#2968 Stored Cross-Site Scripting.

URL / Location of vulnerability

/nukeviet/admin/index.php?language=en&nv=menu&op=rows&mid=1

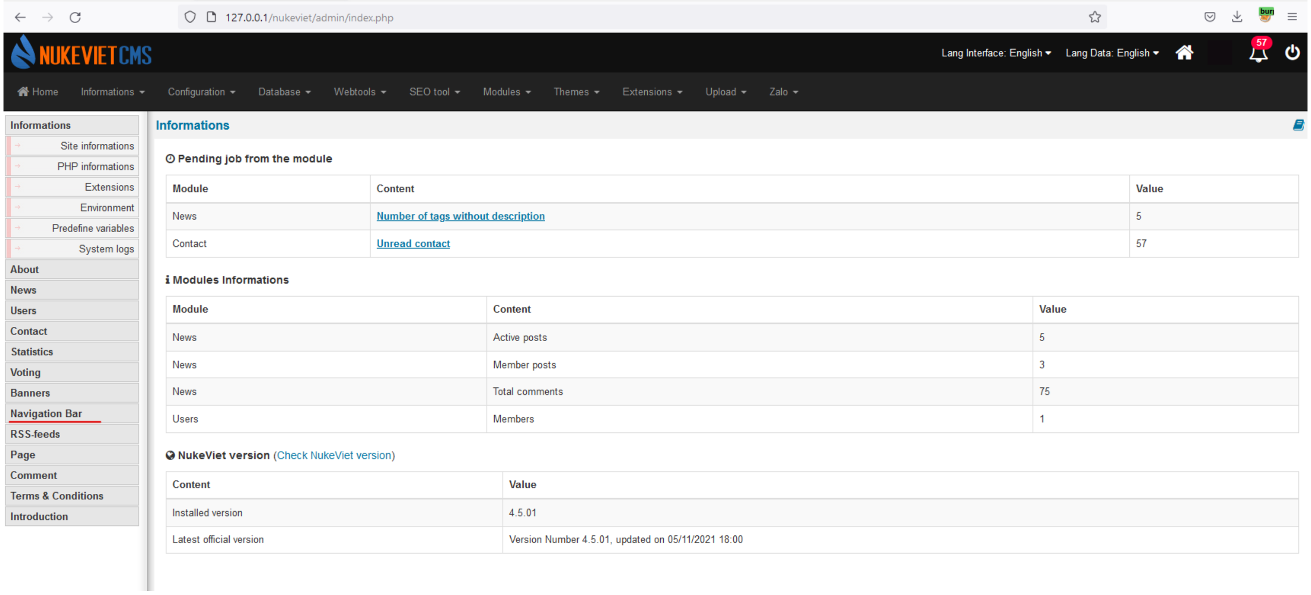
Description

Hi Nukeviet Team.

I managed to exploit Stored XSS in Nukeviet CMS. Vulnerability is being exploited from the privilaged user account. Vulnerability suffers from imporer input encoding and sanitization of the Link Parameter.

Steps to reproduce

1. Navigate to Admin Panel which is located at /nukeviet/admin/index.php
2. Next navigate to Navigation Bar option:



Informations

Pending job from the module

Module	Content	Value
News	Number of tags without description	5
Contact	Unread contact	57

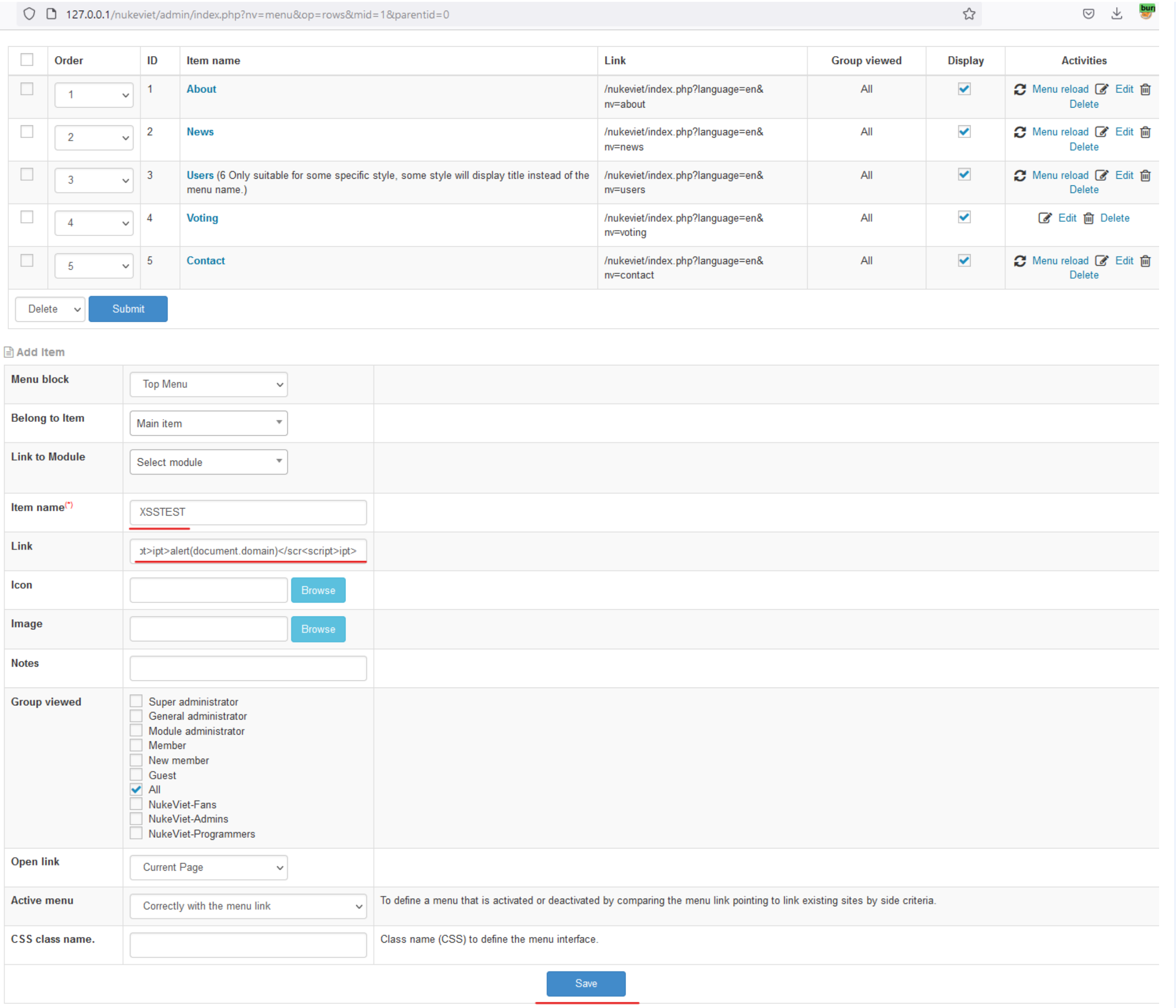
Modules Informations

Module	Content	Value
News	Active posts	5
News	Member posts	3
News	Total comments	75
Users	Members	1

NukeViet version (Check NukeViet version)

Content	Value
Installed version	4.5.01
Latest official version	Version Number 4.5.01, updated on 05/11/2021 18:00

3. Navigate to "Top Menu" (location: /admin/index.php?language=en&nv=menu&op=rows&mid=1)
4. Add item with following values and click Save:
   Item Name: XSSTEST
   Link: "> <scr<script>ipt>alert(document.domain)</scr<script>ipt>



127.0.0.1/nukeviet/admin/index.php?nv=menu&op=rows&mid=1&parentid=0

□	Order	ID	Item name	Link	Group viewed	Display	Activities
□	1	1	About	/nukeviet/index.php?language=en&nv=about	All	☑	Menu reload Edit Delete
□	2	2	News	/nukeviet/index.php?language=en&nv=news	All	☑	Menu reload Edit Delete
□	3	3	Users (6 Only suitable for some specific style, some style will display title instead of the menu name.)	/nukeviet/index.php?language=en&nv=users	All	☑	Menu reload Edit Delete
□	4	4	Voting	/nukeviet/index.php?language=en&nv=voting	All	☑	Edit Delete
□	5	5	Contact	/nukeviet/index.php?language=en&nv=contact	All	☑	Menu reload Edit Delete

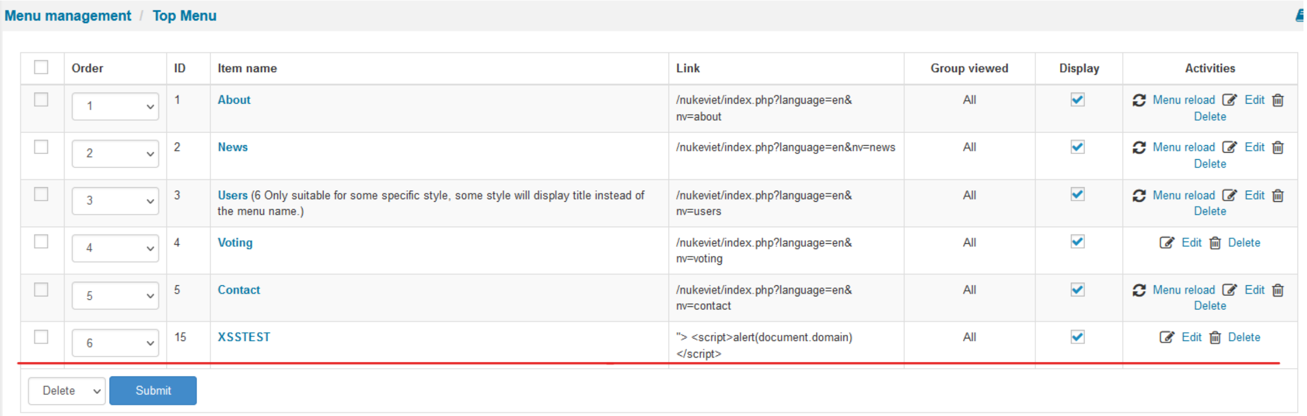
Delete Submit

Add Item

Menu block	Top Menu	
Belong to Item	Main item	
Link to Module	Select module	
Item name(*)	XSSTEST	
Link	›t>ipt>alert(document.domain)</scr<script>ipt>	
Icon	Browse	
Image	Browse	
Notes		
Group viewed	□ Super administrator □ General administrator □ Module administrator □ Member □ New member □ Guest ☑ All □ NukeViet-Fans □ NukeViet-Admins □ NukeViet-Programmers	
Open link	Current Page	
Active menu	Correctly with the menu link	To define a menu that is activated or deactivated by comparing the menu link pointing to link existing sites by side criteria.
CSS class name.		Class name (CSS) to define the menu interface.

Save

5. Item should be saved as follows:

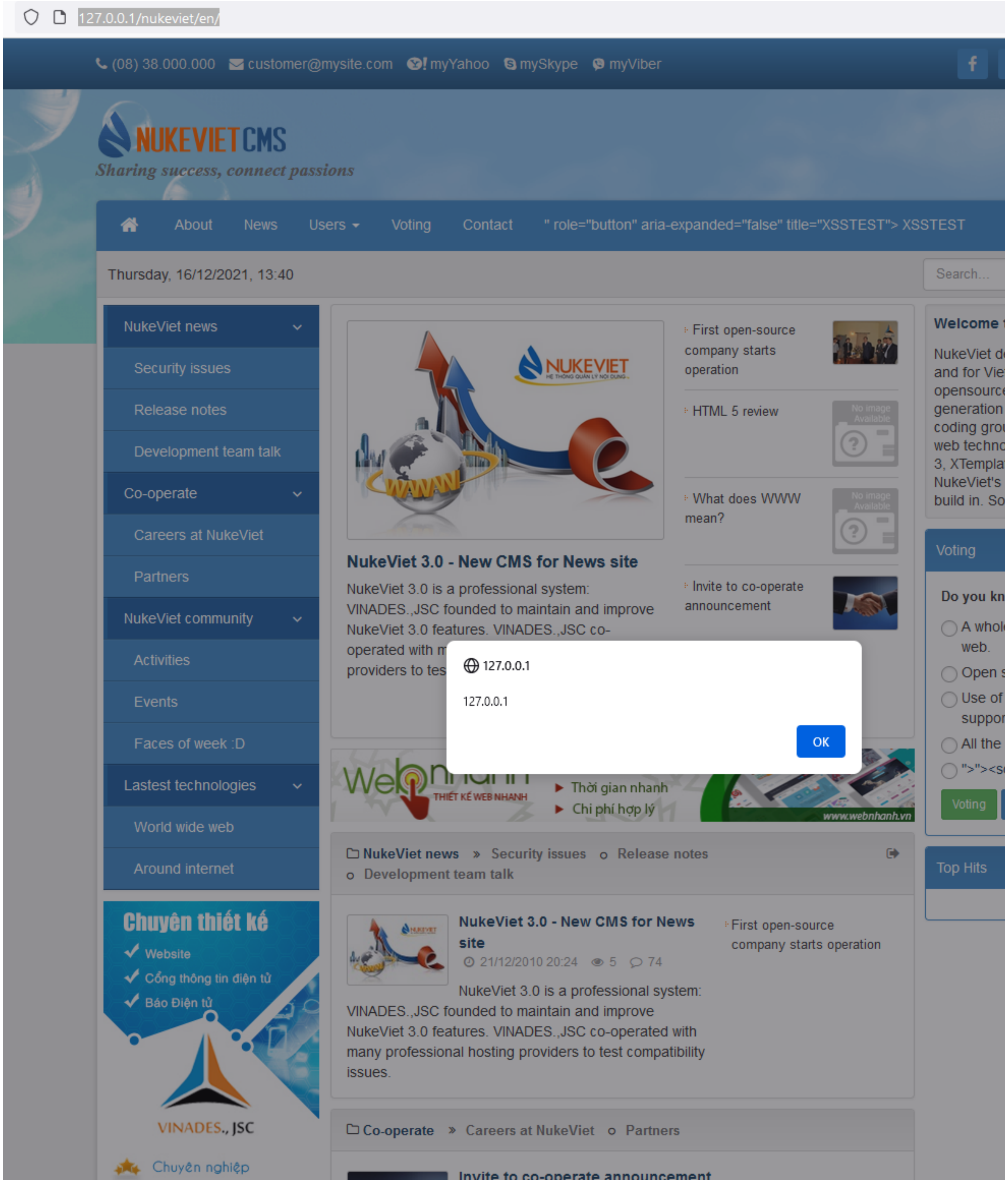


Menu management / Top Menu

□	Order	ID	Item name	Link	Group viewed	Display	Activities
□	1	1	About	/nukeviet/index.php?language=en&nv=about	All	☑	Menu reload Edit Delete
□	2	2	News	/nukeviet/index.php?language=en&nv=news	All	☑	Menu reload Edit Delete
□	3	3	Users (6 Only suitable for some specific style, some style will display title instead of the menu name.)	/nukeviet/index.php?language=en&nv=users	All	☑	Menu reload Edit Delete
□	4	4	Voting	/nukeviet/index.php?language=en&nv=voting	All	☑	Edit Delete
□	5	5	Contact	/nukeviet/index.php?language=en&nv=contact	All	☑	Menu reload Edit Delete
□	6	15	XSSTEST	"> <script>alert(document.domain)</script>	All	☑	Edit Delete

Delete Submit

6. Next visit the website as a regular non-privilaged user or an admin user. XSS Alert should appear.

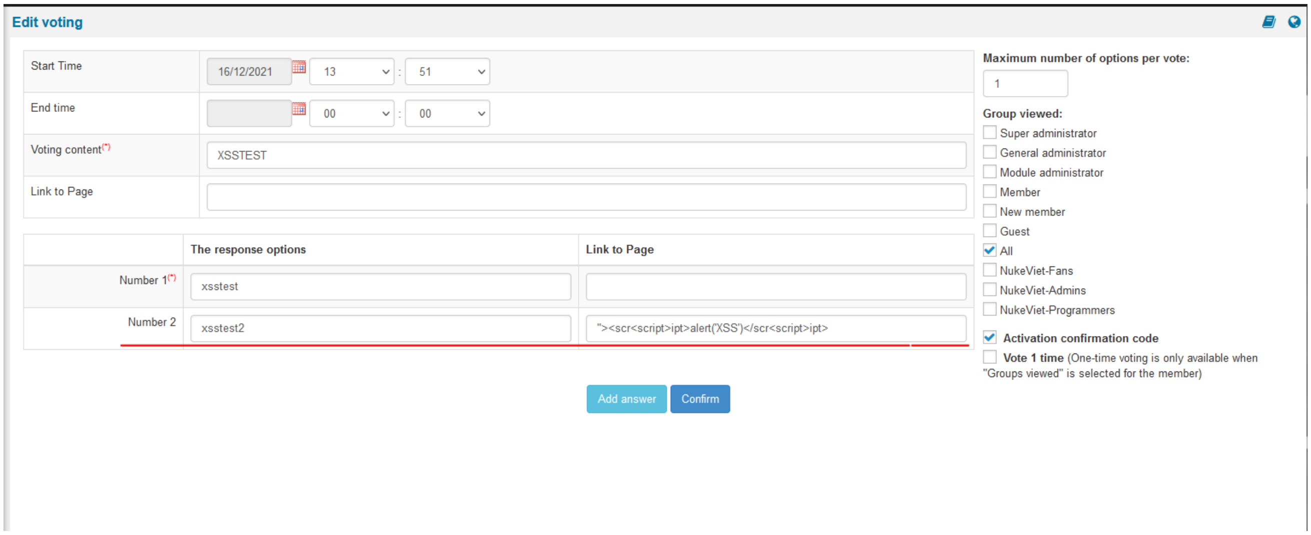


127.0.0.1

127.0.0.1

There are many affected input fields of the same issue in your CMS for example :

1. "Voting Option" (/nukeviet/admin/index.php?language=en&nv=voting) -> "Link to Page" * Modify second option from the list as it is not checking whether input is a URL or not:



Edit voting

Start Time	16/12/2021 13 : 51
End time	00 : 00
Voting content(*)	XSSTEST
Link to Page	

	The response options	Link to Page
Number 1(*)	xsstest	
Number 2	xsstest2	"><scr<script>ipt>alert('XSS')</scr<script>ipt>

Maximum number of options per vote: 1

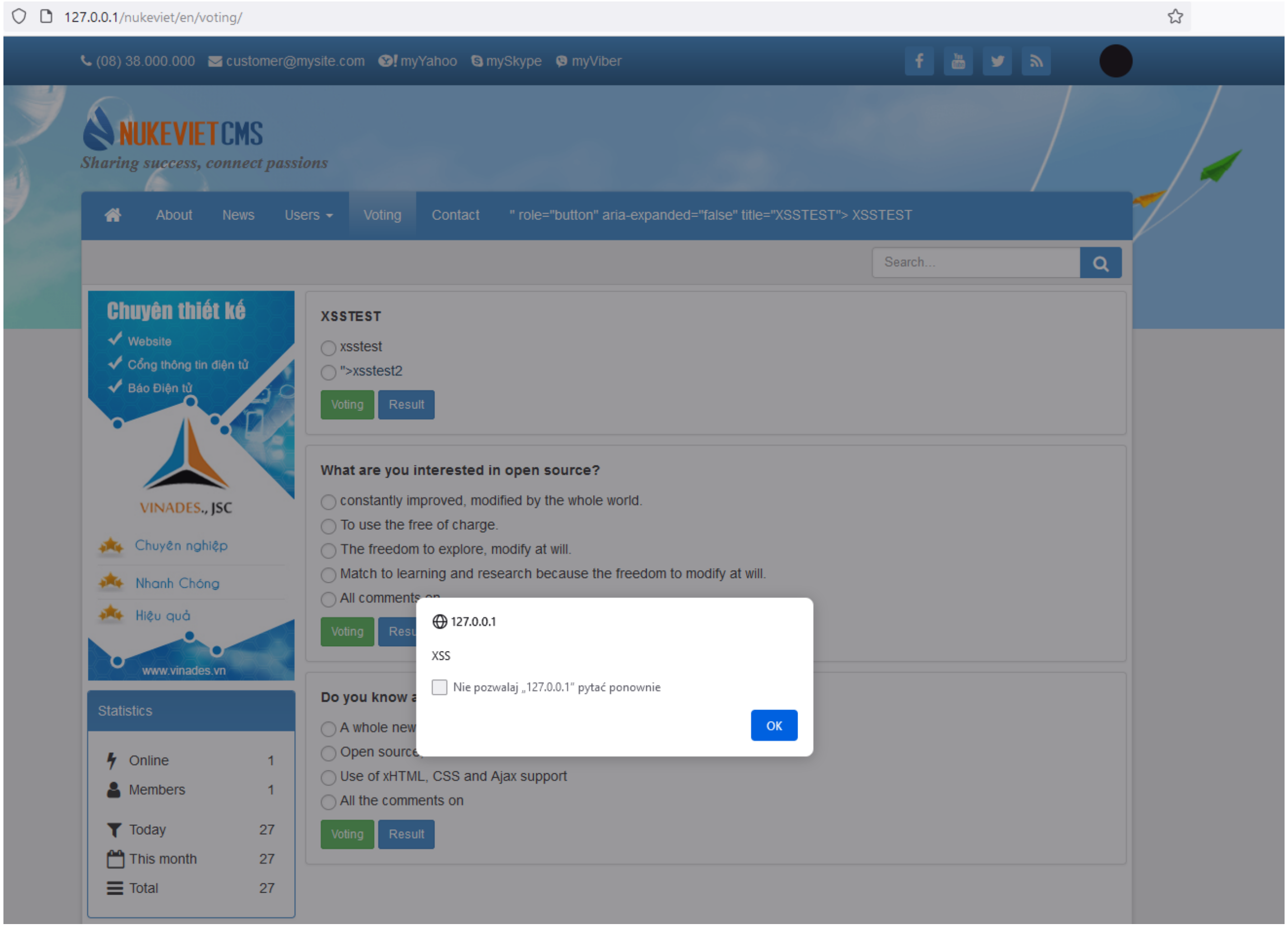
Group viewed:

- □ Super administrator
- □ General administrator
- □ Module administrator
- □ Member
- □ New member
- □ Guest
- ☑ All
- □ NukeViet-Fans
- □ NukeViet-Admins
- □ NukeViet-Programmers

☑ **Activation confirmation code**

□ **Vote 1 time** (One-time voting is only available when "Groups viewed" is selected for the member)

Visit voting page(/nukeviet/en/voting/) as a regular or admin user - XSS alert should appear:



127.0.0.1/nukeviet/en/voting/

XSSTEST

○ xsstest

○ ">xsstest2

Voting Result

What are you interested in open source?

○ constantly improved, modified by the whole world.

○ To use the free of charge.

○ The freedom to explore, modify at will.

○ Match to learning and research because the freedom to modify at will.

○ All comments on

Do you know a

○ A whole new

○ Open source

○ Use of xHTML, CSS and Ajax support

○ All the comments on

Voting Result

127.0.0.1

XSS

□ Nie pozwalaj „127.0.0.1" pytać ponownie

OK

Statistics

Online	1
Members	1
Today	27
This month	27
Total	27

Impact

It is reasonable to fix the issue as the vulnerability would allow privilaged user who exploit the vulnerability to steal other user's or admin's session cookies which lead to account takeover and manipulating the voting results.

Recommendation

Encode and sanitize all parameters input fields.

OWASP Cross Site Scripting Prevention Cheat Sheet:

`https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html`

Attachments

- POC-29681
- POC-29682
- POC-29683
- POC-29684
- POC-29685
- POC-29686
- POC-29687

Dawid Bakaj created a report

a year ago

NukeViet changed the status to `Unresolved`

a year ago

NukeViet changed the severity to `HIGH`

a year ago

NukeViet added a comment

a year ago

Thank you very much, we have noted and will resolve it as soon as possible

NukeViet changed the severity to `MEDIUM`

a year ago

Dawid Bakaj added a comment

a year ago

Hello,

Is the vulnerability fully fixed ?

NukeViet added a comment

a year ago

We fixed it at this commit https://github.com/nukeviet/nukeviet/commit/5eb43adda8434d7671899d5c634d3b75b5179a74, please check again.
The official updates will be in the upcoming release.
Thanks Dawid Bakaj

Dawid Bakaj added a comment

a year ago

Hello NukeViet Team,

I found a bypass for a fix.
try this payload:

"> <iframe src=javascript:alert(document.domain) <

In order to fix the vulnerability properly i suggest not using the Regex. You can implement allow list of tags and attributes or just use DOMPurify library instead: https://github.com/cure53/DOMPurify (Remember to update the dependicies regularly.

Kind regards,

Dawid Bakaj

NukeViet added a comment

a year ago

Thank you very much, we will check again

Dawid Bakaj added a comment

10 months ago

Hi, any updates about the issue?

Dawid Bakaj added a comment

10 months ago

Hi, any updates?

NukeViet added a comment

9 months ago

We have solved this problem, the latest code is here https://github.com/nukeviet/nukeviet/tree/nukeviet4.6 please check again

Dawid Bakaj added a comment

9 months ago

Hi Nukeviet team.

Vulnerability has not been fixed. Try following payload:
javascript:alert(document.domain)

Afterwards go to the home page and click on the modified tab, JavaScript will execute and alert box should appear.

NukeViet added a comment

8 months ago

Dear Dawid Bakaj

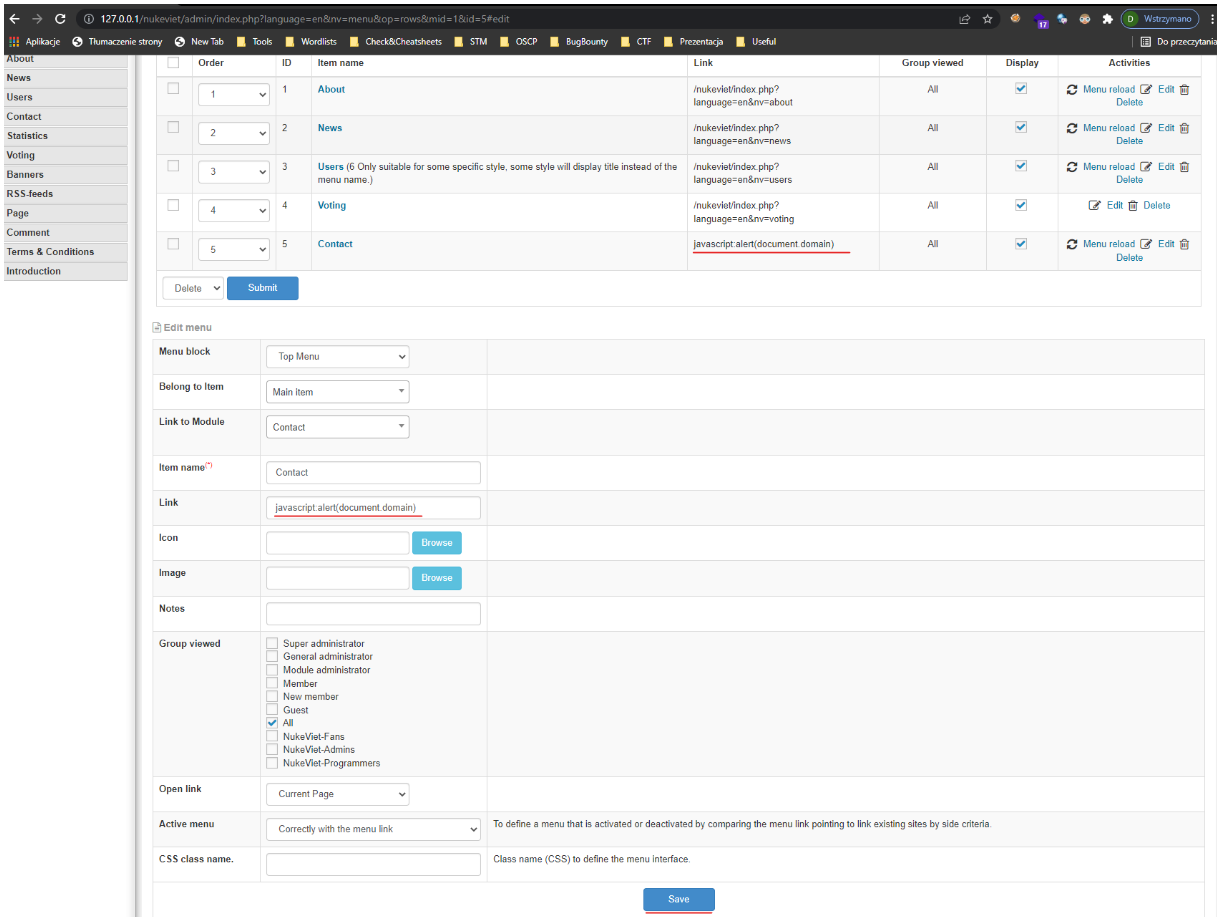
We fixed it here https://github.com/nukeviet/nukeviet/commit/c8f895aa40d2c4f9b8fe64126b0c5ee240fd5633
Please check again.
Thank you

Dawid Bakaj added a comment

8 months ago

The vulnerability still exists. To reproduce inject the same payload:

javascript:alert(document.domain)



127.0.0.1/nukeviet/admin/index.php?language=en&nv=menu&op=rows&mid=1&id=5#edit

□	Order	ID	Item name	Link	Group viewed	Display	Activities
□	1	1	About	/nukeviet/index.php?language=en&nv=about	All	☑	Menu reload Edit Delete
□	2	2	News	/nukeviet/index.php?language=en&nv=news	All	☑	Menu reload Edit Delete
□	3	3	Users (6 Only suitable for some specific style, some style will display title instead of the menu name.)	/nukeviet/index.php?language=en&nv=users	All	☑	Menu reload Edit Delete
□	4	4	Voting	/nukeviet/index.php?language=en&nv=voting	All	☑	Edit Delete
□	5	5	Contact	javascript:alert(document.domain)	All	☑	Menu reload Edit Delete

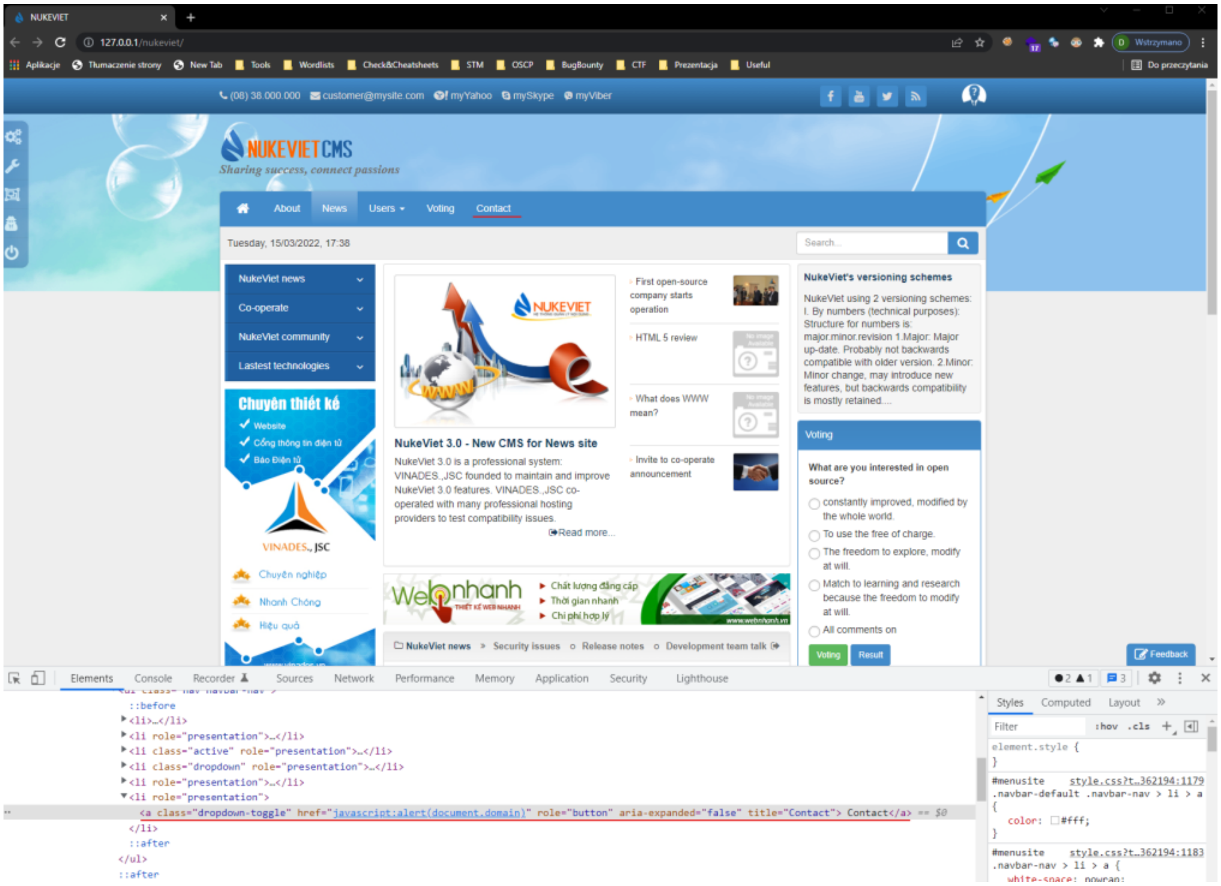
Delete Submit

Edit menu

Menu block	Top Menu	
Belong to Item	Main item	
Link to Module	Contact	
Item name(*)	Contact	
Link	javascript:alert(document.domain)	
Icon	Browse	
Image	Browse	
Notes		
Group viewed	□ Super administrator □ General administrator □ Module administrator □ Member □ New member □ Guest ☑ All □ NukeViet-Fans □ NukeViet-Admins □ NukeViet-Programmers	
Open link	Current Page	
Active menu	Correctly with the menu link	To define a menu that is activated or deactivated by comparing the menu link pointing to link existing sites by side criteria.
CSS class name.		Class name (CSS) to define the menu interface.

Save

Payload succesfully injected into the fred attribute:



127.0.0.1/nukeviet/

Tuesday, 15/03/2022, 17:38

NukeViet 3.0 - New CMS for News site

NukeViet 3.0 is a professional system: VINADES.,JSC founded to maintain and improve NukeViet 3.0 features. VINADES.,JSC co-operated with many professional hosting providers to test compatibility issues.

Read more...

First open-source company starts operation

HTML 5 review

What does WWW mean?

Invite to co-operate announcement

NukeViet's versioning schemes

NukeViet using 2 versioning schemes: I. By numbers (technical purposes): Structure for numbers is: major.minor.revision 1.Major: Major up-date. Probably not backwards compatible with older version. 2.Minor: Minor change, may introduce new features, but backwards compatibility is mostly retained....

Voting

What are you interested in open source?

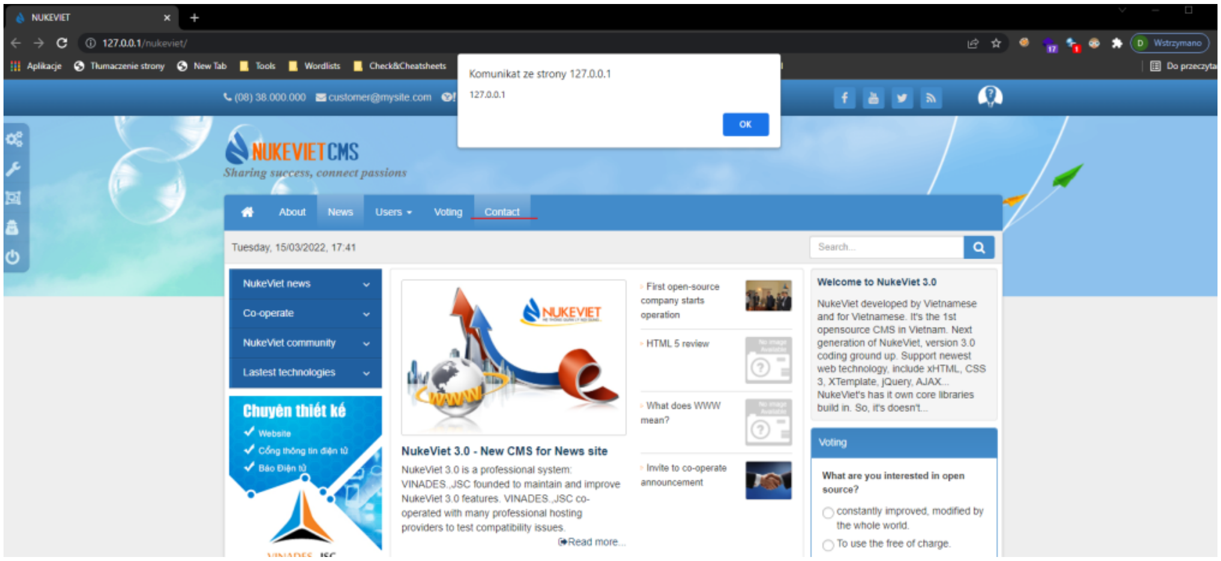
○ constantly improved, modified by the whole world.
○ To use the free of charge.
○ The freedom to explore, modify at will.
○ Match to learning and research because the freedom to modify at will.
○ All comments on

Voting Result

```
      ::before
    ▸<li>…</li>
    ▸<li role="presentation">…</li>
    ▸<li class="active" role="presentation">…</li>
    ▸<li class="dropdown" role="presentation">…</li>
    ▸<li role="presentation">…</li>
    ▾<li role="presentation">
        <a class="dropdown-toggle" href="javascript:alert(document.domain)" role="button" aria-expanded="false" title="Contact"> Contact</a> == $0
      </li>
      ::after
    </ul>
    ::after
```

```
element.style {
}
#menusite .navbar-default .navbar-nav > li > a      style.css?t…362194:1179
{
  color: #fff;
}
#menusite .navbar-nav > li > a {                    style.css?t…362194:1183
  white-space: nowrap;
```

Click the Contact button to execute XSS:



Komunikat ze strony 127.0.0.1

127.0.0.1

OK

Tuesday, 15/03/2022, 17:41

NukeViet 3.0 - New CMS for News site

NukeViet 3.0 is a professional system: VINADES.,JSC founded to maintain and improve NukeViet 3.0 features. VINADES.,JSC co-operated with many professional hosting providers to test compatibility issues.

Read more...

First open-source company starts operation

HTML 5 review

What does WWW mean?

Invite to co-operate announcement

Welcome to NukeViet 3.0

NukeViet developed by Vietnamese and for Vietnamese. It's the 1st opensource CMS in Vietnam. Next generation of NukeViet, version 3.0 coding ground up. Support newest web technology, include xHTML, CSS 3, XTemplate, jQuery, AJAX... NukeViet's has it own core libraries build in. So, it's doesn't...

Voting

What are you interested in open source?

○ constantly improved, modified by the whole world.

○ To use the free of charge.

POC-29688

POC-29689

POC-296810

Dawid Bakaj added a comment

8 months ago

Payload succesfully injected into the href attribute* ^

Dawid Bakaj added a comment

8 months ago

UPDATE: Vulnerability has been fixed properly. I used wrong commit. Please ignore last comment.

Dawid Bakaj requested to disclose this report

8 months ago

May I ask for full disclosure and the CVE for this finding ?

NukeViet added a comment

8 months ago

Yes Dawid Bakaj, you can. We will announce when new version is released.

Dawid Bakaj added a comment

8 months ago

Hi Nukeviet.

I found a bypass for the latest fix. To reproduce the vulnerability use this payload:

javascript://%0aalert%28alert%29

NukeViet added a comment

8 months ago

Thank you very much.
We continue to fix that bug here https://github.com/nukeviet/nukeviet/commit/88fca9eab7def176fdf63a5ada1c137827218705 .

Would you mind checking again

Dawid Bakaj added a comment

8 months ago

Vulnerability has been fixed properly.

Dawid Bakaj added a comment

7 months ago

Hello Nukeviet team. May i request a CVE for the vulnerability?

NukeViet added a comment

7 months ago

Hi,

We have no experience with CVE.
Can you tell us what to do to help you? Or you can get your own CVE and we publish it for you?

Dawid Bakaj added a comment

7 months ago

Hi,

I requested for CVE by myself. May I ask for a full disclosure of the vulberability?

Kind regards,
Dawid

NukeViet added a comment

7 months ago

Hi,

This error only occurs for accounts with website administrator rights.
There would be no serious effect if it was announced.
We will include the CVE in the changelog when the new version is released

Dawid Bakaj added a comment

5 months ago

Hi Nukeviet Team

Please use this CVE as a reference to this vulnerability :

CVE-2022-30874.

Let mne know when included to the changlelog.

NukeViet added a comment

5 months ago

Thank you,

We have released two versions of these security patches, NukeViet 4.4.05 and 4.5.02: https://github.com/nukeviet/nukeviet/releases
We have attached the CVE in the changelog here:
https://github.com/nukeviet/nukeviet/blob/nukeviet4.4/CHANGELOG.txt
https://github.com/nukeviet/nukeviet/blob/nukeviet4.5/CHANGELOG.txt

NukeViet changed the status to `Resolved`

5 months ago

NukeViet changed the severity to `HIGH`

5 months ago

Dawid Bakaj added a comment

5 months ago

May i ask to change a nickname "abstrabakus" to my name and surname in the changelog?

Kind regards
Dawid Bakaj

Dawid Bakaj requested to disclose this report

5 months ago

NukeViet added a comment

5 months ago

We have updated.
https://github.com/nukeviet/nukeviet/blob/nukeviet4.4/CHANGELOG.txt
https://github.com/nukeviet/nukeviet/blob/nukeviet4.5/CHANGELOG.txt

Dawid Bakaj added a comment

5 months ago

Hi Nukeviet Team,
Thank you for updating the changelog. One more question, May I public the PoC now, or should I wait a month from now?

NukeViet added a comment

5 months ago

Hi Dawid Bakaj,

This error is mainly in site administration, less likely to have a major impact on all websites using NukeViet.
So you can publish it now. We have also moved this report from private to public.

Thank you

Program
NukeViet

Target
https://github.com/nukeviet/

Visibility
Public - Full

Status
Accepted - Resolved

Vulnerability
Cross-Site Scripting (XSS) > Stored > Privileged User to Privilege Elevation

Severity
HIGH

Reference
#2968

Submitted at
12/16/2021 08:12:58

Submitted by
Dawid Bakaj

Point
3

Votes
1

Public link
https://whitehub.net/submissions/2968