url中的unicode漏洞引发的域名安全问题

knigh**** / 2019-08-26 08:51:00 / 浏览数 5025 安全技术 WEB安全 顶(1) 踩(0)

url中的unicode漏洞引发的域名安全问题

在今年的blackhat中微软安全研究员Jonathan
Birch，向大家介绍了一个unicode漏洞，此漏洞影响了现在的大部分的软件，语言，浏览器，产生了数个CVE漏洞。跟随着大佬大脚步，我也想去了解这个漏洞。为了记录自

0x00基础知识

在理解漏洞之前，现了解下unicode和ascii编码，IDNA吧

unicode编码

Unicode（中文：万国码、国际码、统一码、单一码）是计算机科学领域里的一项业界标准。它对世界上大部分的文字系统进行了整理、编码，使得计算机可以用更为简单的

Unicode 伴随着通用字符集的标准而发展，同时也以书本的形式对外发表。Unicode
至今仍在不断增修，每个新版本都加入更多新的字符。当前最新的版本为2019年5月公布的12.1.0，已经收录超过13万个字符（第十万个字符在2005年获采纳）。Unicode

ascii编码

ASCII（American Standard Code for Information
Interchange，美国信息交换标准代码）是基于拉丁字母的一套电脑编码系统，它主要用于显示现代英语，而其扩展版本EASCII则可以部分支持其他西欧语言，并等同于国际
646。

ASCII
由电报码发展而来。第一版标准发布于1963年，1967年经历了一次主要修订，最后一次更新则是在1986年，至今为止共定义了128个字符；其中33个字符无法显示（一些

ASCII码大致由三部分组成：ASCII 打印字符、ASCII 非打印控制字符、扩展 ASCII 打印字符

IDNA（Internationalizing Domain Names in Applications）应用程序国际化域名

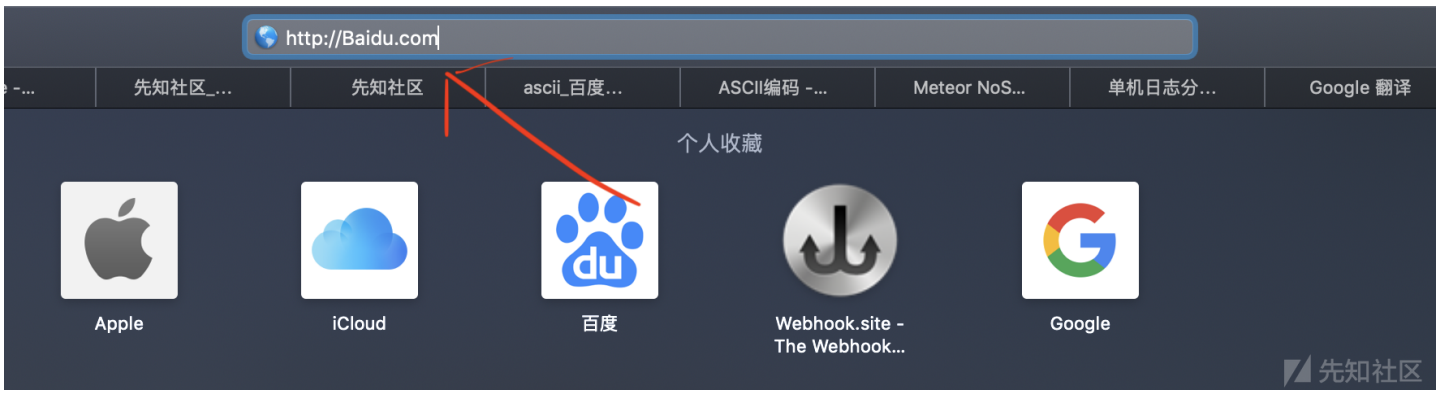
IDNA是一种以标准方式处理ASCII以外字符的一种机制，它从unicode中提取字符，并允许非ASCII码字符以允许使用的ASCII字符表示。

国际化域名(IDN)最初是由马丁·杜斯特于1996年12月提出。1998年在新加坡国立大学教授陈定炜的指导下，Tan Juay Kwang和Leong Kok
Yong将其付诸实施。经过许多讨论和对比各种提案后，应用程序国际化域名（IDNA)被采纳为正式标准，并被用在许多顶级域名中。在IDNA中，“国际化域名”特指可以成功

0x01漏洞分析

1、域名欺骗

先看一个有趣的东西，访问此网站`http://■aidu.com`(其中的B是unicode U+0412)



它是不是跳转到了`http://xn--aidu-f4d.com/`。

当然，你也可以试试使用其他特殊的unicode编码。

 下面，看下整个过程吧

 先讲下跳转的url的含义

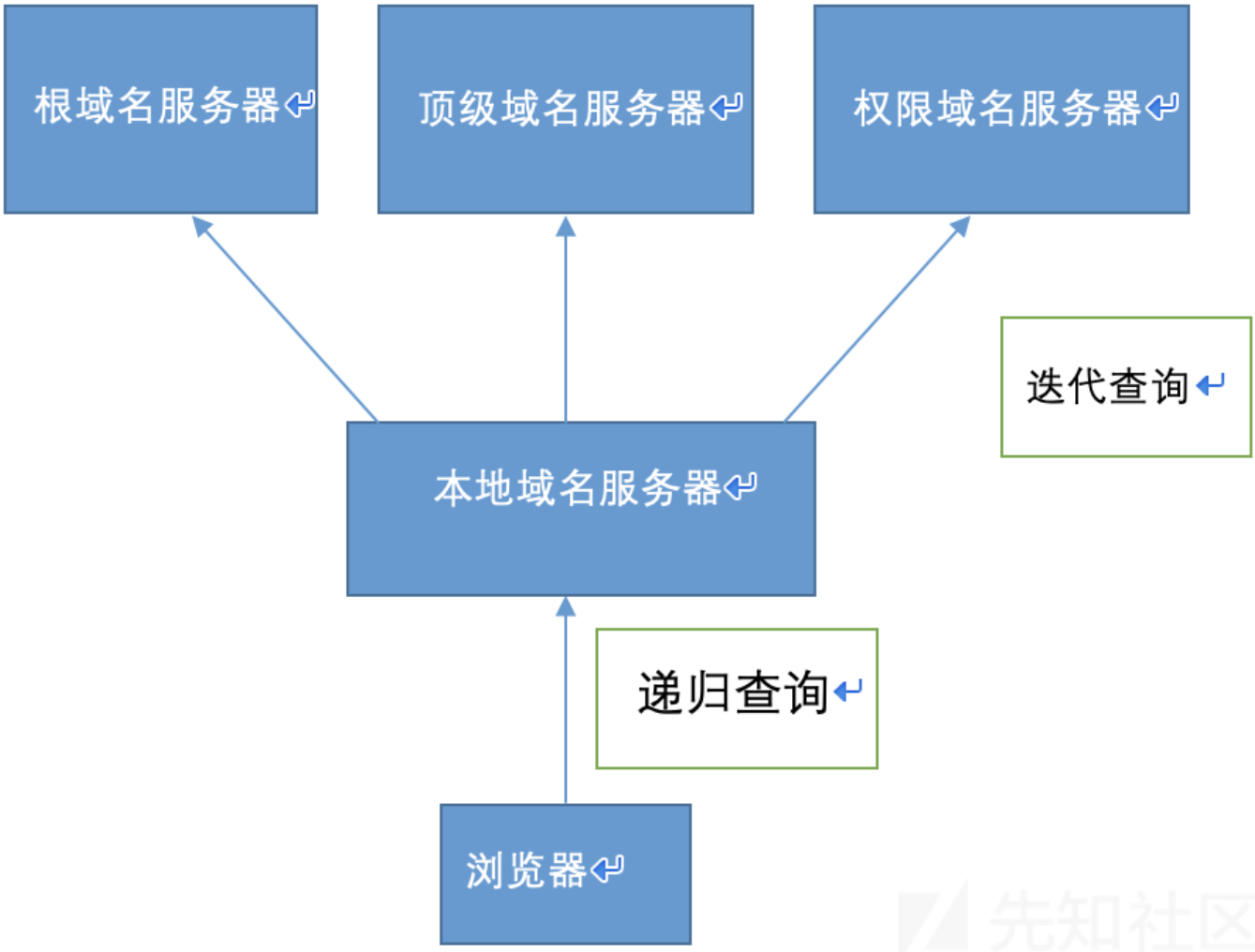
http://xn--aidu-f4d.com/

xn:ACE(这是一个国际化域名编码)

aidu:ASCII码

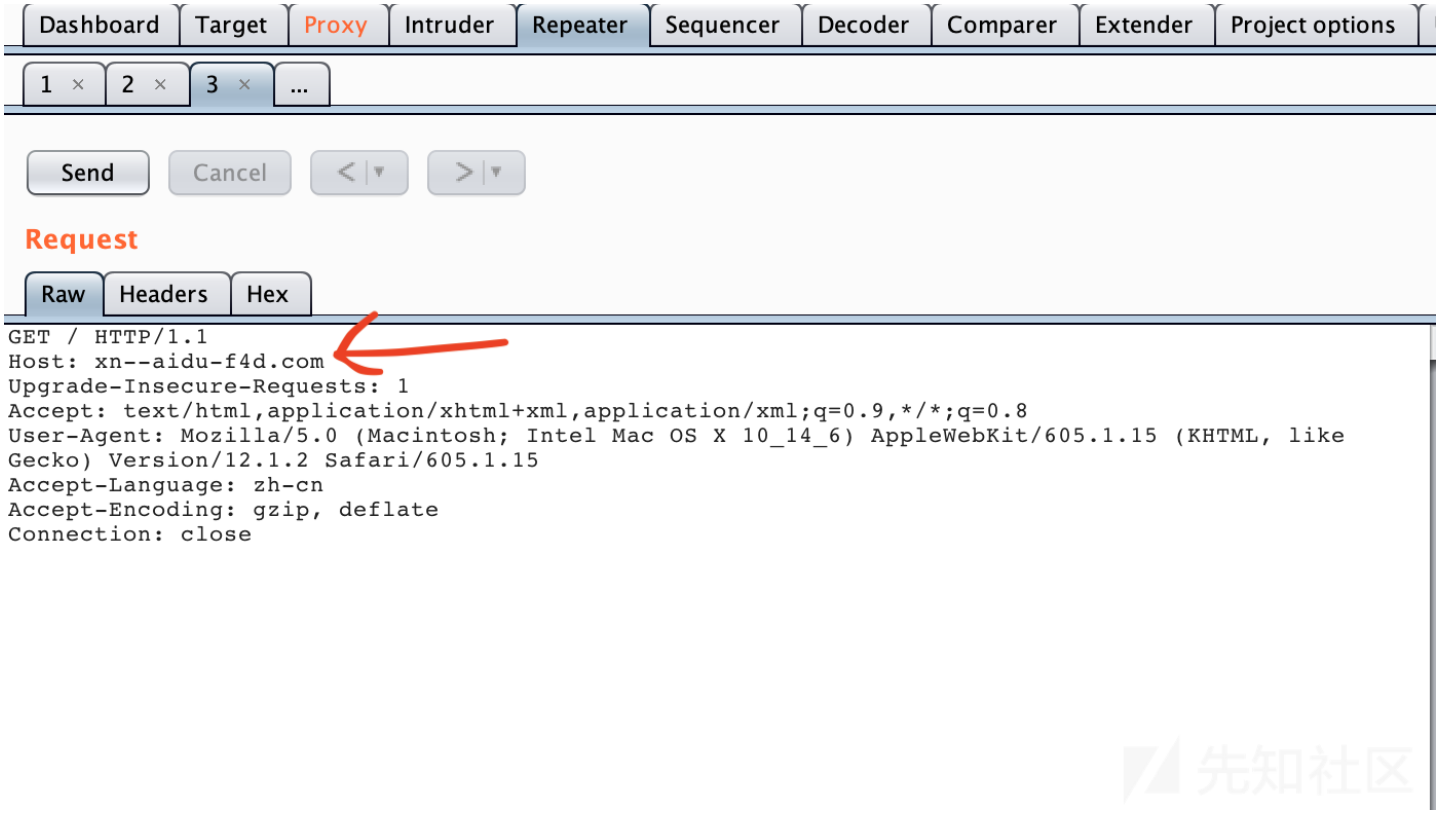
f4d:状态机指令

 现在，我们来看看具体过程



当我们访问http://■aidu.com时，浏览器会将我们访问的url交给域名系统(DNS)解析url为ip地址，在解析url的过程中采用递归查询和迭代查询，即先递归搜索浏览器自

下面是burpsuite抓取的本地解析完成后的截图。



而IDNA转写ASCII的过程又分为两步

1. Normalization

Convert characters to a “standardized form”.

第一步：正常化，将字符转化为标准形式

例如：Å (U+00C5),Å (U+212B),Å (U+0041, U+030A)将会被标准化为å (U+00E5)

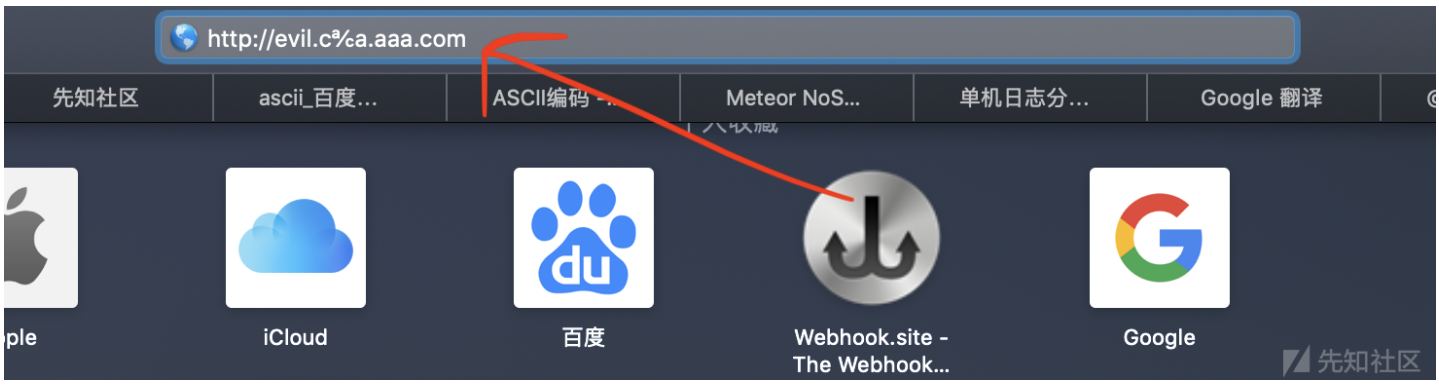
2. Punycoding
Turn Unicode into ASCII.

第二步：用punycode编码将unicode编码成ASCII码

□
现在我们已经知道，在我们访问域名`http://■aidu.com`时，浏览器会将此unicode转化为ASCII码，然后访问`http://xn--aidu-f4d.com/`,如果我们注册了`http://x`

2、域名分割

□ 如果你再尝试下访问`http://evil.c■a.aaa.com`



□ 这个时候你会发现你的浏览器会访问`http://evil.ca/ca.aaa.com`。

在unicode中还有一种字符■(U+2100)，当IDNA处理此字符时，会将■变成a/c，因此当你访问此url时，dns服务器会自动将url重定向到另一个网站。如果服务器引用前端u

但是为什么同样是unicode字符，但是会产生不同结果呢？

首先我们要明确一点就是，IDNA并不是所有unicode都可以以ASCII码呈现的

unicode转ASCII发生在IDNA中的TOASCII操作中。如果能通过TOASCII转换时，将会以正常的字符呈现。而如果不能通过TOASCII转换时，就会使用“ACE标签”，“ACE”标

那还有其他可以利用的unicode字符吗？

U+2100, ■ U+2101, ■ U+2105, ■ U+2106, ■ U+FF0F,■ U+2047, ■ U+2048, ■ U+2049, ■

U+FE16, ■ U+FE56, ■ U+FF1F,■ U+FE5F, ■ U+FF03, ■ U+FE6B, ■ U+FF20, ■

3、漏洞IDNA版本

IDNA2008阻断了分割域名的字符

IDNA2003 和 IDNA2008 + UTS46存在漏洞

0x03关联CVE

- CVE-2019-0654 Microsoft Browser Spoofing Vulnerability
- CVE-2019-0657 .NET Framework and Visual Studio Spoofing Vulnerability
- CVE-2019-9636 Python, urlsplit does not handle NFKC normalization
- CVE-2019-10160 Python, urlsplit NFKD normalization vulnerability in user:password@
- CVE-2019-2816 Oracle Java SE/Java SE Embedded, “Normalize normalization”
- CVE-2019-12290 LibIDN2, “Perform A-Label roundtrip for lookup functions by default”

0x04参考

此文章来源于对2019blackhat `HostSplit-Exploitable-Antipatterns-In-Unicode-Normalization`议程的理解。

`https://i.blackhat.com/USA-19/Thursday/us-19-Birch-HostSplit-Exploitable-Antipatterns-In-Unicode-Normalization.pdf`

`https://tools.ietf.org/html/rfc3490`

`https://zh.wikipedia.org/wiki/■■■■■`

`https://blog.csdn.net/kexiuyi/article/details/81125588`

`https://blog.csdn.net/qq_21993785/article/details/81188253`

点击收藏 | 1 关注 | 2

上一篇：第一次渗透测试的分享和小结 下一篇：路由器漏洞挖掘测试环境的搭建之问题...

1. 5 条回复

pic4xiu 2019-08-26 09:19:53

大佬ddw

0 回复Ta

panda 2019-08-26 09:23:00

SUCTF 有一个web也是根据这个思路来的

0 回复Ta

knigh**** 2019-08-26 09:27:45

@panda 对，就是看着那个思路，然后发现自己不懂，然后下去研究的

0 回复Ta


darkless 2019-08-29 19:39:28

大佬，那个 B 怎么打出来的？

0 回复Ta


knigh**** 2019-08-29 23:16:30

@darkless 如果复制不了，就去查unicode表U+0412

1 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板