2018

短网址攻击与防御

演讲人：彦修

About Me

- 腾讯安全工程师
- 微博:@彦修_
- 喜美食、好读书，不求甚解
- Tencent Blade Team

BLADE Tencent Blade

- 由腾讯安全平台部创立。
- 专注于AI、移动互联网、IoT、无线电等前沿技术领域安全研究。
- 报告了谷歌、苹果、亚马逊等多个国际知名厂商70+安全漏洞。

KCon

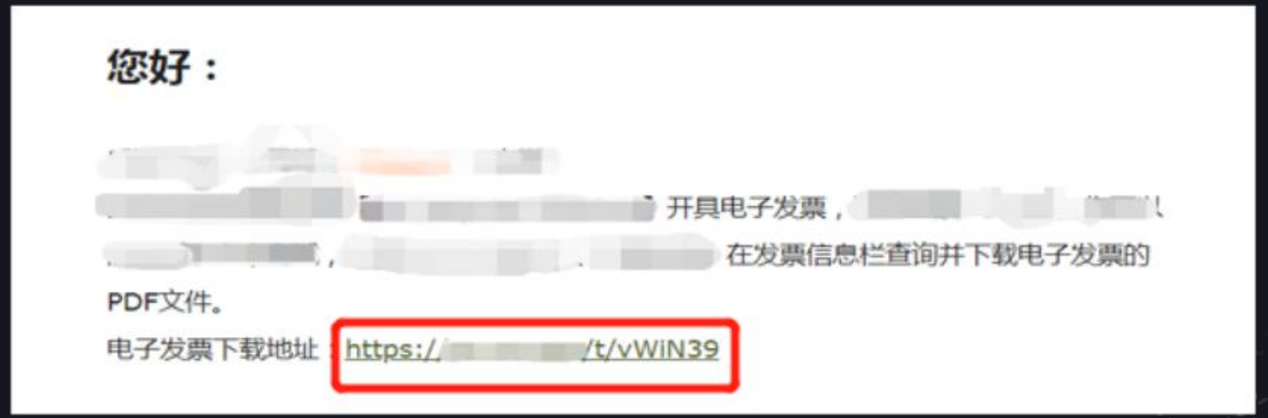
目录
CONTENTS

KCon

PART 01

短网址猜想

某个惠风和畅的下午收到这么一封邮件……



KCon

改变短网址后缀，是否可以获取他人的发票链接：

由短网址：http://xx.com/t/*vWiN39*　　——>　　http://xx.com/t/*vWiN40*

进而：

http://*xx.cn*/t/vWiN39

http://*xx.to*/t/vWiN39

.....

我们随后进行了大批量随机爆破测试，部分结果如下：

Request	Payload1	Payload2	Status	E
435	plqq	00	302	
701	qrwq	00	302	
2601	qttq	00	302	

KCon

短网址第一猜想：

当你发现某处出现了问题，那么出现问题的一般不止这一处！

短网址第二猜想：

如果你要解决一个问题，你需要知道这个问题是什么！

短网址第三猜想：

KCon

PART 02

何谓短网址

短网址：此服务可以提供一个非常短小的URL以代替原来的可能较长的URL，将长的URL地址缩短。用户访问缩短后的URL时，通常将会重定向到原来的URL。（摘自维基百科）

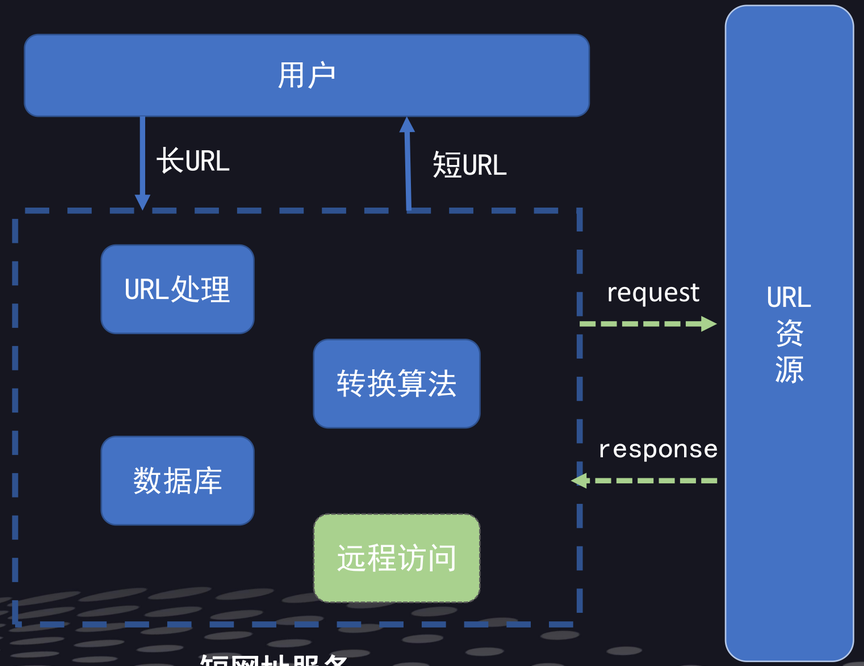
比如微博中常见的：http://t.cn/h5BBi

短网址服务主要起源于一些具有字数限制的微博客服务，现在广泛用于**短信、邮件等。**

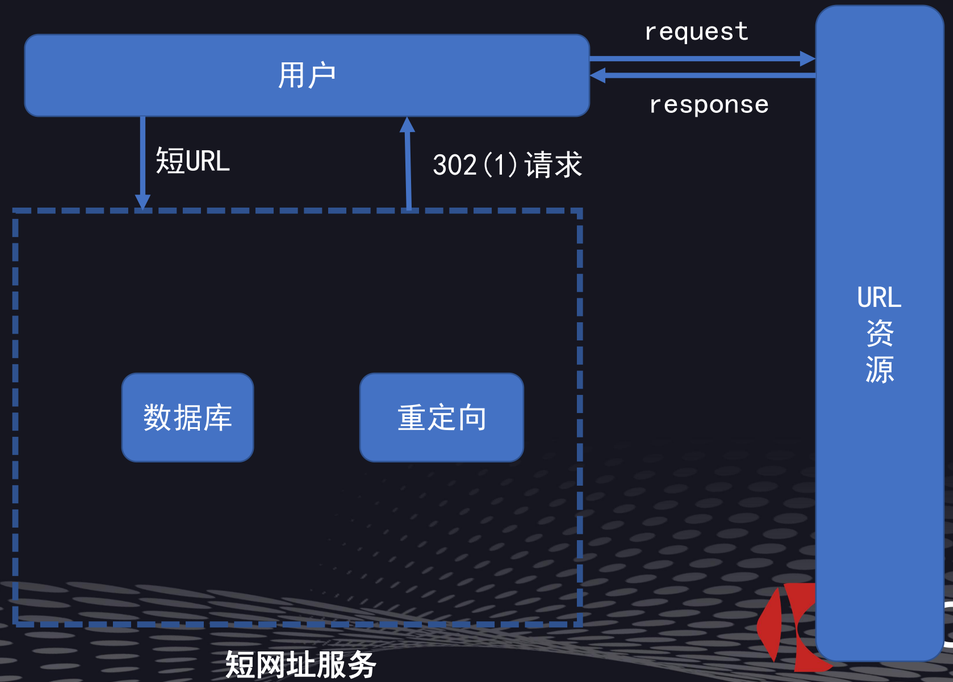
自用短网址服务产品（部分）：

第三方短网址服务产品（部分）：

长网址转换短网址



短网址转换长网址

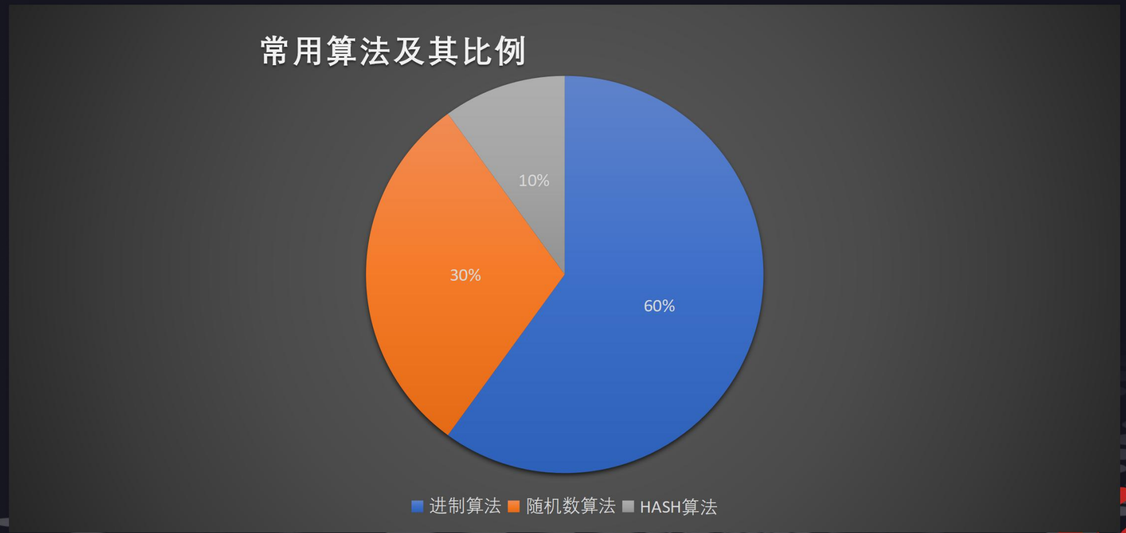


我们分析了GITHUB上star数最多的10个短网址开源项目，其转换算法大致分为三类，即进制算法、HASH算法和随机数算法

进制算法：结果连续。

随机数算法：结果不连续。

HASH算法：结果不连续。



进制算法：

算法简述：一个以数字、大小写字母共62个字符的任意进制的算法。

数据库中ID递增，当ID为233，则对应短网址计算过程如下：

① 设置序列为“0123456789abcdefghijklmnopqrstuvwxyz”
② 233/36=6
③ 233%36= 17
④ 依次取上述字符的6位，17位，则为6h

其生成之后的短网址为xx.xx/6h

随机数算法：

算法简述：每次对候选字符进行任意次随机位数选择，拼接之后检查是否重复

若要求位数为2，则其对应短地址为计算过程如下：

① 设置字符序列“0123456789abcdefghijklmnopqrstuvwxyz”
② 根据字符个数设置最大值为35，最小值为0，取2次随机数假设为：6,17
③ 依次取上述字符的6位和17位，则为6h

其生成之后的短网址为xx.xx/6h

HASH算法：

算法简述：对id进行hash操作（ 可选：利用随机数进行加盐），并检查是否重复

设置ID自增，若ID=233，则其对应短地址为计算过程如下：

① 取随机数为盐
② 对233进行sha1加密为： aaccb8bb2b4c442a7c16a9b209c9ff448c6c5f35:2
③ 要求位数为7，直接取上述加密结果的前7位为：aaccb8

其生成之后的短网址为xx.xx/2e8c027

PART 03

短网址攻击实战

根据短网址第一猜想：

当你发现某处出现了问题，那么出现问题的一般不止这一处！

存在短网址问题并非上述一家例子中的厂商？！

所以如何高效、有效爆破？

短网址爆破最佳实践

KCon

算法识别：第三方进制算法

可以多次输入网址，查看返回短网址是否连续，连续则为进制算法，如下：

Tips：个别为分布式短链接，id非单一递增，会出现多个字符规律变化，如：87BNwj、87BO82、87BOqw、87BOGz、87BPpD

算法识别：自营进制算法

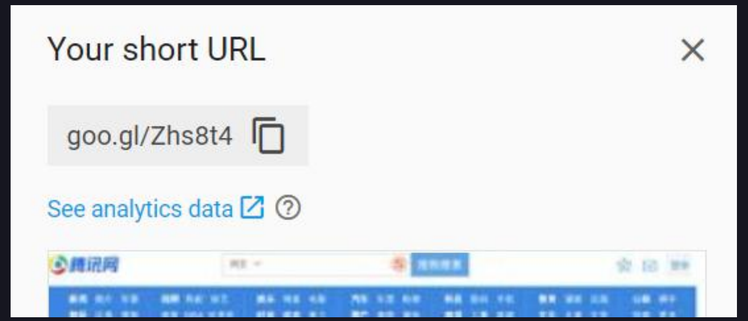
① 直接测试xx.xx/1及xx.xx/2 等低位后缀。

② 对存在记录的后缀单字母进行增加或减少测试，若均存在记录或者有规律存在记录。

若某短网址存在http://xx.xx/Abzc4 ，对Abzc4中最后一个单字符{0-Z}共62次变化。若均存在记录或存在a，c，e等有规律间隔情况，则基本可以认为使用了进制算法。

算法识别：第三方HASH&随机数算法

可以多次输入网址，查看返回短网址是否连续，不连续无规律则为HASH算法&随机数算法。



算法识别：自营HASH&随机数算法

① 直接访问xx.xxx/1及xx.xxx/2低位等后缀，若均不存在则进行步骤2。

② 对存在记录的后缀进行增加或减少尝试，若非均匀间隔存在记录。

即：若某短网址存在http://xxx.xx/Abzc4 ，对Abzc4中最后一个单字符{0-Z}共62次变化。
若无明显规律则基本认为为HASH&随机数算法

TIPS:

部分短网址服务对于不存在的记录会返回不同的处理结果，常见如下：

① 返回固定URL，如 http://xxx.xx/sorry

② 返回非固定URL，如 http://xxx.xx/{随机值}

爆破需检测返回值。将非长网址URL加入黑名单之中！

攻击案例一：

爆破短网址服务获取大量服务、系统敏感信息：

1、获取个人信息

http://xx.xx/auth?contractId=d57f17139247036b72******b5554a830305ec139d

2、获取合同

https://xx.xx/get.action?transaction_id=290414****03784&msg_digest=RUQ2MUQ5NjcxQzc5MjcxQ*******4QTExNTZFNjgzQTJENEExQjc5Nw==

3、重置密码

https://xx.xx/resetPassword?emailType=RESET_PASSWORD&encryptionEmail=***GHOsR%2FMfiNEv8xOC29.&countersign=eyJhbGciOiJIUzUxMiJ9.eyJBQINPTFVURV9FWFBJUkVfVEINRV9NSUxMUyI6IjE1M******zA1OTMxNjU4OTQiLCJORVdfRU1BSUwiOiJ5YW54aXUwNjE0QGdtYWIsLmNvbSIsIlRPS0VOX1RZUEUiOiJSRVNFVF9QQVNTV09SRCIsIkVNQUIMIjoieWFueGI1MDYxNEBnbWFpbC5jb20ifQ

攻击案例二：

业务安全攻击链：某应用邀请新人注册送红包活动

1、邀请链接直接发送给邀请人，邀请人点击即可完成注册；

2、邀请链接以短网址发送；

3、批量邀请，爆破短网址，批量点击注册，即可完成薅羊毛；

PART 04

扩展短网址攻击面

根据短网址第一猜想：

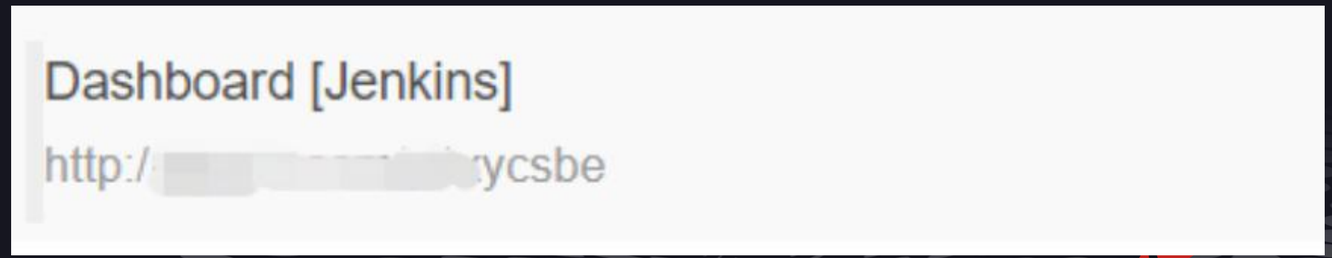
当你发现某处出现了问题，那么出现问题的一般不止这一处！

短网址存在算法可以被识别，从而被遍历的问题？是不是还存在其他的问题？！

以下均为猜想，如有雷同，概不负责

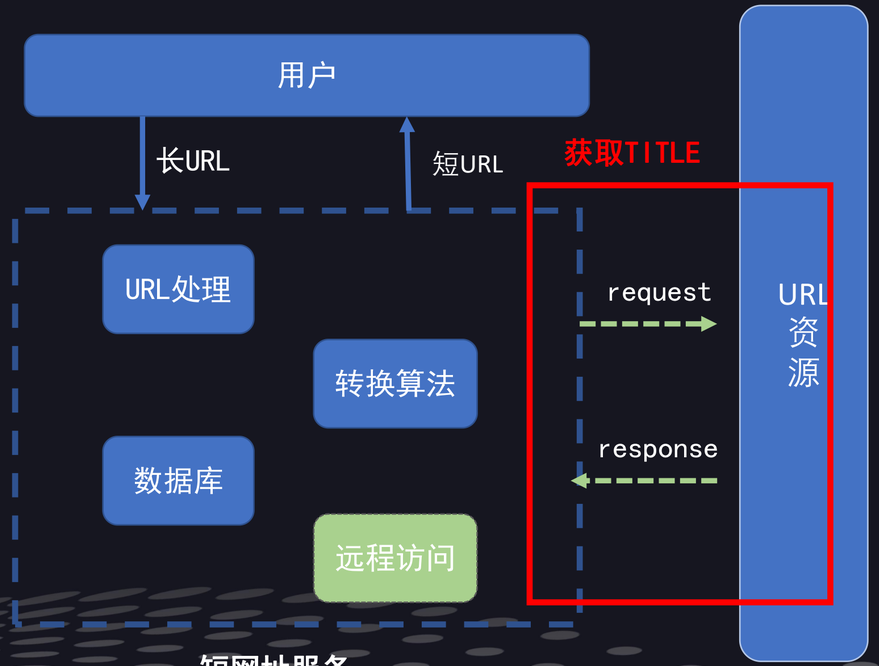
长网址转换短网址

1、远程访问功能在过滤不严谨的情况下会造成SSRF！



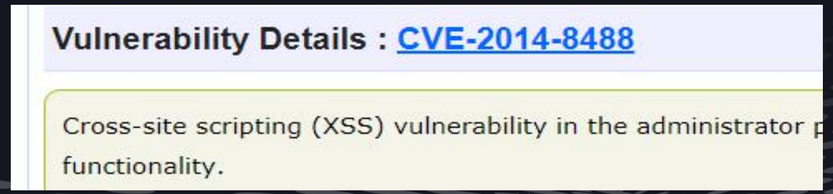
KCon

长网址转换短网址

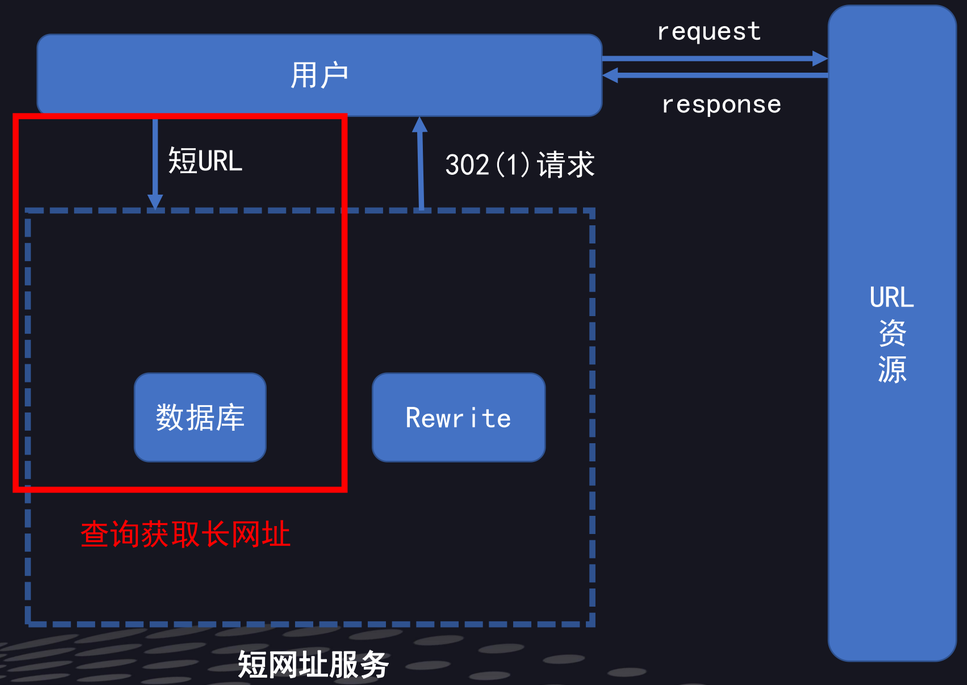


2、获取TITLE功能和展示长网址页面，在过滤不严谨的情况下，造成XSS。

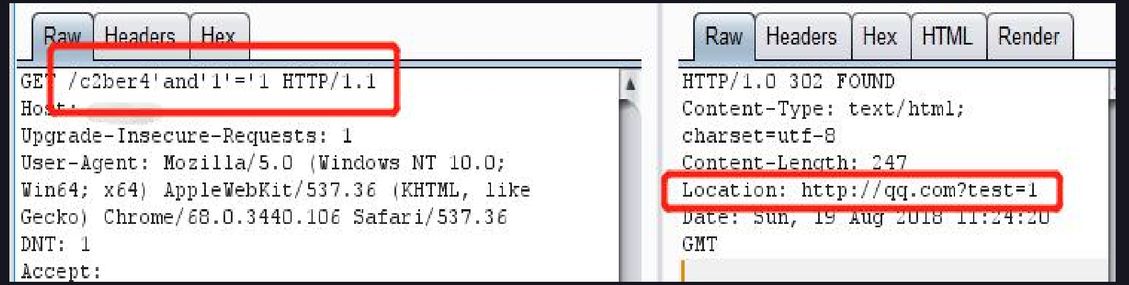
```
<img src=x onerror=prompt(1)>*
<title><script>alert(1)</script> </title>
```

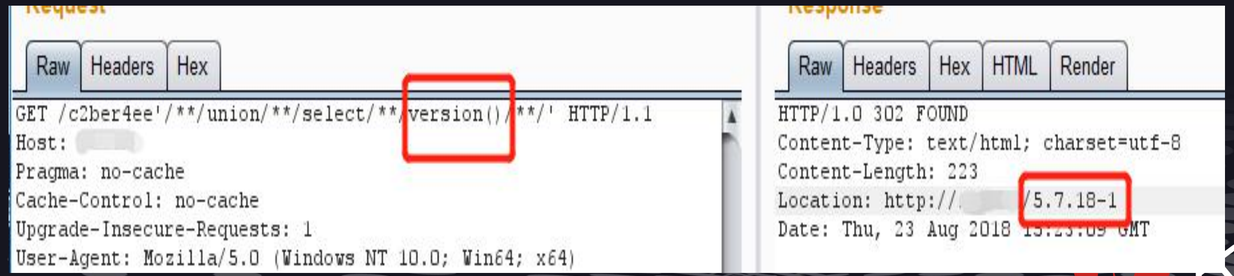


短网址转换长网址



1、进行拼接查询时会造成SQL注入。





PART 05

短网址防御实践

补救措施（存量）

1、增加单IP访问频率和单IP访问总量的限制，超过阈值进行封禁。

2、对包含权限、敏感信息的短网址进行过期处理。

3、对包含权限、敏感信息的长网址增加二次鉴权。

改造措施（增量）

1、不利用短网址服务转化任何包含敏感信息、权限的长网址。

2、尽量避免使用明文token等认证方式。

致谢

@Wester的小号

@Mart1n_ZHOU

KCon

谢谢观看

演讲人：彦修