http://192.168.0.138:81存在文件上传测试漏洞

# 漏洞地址

http://192.168.0.138:81

# 漏洞详情

一共1组payload

## 第1组payload共发送2次请求

### **发送第1次请求:**

**请求数据包**

**POST /net/controller.ashx?action=uploadimage HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Host: 192.168.0.138:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryorgXkX1mg3QTLDKr
Content-Length: 188
------WebKitFormBoundaryorgXkX1mg3QTLDKr
Content-Disposition: form-data; name="upfile"; filename="test.png"
Content-Type: image/png
�PNG
123
------WebKitFormBoundaryorgXkX1mg3QTLDKr--**

**请求响应包**

**HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Date: Fri, 10 Mar 2023 08:59:53 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 133
Cache-Control: private
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
{"state":"SUCCESS","url":"upload/image/20230310/6381406439412552854973405.png","title":"test.png","original":"test.png","error":null}**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**

### **发送第2次请求:**

**请求数据包**

**GET /net/upload/image/20230310/6381406439412552854973405.png HTTP/1.1
User-Agent: fasthttp
Host: 192.168.0.138:81**

**请求响应包**

**HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Date: Fri, 10 Mar 2023 08:59:53 GMT
Content-Type: image/png
Content-Length: 11
Last-Modified: Fri, 10 Mar 2023 08:59:54 GMT
Accept-Ranges: bytes
Etag: W/"754841ae2e53d91:0"
X-Powered-By: ASP.NET
�PNG
123**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**