

论src漏洞挖掘的前期信息 收集

fcmit.cc

二零卫士·木星安全实验室

郑铭扬 (root0er)



About Me

ID: root0er

目前就职于： 二零卫士•木星安全实验室

百度、阿里、滴滴、京东等src响应平台活跃白帽子

icmit.cc



目录

- 常规的资产收集
- 搜索引擎的妙用
- 企业动态早知道
- 我的src漏洞挖掘技巧
- 综合案例分析

fcmit.cc



- 常规的资产收集

fcmit.cc



子域名的收集技巧

- 子域名爆破: subDomainsBrute, Sublist3r, subfinder

```
[0] <git:(master 2e1b5cd*) > python subDomainsBrute.py baidu.com
[+] Validate DNS servers
[+] Server 223.6.6.6 < OK > Found 4
[+] 4 available DNS Servers found in total
[+] Init 6 scan process.
[*] 184 found, 7005 scanned in 17.0 seconds, 8288 groups left
KeyboardInterrupt
2019-05-25T07:00:50Z
[ERROR] User aborted the scan!
[+] All Done, 184 found, 7014 scanned in 17.5 seconds.
[+] The output file is baidu.com.txt
```

```
[2] <> subfinder -d baidu.com
=====
Subfinder v1.1.3 github.com/subfinder/subfinder
=====
```

fcmit.cc

```
[0] <> python sublist3r.py -d baidu.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[-] Enumerating subdomains now for baidu.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
```



- 在线的子域名收集平台：fofa、myssl、云悉资产、VirusTotal, shodan



fcmit.cc



端口扫描

- 漏洞挖掘中的端口扫描神器：nmap、masscan

```
root@kali:~/sub000MATHSBrute]# [2019-03-23 03:42:34]
root@kali:~/sub000MATHSBrute]# [0] <git:(master 2e1b5cd*) > nmap -h
nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given port
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

```
root@kali:~/sub000MATHSBrute]# [0] <git:(master 2e1b5cd*) > masscan -h
Usage:
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000
scan some web ports on 10.x.x.x at 10kpps
masscan --nmap
list those options that are compatible with nmap
masscan -p80 10.0.0.0/8 --banners -oB <filename>
save results of scan in binary format to <filename>
masscan --open --banners --readscan <filename> -oX <savefile>
read binary scan results in <filename> and save them as xml in
```



目录扫描

敏感文件扫描：dirsearch、burpsuite、dirb

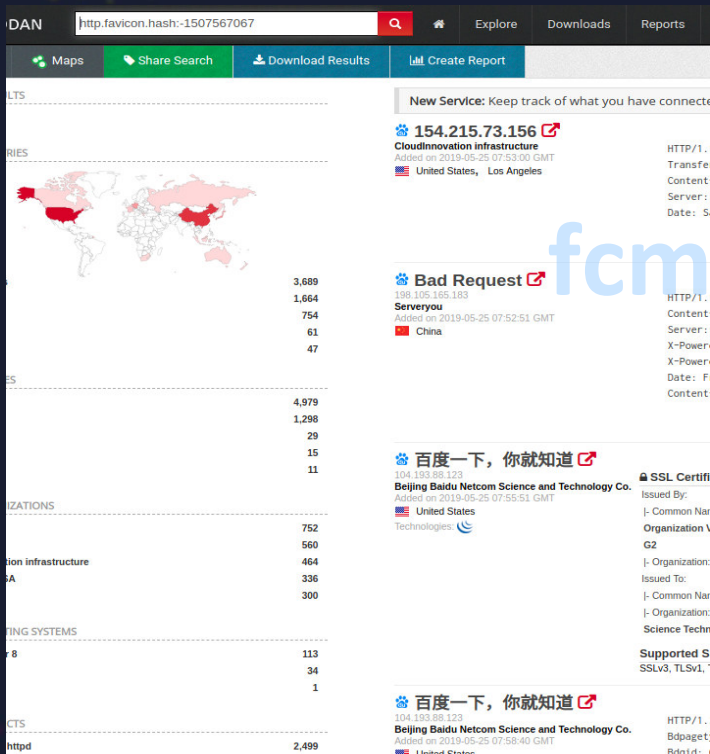
```
Usage: dirsearch.py [-u|--url] target [-e|--extensions] extensions [options]
Options:
  -h, --help            show this help message and exit
  -u URL, --url=URL      URL target
  -L URLLIST, --url-list=URLLIST
                        URL list target
  -e EXTENSIONS, --extensions=EXTENSIONS
                        Extension list separated by comma (Example: php,asp)
  -w WORDLIST, --wordlist=WORDLIST
                        Wordlist to use
  -l, --lowercase        Force extensions for every wordlist entry (like in
                        DirBuster)
  -f, --force-extensions
                        Force extensions for every wordlist entry (like in
                        DirBuster)
```

fcmit.cc



厂商ip段的收集

大范围收集厂商ip段: shodan、https://bgp.he.net



AS Info	Graph v4	Graph v6	Prefixes v4	Prefixes v6	Peers v4	Peers v6	Whois	IRR	IP
Prefix	Description								
45.113.195.0/24		AS55967							
106.12.0.0/16		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.0.0/18		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.0.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.2.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.4.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.6.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.8.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.10.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.12.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.14.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.16.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.18.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.20.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.22.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.24.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.26.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.28.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.30.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							
106.12.32.0/23		Beijing Baidu Netcom Science and Technology Co., Ltd.							

整理报告

EyeWitness -- 可用于网站截图，以及提供一些服务器头信息，并在可能的情况下识别默认凭据。

Table of Contents

- [Uncategorized \(Page 1\)](#)
- [401/403 Unauthorized \(Page 9\)](#)
- [404 Not Found \(Page 10\)](#)

fcmit.cc

Uncategorized	222
401/403 Unauthorized	15
404 Not Found	23
Errors	101
Total	361

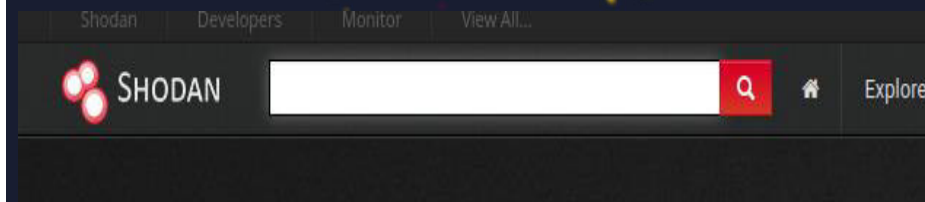
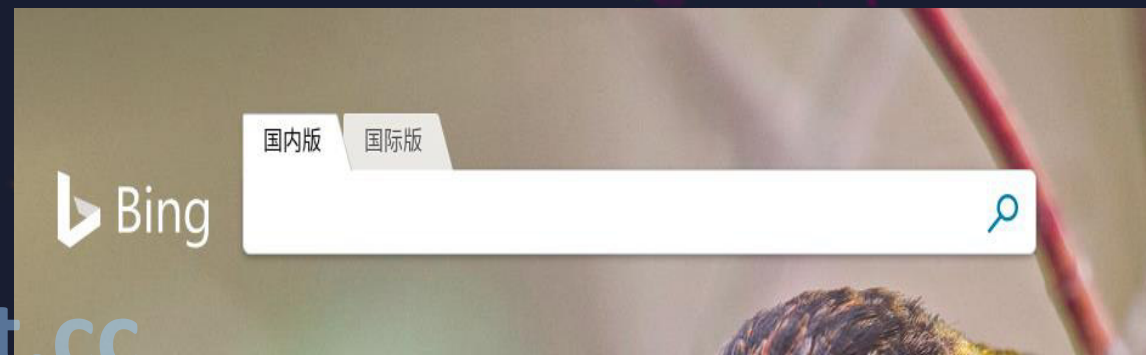


- 搜索引擎的妙用

fcmit.cc



挖洞必备的几个搜索引擎:百度,谷歌,bing,shodan



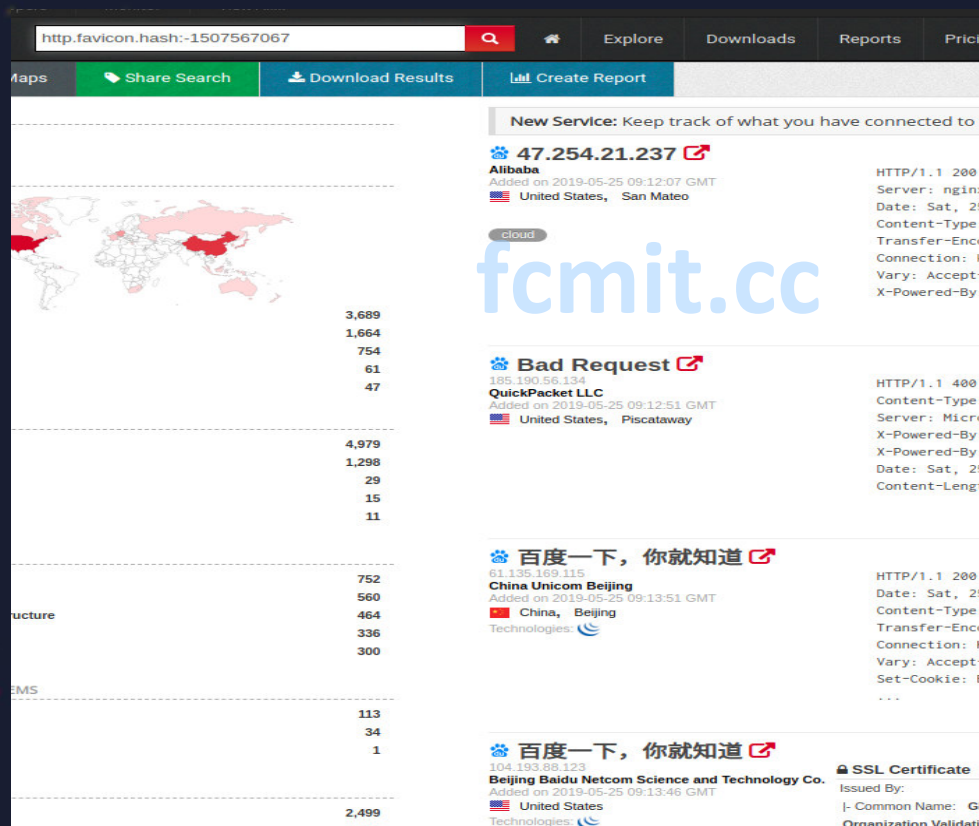
fcmit.cc

不同的搜索引擎对于同一个站点收录的内容是不同的，使用多个搜索引擎进行搜索，会达到事半功倍的效果。对于厂商众测，需要做到的就是争分夺秒，我们需要巧用搜索引擎来摸清站点结构，借助搜索引擎不仅能发现隐藏系统，更能在众测中获得不菲的奖金。



最可怕的搜索引擎 -- shodan

- 通过搜索厂商logo来获取厂商资产信息



The screenshot displays the Shodan search engine interface. The search bar at the top contains the query `http.favicon.hash:-1507567067`. Below the search bar, there are tabs for `Maps`, `Share Search`, `Download Results`, and `Create Report`. The main content area shows search results for the query. On the left, there is a world map with red dots indicating the locations of the search results. To the right of the map, there is a list of results. Each result includes a company logo, the company name, the IP address, the date added, the location, and the HTTP status code. The results are as follows:

Company	IP Address	Date Added	Location	HTTP Status
Alibaba	47.254.21.237	2019-05-25 09:12:07 GMT	United States, San Mateo	200
Bad Request	185.190.56.134	2019-05-25 09:12:51 GMT	United States, Piscataway	400
China Unicom Beijing	61.135.169.115	2019-05-25 09:13:51 GMT	China, Beijing	200
Beijing Baidu Netcom Science and Technology Co.	104.193.88.123	2019-05-25 09:13:46 GMT	United States	200

On the right side of the screenshot, there is a large blue watermark that reads `fcmit.cc`. Below the watermark, there is a section titled `SSL Certificate` with the following information:

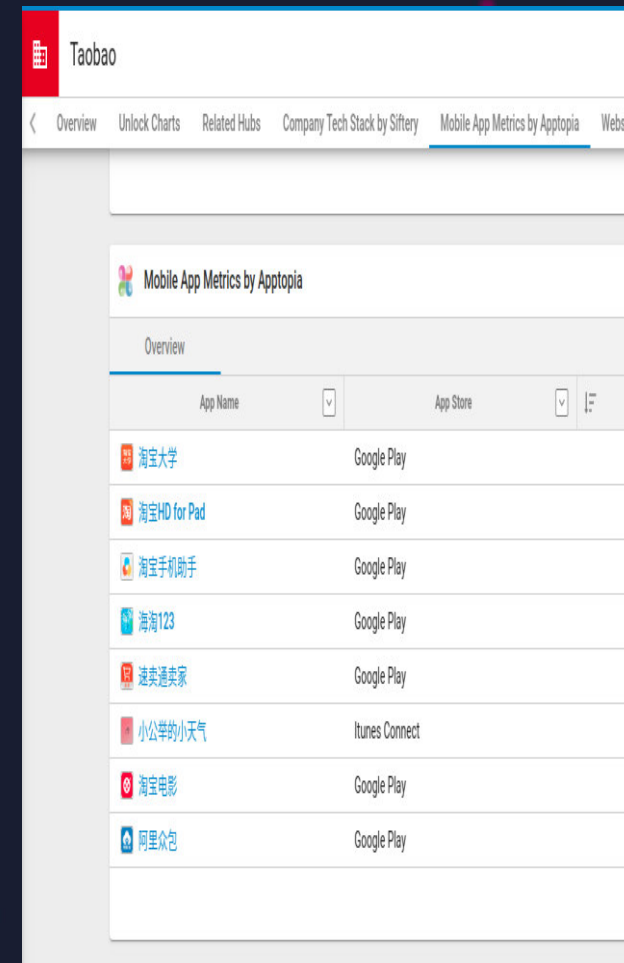
- Issued By:
- Common Name:
- Organization Validation:

- 企业动态早知道

fcmit.cc



公众号、app的收集：微信、天眼查、crunchbase



利用企查查监控站点

企查查
qichacha.com

请输入企业名称、人名、产品名、地址等关键词

Q

首页 个人中心 企业中心

企鹅cvtiqq
[立即开通vip](#)

消息中心

雷达监控

监控概览

监控动态

监控列表

监控日报

个人中心

工商变更	司法诉讼
0条	0条

北京小桔科技有限公司

变动类型	风险级别	变更/新增类型	变动日期	
经营状况	良好信息	对外投资	2019-05-21	对外投资移除一家公司滴滴出行科技有限公司

2019-05-18



- 我的src漏洞挖掘技巧

fcmit.cc



新手常见的挖洞困境

错误摘要

HTTP 错误 404.0 - Not Found

您要找的资源已被删除、已更名或暂时不可用。

无法找到该页

您正在搜索的页面可能已经删除、更名或暂时不可用。

请尝试以下操作：

- 确保浏览器的地址栏中显示的网站地址的拼写和格式正确无误。
- 如果通过单击链接而到达了该网页，请与网站管理员联系，通知他们该链接的格式不正确。
- 单击[后退](#)按钮尝试另一个链接。

HTTP 错误 404 - 文件或目录未找到。
Internet 信息服务 (IIS)

技术信息（为技术支持人员提供）

- 转到 [Microsoft 产品支持服务](#) 并搜索包括“HTTP”和“404”的标题。
- 打开“IIS 帮助”（可在 IIS 管理器 (inetmgr) 中访问），然后搜索标题为“网站设置”、“常规管理任务”和“关于自定义错误消息”的主题。

404 Not Found

nginx



不要错过任何一个站点，细心决定成败！



工单详情:

工单详情:

是否成立:

责任归属:

关单类型:

工单详情:

退回

流转至EP

上一张

漏洞挖掘应该重点关注的漏洞

- 跨域劫持漏洞
- 业务逻辑漏洞

tcmit.cc



- 综合案例分析

fcmit.cc



经过前期的一系列信息收集，遇见一个登录站点：



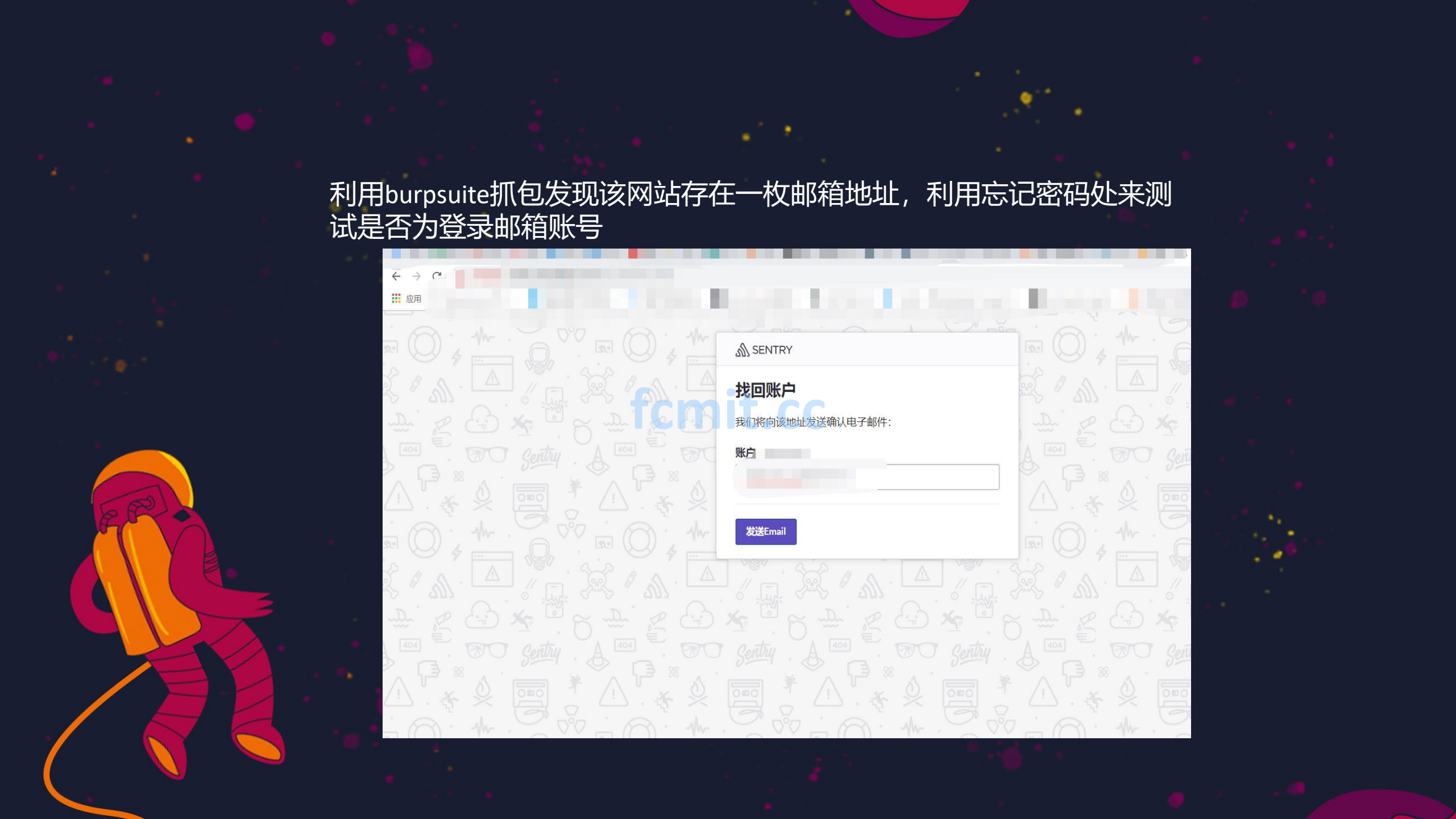
Django 管理

用户名:

密码:

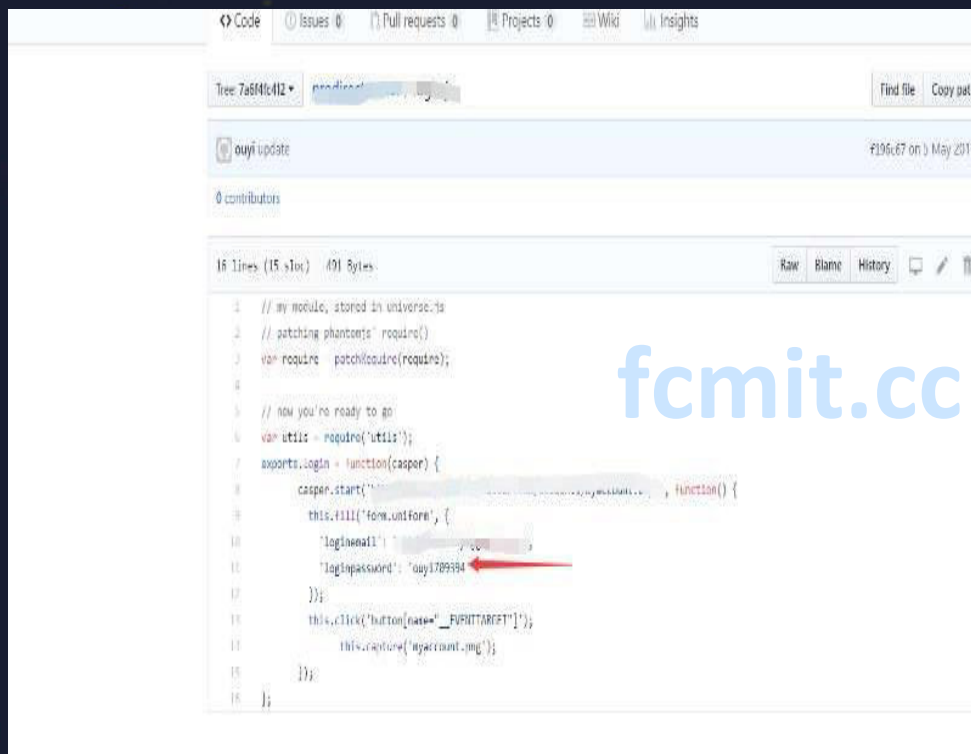
登录





爆破不是唯一的手段

利用github查看是否存在泄密



Tree: 7a6f41c412

Find file Copy path

ouyi update F196:67 on 3 May 2017

0 contributors

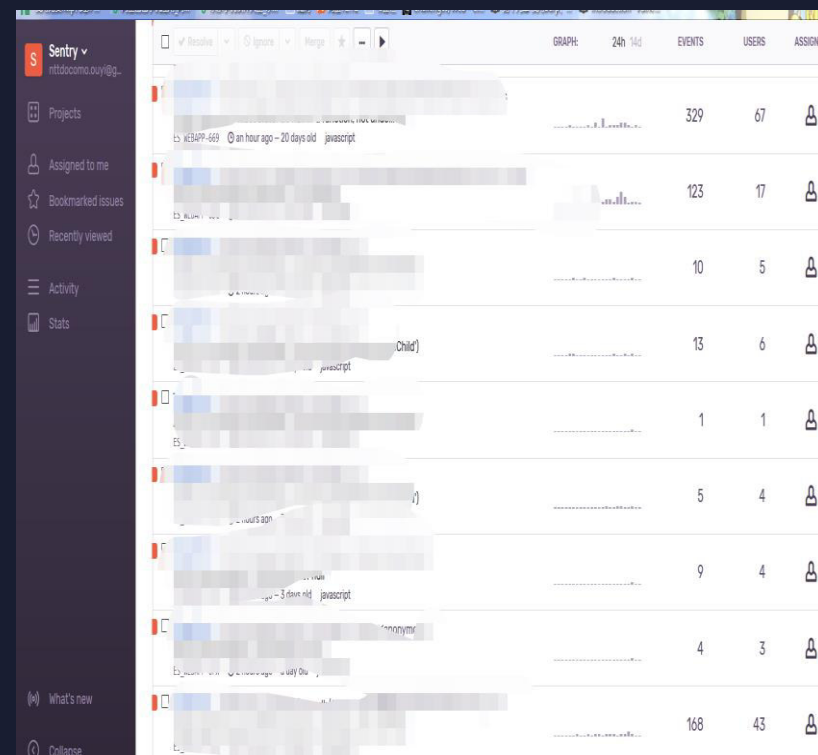
15 lines (15 slot) 491 Bytes

Raw Blame History

```
1 // my module, stored in universe.js
2 // patching phantomjs require()
3 var require = patchRequire(require);
4
5 // now you're ready to go
6 var utils = require('utils');
7 exports.login = function(casper) {
8   casper.start('...', function() {
9     this.fill('form-uniform', {
10       'loginemail': '...',
11       'loginpassword': 'ouy1789394'
12     });
13     this.click('button[name="_FVMITARFT"]');
14     this.capture('myaccount.png');
15   });
16 }
```

fcmit.cc

成功打入后台



Event ID	Message	Count	Users
...	...	329	67
...	...	123	17
...	...	10	5
...	...	13	6
...	...	1	1
...	...	5	4
...	...	9	4
...	...	4	3
...	...	168	43



THANKS

fcmil.cc

