Bypass WAF实战总结

Azjj98

于 2021-01-09 17:07:53 发布

0X00前言

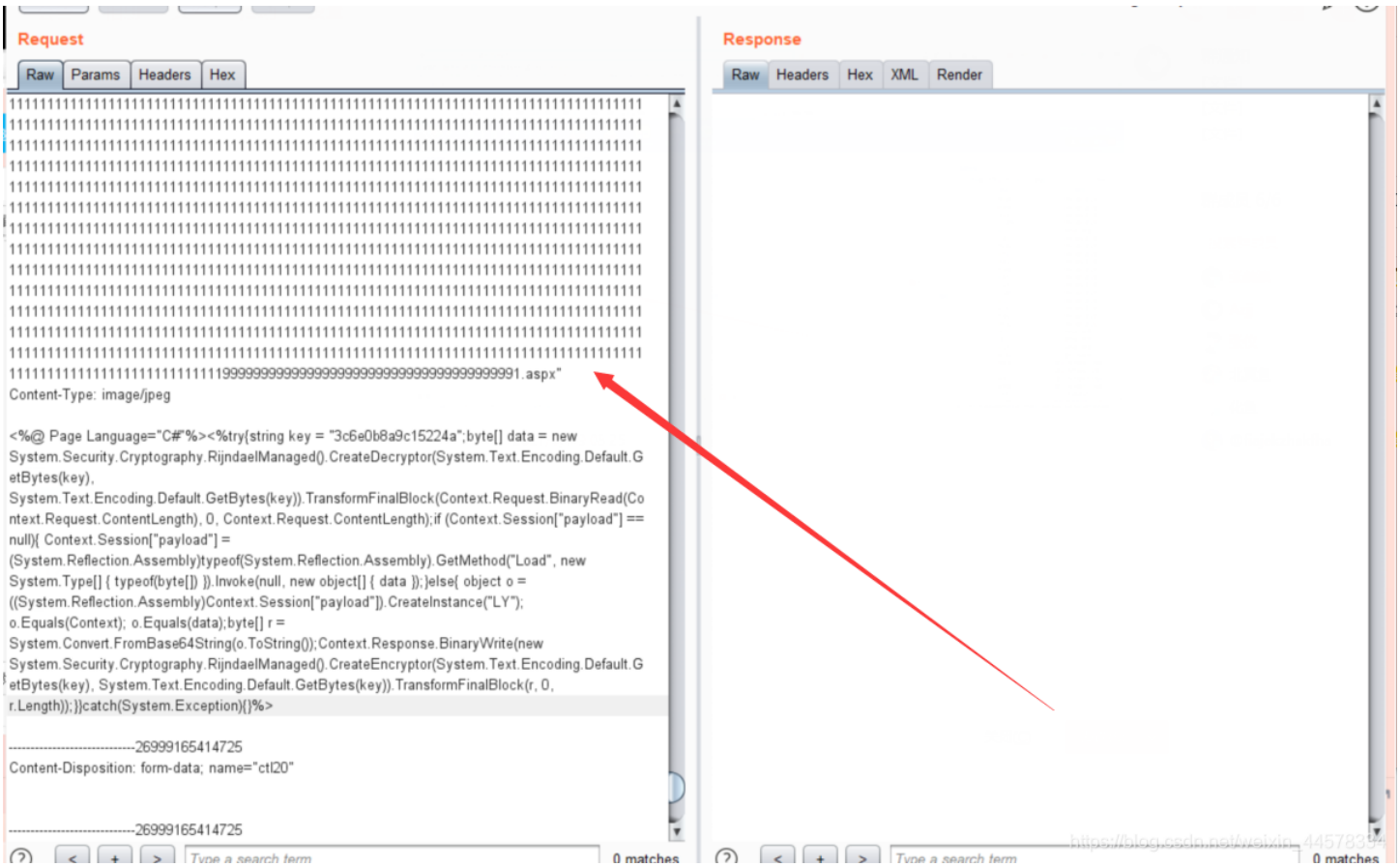
上个月刷了一波洞，然后这个月初远程支持了一个HW，在文件上传getshell的时候，碰到个各式各样的云waf，通过一个月的实战，总结了几个比较实用的技巧，文章总结的不全，只是基于我实战中用到的一些方法。

0x01垃圾填充

这是众所周知、而又难以解决的问题。如果HTTP请求POST 太大，检测所有的内容，WAF集群消耗太大的CPU、内存资源。因此许多WAF只检测前面的几K字节、1M、或2M。对于攻击者而然，只需要在前面添加许多无用数据，把攻击payload放在最后即可绕过WAF检测。

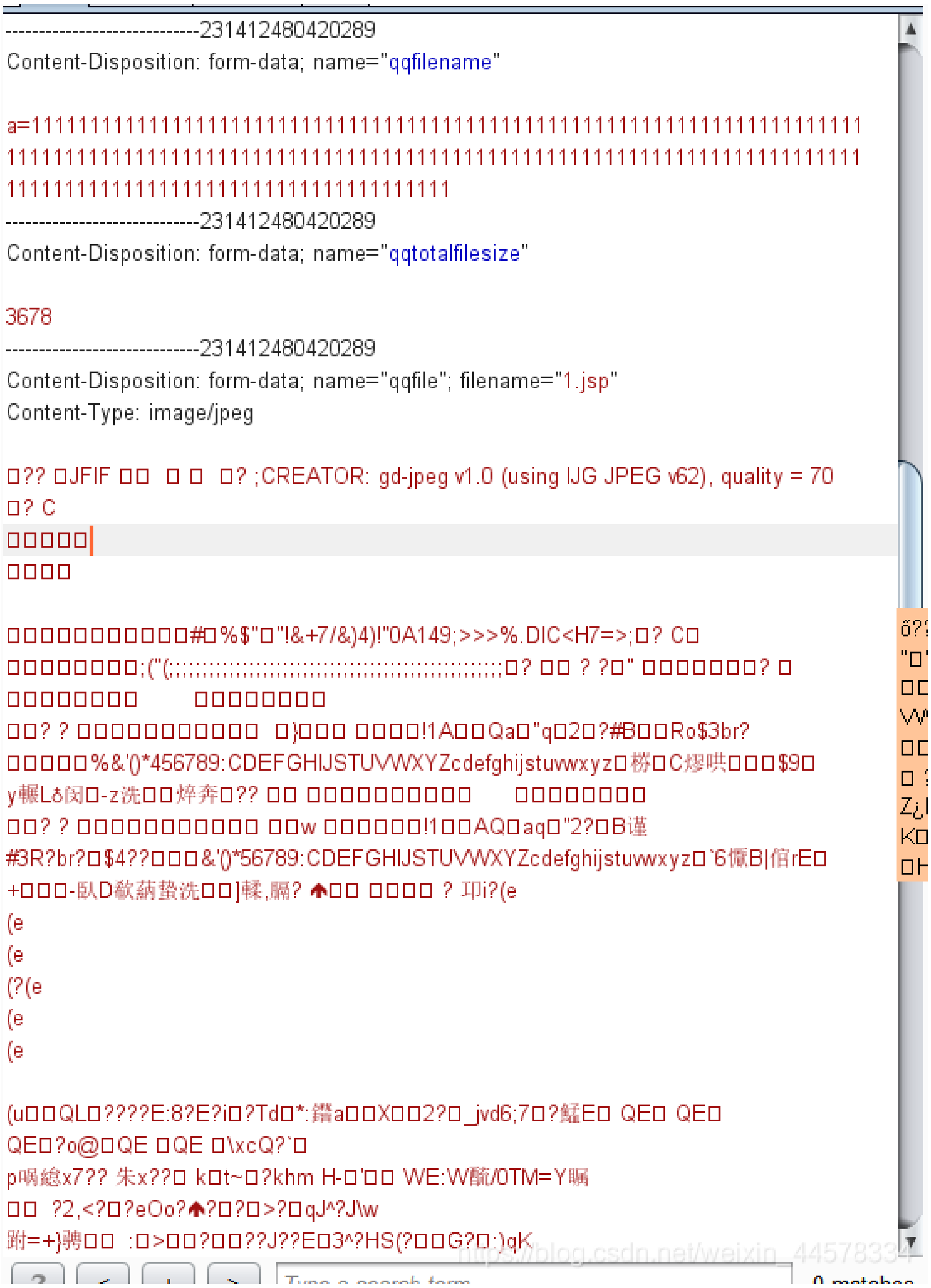
1.超长文件名

这个主要是对于waf检测文件后缀的时候起作用，利用超长的文件名，可以逃过文件后缀名的检测



2.上传内容使用垃圾字符

上传一个比较大的文件，将马子藏在其中



0x02使用参数污染成功执行命令

简而言之，就是给参数赋上多个值

Technology/HTTP back-end	Overall Parsing Result	Example
ASP.NET/IIS	All occurrences of the specific parameter	par1=val1,val2
ASP/IIS	All occurrences of the specific parameter	par1=val1,val2
PHP/Apache	Last occurrence	par1=val2
PHP/Zeus	Last occurrence	par1=val2
JSP,Servlet/Apache Tomcat	First occurrence	par1=val1
JSP,Servlet/Oracle Application Server 10g	First occurrence	par1=val1
JSP,Servlet/Jetty	First occurrence	par1=val1
IBM Lotus Domino	Last occurrence	par1=val2
IBM HTTP Server	First occurrence	par1=val1
mod_perl,libapreq2/Apache	First occurrence	par1=val1
Perl CGI/Apache	First occurrence	par1=val1
mod_perl,lib???/Apache	Becomes an array	ARRAY(0x8b9059c)
mod_wsgi (Python)/Apache	First occurrence	par1=val1
Python/Zope	Becomes an array	['val1', 'val2']
IceWarp	Last occurrence	par1=val2
AXIS 2400	All occurrences of the specific parameter	par1=val1,val2
Linksys Wireless-G PTZ Internet Camera	Last occurrence	par1=val2
Ricoh Aficio 1022 Printer	First occurrence	par1=val1
webcamXP PRO	First occurrence	par1=val1
DBMan	All occurrences of the specific parameter	par1=val1~~val2

0x03构造畸形请求包

还是基于waf的检测一般都会判断请求类型再去检测内容

有些可以通过修改POST为GET绕过waf

还有的waf通过Content-Type: multipart/form-data来判定这是个上传包，然后检测内容

这个方法，又能细分出很多来，而且屡试不爽，这里总结下我个人常用的

(1) 删掉content-type

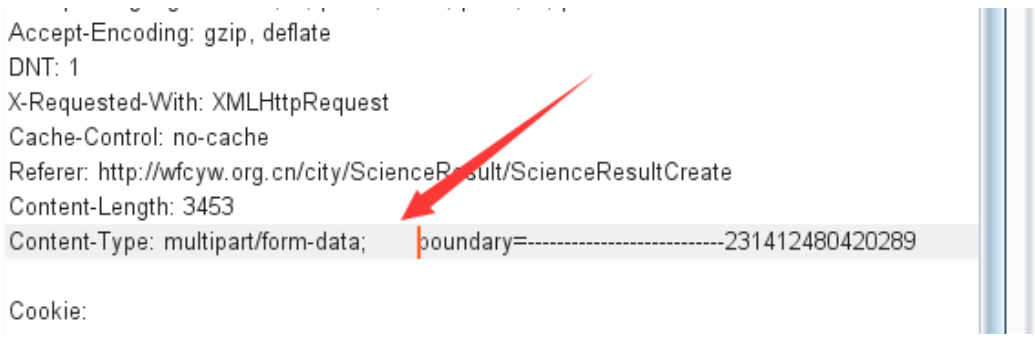
(2) 构造多个filename

(3)content-type后面加TABLE键

(4)换行boundary

(5)文件名前面加空格

(6)文件名前面加单引号



.....这里是实在是太多了，就不一一举例了

0x04文件内容编码绕过

这个就比较考验个人能力了,既可以让waf检测不到，有能成功执行命令，这里是真正的硬实力绕waf。

0X05大力出奇迹

这是我形象化的一个词语，这里没什么技巧，就是不断发包，让waf反应不过来，在碰到一些比较老的服务器，或者waf这招还是比较有用的。

0x05总结

绕Waf是门艺术，基于waf的规则绕过是核心点，机器是死的人是活的，fuzz是测试waf的较好的方法，只要你思路够骚，waf那还不是笋尖缪杀！

————————————————

原文链接：https://blog.csdn.net/weixin_44578334/article/details/112393475