|  |  |
| --- | --- |
| 序号 | 22 |

桂林电子科技大学2023-2024学年第3学期

**网络渗透测试技术** 实验报告

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 实验七 | | | | | | | |  | 指导意见：  成绩：    指导教师： |
| 姓 名 | 陈霖汕 | | | 学 号 | | 2300360102 | | |
| 专 业 | 网络空间安全 | | | | | | | |
| 实验日期 | 2024 | 年 | 7 | | 月 | | 13 | 日 |
|  |  | | | | | | | |

**一、实验目的**

（1）熟悉渗透测试的执行标准；

（2）掌握渗透测试的常用方法与技巧；

（3）掌握渗透测试报告的撰写步骤及关键要点。

**二、实验任务**

（1）对公开安全网站实施针对性的渗透测试，挖掘漏洞并获取信息；

（2）撰写渗透测试报告。

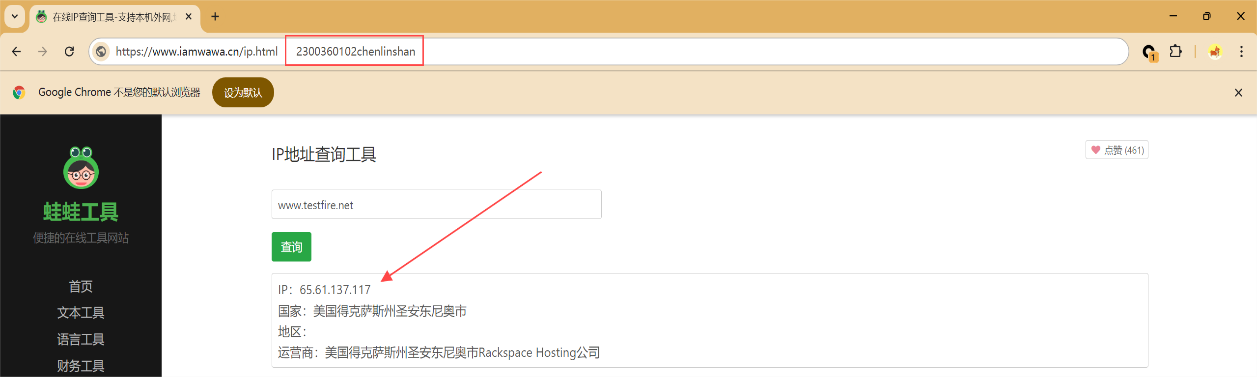
**三、实验环境**

1. 靶机地址：

2、攻击机地址：65.61.137.117

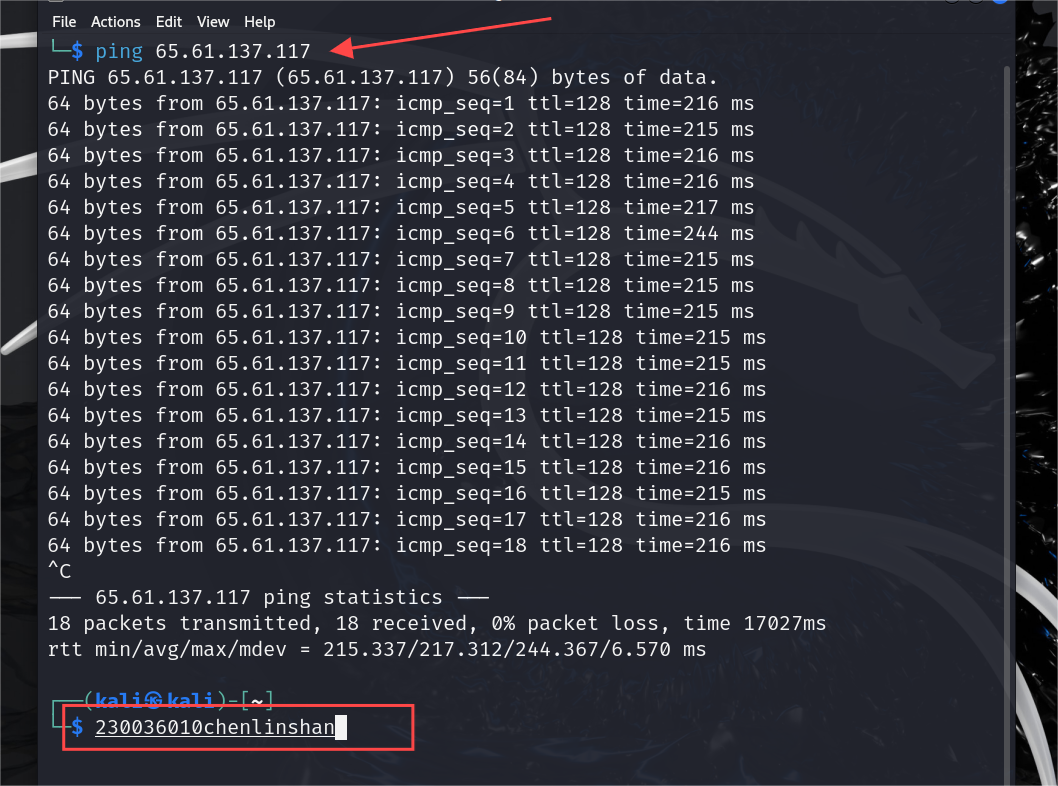
**四、实验过程和实验结果**

1. **先将该网址所在的ip通过工具转化出来。**

****

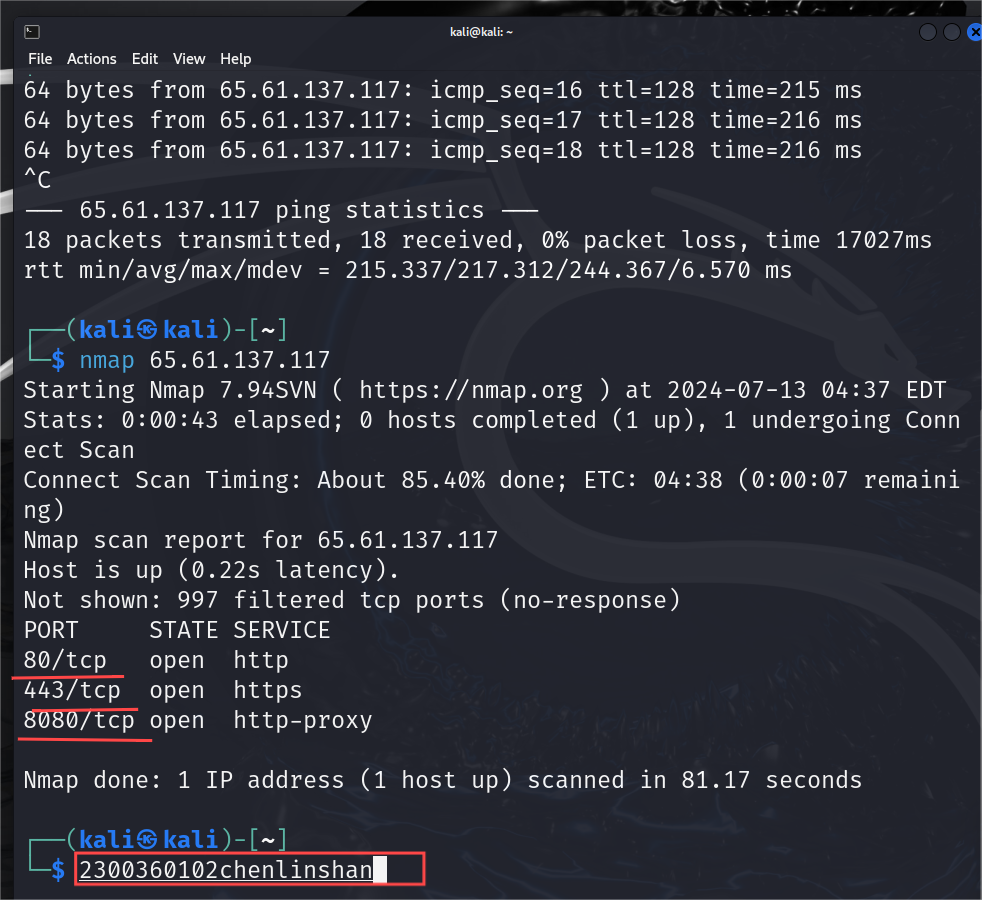
1. **使用ping命令确认该主机是否活动**

其中我们能够知道ttl=128，则大概率操作系统为windows系统。

****

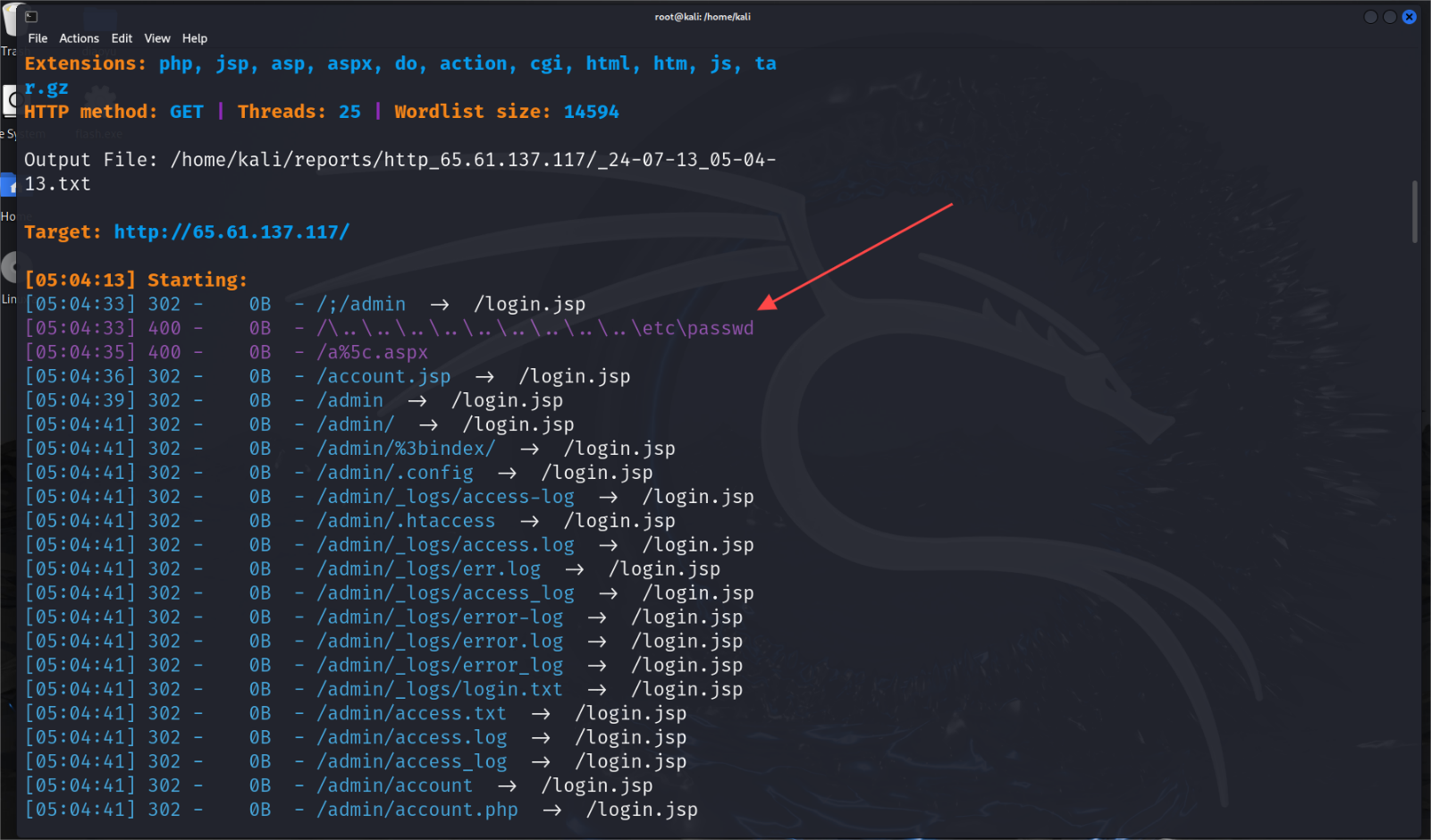
1. **使用nmap扫描**

发现该网站的端口有80、443、8080

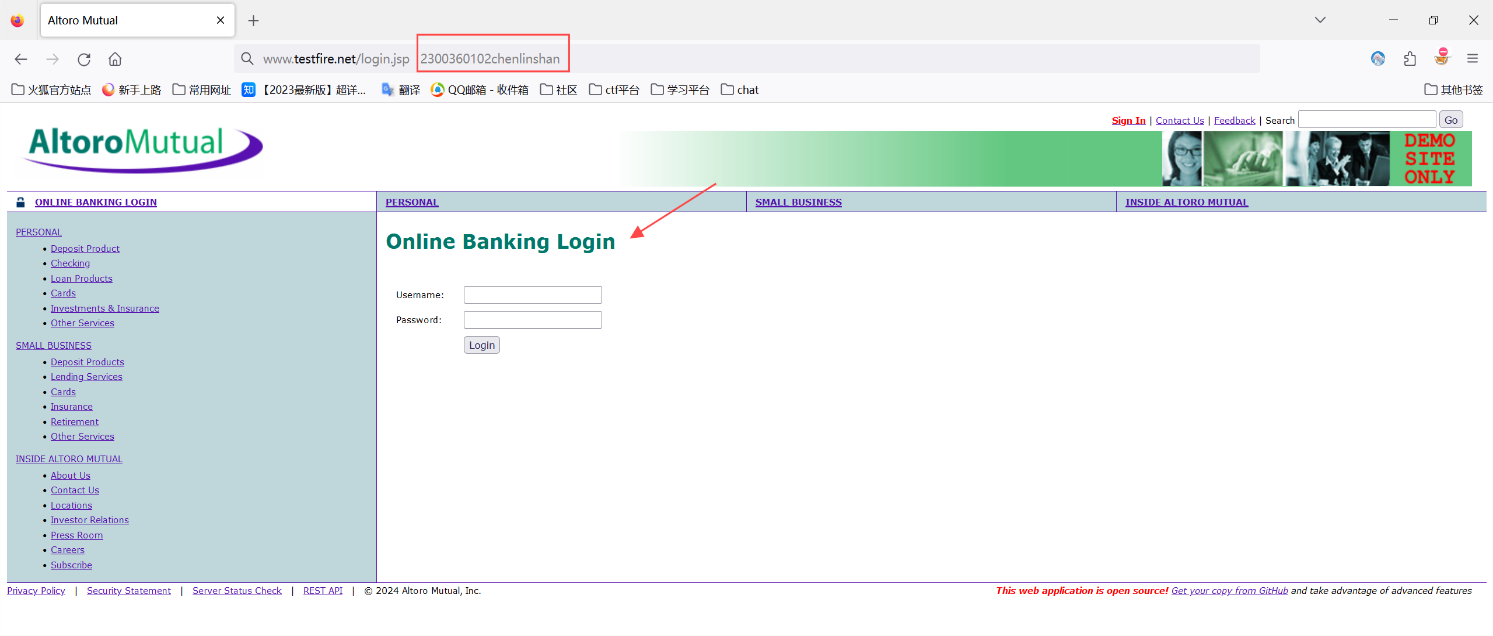
****

1. **使用dirsearch对网站进行扫描**

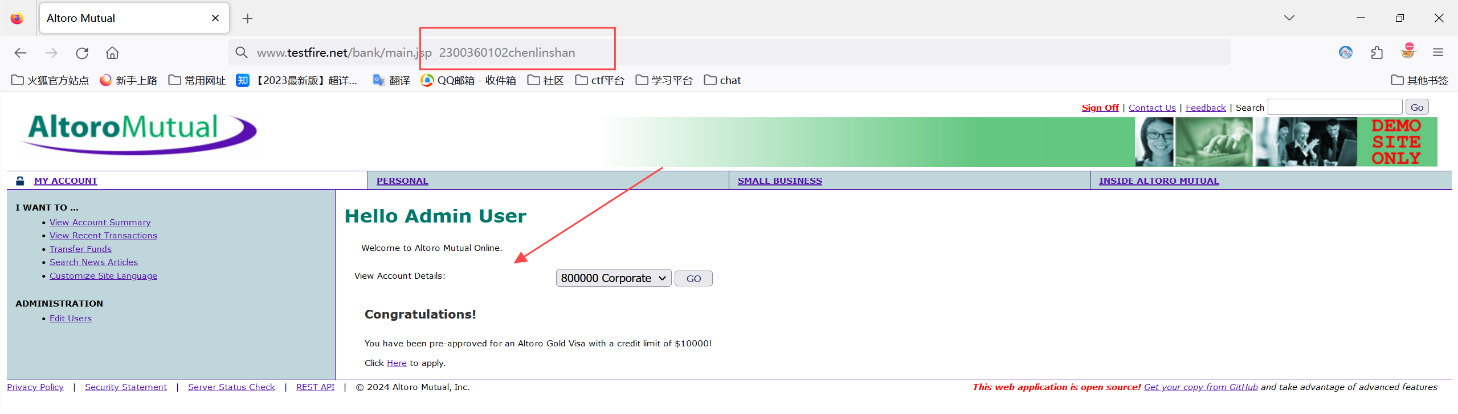
根据扫描出的目录，我们能看出来存在一个后台登入路径/admin ，还有可能存在一个目录穿越读取文件的漏洞。

****

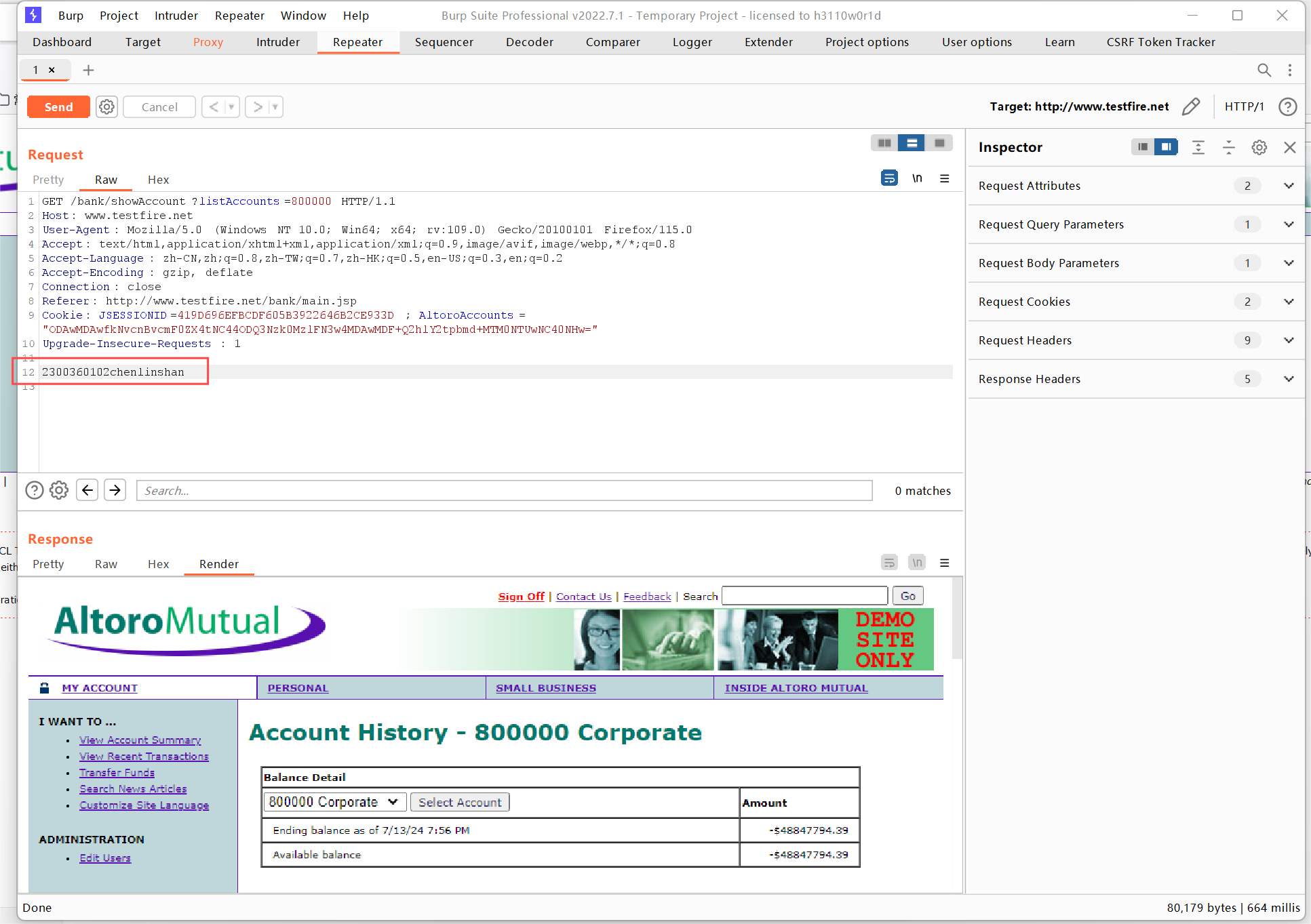
1. **登入admin界面，进入login.jsp界面**

****

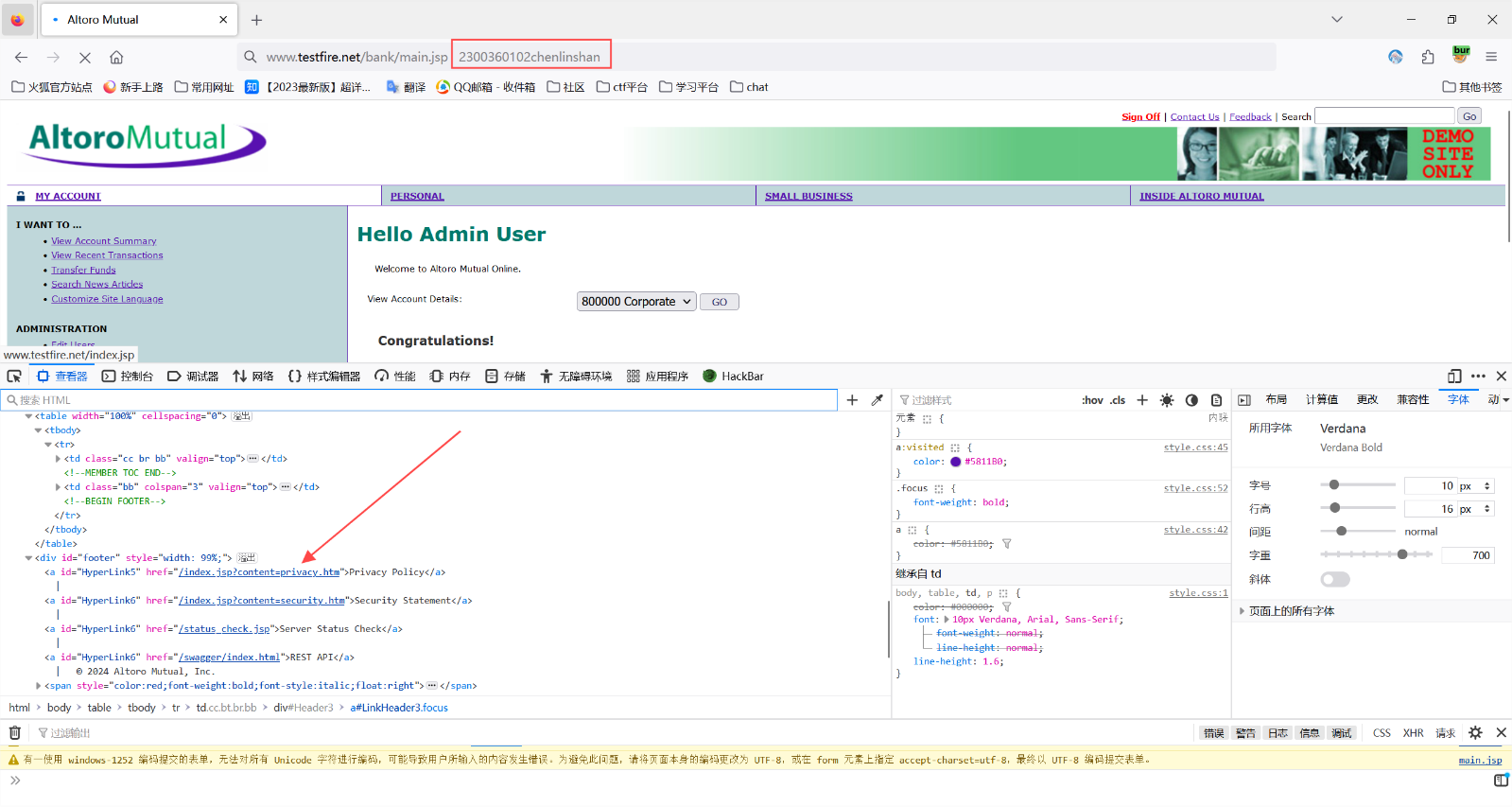
1. **使用bp爆破得到用户名和密码都为admin**

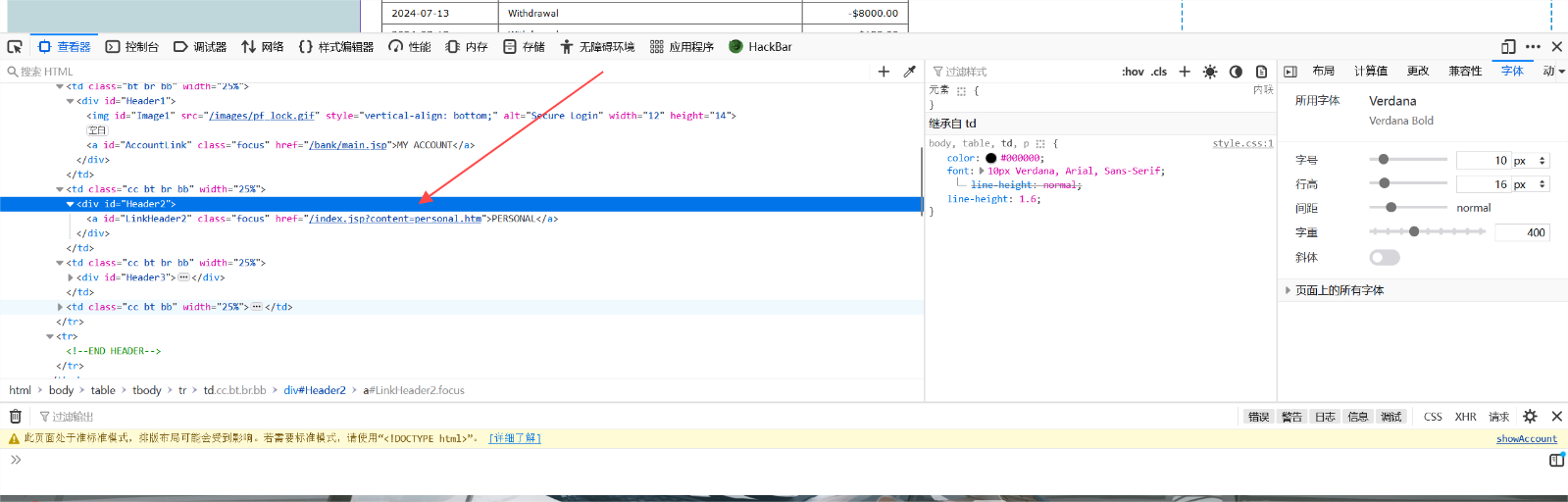
****

1. **登入后台查看弱口令漏洞。**

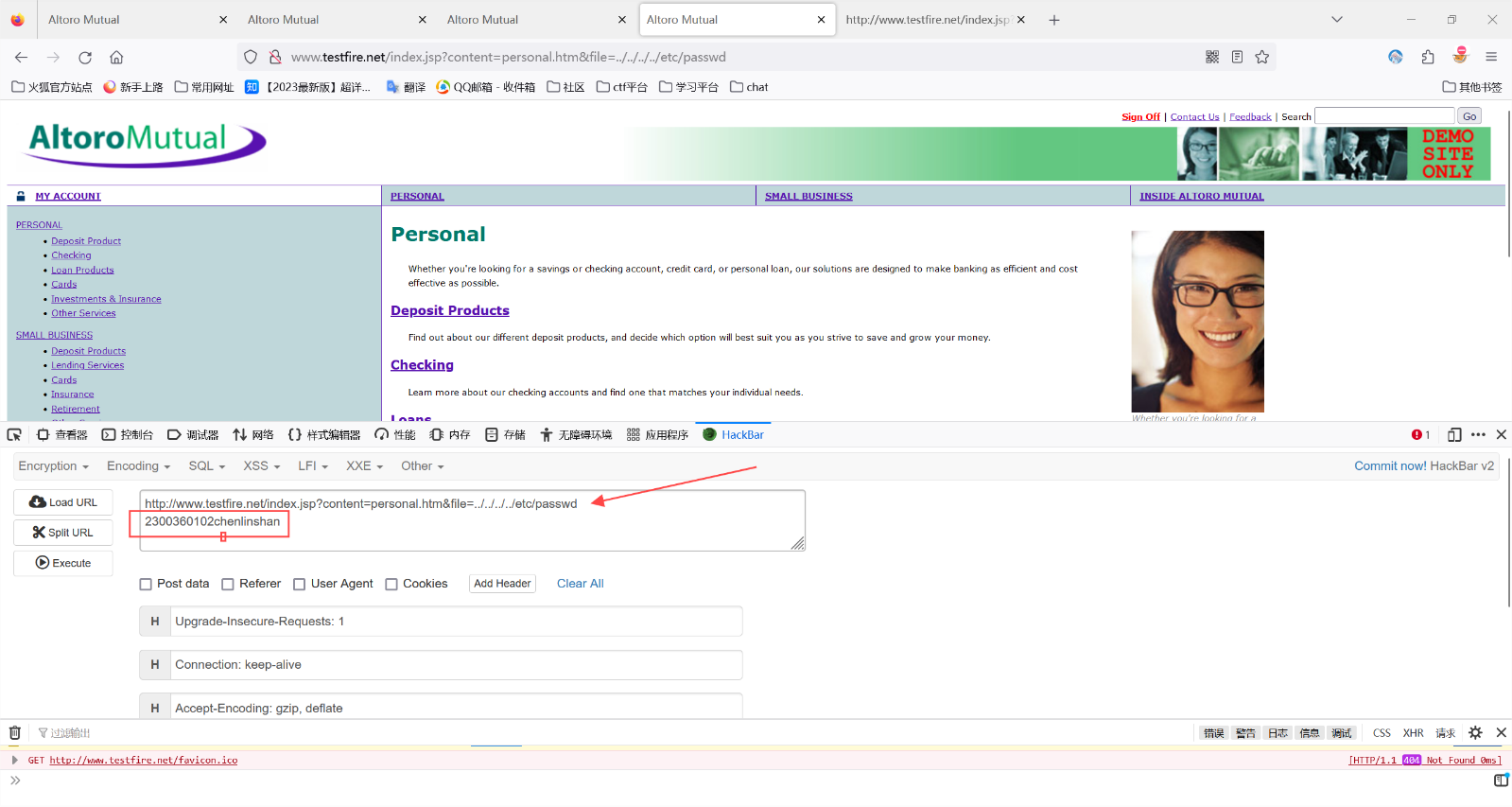
****

1. **查看页面源代码，尝试登入以下界面**

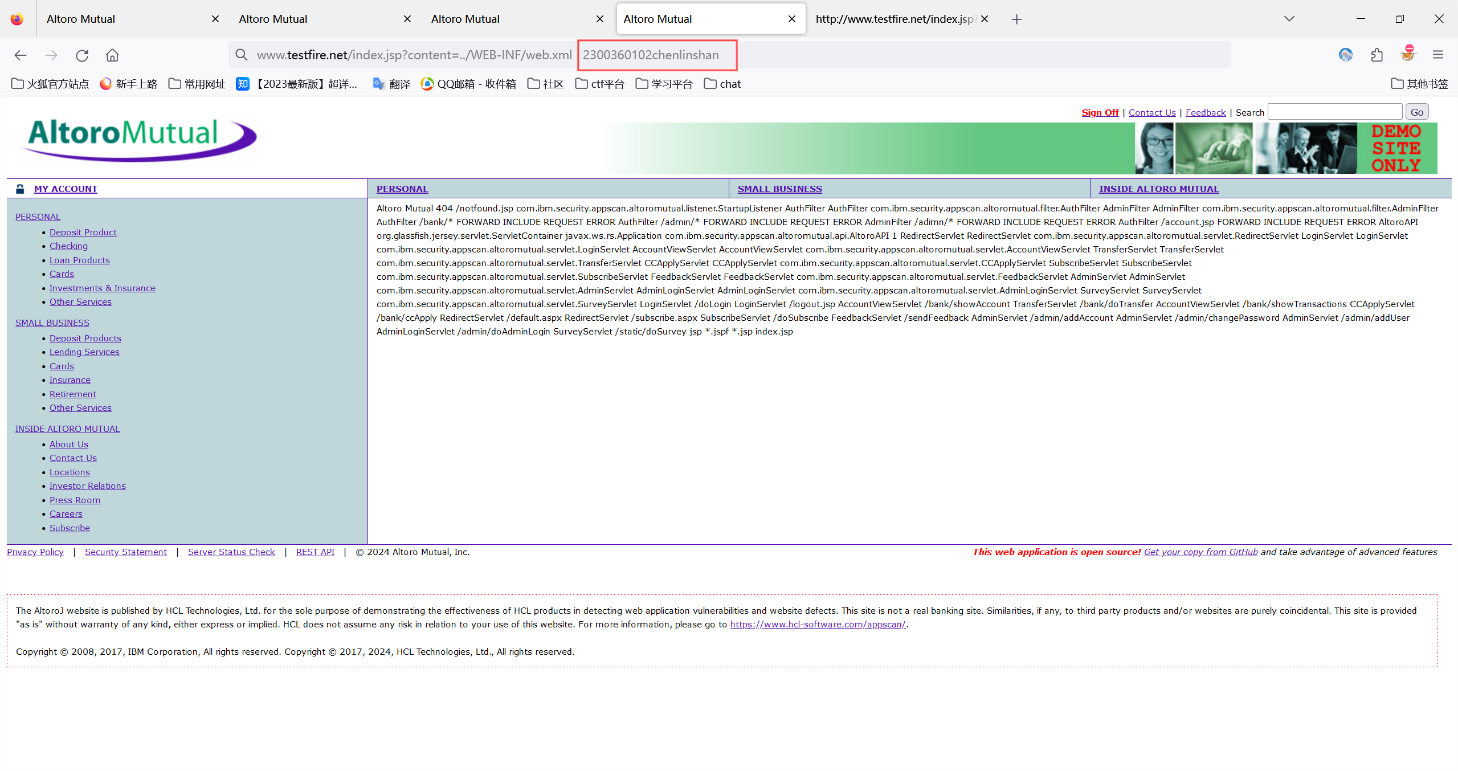
****

****

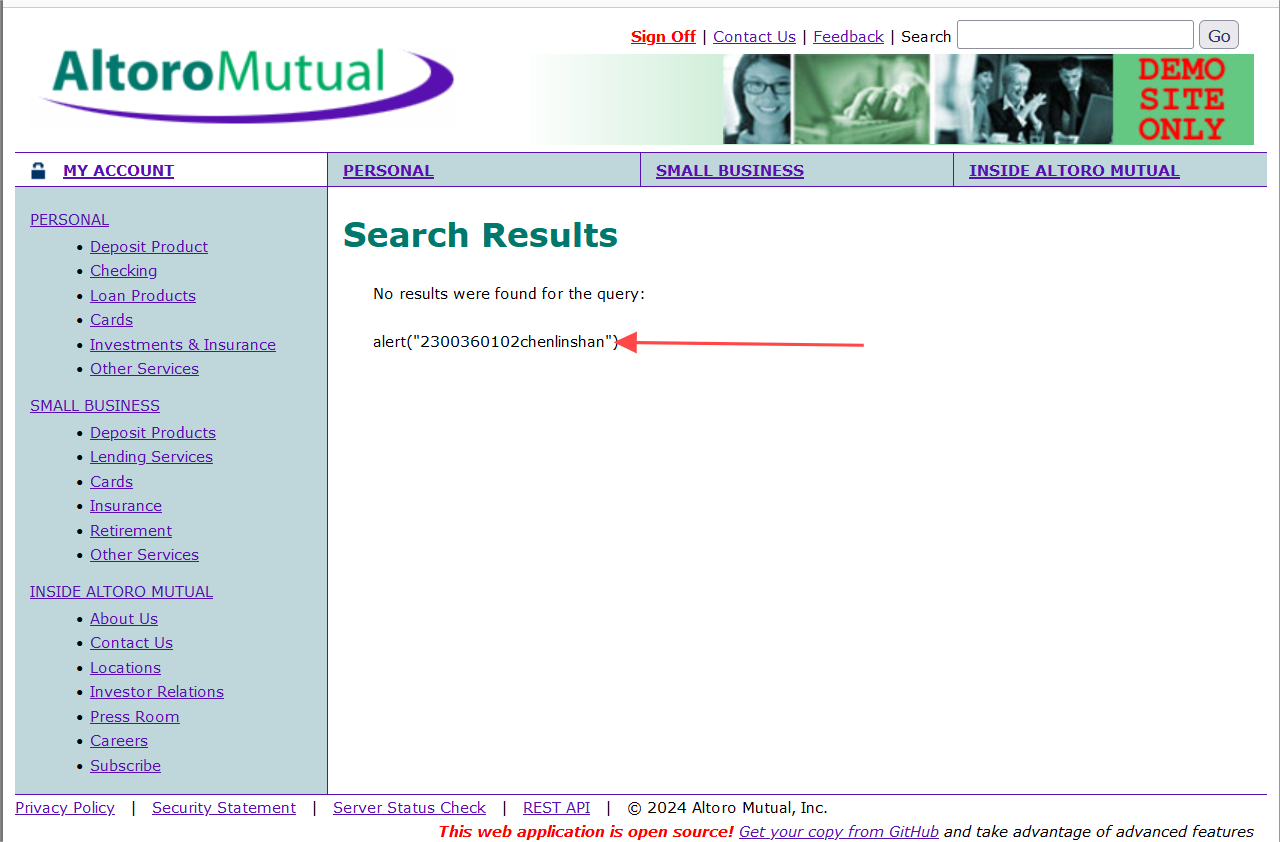
1. **发现登入之后想通过路径的方式获取passwd的信息，发现无法获取。**

****

1. **发现能够读取WEB-INF/web.xml的配置信息。**

****

1. **在搜索栏，尝试xss漏洞，输入<scipt>alert(“2300360102chenlinshan”)</scipt>，发现能够输出结果，证明存在xss漏洞。**



1. 尝试sql注入登录，在username处写a ‘OR 1=1--+，后面返回网站登入成功。



**五、实验总结**

1. TTL:ttl是ip协议包中的一个值，他告诉网络路由器包在网络中的时间是否太长而应被丢弃，有很多原因使包在一定内不能被传递到目的地。每个操作系统对ttl的值的定义都不同，这个值可以通过修改某些系统的参数来修改。Window默认ttl的值为128，该实验中我们就能够从Ping命令中得到ttl的值。
2. 通过扫描地址目录，我们有可能能够看出该网址可能存在的漏洞，本实验我们使用dirsearch扫描网站的时候看出来../etc/passwd存在于网站目录中，在后续我们进入Index.jsp漏洞的时候就会尝试使用该路径去查找该重要文件。
3. Web.xml是应用程序的配置文件，通常位于项目的WEB-INF目录下，主要作用是配置web应用程序的参数和组件，在本实验中，我们通过WEB-INF/web.xml路径能够找出该网站的配置信息，例如服务器信息等。
4. 当看到search框时，我们可以多尝试一些基础的漏洞，比如xss漏洞、sql注入漏洞，多次尝试就能发现有漏洞。
5. 在看到网站的时候首先查看该网站的源代码，在源代码中可能发现一些配置文件泄露的可能，例如在本实验中index.jsp路径下，存在web.xml配置文件的泄露，可以被远程攻击。
6. 在看到可以输入或者是可以上传文件的地方，就可以上传一句话木马进行攻击。