New issue   **Jump to bottom**

eZiosuite2.0.7_任意文件下载 eZiosuite_任意文件下载 eZiosuite2.0.7_ Any file download #1

⊙ **Open**   **Chu1z1** opened this issue on Mar 3 · 0 comments

Chu1z1 commented on Mar 3   Owner

#eZiosuite_任意文件下载 eZiosuite_任意文件下载 eZiosuite_ Any file download
##需要登陆到德实任意用户才可以利用
##Users need to log in to exploit the vulnerability
###You can find the interface at the avatar upload to obtain the key generated by the uploaded file path, modify the path of the generated key to generate a malicious key, and import the key at the avatar file reading, resulting in arbitrary file download
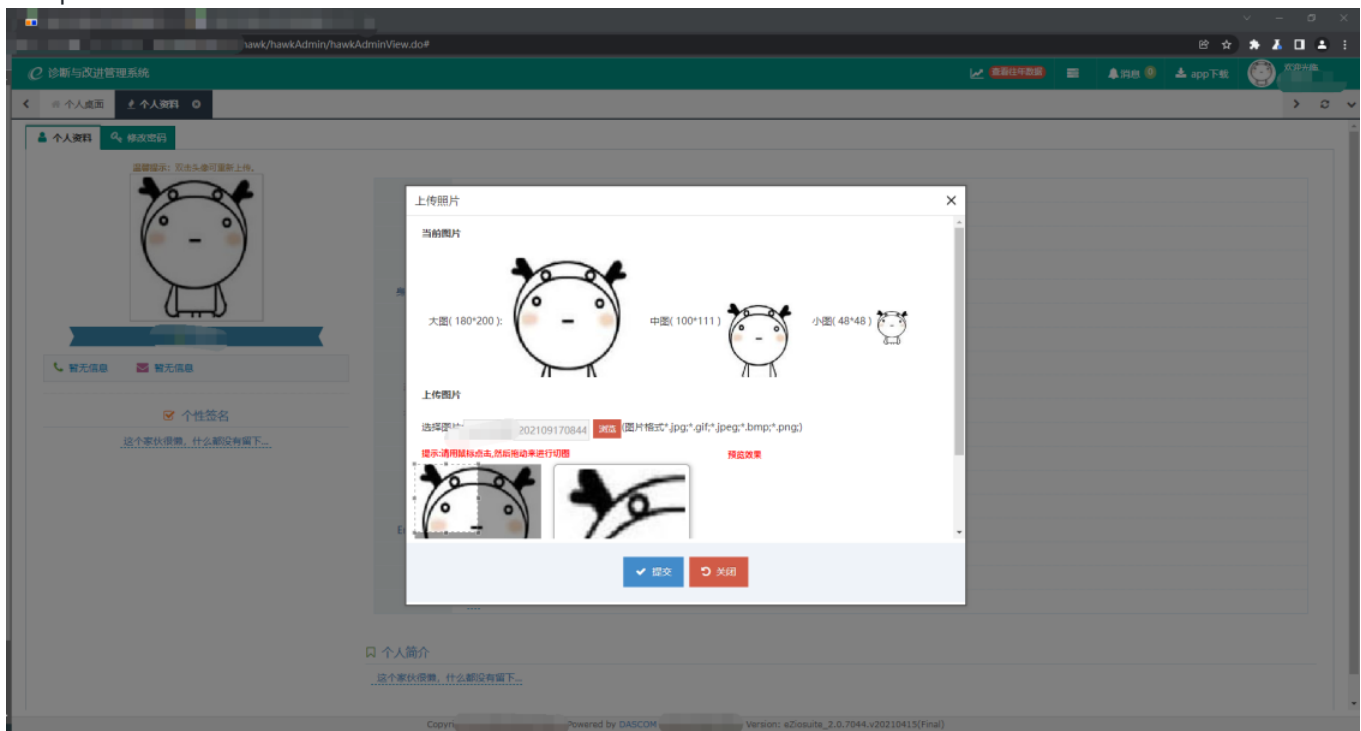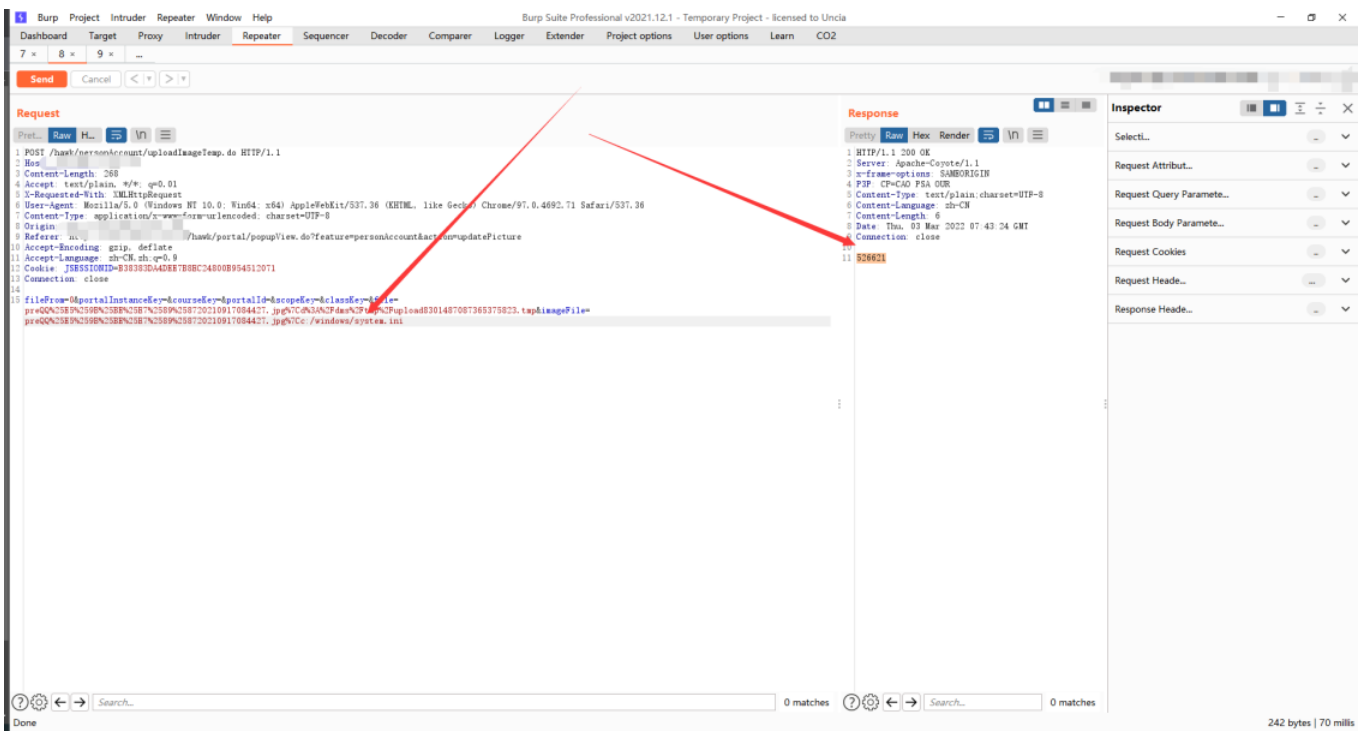###可在头像上传处找到接口，获取上传文件路径生成的key，修改生成key的路径生成恶意key，可在头像文件读取处导入key，从而导致任意文件下载
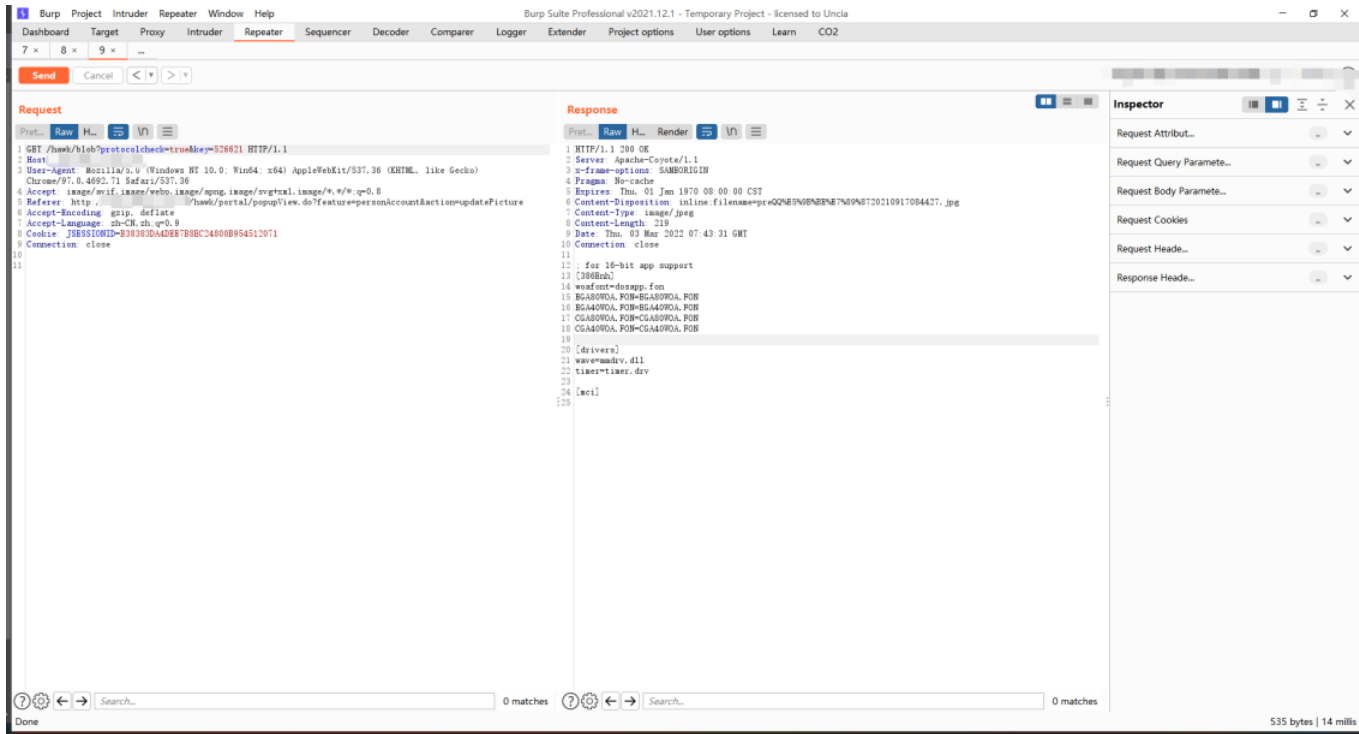
用户界面

UI
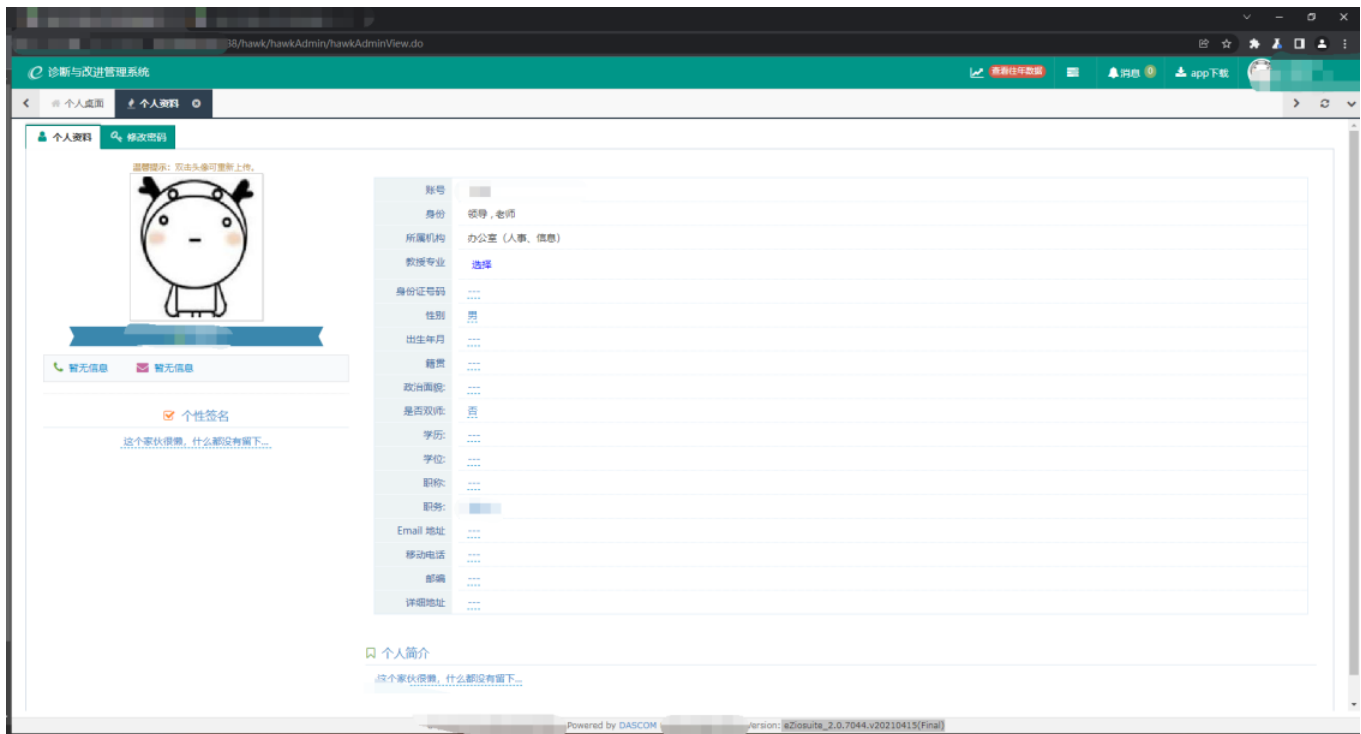
上传文件

Upload file

可以修改返回路径也可以更改下一个包的路径获取key

You can modify the return path or change the path of the next package to obtain the key

↓↓↓

漏洞利用成功

Successful exploit

请勿非法渗透！请勿未授权渗透！请勿使用该漏洞做违法犯罪活动！此文章仅供学习！造成后果与作者无关！
Do not infiltrate illegally! Do not penetrate without authorization! Please do not use this vulnerability for illegal and criminal activities! This article is for learning only! The consequences of breaking the law have nothing to do with the author!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant