测试存在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

http://github.com/qmdemon/qingmu

# 漏洞详情

一共2组payload

## 第1组payload共发送2次请求

第1组paylaod: base64('abc')

### **发送第1次请求:**

**请求描述**

**用于发送测试get请求**

**请求数据包**

**GET /get?key=e10adc3949ba59abbe56e057f20f883e 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/1.1 200 OK
Server: gunicorn/19.9.0
Date: Sun, 12 Mar 2023 05:05:58 GMT
Content-Type: application/json
Content-Length: 440
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
{
"args": {
"key": "e10adc3949ba59abbe56e057f20f883e"
},
"headers": {
"Host": "httpbin.org",
"Tst": "YWJj",
"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",
"X-Amzn-Trace-Id": "Root=1-640d5db5-670cec8019070866339235ea"
},
"origin": "113.249.186.122",
"url": "http://httpbin.org/get?key=e10adc3949ba59abbe56e057f20f883e"
}**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**

### **发送第2次请求:**

**请求描述**

**用于发送测试post请求**

**请求数据包**

**POST /post?key=YWJj 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
Content-Type: application/json
Content-Length: 39
{"username":"test","password":"123456"}**

**请求响应包**

**HTTP/1.1 200 OK
Server: gunicorn/19.9.0
Date: Sun, 12 Mar 2023 05:05:58 GMT
Content-Type: application/json
Content-Length: 596
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
{
"args": {
"key": "YWJj"
},
"data": "{\"username\":\"test\",\"password\":\"123456\"}",
"files": {},
"form": {},
"headers": {
"Content-Length": "39",
"Content-Type": "application/json",
"Host": "httpbin.org",
"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",
"X-Amzn-Trace-Id": "Root=1-640d5db6-295ad4aa7c40a2c84da7ec13"
},
"json": {
"password": "123456",
"username": "test"
},
"origin": "113.249.186.122",
"url": "http://httpbin.org/post?key=YWJj"
}**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**

## 第2组payload共发送2次请求

第2组paylaod: md5('123456')

### **发送第1次请求:**

**请求描述**

**用于发送测试get请求**

**请求数据包**

**GET /get?key=e10adc3949ba59abbe56e057f20f883e 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/1.1 200 OK
Server: gunicorn/19.9.0
Date: Sun, 12 Mar 2023 05:06:00 GMT
Content-Type: application/json
Content-Length: 468
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
{
"args": {
"key": "e10adc3949ba59abbe56e057f20f883e"
},
"headers": {
"Host": "httpbin.org",
"Tst": "e10adc3949ba59abbe56e057f20f883e",
"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",
"X-Amzn-Trace-Id": "Root=1-640d5db7-56390e853460f3e23e5be288"
},
"origin": "113.249.186.122",
"url": "http://httpbin.org/get?key=e10adc3949ba59abbe56e057f20f883e"
}**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**

### **发送第2次请求:**

**请求描述**

**用于发送测试post请求**

**请求数据包**

**POST /post?key=YWJj 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
Content-Type: application/json
Content-Length: 39
{"username":"test","password":"123456"}**

**请求响应包**

**HTTP/1.1 200 OK
Server: gunicorn/19.9.0
Date: Sun, 12 Mar 2023 05:06:02 GMT
Content-Type: application/json
Content-Length: 596
Connection: keep-alive
Access-Control-Allow-Origin: \*
Access-Control-Allow-Credentials: true
{
"args": {
"key": "YWJj"
},
"data": "{\"username\":\"test\",\"password\":\"123456\"}",
"files": {},
"form": {},
"headers": {
"Content-Length": "39",
"Content-Type": "application/json",
"Host": "httpbin.org",
"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",
"X-Amzn-Trace-Id": "Root=1-640d5dba-05a216e51cc8493c4f3b126d"
},
"json": {
"password": "123456",
"username": "test"
},
"origin": "113.249.186.122",
"url": "http://httpbin.org/post?key=YWJj"
}**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**