CVE-2023-46747| F5 BIG-IP RCE详细完整分析

原创 老呆 阿呆攻防 2023年10月30日 17:04

此文章由SpringKiller安全研究师傅产出，这位佬是一个能独立开发一款企业级IAST，伸手0day伸脚1day，能手搓操作系统用脚逆向的师傅，还是OWASP的代码贡献者之一。哦，差点忘了，这个师傅能书会画，上厅堂下厨房无所不能，呆哥建议爱学习的可以找他击剑一下。

SpringKill师傅的Github地址：https://github.com/springkill

01

影响版本

全版本

02

环境搭建

链接: https://my.f5.com/manage/s/downloads?productFamily=BIG-IP&productLine=big-ip_v15.x&version=15.1.8&container=Virtual-Edition&files=BIGIP-15.1.8-0.0.7.ALL-vmware.ova&locations=JAPAN

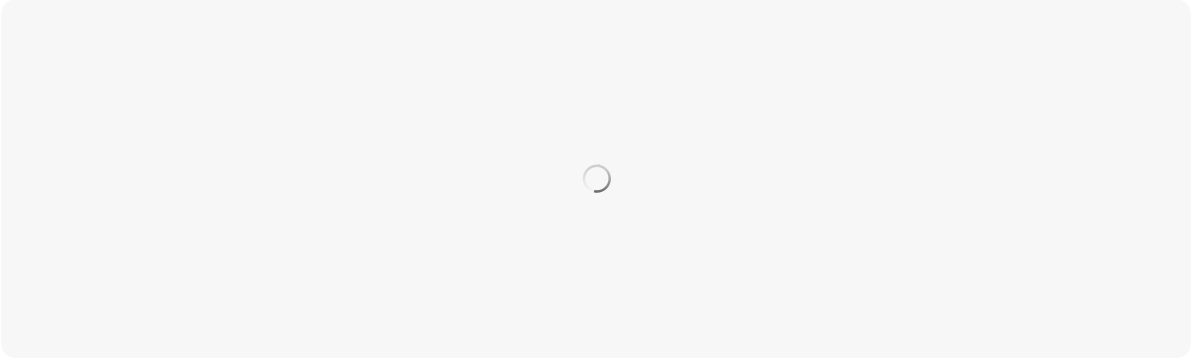
直接下载镜像用vmware启动即可。

默认账号密码为：admin/default

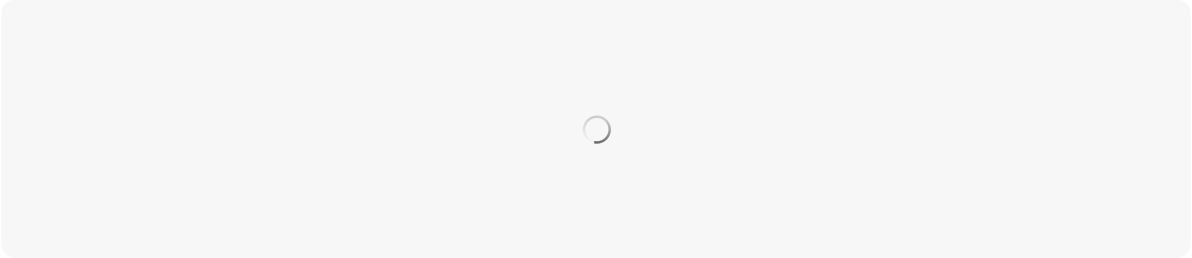
03

漏洞分析&复现

通过官方的修复补丁可以看出来和权限验证相关，并且修改了 `proxy_ajp_conf` 文件中的内容，再结合已有信息推测这是一个AJP走私问题（然而就在初步验证成功的时候chen师傅发了一句话……）



擦，点开一看竟然是poc，看了下poc和 /usr/share/tomcat/conf/server.xml



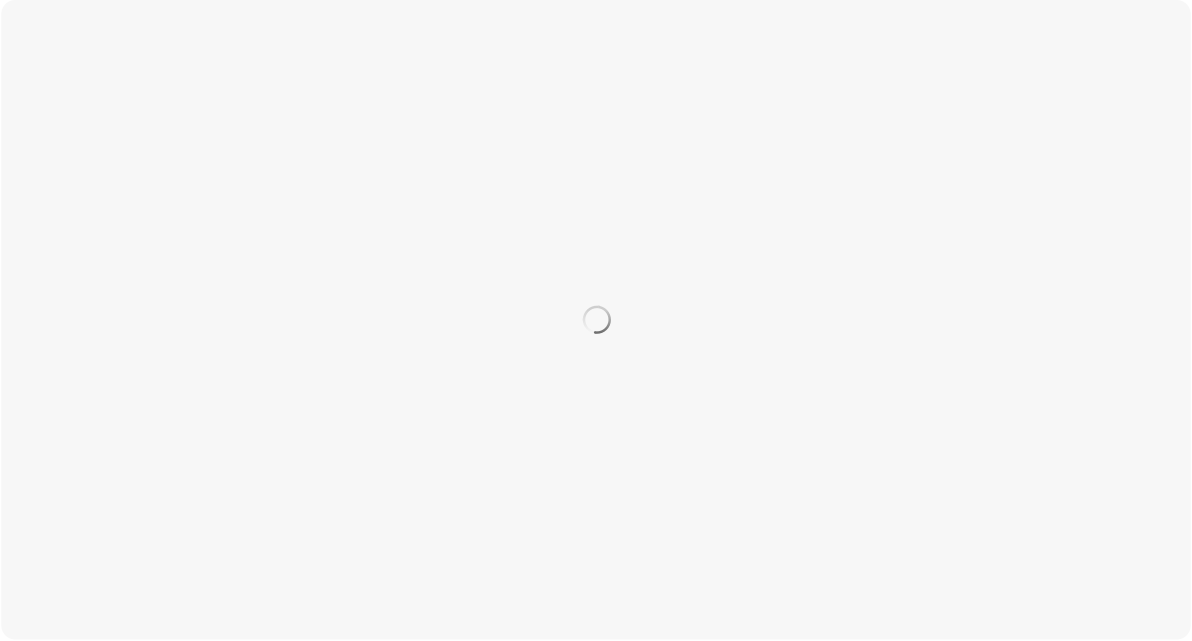
省了很多事，这下确定了是AJP走私的问题，因为BIG-IP的Apache是基于Apache 2.4.6的定制版，所以也会受AJP走私的影响。

AJP走私大家并不陌生，比如ghostcat和CVE-2022-26377这类的漏洞就是AJP走私造成的，那么接下来的利用就比较简单了：

1. 在BIG-IP的历史漏洞CVE-2022-1388中得知，我们可以从 `/mgmt/tm/util/bash` 来执行命令，但是当时是基于 `X-F5-Auth-Token` 权限的绕过，那么既然权限绕过已经修复了，我们就需要一个可以通过认证的 `X-F5-Auth-Token`，那么也就是需要创建一个管理员用户。

2. 那么创建账户这个问题就来到了tmui上，我们通过AJP走私到 `/tmui/Control/form` 调用 `/tmui/system/user/create.jsp` 来创建一个新的用户。

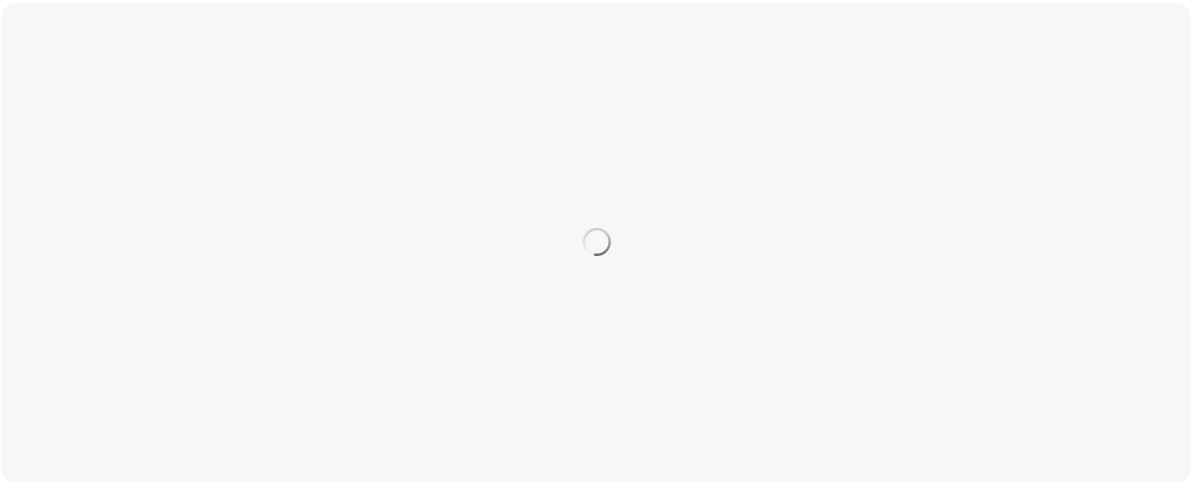
3. 参考官方文档的方式，创建完新的用户之后就可以通过 `/mgmt/shared/authn/login` 然后返回第一步来执行命令。



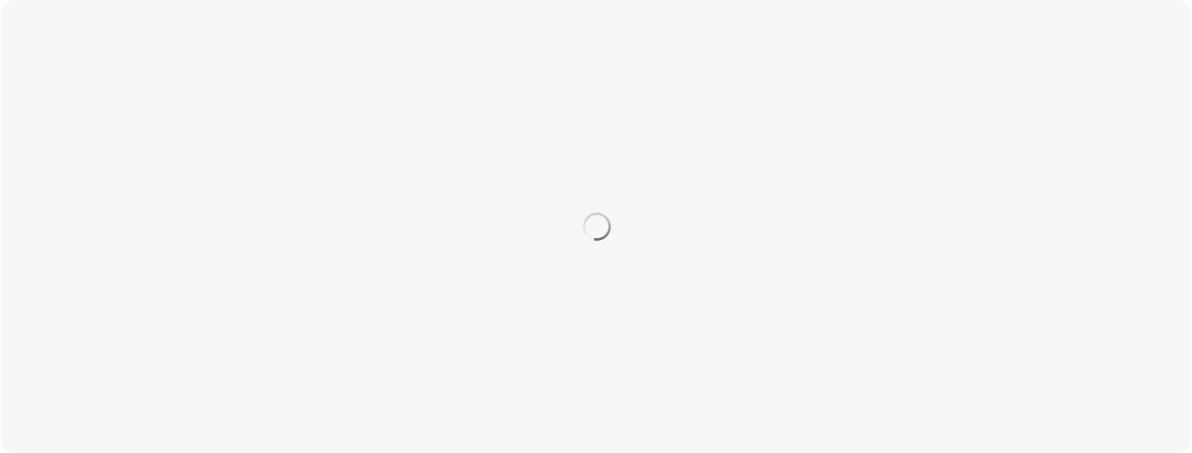
流程概括下来就是：通过 `/tmui/Control/form` 来调用 `user/create.jsp` 然后从 `/mgmt/shared/authn/login` 获取新的token，最后在 `/mgmt/tm/util/bash` 执行命令。

这其中有一个需要注意的点：

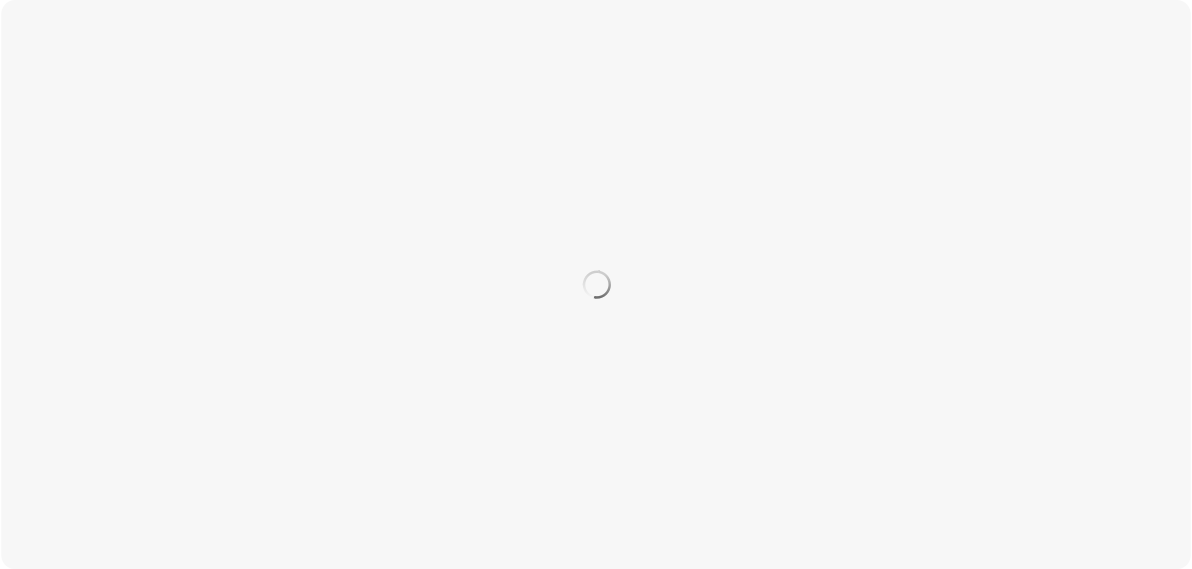
tmsh中进行了csrf检测，所以在第一步调用的时候需要构造好三个参数 `_timenow` `Tmui-Dubbuf` 和`_bufvalue`，满足 `_bufvalue` 的值等于 `Tmui-Dubbuf` + `Tmui-Dubbuf` 。



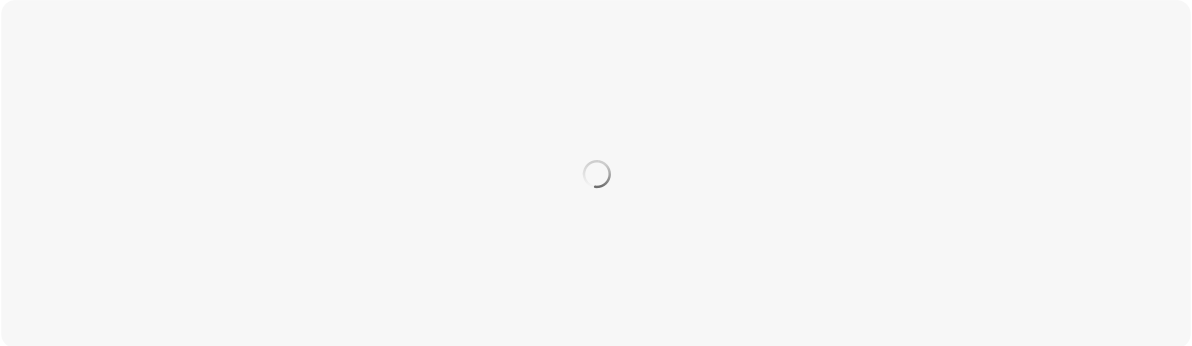
在 nuclei 给的 poc 中用的是 `Tmui-Dubbuf` =BBBBBBBBBBB 、 `_timenow` =a 、 `_bufvalue` =eIL4RUnSwXYoPUIOGcOFx2o00Xc=



我们也使用这三个键值对进行构造，那么最后得到的poc就是：

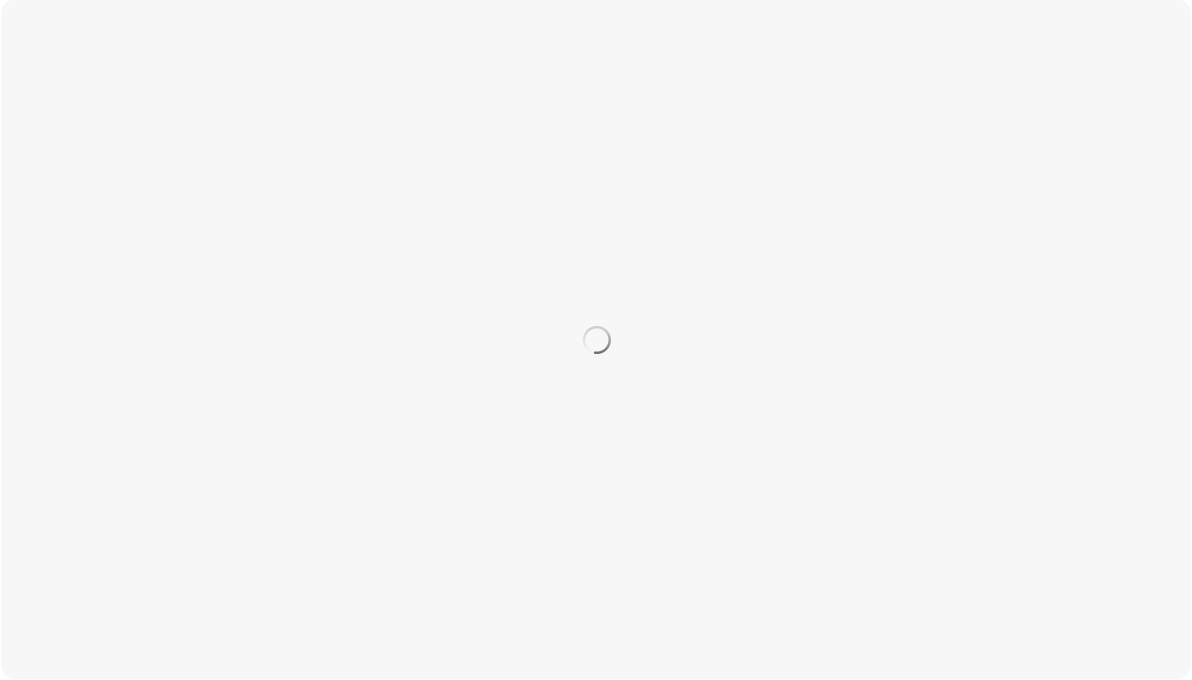


使用 `Transfer-Encoding: chunked` 时，会使用分块传输编码,第一个204就是trunk size的大小，用十进制转换为十六进制后对应516，也就是我们走私请求的长度，最后的0表示结尾，如果不是用https看到的明文如下：

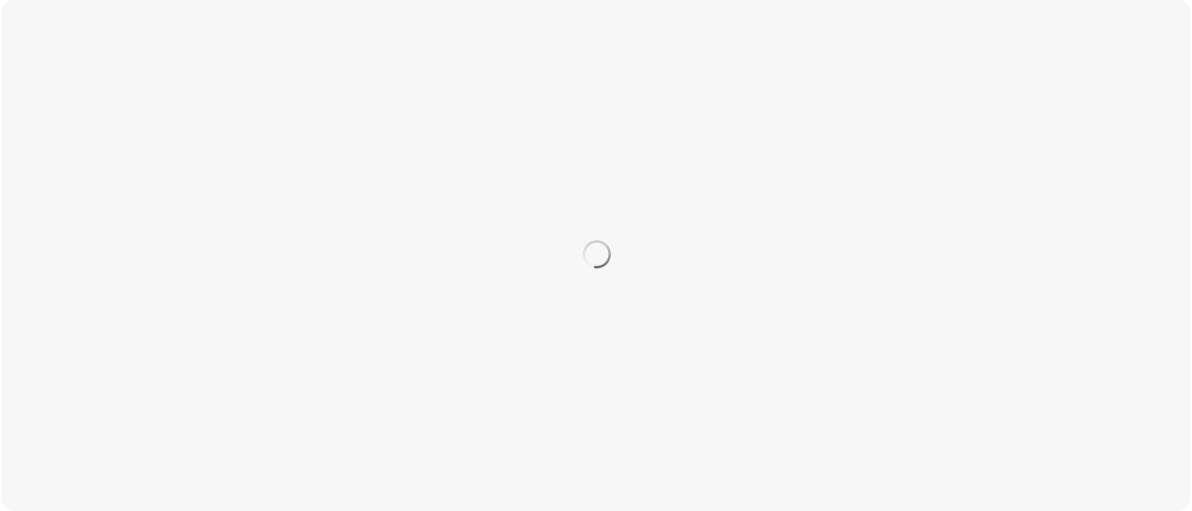


这个步骤需要多试几次，不一定第一次就成功，发现返回的不是登录界面后就可以进行下一步了：

通过账号密码获取到token的值。



然后执行命令：



#SpringKill师傅的代码审计系列 13

#SpringKill师傅的代码审计系列 · 目录 ≡

下一篇 · XVE-2023-21328|XXL-JOB默认密钥审计分析 >