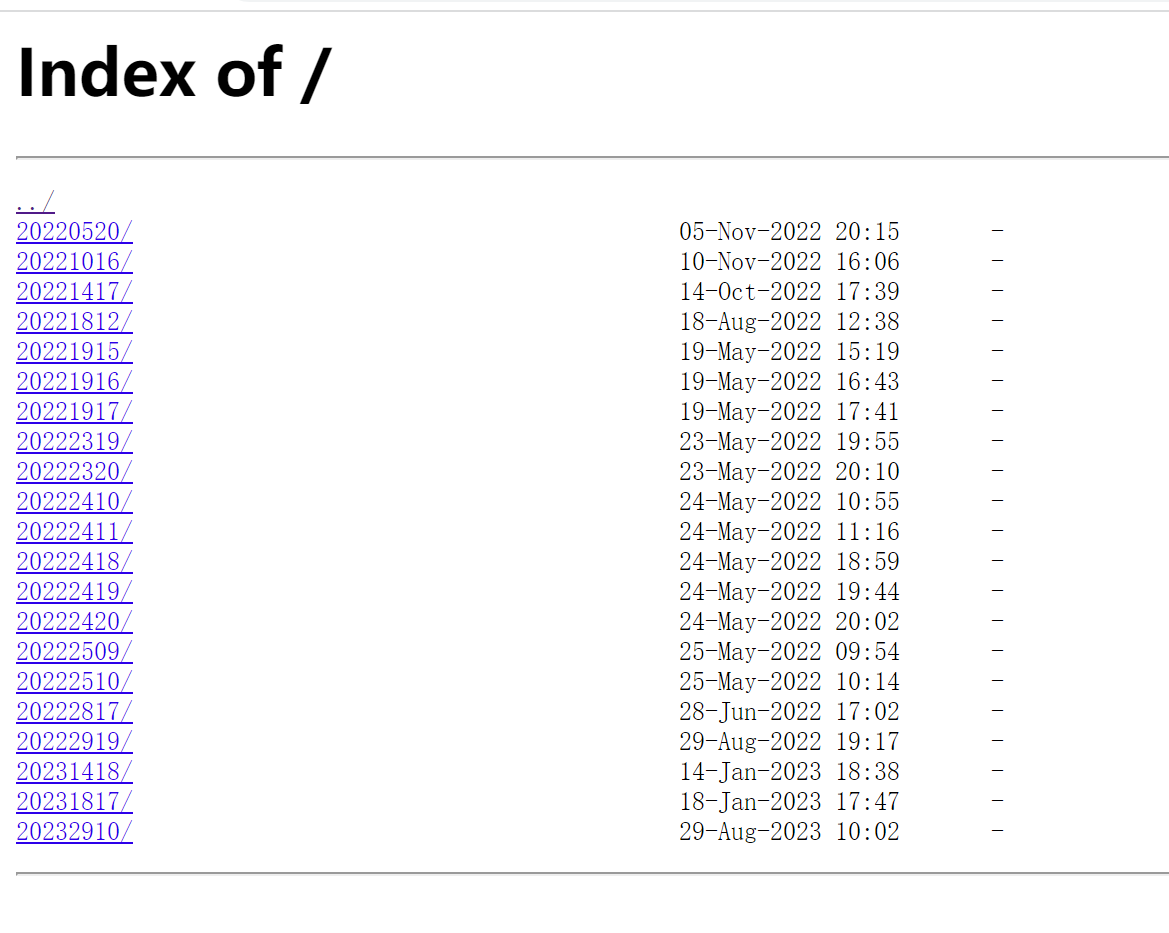
1. 目录遍历

请求URL无特征，可以是任意URL

响应内容一般如下：



<html>

<head><title>Index of /</title></head>

<body bgcolor="white">

<h1>Index of /</h1><hr><pre><a href="../">../</a>

<a href="20220520/">20220520/</a> 05-Nov-2022 20:15 -

<a href="20221016/">20221016/</a> 10-Nov-2022 16:06 -

<a href="20221417/">20221417/</a> 14-Oct-2022 17:39 -

<a href="20221812/">20221812/</a> 18-Aug-2022 12:38 -

<a href="20221915/">20221915/</a> 19-May-2022 15:19 -

<a href="20221916/">20221916/</a> 19-May-2022 16:43 -

<a href="20221917/">20221917/</a> 19-May-2022 17:41 -

<a href="20222319/">20222319/</a> 23-May-2022 19:55 -

<a href="20222320/">20222320/</a> 23-May-2022 20:10 -

<a href="20222410/">20222410/</a> 24-May-2022 10:55 -

<a href="20222411/">20222411/</a> 24-May-2022 11:16 -

<a href="20222418/">20222418/</a> 24-May-2022 18:59 -

<a href="20222419/">20222419/</a> 24-May-2022 19:44 -

<a href="20222420/">20222420/</a> 24-May-2022 20:02 -

<a href="20222509/">20222509/</a> 25-May-2022 09:54 -

<a href="20222510/">20222510/</a> 25-May-2022 10:14 -

<a href="20222817/">20222817/</a> 28-Jun-2022 17:02 -

<a href="20222919/">20222919/</a> 29-Aug-2022 19:17 -

<a href="20231418/">20231418/</a> 14-Jan-2023 18:38 -

<a href="20231817/">20231817/</a> 18-Jan-2023 17:47 -

<a href="20232910/">20232910/</a> 29-Aug-2023 10:02 -

</pre><hr></body>

</html>

1. 文件上传

请求URL无特征，关注请求体重和filename等相关参数，例如：

图形用户界面, 文本, 应用程序

描述已自动生成

这里的filename=1.html，一般来说，上传图片格式、文档格式一般没什么问题，如果这里是html、jsp、php、asp、aspx等脚本格式，就需要注意可能正在尝试利用上传功能上传恶意文件等，上传成功的响应包有几种可能

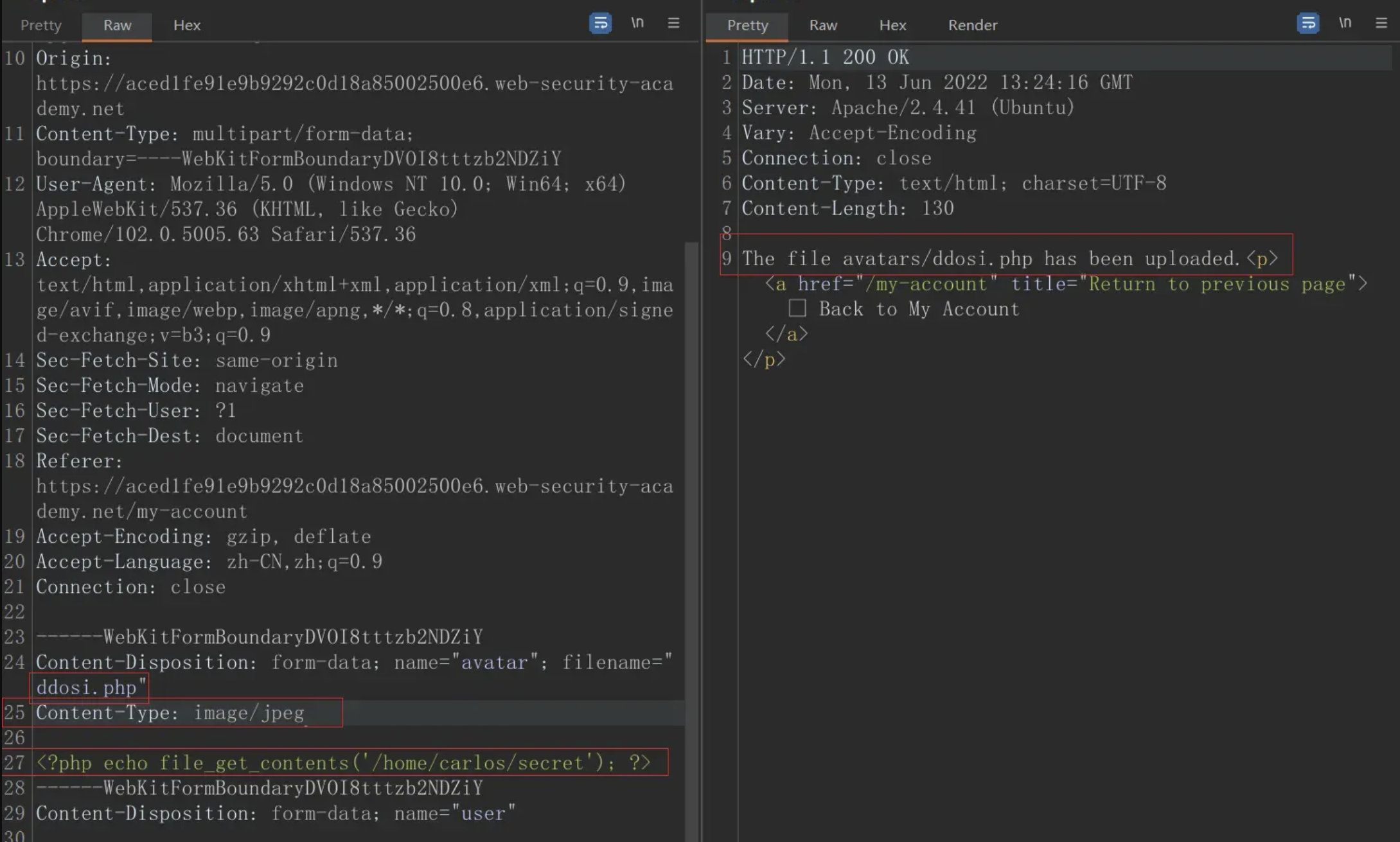
2.1响应包中响应状态码200，内容含有路径，最后带有filename传过来的文件名，例如：/aaa/bbb/upload/1.html、/aaa/bbb/upload/1.jsp

2.2 响应包中响应状态码200，内容可能会如下等形式，不会直接返回相关文件路径

{“status”:200}，{“status”:200,”data”:”文件上传成功”}，{“status”:200,”data”:”success”}

2.3也可能响应包直接文本响应，这就需要大量的样本支撑

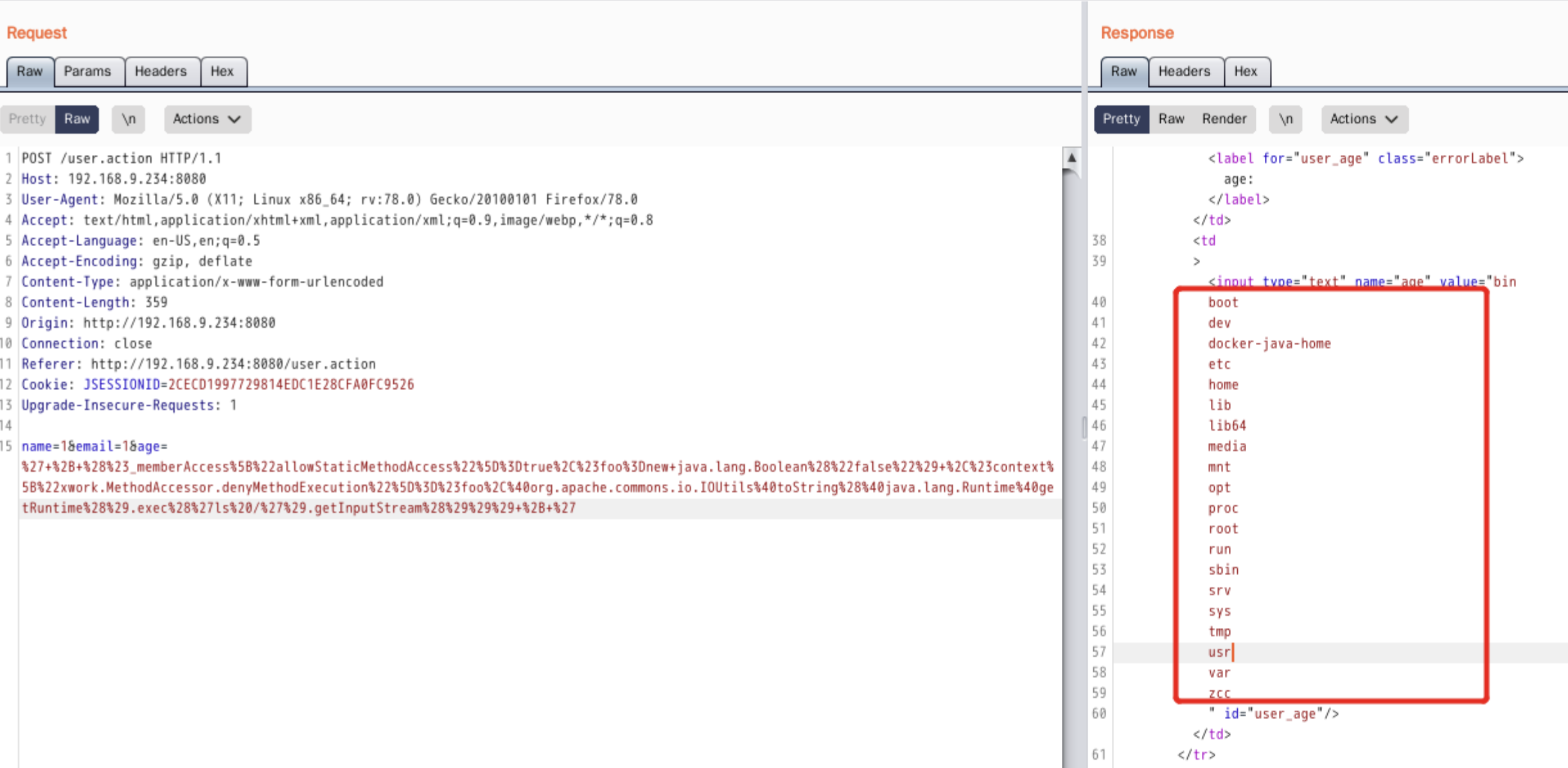
当然也可能有失败的包会返回相同形式：{“status”:200,”data”:”failed”}



1. 命令执行

请求URL没有明显特征

响应包一般会包含命令执行结果，这个需要结合请求内容的命令来看



这里举的例子是struts2命令执行，可直接回包看到结果。

但有很多命令执行漏洞无法一次搞定，如Spring Cloud Gateway RCE

第一次发包会带有RCE相关字眼，但回包不会有任何RCE特征

图形用户界面, 文本, 应用程序

描述已自动生成

只有请求的时候，才会返回命令执行结果

