1. 登陆&Cookies测试

测试登陆和Cookies的有效性（logintest.py）

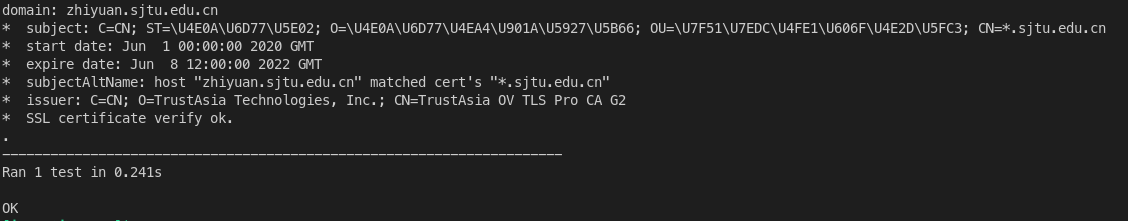


测试步骤：

1. 打开致远学院官网，测试标题存在
2. 验证已经设置了两条Cookies
3. 点击登陆，验证跳转至JACCOUNT登陆页面
4. 数据加密

网站使用了https，测试证书的有效性（ssltest.py)

证书信息：



1. 超时限制

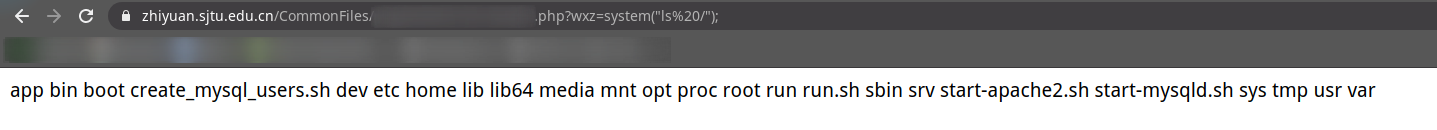
网站cookies设置了120分钟超时限制，然而由于使用的是JACCOUNT认证，而JACCOUNT授权有效期为浏览器会话级，同时采用了SSO单点登陆技术，因此在网站登陆失效后会跳至JACCOUNT认证自动再次登陆，因此在浏览器不关闭的情况下站点Cookies实际上没有超时限制。

1. 渗透测试

网站前台内容大部分为静态，搜索框处使用了ORM技术避免了SQL注入，浏览PDF处也限制了目录，无法读取其他文件，因此较为安全。

但是在取得低权限账户后，拥有上传权限，在上传校验处存在校验不当，可以上传任意php文件，通过CommonFiles路由访问造成任意命令执行。

如图所示在根目录下执行了ls命令



修复建议：

1. 限制上传文件类型
2. 取消上传目录php文件执行权限
3. 增加php disabled\_function不允许危险函数执行