漏洞挖掘经验分享

目录

战前准备

- 挖SRC好比是一场一对多的较量，对手是研发测试运维安全等人员，也是跟自己打一场持久战。
- 挖洞难在你选的目标不知道被多少人挖过，反反复复一轮又一轮。
- 挖洞容易在产品系统在不断的更新迭代，谁也不敢说自己完整的测过每一个功能点。
- 心态很重要。

了解目标SRC

- 1、首先是评分标准，不同SRC的评分标准是不一样的，先看哪些漏洞类型会被忽略处理，以免浪费时间。
- 2、其次是授权测试范围，尽量不要超出范围测试，很大可能做无用功，还冒非法测试的风险。
- 3、遵循安全测试规范，比如发现SQL注入不能拖库，读取数据库名即可。
- 4、最后看看礼品，有没有值得兑换的，啥时候发货。

信息收集

- 1、什么是信息收集、信息收集的重要性、具体怎么搞可以上FreeBuf和先知社区搜索文章
- 2、信息收集的目标：目标子域名、IP端口、系统服务、框架组件、
- 产品业务、APP、公众号、小程序等
- 3、半自动化思路：
- 脚本工具收集子域名->合并去重验证有效性->识别网站“指纹”信息->截取屏幕快照->获取IP->扫描开放端口及服务->输出

资产侦察灯塔系统

资产灯塔系统

任务管理

搜索

admin 修改密码

zhuanzhuan.com相关资产

IP | SSL证书 | 子域名 | 站点 | 服务 | 文件泄露 | URL信息

IP: 请输入站点进行搜索 端口: 请输入主机名进行搜索 操作系统: 请输入标题进行搜索 域名: 请输入Web Server进行搜索 状态码: 请输入状态码进行搜索

标头: 请输入标头进行搜索 指 纹: 请输入指 纹进行搜索 favicon hash: 请输入favicon hash进行搜索

序号	站点	标题	headers	finger	截图
11	https://dev-open.zhuanzhuan.com	Welcome to tengine!	HTTP/1.1 200 OK Server: Tengine Date: Tue, 20 Oct 2020 07:48:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 555 Last-Modified: Mon, 17 Jul 2017 06:27:03 GMT Connection: keep-alive ETag: "596c58b7-22b" Accept-Ranges: bytes	Tengine	
12	https://www.zhuanzhuan.com Favicon Hash: -1241002485	【转转】二手交易网,二手手机交易网,58闲置交易APP,转转客服	HTTP/1.1 200 OK Server: Tengine Date: Tue, 20 Oct 2020 07:48:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Thu, 15 Oct 2020 12:21:23 GMT Vary: Accept-Encoding ETag: W/"5f883ec3-a28" Content-Encoding: gzip Set-Cookie: idzz=c5/nR1+Olkhdl0lyErqsAg==; expires=T P3P: policyref="/w3c/p3p.xml", CP="CUR ADM OUR NOR S	Baidu Analytics (百度统计) Tengine jQuery	

关于漏扫

司组件 — Shiro

关漏洞

V ID	提交时间	漏洞等级	漏洞名称
V-98351	2020-08-18	▬▬▬	Apache Shiro 权限绕过漏洞（CVE-2020-13933）
V-98196	2020-03-30	▬▬▬	Apache Shiro 628 权限绕过漏洞（CVE-2020-2957）
V-98104	2019-11-20	▬▬▬	Apache Shiro 721 Padding Oracle漏洞
V-92540	2016-11-17	▬▬▬	Apache Shiro远程安全限制绕过漏洞（CVE-2016-6802）
V-92180	2016-07-25	▬▬▬	Shiro RememberMe 1.2.4 反序列化导致的命令执行漏洞

面对众多站点，怎么开始下手，先漏扫看能不能找到突破口，看看有没有开放危险端口，有没有使用含有历史漏洞的系统、框架组件。

不要将希望过多寄托在漏扫，除非你的扫描器更牛逼。

关于扫描

- 1、很多新手白帽喜欢直接用重量级工具扫，比如AWVS，不仅费时还容易被封IP。这里推荐先用BBScan扫下，当然大多时候是发现不了什么问题。
- 2、路径扫描，对于一些403、404等没有内容的站点，爆破API接口、端点、路径会有意想不到的收获。
- 3、扫描端口，直接扫1-65535个端口是非常粗暴的。目标小的话还可以，量大的话建议扫常用的几百个端口就行。
- 4、去重，像扫58子域名的话，有很多以城市拼音作为子域名。每个都扫的话有点重复劳动力，可以先使用脚本去除掉城市子域名

58同城

深圳58同城 >>

全国58同镇 >>

新

周边城市推荐: 深圳 中国香港 东莞 珠海 中山 中国澳门 广州 顺

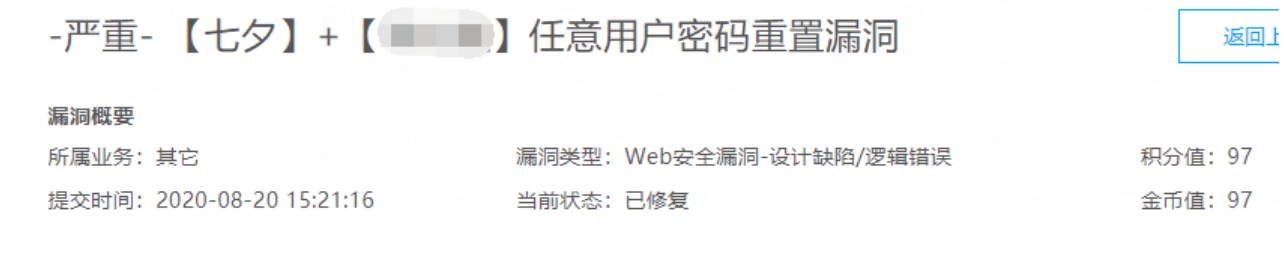
关注58同镇，掌握家乡信息

热门城市 北京 上海 广州 深圳 成都 杭州 南京 天津 武汉 重庆

城市选择 省份 城市 直接搜索 搜索

按省份首字母选择

A	安徽	合肥	芜湖	蚌埠	阜阳	淮南	安庆	宿州	六安	淮北	滁州	马鞍山	铜陵	宣城	亳州	黄山	池州	巢湖	和县	霍邱	桐城	宁国	天长
		东至	无为																				
F	福建	福州	厦门	泉州	莆田	漳州	宁德	三明	南平	龙岩	武夷山	石狮	晋江	南安	龙海	上杭	福安	福鼎	安溪	永春	永安	漳浦	
	广东	深圳	广州	东莞	佛山	中山	珠海	惠州	江门	汕头	湛江	肇庆	茂名	揭阳	梅州	清远	阳江	韶关	河源	云浮	汕尾	潮州	台山
		阳春	顺德	惠东	博罗	海丰	开平	陆丰															
	广西	南宁	柳州	桂林	玉林	梧州	北海	贵港	钦州	百色	河池	来宾	贺州	防城港	崇左	桂平	北流	博白	岑溪				



- 大多新手认为大佬挖洞使用了很多奇淫巧技，自己挖不到是因为掌握的技巧不够多。我认为是不够细心和自我否定。
- 就潜意识里认为漏洞都被大佬挖完了、这里不会存在这么简单的漏洞，从而说服自己不去尝试。

相信自己

勇于尝试

目标选择

- 没有扫描出突破口，选哪些站点进行测试
- 0、优先选择第三方系统，看是否含有历史漏洞直接秒。
- 1、然后是能注册的后台系统。后台系统功能多，越权漏洞重点测。
- 2、其次是能注册的用户系统。里面业务多，每个功能点走一遍。
- 3、没有账号的系统，弱口令、未授权访问接口、密码重置漏洞想方设法进后台。

关于工具

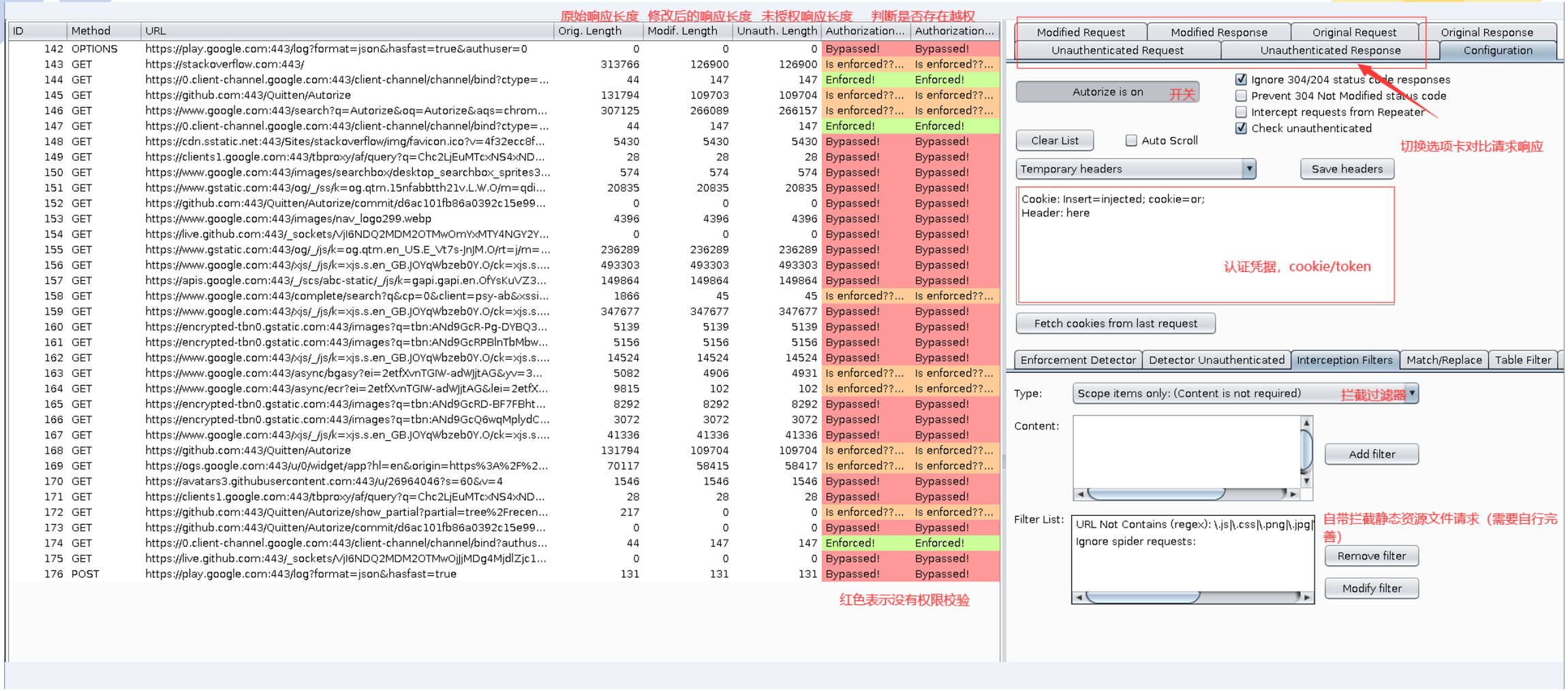
- 工具可以提高工作效率，不能不利用工具也不能只会利用工具。
- 信息收集：域名扫描（OneForAll）、IP端口探测（Nmap）、敏感文件路径扫描(BBScan、dirsearch)、git源码扫描(github-search)、网站指纹识别(WhatWeb)、框架组件信息（ wappalyzer ）
- 漏洞挖掘：抓包（BurpSuite）、弱口令爆破(hydra)、漏洞库（CVE/SeeBug）、payload合集（PayloadsAllTheThings）
- 资产监控： XSS平台、 dnslog平台、Git泄露监控、app更新监控、域名端口变更监控、产品业务舆情监控

关于插件

- BurpSuite集成了很多工具，也可以自己研发插件。
- 越权测试：Autorize
- 日志插件：Logger++
- 个性化扫描器：BurpBounty

Autorize

- 下载安装后，Burp上会有Autorize的选项卡。
- Configuration选项里会有默认配置，可以自行配置。
- 将低权限的账号认证信息（cookie/token）复制到文本框。
- 配置拦截器，过滤掉静态资源文件以及不属于测试目标的URL。
- 浏览器配置代理将流量传递给Burp，插件运行后会自动执行检查授权。
- 左侧显示请求的URL和执行状态，红色意味存在越权，绿色意味不存在越权，黄色意味不确定。
- 是否存在越权是根据替换认证信息，然后对比响应长度来判断的。如果请求的内容，高权限和低权限响应的长度一致表示不存在权限校验，删除认证信息也响应一致表示存在未授权访问漏洞。
- 可以指定特定的URL查看原始/修改/未授权的请求/响应，对比差异。


原始响应长度 修改后的响应长度 未授权响应长度 判断是否存在越权
ID Method URL Orig. Length Modif. Length Unauth. Length Authorization... Authorization...
142 OPTIONS https://play.google.com:443/log?format=json&hasfast=true&authuser=0 0 0 0 Bypassed! Bypassed!
143 GET https://stackoverflow.com:443/ 313766 126900 126900 Is enforced??... Is enforced??...
144 GET https://0.client-channel.google.com:443/client-channel/channel/bind?ctype=... 44 147 147 Enforced! Enforced!
145 GET https://github.com:443/Quitten/Autorize 131794 109703 109704 Is enforced??... Is enforced??...
146 GET https://www.google.com:443/search?q=Autorize&oq=Autorize&aqs=chrom... 307125 266089 266157 Is enforced??... Is enforced??...
147 GET https://0.client-channel.google.com:443/client-channel/channel/bind?ctype=... 44 147 147 Enforced! Enforced!
148 GET https://cdn.sstatic.net:443/Sites/stackoverflow/img/favicon.ico?v=4f32ecc8f... 5430 5430 5430 Bypassed! Bypassed!
149 GET https://clients1.google.com:443/tbproxy/af/query?q=Chc2LjEuMTcxNS4xND... 28 28 28 Bypassed! Bypassed!
150 GET https://www.google.com:443/images/searchbox/desktop_searchbox_sprites3... 574 574 574 Bypassed! Bypassed!
151 GET https://www.gstatic.com:443/og/_/ss/k=og.qtm.15nfabbtth21v.L.W.O/m=qdi... 20835 20835 20835 Bypassed! Bypassed!
152 GET https://github.com:443/Quitten/Autorize/commit/d6ac101fb86a0392c15e99... 0 0 0 Bypassed! Bypassed!
153 GET https://www.google.com:443/images/nav_logo299.webp 4396 4396 4396 Bypassed! Bypassed!
154 GET https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOmYxMTY4NGY2Y... 0 0 0 Bypassed! Bypassed!
155 GET https://www.gstatic.com:443/og/_/js/k=og.qtm.en_US.E_Vt7s-JnJM.O/rt=j/m=... 236289 236289 236289 Bypassed! Bypassed!
156 GET https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s.... 493303 493303 493303 Bypassed! Bypassed!
157 GET https://apis.google.com:443/_/scs/abc-static/_/js/k=gapi.gapi.en.OfYsKuVZ3... 149864 149864 149864 Bypassed! Bypassed!
158 GET https://www.google.com:443/complete/search?q&cp=0&client=psy-ab&xssi... 1866 45 45 Is enforced??... Is enforced??...
159 GET https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s.... 347677 347677 347677 Bypassed! Bypassed!
160 GET https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcR-Pg-DYBQ3... 5139 5139 5139 Bypassed! Bypassed!
161 GET https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcRPBlnTbMbw... 5156 5156 5156 Bypassed! Bypassed!
162 GET https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s.... 14524 14524 14524 Bypassed! Bypassed!
163 GET https://www.google.com:443/async/bgasy?ei=2etfXvnTGIW-adWJjtAG&yv=3... 5082 4906 4931 Is enforced??... Is enforced??...
164 GET https://www.google.com:443/async/ecr?ei=2etfXvnTGIW-adWJjtAG&lei=2etfX... 9815 102 102 Is enforced??... Is enforced??...
165 GET https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcRD-BF7FBht... 8292 8292 8292 Bypassed! Bypassed!
166 GET https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcQ6wqMplydC... 3072 3072 3072 Bypassed! Bypassed!
167 GET https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s.... 41336 41336 41336 Bypassed! Bypassed!
168 GET https://github.com:443/Quitten/Autorize 131794 109704 109704 Is enforced??... Is enforced??...
169 GET https://ogs.google.com:443/u/0/widget/app?hl=en&origin=https%3A%2F%2... 70117 58415 58417 Is enforced??... Is enforced??...
170 GET https://avatars3.githubusercontent.com:443/u/26964046?s=60&v=4 1546 1546 1546 Bypassed! Bypassed!
171 GET https://clients1.google.com:443/tbproxy/af/query?q=Chc2LjEuMTcxNS4xND... 28 28 28 Bypassed! Bypassed!
172 GET https://github.com:443/Quitten/Autorize/show_partial?partial=tree%2Frecen... 217 0 0 Is enforced??... Is enforced??...
173 GET https://github.com:443/Quitten/Autorize/commit/d6ac101fb86a0392c15e99... 0 0 0 Bypassed! Bypassed!
174 GET https://0.client-channel.google.com:443/client-channel/channel/bind?authus... 44 147 147 Enforced! Enforced!
175 GET https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOjjjMDg4MjdlZjc1... 0 0 0 Bypassed! Bypassed!
176 POST https://play.google.com:443/log?format=json&hasfast=true 131 131 131 Bypassed! Bypassed!
红色表示没有权限校验
Modified Request
Modified Response
Original Request
Original Response
Unauthenticated Request
Unauthenticated Response
Configuration
Autorize is on
开关
Ignore 304/204 status code responses
Prevent 304 Not Modified status code
Intercept requests from Repeater
Check unauthenticated
切换选项卡对比请求响应
Clear List
Auto Scroll
Temporary headers
Save headers
Cookie: Insert=injected; cookie=or;
Header: here
认证凭据，cookie/token
Fetch cookies from last request
Enforcement Detector
Detector Unauthenticated
Interception Filters
Match/Replace
Table Filter
Type:
Scope items only: (Content is not required)
拦截过滤器
Content:
Add filter
Filter List:
URL Not Contains (regex): \.js|\.css|\.png|\.jpg|
Ignore spider requests:
自带拦截静态资源文件请求（需要自行完善）
Remove filter
Modify filter