text/html存在httpbin.org接口测试1漏洞

漏洞地址： https://httpbin.org
参考链接： https://github.com/th3gundy/CVE-2019-7192\_QNAP\_Exploit
漏洞详情：
一共发送2次请求:
发送第1次请求:
请求数据包：
GET /ge123t?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/1.1 404 NOT FOUND
Server: gunicorn/19.9.0
Date: Wed, 22 Feb 2023 09:29:02 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
发送第2次请求:
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
Token: qmteseteaajfdfjkdjfk
{"username":"test","password":"123456"}
请求响应包：
HTTP/1.1 200 OK
Server: gunicorn/19.9.0
Date: Wed, 22 Feb 2023 09:29:03 GMT
Content-Type: application/json
Content-Length: 632
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",
"Token": "qmteseteaajfdfjkdjfk",
"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=1-63f5e05f-0ab52b8137c01a5a69f2b7fe"
},
"json": {
"password": "123456",
"username": "test"
},
"origin": "125.85.85.78",
"url": "https://httpbin.org/post?key=YWJj"
}
漏洞存在判断条件：
response.status == 200
结果：
存在漏洞