Syclover

# 穿梭在站与站之间的夜行者

——Syclover l0ca1

# About Me


## L0ca1

- **Syclover** 端茶递水
- 二向泊安全扫地
- 脚本小子，平时写 **Node Js**
- 开发，学习，膜师傅
- 还有很多问题，一直保持热情

# 目录

# 目录


- 第三方 **Cookie**
- 子域名劫持 **Takeover subdomain**
- 第三方服务安全

# 第三方 Cookie

# 第三方 Cookie


a.com
1
2
3
4
b.com


Cookie
允许网站保存和读取 Cookie 数据（推荐）
仅将本地数据保留到您退出浏览器为止
阻止第三方 Cookie
阻止第三方网站保存和读取 Cookie 数据
查看所有 Cookie 和网站数据

# 第三方 Cookie

Syclover

new Image().src = 'https://www.zhihu.com';

```
GET / HTTP/1.1
Host: www.zhihu.com
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: https://developer.mozilla.org/en-US/docs/Web/API/MutationObserverInit
Accept-Encoding: gzip, deflate
Accept-Language: zh,en-US;q=0.9,en;q=0.8,ja;q=0.7,zh-CN;q=0.6
Cook [redacted] xsrf=e5979dd2-74df-[redacted]; d_c0="ALDo[redacted]
q_c1[redacted] n_c=1; n_c=1;
l_cap_id="M[redacted]
r_cap_id="M[redacted]
cap_id="YWJ[redacted]
capsion ti[redacted]
z_c0[redacted]
8851[redacted] ==; tgw_l7_route=7139[redacted]
```

# 第三方 Cookie


中间人攻击 + Cookie 嗅探 + Cookie 安全设置

```
// EtherDream
const target_list = ['www.zhihu.com','www.weibo.com','www.qq.com','www.baidu.com'];
target_list.forEach(url=>{
    new Image().src = `http://${url}`;
});
```

Cookie 作用域：domain 本身及其 子域名

Cookie: UID=xxxxxxxxxxx;Secure;

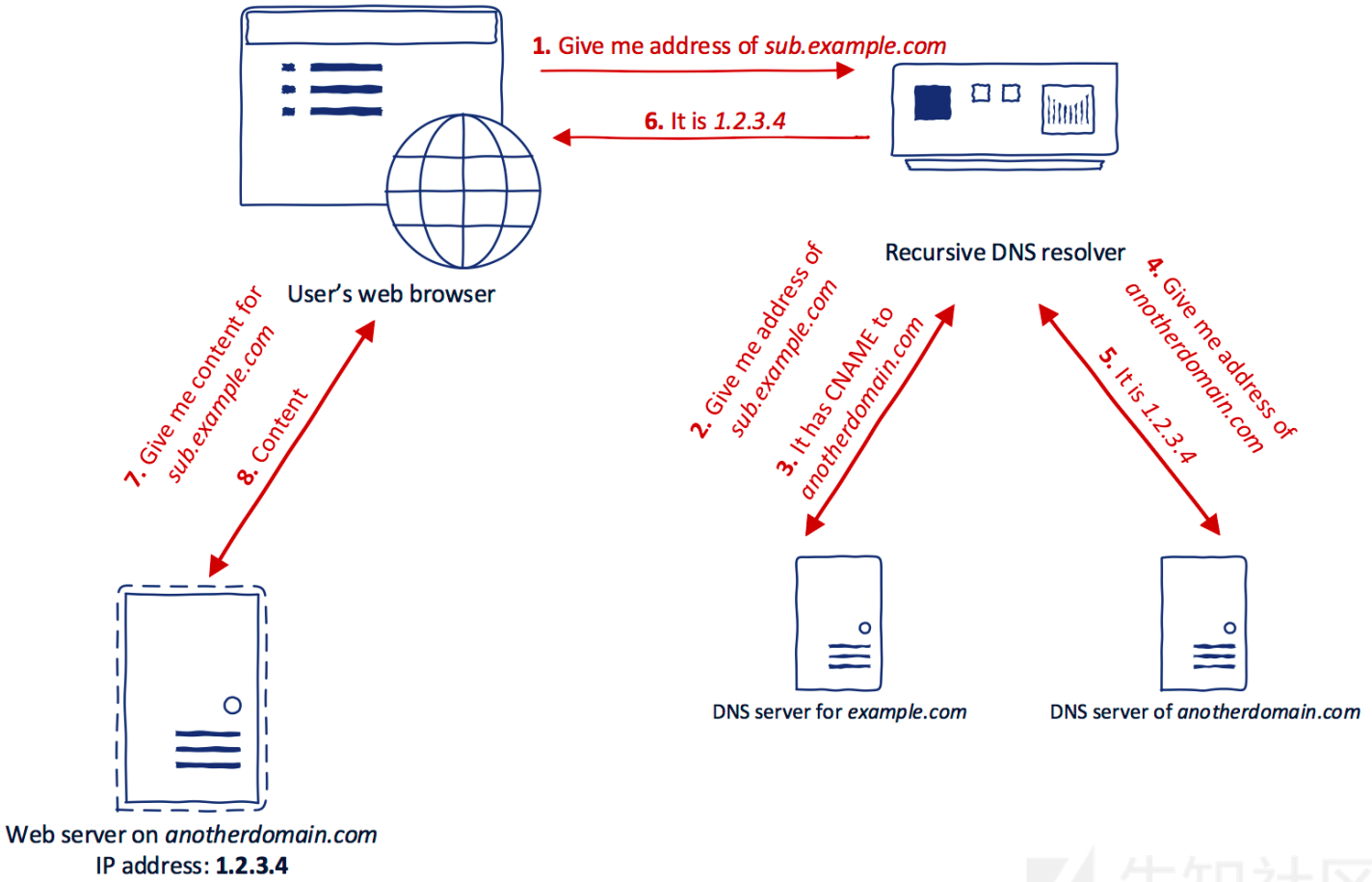
当使用 HTTPS 的时候才使用此 cookie

# 子域名劫持

# 子域名劫持

Syclover

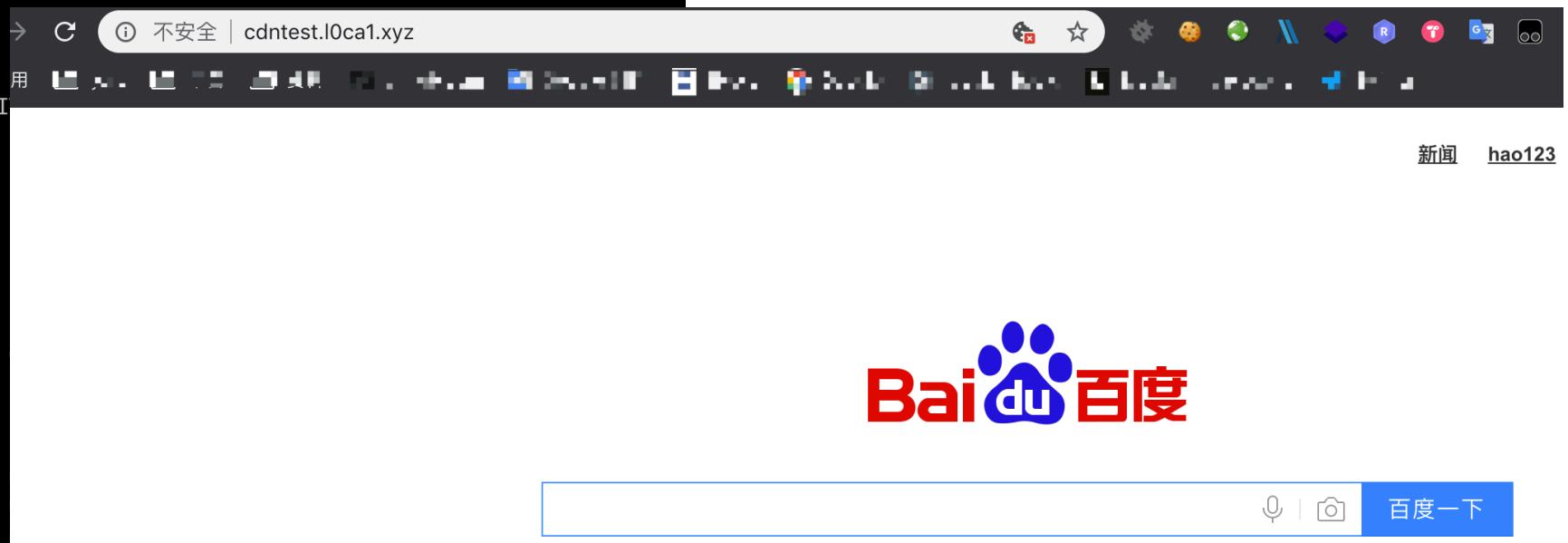
## 什么是子域名劫持



# 子域名劫持

Syclover

```
bash
l0ca1deMacBook-Pro:~ l0ca1$ dig cdntest.l0ca1.xyz

; <<>> DiG 9.10.6 <<>> cdntest.l0ca1.xyz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORI

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cdntest.l0ca1.xyz.             IN      A

;; ANSWER SECTION:
cdntest.l0ca1.xyz.      436     IN      CNAME
d2cnv2pop2xy4v.cloudfront.net. 60 IN    A

;; AUTHORITY SECTION:
d2cnv2pop2xy4v.cloudfront.net. 1667 IN  NS
d2cnv2pop2xy4v.cloudfront.net. 1667 IN  NS
d2cnv2pop2xy4v.cloudfront.net. 1667 IN  NS
d2cnv2pop2xy4v.cloudfront.net. 1667 IN  NS

;; ADDITIONAL SECTION:
```




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Web | EQKPG5ZGV95BO | d2muj1uvq8it9n.clou | - | www.baidu.c | cdntest.l0ca1.x | In Progres | Enabled | 2018-11-01 16:36 U |

# 子域名劫持


利用

- 钓鱼
- 资源控制
- Cookie 获取

# 第三方服务安全

# 第三方服务安全

Syclover

## 第三方应用

案例：百度统计 DOM X

# 第三方服务安全


## 第三方应用

- 不正确的使用

  Firebase 数据库权限配置

- 站点本身安全 + 第三方应用

  Oauth 认证安全

# 第三方服务安全


## Subresource Integrity 策略

<script crossorigin="anonymous" integrity="sha256-+Ec97OckLaaiDVIxNjSlGzl1xSzrqh5sOBV8DyYYVpE=" src="http://cdn.xx.com/jquery.js"></script>

- csp 的保护
- https 内容 + http 资源、http 内容 + http 资源

# Thanks