HackTheBox-baby CachedView

原创

galaxy3000 于 2022-02-16 10:10:15 发布 968 收藏

分类专栏： # Web 文章标签： CTF writeup 网络安全 hackthebox 靶机

本文链接：https://blog.csdn.net/galaxy3000/article/details/122956671

Web 专栏收录该内容

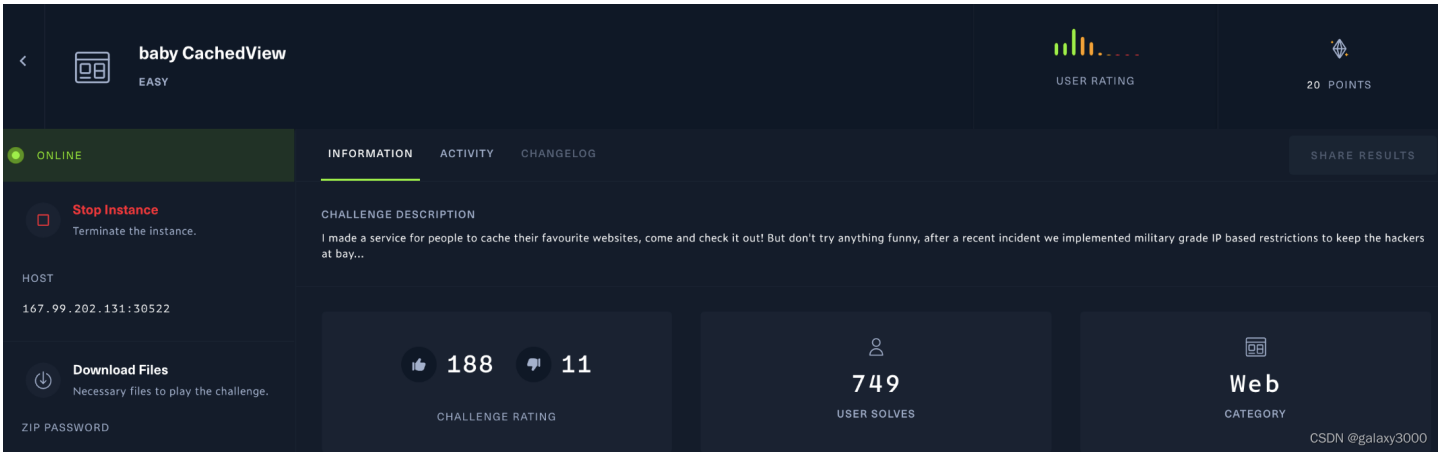
16 篇文章 0 订阅

订阅专栏

文章目录

概述

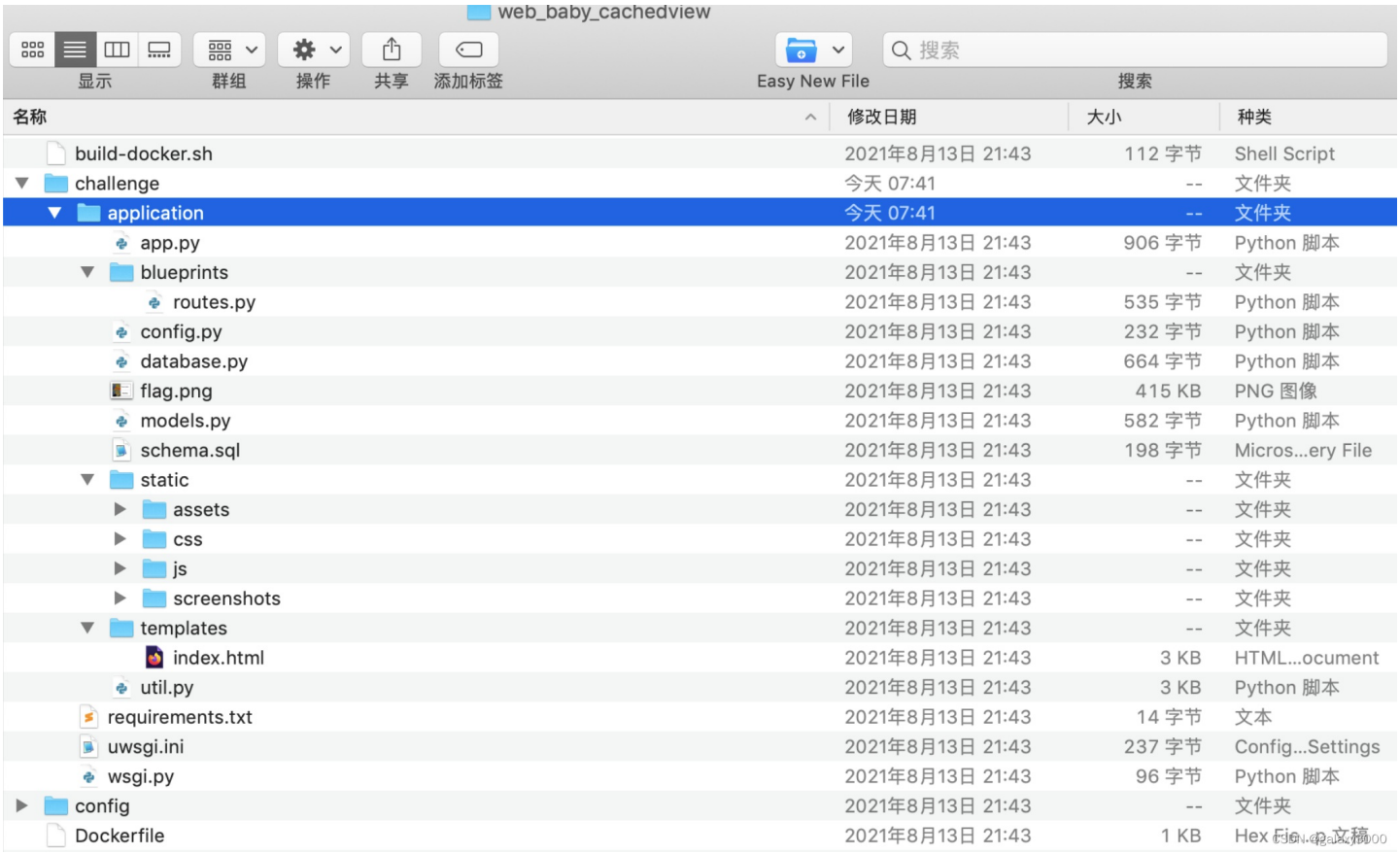
HackTheBox 网站CTF靶场Web相关题目baby CachedView，题目地址https://app.hackthebox.com/challenges/baby-cachedview，主要考察的是IP地址限制的绕过思路。



题目

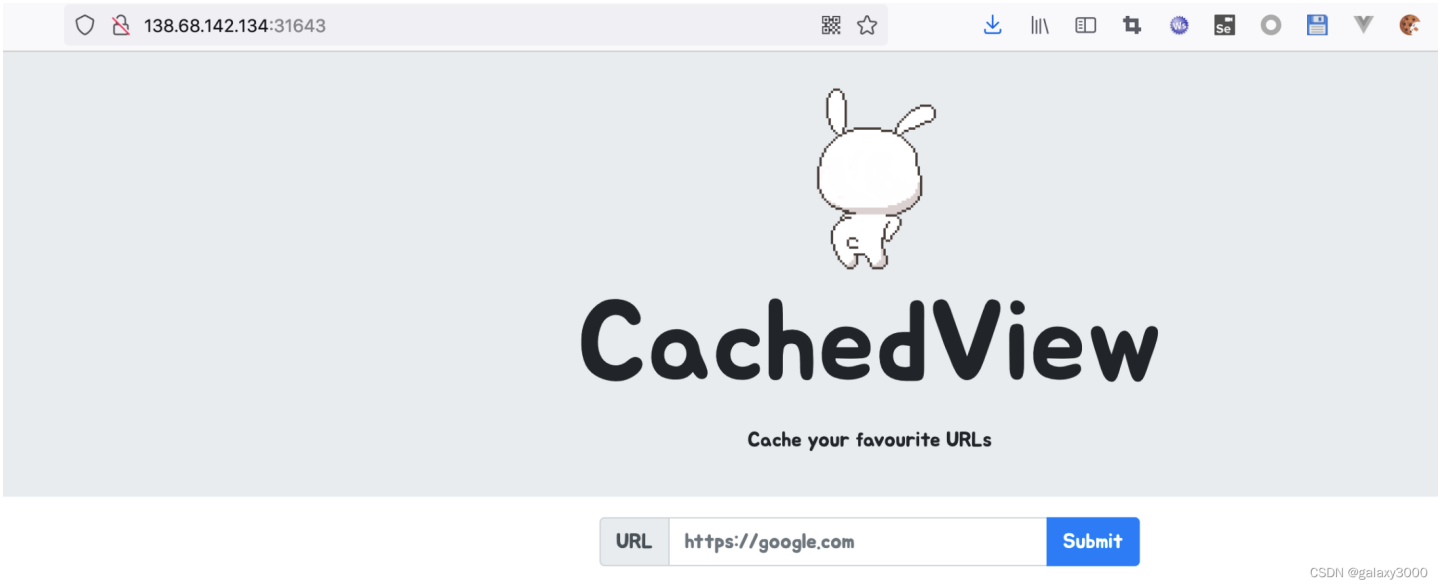
题目概述

题目提供了附件下载，解压后如图



题目提示大意为经历了安全事故后对网站的服务进行了基于IP地址的限制。

开启程序实例后，提示访问`138.68.142.134:31643`，访问http://138.68.142.134:31643，看到如下Web界面



查看requirements.txt，发现为Flask应用

```
Flask
selenium
```

源代码

routes.py

```
from flask import Blueprint, request, render_template, abort, send_file
from application.util import cache_web, is_from_localhost

web = Blueprint('web', __name__)
api = Blueprint('api', __name__)

@web.route('/')
def index():
    return render_template('index.html')

@api.route('/cache', methods=['POST'])
def cache():
    if not request.is_json or 'url' not in request.json:
        return abort(400)

    return cache_web(request.json['url'])

@web.route('/flag')
@is_from_localhost
def flag():
    return send_file('flag.png')
```

可以在路由中看到`/flag`路径，这个路由有两个装饰器，其中用到了util.py

util.py

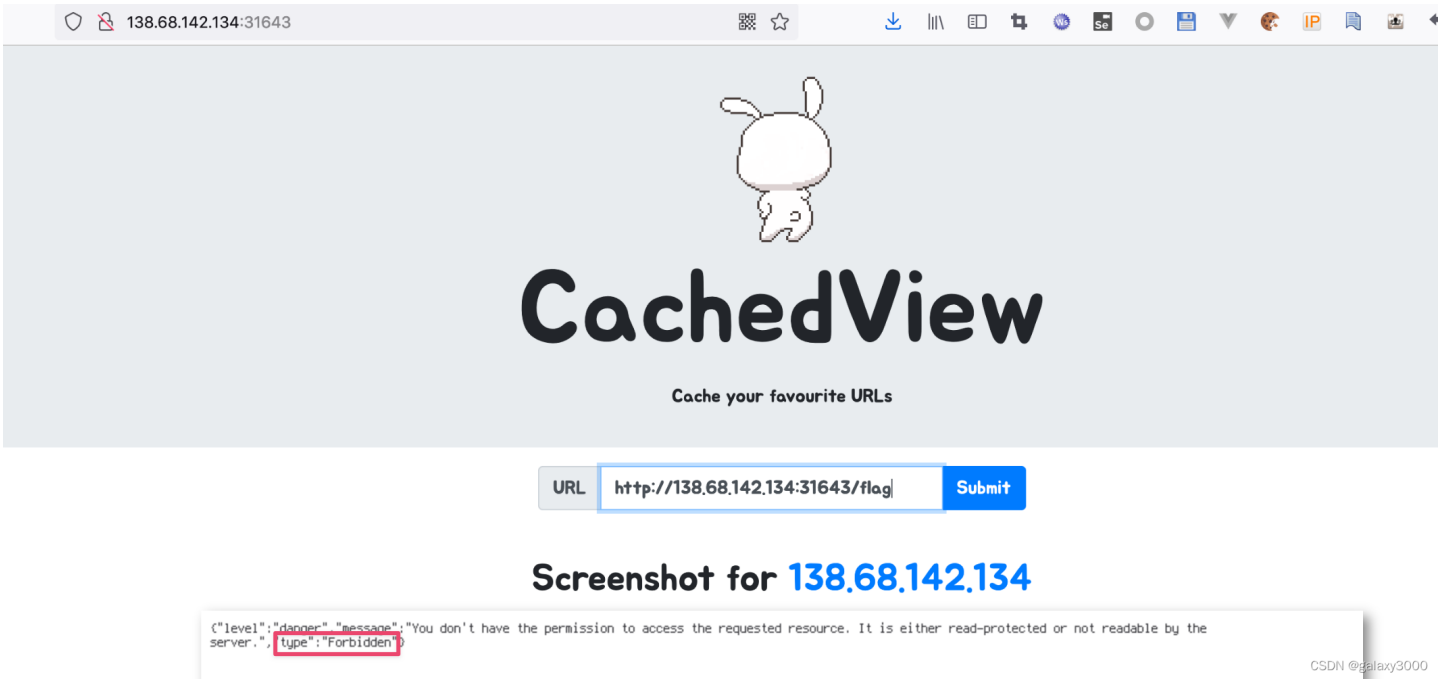
```python
def cache_web(url):
    scheme = urlparse(url).scheme
    domain = urlparse(url).hostname

    if not domain or not scheme:
        return flash(f'Malformed url {url}', 'danger')

    if scheme not in ['http', 'https']:
        return flash('Invalid scheme', 'danger')

    def ip2long(ip_addr):
        return struct.unpack('!L', socket.inet_aton(ip_addr))[0]

    def is_inner_ipaddress(ip):
        ip = ip2long(ip)
        return ip2long('127.0.0.0') >> 24 == ip >> 24 or \
                ip2long('10.0.0.0') >> 24 == ip >> 24 or \
                ip2long('172.16.0.0') >> 20 == ip >> 20 or \
                ip2long('192.168.0.0') >> 16 == ip >> 16 or \
                ip2long('0.0.0.0') >> 24 == ip >> 24

    if is_inner_ipaddress(socket.gethostbyname(domain)):
        return flash('IP not allowed', 'danger')

    return serve_screenshot_from(url, domain)

def is_from_localhost(func):
    @functools.wraps(func)
    def check_ip(*args, **kwargs):
        if request.remote_addr != '127.0.0.1' or request.referrer:
            return abort(403)
        return func(*args, **kwargs)
    return check_ip
```


源代码分析

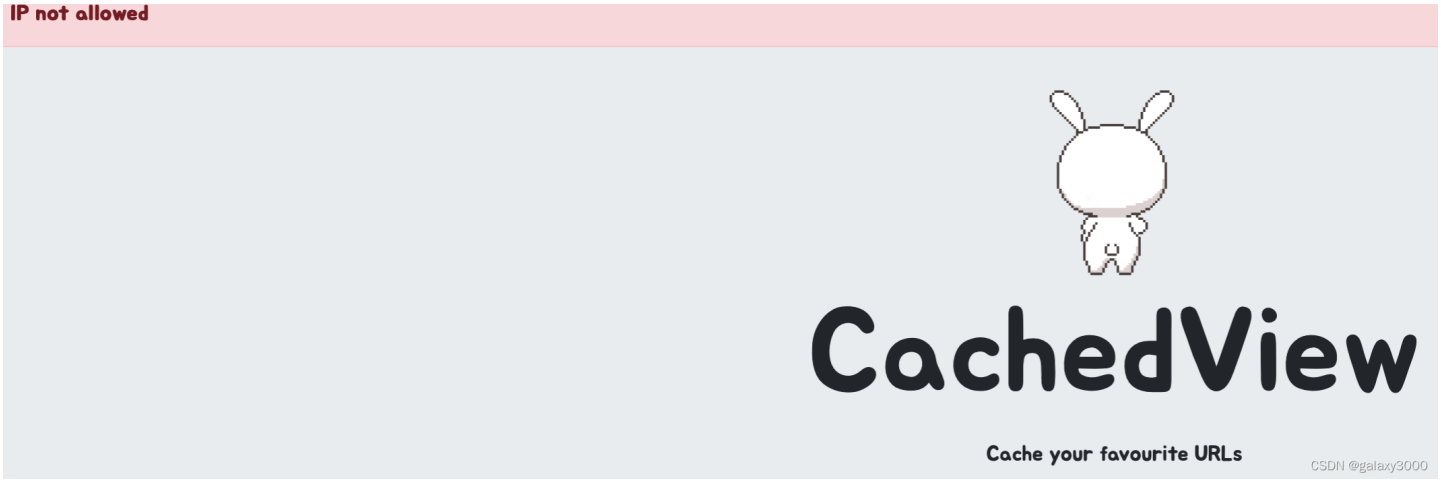
在目标首页提交的源代码，由`/cache`响应，经过`cache_web`函数处理后返回结果，在`cache_web`函数中有IP地址的限制，主要是对127网段、172.16网段、192.168等内网网段的限制。

而如果访问`/flag`路径，会被装饰器中的`check_ip`处理，如果不是本地地址（127.0.0.1）会被禁止。

实际验证，首先在输入框输入http://138.68.142.134:31643/flag，触发了`check_ip`的检查



如果在输入框输入http://127.0.0.1:31643/flag，触发了`cache_web`的检查，提示**IP not allowed**



解题思路

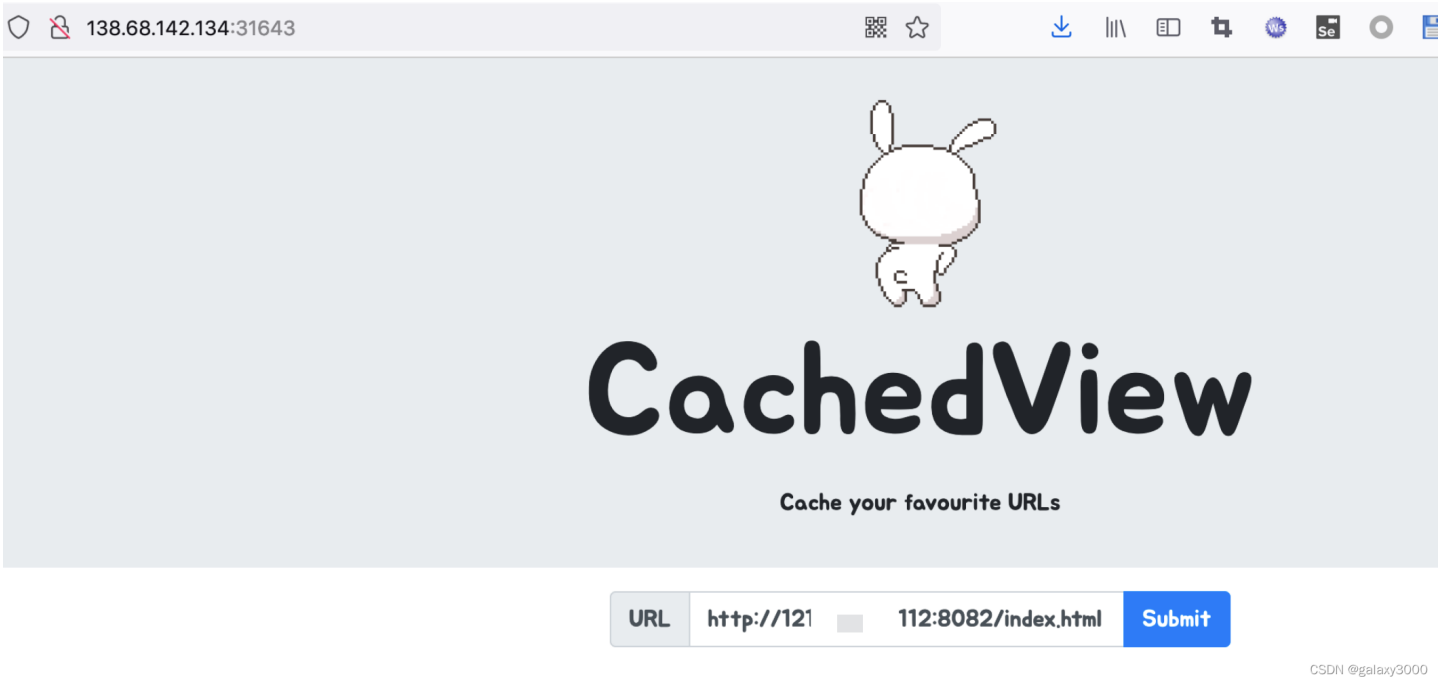
在云服务器上部署Web服务，输入框输入地址为云服务器地址，通过`cache_web`的检查，而服务器上Web的内容为本地访问flag

题目解答

在云服务器上部署网页index.html，内容为

```
<meta http-equiv="refresh" content="0; URL=http://127.0.0.1:31643/flag" />
```

在输入框输入云服务器地址



得到flag