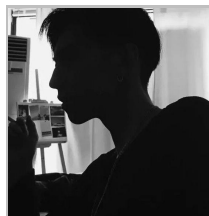


你与SRC挖洞只差一小时

难度系数：★★★★☆



本期大咖

大咖ID：小陈

大咖简介：

简介：w3bsafe核心成员，网络尖刀s小队成员，一枚专心研究信息安全的技术爱好者，混迹于各大漏洞平台，热爱技术分享，目前专注技能修炼中

内容目录

- 1、SRC就是一场游戏
- 2、快速有效的精准定位
- 3、漏洞挖掘小技巧
- 4、扩展思维—漏洞案例分享

大咖面对面

该信息安全技术公益讲座由漏洞银行方主办
每周五晚20:00，业内大咖与你零距离分享
答疑解惑 | 资源交换 | 剖析动态 | 认知升级

众多专家与你我共同扬帆，畅游知识海洋
加入我们的技术社群（Q群 598562771）

2019

大咖面对面

你与SRC挖洞只差一小时

W3bSafe Team

主讲：小陈

漏洞银行官网：www.bugbank.cn 大咖团队官网：www.w3bsafe.cn

参与讲座 | 现场答疑 | 后续交流 漏洞银行技术社群：598562771 (Q群号)

目录

1. SRC就是一场游戏
2. 快速有效的精准定位
3. 漏洞挖掘小技巧
4. 扩展思维—漏洞案例分享



1 SRC就是一场游戏

1.1 SRC是什么游戏？

- 既然是一场游戏，我们首先肯定是要遵守游戏规则

- 以某SRC为例：

【低】业务等级系数【1-10】，基础安全币【1-5】，本等级包括：

1. 本地拒绝服务漏洞。包括但不限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等。
2. 轻微信息泄漏。包括但不限于路径信息泄漏、非核心系统的 SVN 信息泄漏、PHPinfo、异常信息泄露，以及客户端应用本地 SQL 注入（仅泄漏数据库名称、字段名、cache 内容）、日志打印、配置信息、异常信息等。
3. 难以利用但存在安全隐患的漏洞。包括但不限于难以利用的 SQL 注入点、可引起传播和利用的 Self-XSS、需构造部分参数且有一定影响的 CSRF。
4. 其他只能造成轻微影响的漏洞，反射型 XSS（包括反射型 DOM-XSS）、普通 CSRF、URL 跳转漏洞。例如：CRLF 漏洞、URL 跳转、Crossdomain.xml 配置问题。

【高】非核心系统中的高危漏洞，或核心系统中的一般漏洞，业务等级系数【1-10】，基本安全币【45-60】，本等级包括：

1. 属于严重级别中所描述的漏洞类型，但是产生在非核心系统中的漏洞（例如非核心系统的远程任意命令执行、可 dump 出数据的 SQL 注入），以及移动端 App 命令执行类漏洞（例如 Android WebView 远程代码执行漏洞）
2. 访问任意系统文件的漏洞，包括但不限于任意文件包含、任意文件读取。
3. 其它敏感信息泄漏。包括但不限于源代码压缩包漏洞、UC-Key 泄露、HEARTBLEED 漏洞等。同时包括通过 SVN 信息泄漏、Git 信息泄露导致的重要产品线源码泄露。
4. 包含敏感信息的非授权访问。包括但不限于绕过认证直接访问管理后台、后台弱密码、可直接获取大量内网敏感信息的 SSRF。
5. 包含敏感信息的越权操作及核心系统的越权操作。包括但不限于越权修改其他用户重要信息、进行订单操作、重要业务配置修改等较为重要的越权行为。
6. 大范围影响用户的其他漏洞。包括但不限于可造成自动传播的重要页面的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、重要操作的 CSRF，以及可获取 BDUSS 等敏感信息的各种 XSS。

1 SRC就是一场游戏

1.2 如何在游戏中升级？

- 1.首先遵守游戏规则，接着就是在游戏规则上找到升级方法
- 2.观察各个SRC对漏洞评价等级，各个平台还是有差别的
- 3.知道了漏洞评价等级，再去观察他对业务范围的定级，如边缘业务多少分
- 4.接下来就看你基础知识扎不扎实了，如果不扎实先去学习各个漏洞原理以及利用方法

一名路过的小学生



2 快速有效的精准定位

2.1 如何做到快速有效？

知己知彼，百战不殆

zhī jǐ zhī bǐ, bǎi zhàn bù dài

- 俗话说“知己知彼百战不殆”
- 在漏洞挖掘方面也一样，知道产商有什么样的业务，我们就可以根据他业务可能存在的缺陷去挖掘漏洞。
- 例：某电商，想一下有哪些可以测试的地方

2 快速有效的精准定位

2.2 什么漏洞最好挖？

- 当然是逻辑方面的漏洞，逻辑就是根据开发人员的思维造成的漏洞，如果思维处理出现问题，就会出现这样的漏洞，所以只要你逻辑思维能力强，基础知识扎实，你就不怕挖不到漏洞。
- 为什么说逻辑漏洞最好挖？
- 因为现在互联网还没有可以防御逻辑漏洞的WAF，目前大多是Token，Session，加密等方式进行防御

2 快速有效的精准定位

2.3 某电商，想一下有哪些可以测试的地方？

- 1.注册处→任意用户注册→XXX
- 2.登录处→任意用户登录→XXX
- 3.收货地址→越权→XXX
- 4.订单信息→遍历→XXX
- 5.充值→逻辑缺陷→XXX
- 6.....→XXX



2 快速有效的精准定位

2.4 定位漏洞触发点

- 1.登录时 — 登录框 — 注入 — 任意用户登录 — 撞库爆破 — 弱口令 — URL跳转 — 凭证劫持
- 2.登陆后 — 个人信息 — 储存XSS — 越权 — 注入 — Csrp — 越权+Xss? — Xss+Csrp?
- 3.登陆后 — 上传点 — Getshell
- 4.Fuzz — Burp (Intruder Repeater) — 自动化扫描 — Awvs — Appscan — Netsparker

一切存在 输入 与 输出 均有害

2 快速有效的精准定位

2.5 精准定位来源于基础知识

- 谨记：观察业务功能，同时进行思考可能存在的缺陷，逐步测试，不要怕麻烦

- 演示：

- <http://127.0.0.1/1.php>
- <http://127.0.0.1/news.php?id=1>

你输入的字符为
我是菜鸟

3 漏洞挖掘小技巧

3.1 关注新增业务

- 关注新上线的业务，刚上线的业务往往是最脆弱的，比如新功能，新上线的子域名

新功能：

- python脚本 浏览器插件（网页哨兵，Distill Web Monitor） github（监控）

新域名：

- 监控子域名（Sublert）

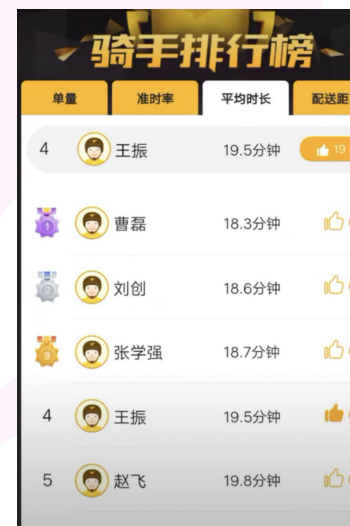
3 漏洞挖掘小技巧

3.2 尝试申请非普通用户拥有的权限

- 比如饿了么，普通用户可以定外卖，商家可以卖餐，骑手可以接订单，分别注册三个不同权限的用户进行测试，也许你会发现很多漏洞



我要开店



3 漏洞挖掘小技巧

3.3 留意以前没挖到洞的功能

- 为什么要留意以前没挖到洞的功能呢？因为技术原因可能还无法对这个功能进行测试，在后面你不断的学习，发现到了新的思路，突然想起和以前测试的功能一样，以前没测出问题，而这次你不但测出了问题，还重复了！

重复漏洞

3 漏洞挖掘小技巧

3.4 思考一下什么是漏洞？

- 漏洞就是指可以对系统造成一定的影响，只要可以造成一定影响，危害正常业务运行，它就算漏洞！
- 漏洞挖掘三要素：

第一、**广度** 第二、**深度** 第三、**认知**

3 漏洞挖掘小技巧

3.5 挖了一天没挖到漏洞怎么办？

- 如果一天没挖到可能是运气不好，如果两天没挖到也许是因为你业务范围比较少，挖的可能已经是大佬们挖过很多次了，如果三天还没挖到，也许是太累了，你需要休息一下，如果一星期还没挖到一个漏洞（当然这里包括忽略重复的，毕竟你挖到了），那你可能是基础知识不扎实，建议你从0学起，各个漏洞的原理以及利用修复方法都要掌握，同时能想出自己新的扩（多）展（尝）思（试）路！

4 扩展思维—漏洞案例分享

4.1 垂直越权

- 思考一下，有没有缺陷？
- Cookie: SESSION=USER-334dsf9ref8esg8erg390g
- Cookie: SESSION=USER-2dfg34768jh4h234g5h5jk
- Cookie: SESSION=USER-1dfg34768jh4h234g5h5jk

4 扩展思维—漏洞案例分享

4.1 垂直越权

- 用户检查：session=USER-34dsf9ref8esg8erg390g
- 权限：level=3
- level=1：admin
- level=2：vip user
- level=3：normal user

4 扩展思维—漏洞案例分享

4.2 并发请求

输入手机号领取红包

请输入手机号码


马上领取


红包已放至账户 修改 >
登录 App 即可使用


4 扩展思维—漏洞案例分享


4.2 并发请求


- 攻击方法：


 **Request Engine**

 These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 

Number of retries on network failure: 

Pause before retry (milliseconds): 

Throttle (milliseconds): ☒ Fixed 
☐ Variable: start step

Start time: ☒ Immediately
☐ In minutes
☐ Paused

4 扩展思维—漏洞案例分享

4.3 程序溢出

- int最大值：2147483647
- 程序开发时，程序员一般计算数量等操作时，会用到int，而int的最大值为2147483647
- 超出最大值则会溢出，导致程序出错

4 扩展思维—漏洞案例分享

4.3 程序溢出

■ 在游戏里面通常最大数值就是2147483647，那么正溢出就是假如商品单价为2，那么我要做到的就是 $2 * \text{数量} > 2147483647$ ，假如买1073741825个*2就是2147483650，在游戏中由于超出了最大值，总价格就会变成了3（超出后从0开始计算），于是去尝试了一下，果然是这样，经过计算后，成功刷到了符文箱。



4 扩展思维—漏洞案例分享

4.4 不要急着放弃，你不确定开发人员会给你带来哪些惊喜

访问站点发现是403



A screenshot of a web browser window. The address bar shows a local IP address 10.0.0.17. The main content area displays the word "Forbidden" in a large, bold, black font. Below it, in a smaller font, is the message "You don't have permission to access / on this server."

通过目录枚举，发现一个文件



A screenshot of a web browser window. The address bar shows the URL "http://10.0.0.17/adver/landing.php". The main content area displays a JSON response: {"msg":"params error","status":0}.

很明显，提示缺少参数：params error

4 扩展思维—漏洞案例分享

4.4 不要急着放弃，你不确定开发人员会给你带来哪些惊喜

完整URL： http://106.**.**.147/adver/landing.php?mac=1

添加单引号报错，发现SQL注入

```
[*] starting at 16:16:52
[16:16:52] [INFO] resuming back-end DBMS 'mysql'
[16:16:52] [INFO] testing connection to the target URL
[16:16:52] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: mac (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: mac=1' AND 5711=5711 AND 'QKux'='QKux

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: mac=1' AND (SELECT * FROM (SELECT(SLEEP(5)))AiGP) AND 'Bqod'='Bqod
---
[16:16:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7.0 (wheezy)
web application technology: Apache 2.2.22, PHP 5.4.39
back-end DBMS: MySQL 5.0.12
[16:16:52] [INFO] fetching current user
[16:16:52] [INFO] retrieving the length of query output
[16:16:52] [INFO] retrieved: 13
[16:16:57] [INFO] retrieved: ins@localhost
current user: 'ins@localhost'
```

4 扩展思维—漏洞案例分享

4.5 总结

- 在逻辑方面，测试漏洞就是反复对参数进行测试（细心分析每一个参数的作用），GET，POST，COOKIE 等等内容进行反复测试（增，删，改，查），有时也会存在隐藏参数，可利用Fuzz模糊测试以及自动化扫描器进行测试，最后再手动判断。

- 了解业务的运行，才能最大化的发现漏洞缺陷！**

- 在线工具箱：<http://tools.hackxc.cc>

知己知彼，百战不殆

zhī jǐ zhī bǐ, bǎi zhàn bù dài

4 扩展思维—漏洞案例分享

4.6 你以为结束了吗？

- 补充 — 验证码绕过姿势：
- 验证码：验证码可重复使用 — 万能验证码（8888，0000） — 空验证码绕过 — 验证码可识别 — 其他验证后未对比
- 其他验证后未对比：仅仅校验了密码字段和验证码,用户名并未校验,那么这里就可以输入一个弱密码（123456,111111,123123等等）,然后反向去遍历用户,获取正确的口令。

Request	Payload	Status	Error	Redire...	Timeout	Length	Comment
101	wa	200		0		1904	
105	zhu	200		0		1897	
123	zhu	200		0		1897	
157	zhu	200		0		1897	
18	zhu	200		0		1895	
157	zhu	200		0		1892	
75	liu	200		0		1889	
90	liu	200		0		1889	
18	zhu	200		0		1880	
6	te	200		0		1871	
380	zhu	200		0		1869	
162	wa	200		0		430	
8	se	200		0		427	
9	sy	200		0		427	
10	zh	200		0		427	
11	li	200		0		427	
14	wa	200		0		427	
16	li	200		0		427	
19	zh	200		0		427	
..	

4 扩展思维—漏洞案例分享

4.6 你以为结束了吗？

- 补充 — 短信轰炸绕过姿势：
 - 1.无任何限制，可以持续发送短信
 - 2.绕过验证码发送短信（详情看验证码绕过）
 - 3.遍历手机号进行轰炸，消耗资源（一般不会通过）
 - 4.手机号前+86，有时候可以绕过限制
 - 5.手机号输入邮箱，导致无限制轰炸
 - 6.邮箱输入手机号，导致无限制轰炸

4 扩展思维—漏洞案例分享

4.7 你以为结束了吗？

- 补充 — 其他知识：
 - 1.挖漏洞建议有**翻倍活动**的时候挖，有机会获得高分高奖励
 - 2.遇到**法定节假日**也可以挖，根据SRC的节日活动规则，有机会拿到节日礼物
(比如中秋节，挖到一定分数，或者漏洞数量，SRC就有可能会送你一盒月饼，hh)
 - 3.尽量在各大SRC**保留积分**，或者**各类币**，法定节假日时，也许可以拿1分兑换节日礼包（如端午节兑换粽子，较少的积分或币就可以换）
 - 4.若提交漏洞的**评分**与设想有**出入**，一定要找运营人员协商申诉，有可能获得漏洞的重新评分处理
 - 5.如果你是不会挖洞的新人，那么你可以考虑提交**威胁情报**，发现对SRC有威胁的地方，可提交情报（详情看各大SRC提交威胁情报介绍，和漏洞评分文件同理），也许会有奖励

大咖联系方式



- QQ: 758682207

BUGBANK

还没看够？来了解更多技术干货

漏洞银行直播间: <https://www.bugbank.cn/live/>



直播资料 | 社群伙伴 | 听讲通知

QQ群号: 327085041



也想当大咖？还不扫码报名

也可联系运营 QQ: 2272924679



了解更多安全行业热点时事

行长叠报: BUG_BANK