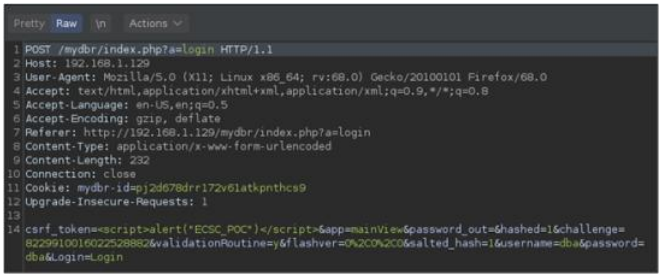
CVE-2020-28149

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.

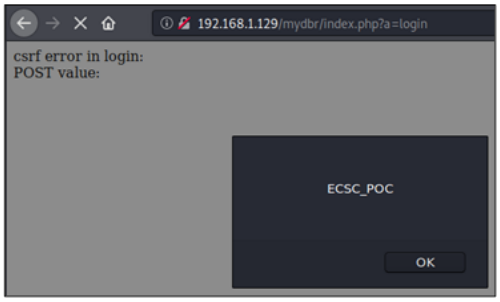
By adding malicious code in the form of the token, the field can be escaped, and additional HTML elements can be added, including arbitrary JavaScript. If the following request is sent to load the login page, the cookie is populated with malicious code.



Unauthenticated request to index.php with injected token.

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

```
csrf error in login: <br>POST value:<script>alert("ECSC_POC")</script><br>Session value:3b8307d568087b37b0a590ef657ef10611863bd926b50e4b82097c075236bdec<br><br>Try deleting the mydbr-id cookie from the browser (if you do not see it, try HTTPS)`
```



Rendered XSS Payload