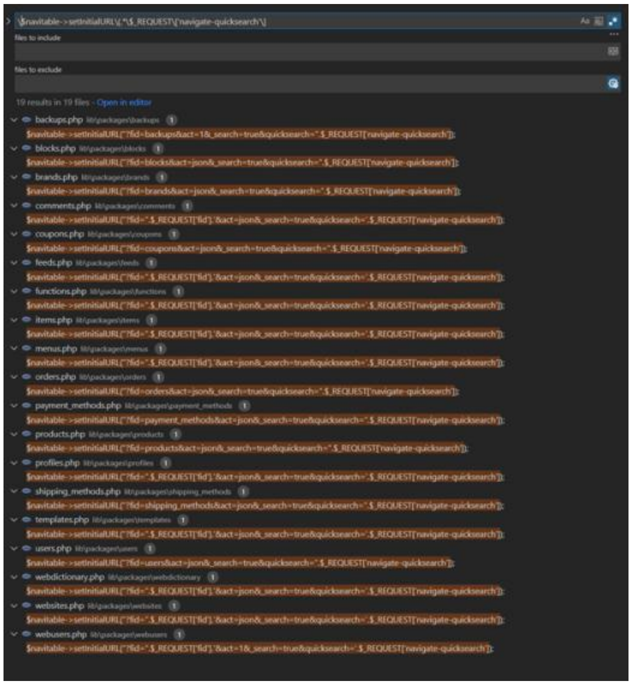
hydrasky-team commented on Jun 22, 2021

EXPECTED BEHAVIOUR
An authenticated malicious user can take advantage of a Reflected XSS vulnerability with navigate-quickse parameter in URL and affect many modules.

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.

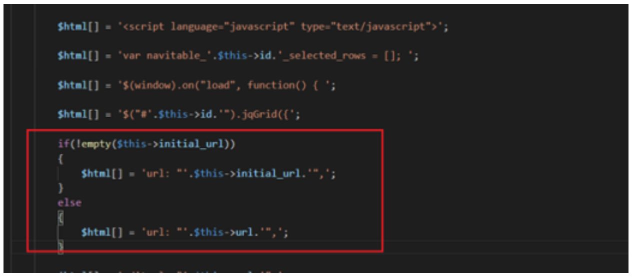
VULNERABILITY CODE
I found the vulnerability code in many files. Because **initial_url** is built in these files.

> lib\packages\backups\backups.php
> lib\packages\blocks\blocks.php
> lib\packages\brands\brands.php
> lib\packages\comments\comments.php
> lib\packages\coupons\coupons.php
> lib\packages\feeds\feeds.php
> lib\packages\functions\functions.php
> lib\packages\items\items.php
> lib\packages\menus\menus.php
> lib\packages\orders\orders.php
> lib\packages\payment_methods\payment_methods.php
> lib\packages\products\products.php
> lib\packages\profiles\profiles.php
> lib\packages\shipping_methods\shipping_methods.php
> lib\packages\templates\templates.php
> lib\packages\users\users.php
> lib\packages\webdictionary\webdictionary.php
> lib\packages\websites\websites.php
> lib\packages\webusers\webusers.php



```
\$navitable->setInitialURL\(.*\$_REQUEST\['navigate-quicksearch'\]
files to include
files to exclude
19 results in 19 files - Open in editor
backups.php lib\packages\backups 1
$navitable->setInitialURL("?fid=backups&act=1&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
blocks.php lib\packages\blocks 1
$navitable->setInitialURL("?fid=blocks&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
brands.php lib\packages\brands 1
$navitable->setInitialURL("?fid=brands&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
comments.php lib\packages\comments 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
coupons.php lib\packages\coupons 1
$navitable->setInitialURL("?fid=coupons&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
feeds.php lib\packages\feeds 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
functions.php lib\packages\functions 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
items.php lib\packages\items 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
menus.php lib\packages\menus 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
orders.php lib\packages\orders 1
$navitable->setInitialURL("?fid=orders&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
payment_methods.php lib\packages\payment_methods 1
$navitable->setInitialURL("?fid=payment_methods&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
products.php lib\packages\products 1
$navitable->setInitialURL("?fid=products&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
profiles.php lib\packages\profiles 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
shipping_methods.php lib\packages\shipping_methods 1
$navitable->setInitialURL("?fid=shipping_methods&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
templates.php lib\packages\templates 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
users.php lib\packages\users 1
$navitable->setInitialURL("?fid=users&act=json&_search=true&quicksearch=".$_REQUEST['navigate-quicksearch']);
webdictionary.php lib\packages\webdictionary 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
websites.php lib\packages\websites 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=json&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
webusers.php lib\packages\webusers 1
$navitable->setInitialURL("?fid=".$_REQUEST['fid'].'&act=1&_search=true&quicksearch='.$_REQUEST['navigate-quicksearch']);
```

After that **initial_url** is used in **\lib\layout\navitable.class.php** file to build HTML.

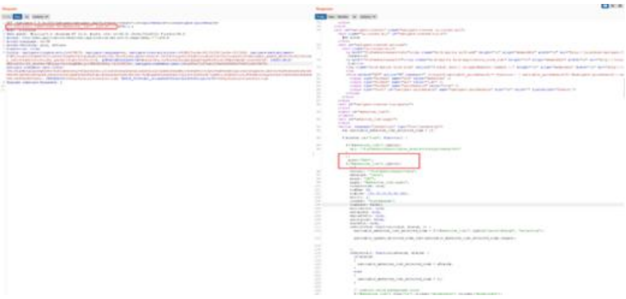


```
$html[] = '<script language="javascript" type="text/javascript">';

$html[] = 'var navitable_'.$this->id.'_selected_rows = []; ';

$html[] = '$(window).on("load", function() { ';

$html[] = '$("#'.$this->id.'").jqGrid({';

if(!empty($this->initial_url))
{
    $html[] = 'url: "'.$this->initial_url.'",';
}
else
{
    $html[] = 'url: "'.$this->url.'",';
}
```

STEPS TO REPRODUCE

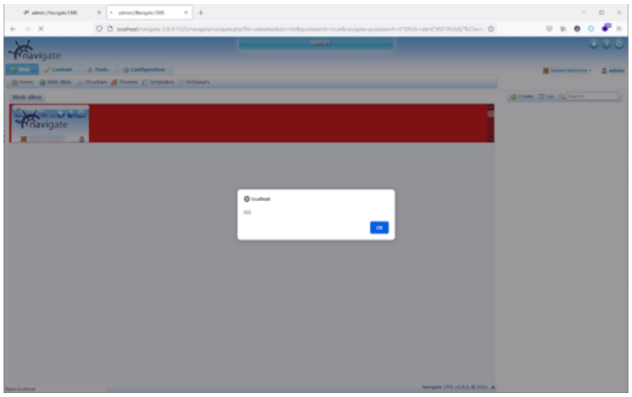
1. We change the request and send the link to user

```
GET /navigate-2.9.3r1525/navigate/navigate.php?fid=websites&act=list&quicksearch=true&navigate-quicksearch=0"})%3b+alert("XSS")%3b$("%23websites_list").jqGrid({//
```



2. People who already login and click to the link above.

3. When loading the page then the Reflected XSS is executed.



NavigateCMS commented on Jun 26, 2021 Owner

Fixed by `466e1f8`

Thank you for all **@hydrasky-team**

NavigateCMS closed this as completed on Jun 26, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants