CVE-2013-4547

影响版本: nginx 0.8.41 ~ 1.5.6

这一漏洞的原理是通过非法字符空格和截至符%00会导致Nginx解析URI的有限状态机混乱，危害是允许攻击者通过一个非编码空格绕过缀名限制

就比如在服务器存在文件为”test.jpg “，注意最后一个字符是空格，则可以通过访问 http://test.com/test.jpg \0.pnp

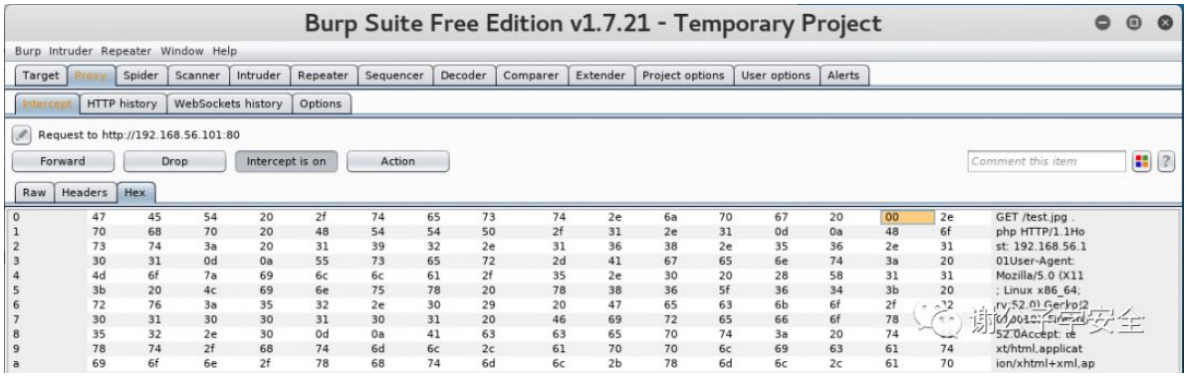
让Nginx认为文件 ”test.jpg “后缀为 “.php”

实战
一张test.png插入图像，注意后面是有空格的， 此时你会发现在浏览器中访问此文件是404，那是因为浏览器自动吧你的空格给及系正为%20编码。

这是我们服务器不存在test.png%20的文件

测试目标是让Nging认为文件是图片并正确并在浏览器中显示出来，使用Burp对其数据包进行修改，首先修改成想要的样子，原本为的URI为 http://test.test.htmltestjpg

使用Suite抓取浏览器发出的请求包，修改A为 20，20是ASCII码中空格的意思，将第二个A改成00，是截至符的意思，降低三个A改成2e，是"."的意思。



修改好后Forword该请求，在浏览器中可以看到确实吧 test.jpg 当作了php去执行，但是只是php看到该文件后缀名为 “.jpg ” 从而拒绝执行，可以判断确实存在此漏洞，，但是由于security.limit_extensions的存在，导致这个漏洞并不会被利用。