404 Not Found存在httpbin.org接口测试1漏洞

# 漏洞地址

http://httpbin.org

# 参考链接

https://github.com/th3gundy/CVE-2019-7192\_QNAP\_Exploit

# 漏洞详情

一共2组payload

## 第1组payload共发送1次请求

第1组paylaod: base64('abc')

### **发送第1次请求:**

**请求数据包**

**GET /get123?key={{var2}} 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: httpbin.org
Tst: YWJj**

**请求响应包**

**HTTP/1.1 404 NOT FOUND
Server: gunicorn/19.9.0
Date: Fri, 10 Mar 2023 06:03:12 GMT
Content-Type: text/html
Content-Length: 233
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>**

**漏洞存在判断条件**

**response.status == 404**

**结果：**

**存在漏洞**

## 第2组payload共发送1次请求

第2组paylaod: md5('123456')

### **发送第1次请求:**

**请求数据包**

**GET /get123?key={{var2}} 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: httpbin.org
Tst: e10adc3949ba59abbe56e057f20f883e**

**请求响应包**

**HTTP/1.1 404 NOT FOUND
Server: gunicorn/19.9.0
Date: Fri, 10 Mar 2023 06:03:12 GMT
Content-Type: text/html
Content-Length: 233
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>**

**漏洞存在判断条件**

**response.status == 404**

**结果：**

**存在漏洞**