Axublog 1.1.0 c_login.php存在sql注入漏洞

Axublog是一款PHP个人博客系统。 Axublog（c_login.php）存在SQL注入漏洞。攻击者可利用漏洞，直接进行注入，获取数据库敏感信息。

漏洞分析： 漏洞出现在后台登录验证的部分。 首先看后台登录页面代码、www/ad/login.php

```
<?php
include_once("all.php");
header("Content-type:text/html;charset=utf-8");

@$user=$_POST["user"];
@$psw=$_POST["psw"];
@$loginlong=$_POST["loginlong"];

@$g=$_GET["g"];
    switch ($g)
    {
    case "jsloginpost":jsloginpost();break;
    case "exit":loginexit();break;
    default:index();break;
    }

function index(){
global $codename,$codeversion,$codeurl;
?>
```

首先看 `user` 和 `psw` 参数没经过然后过滤直接是 post 传递过来的值。 继续跟踪登录验证函数，`jsloginpost`。jsloginpost 方法定义在文件 www/ad/c_login.php 第74行。

```
function jsloginpost(){
global $tabhead;
global $txtchk;
@$user=$_POST["user"];
@$psw=$_POST["psw"];$psw = authcode(@$psw, 'ENCODE', 'key',0);
@$loginlong=$_POST["loginlong"];
$chk=sqlguolv();
if($chk==1){
$json_arr = array("jieguo"=>"<div id=redmsg>登录失败：发现非法字符！</div>");
$json_obj = json_encode($json_arr);
echo $json_obj;die();
}
#-------

#setcookie("lggqsj",date('Y-m-d H:i:s',time()+$loginlong), time()+60*60*24,"/;
HttpOnly" , "","');

$tab=$tabhead."adusers";
$chk=" where adnaa='".$user."' and adpss='".$psw."' ";
mysql_select_db($tab);
$sql = mysql_query("select * from ".$tab.$chk);
if(!$sql){$jieguo="<div id=redmsg>(数据库查询失败!)</div>";}else{
    $num=mysql_num_rows($sql);
```

```
                if($num==0){$jieguo='<div id=redmsg>登录失败：账户或密码错误！
</div>';}
                else{
                loginpass($loginlong);
                $chkmoblie=isMobile();
                if($chkmoblie==1){$jieguo='<div id=bluemsg>登录成功！正在前往<a
href="wap.php">后台</a>。。。</div>
<script>setTimeout("javascript:parent.location.href=\'wap.php\'", 1000);
</script>';}else{$jieguo='<div id=bluemsg>登录成功！正在前往<a href="index.php">后台
</a>。。。</div>
<script>setTimeout("javascript:parent.location.href=\'index.php\'", 1000);
</script>';}
                }
}
$json_arr = array("jieguo"=>$jieguo);
$json_obj = json_encode($json_arr);
echo $json_obj;
}
#-------
```

```
?>
```

这里可以看到 user 和 psw 没有任何过滤直接进入了sql查询，导致sql注入，万能密码登录。 漏洞复现： 访问后台登录页面 `http://localhost/ad/login.php` 账号： `admin' and 1=1#` 密码 随意 点击登录，即可显示登录成功。