Wooyun

从一个被忽略的漏洞到XSS 僵尸网络

gainover

➡ 中国细胞生物学大会

其实，
我是一个生物研究工作者。

不要问我：

转基因到底有没有危害？

XSS漏洞是什么？

XSS漏洞

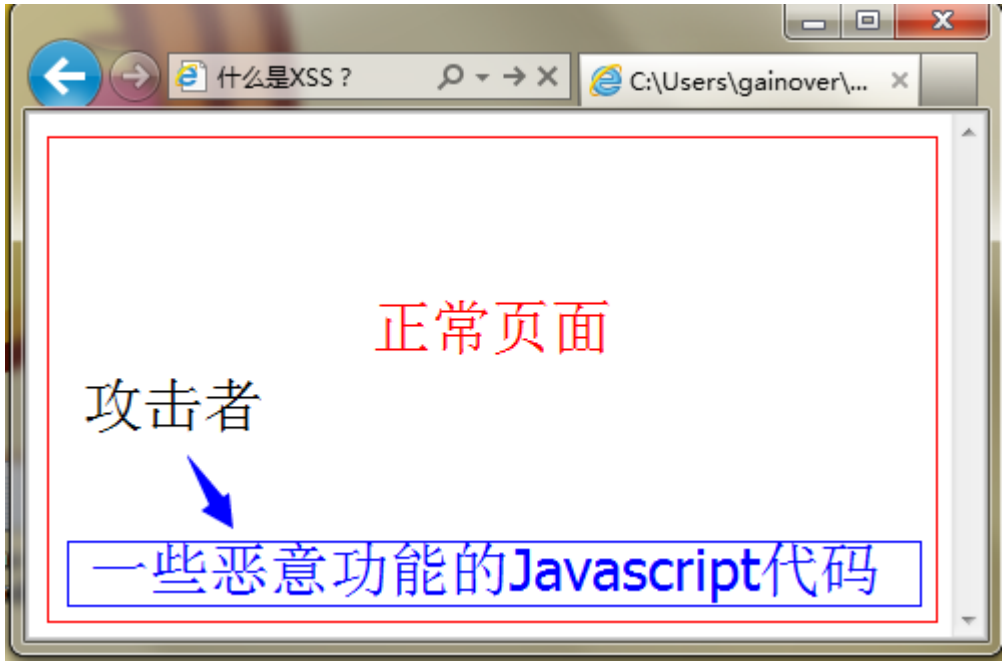
当一个页面允许攻击者向其中插入恶意代码的时候，就说明其代码存在XSS漏洞。

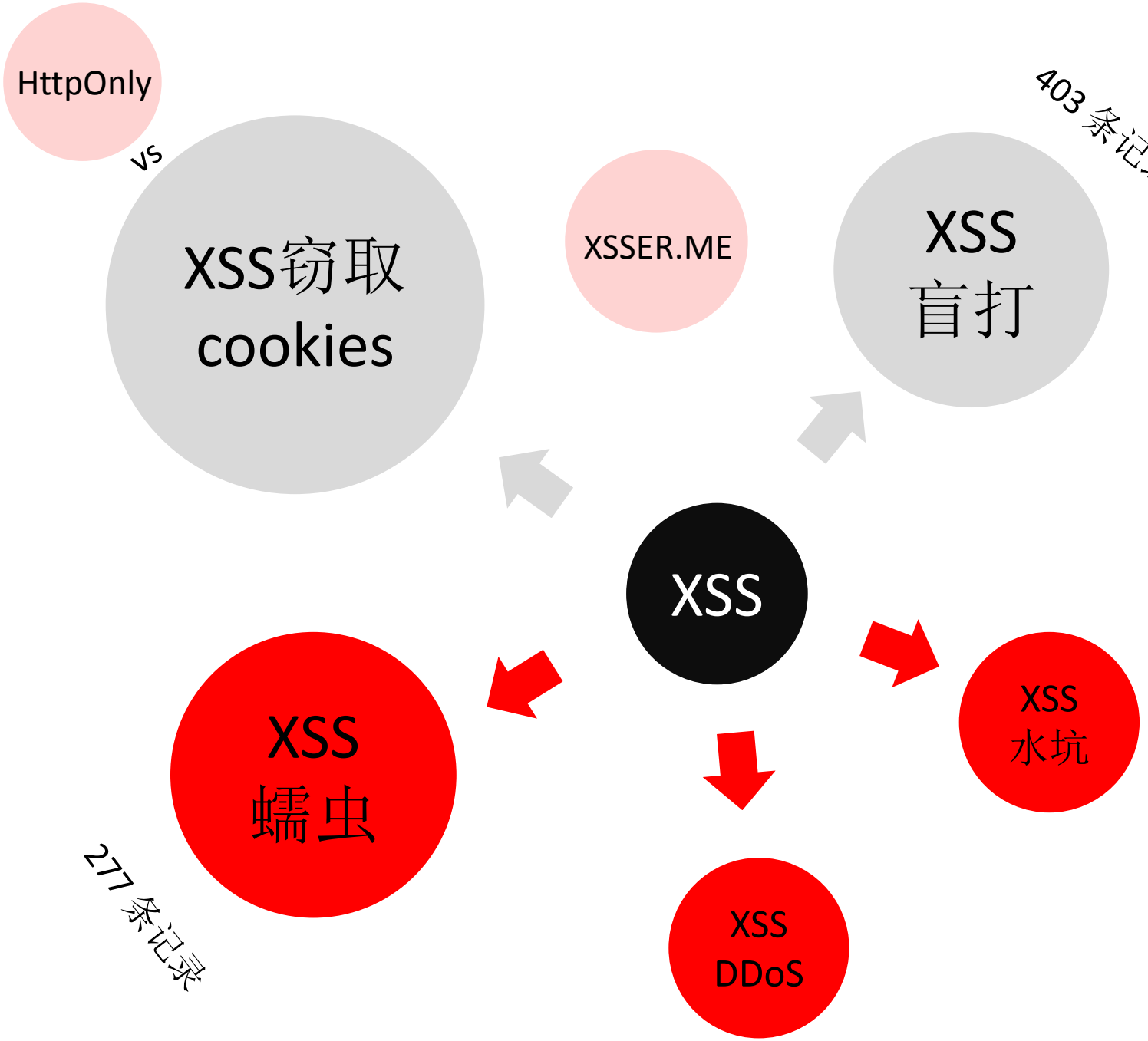
XSS漏洞挖掘

想办法把自己代码插入到目标页面。

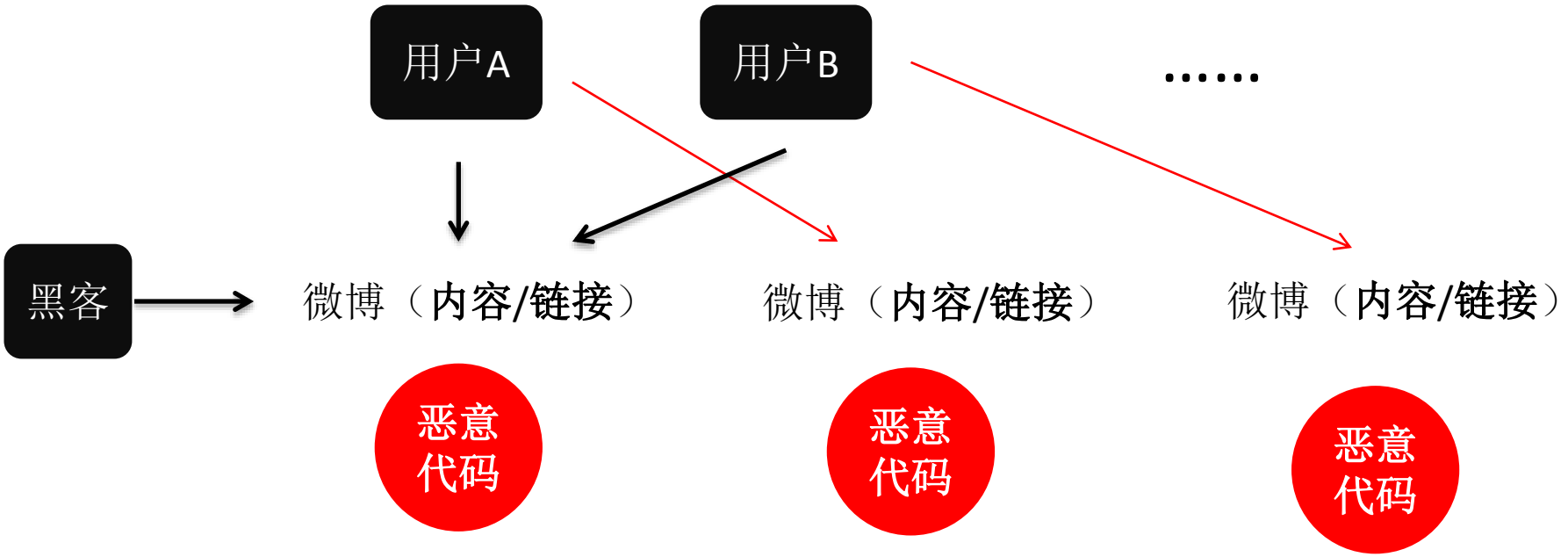
XSS漏洞利用

拿插入的JS代码做你想做且浏览器中能做的事情。



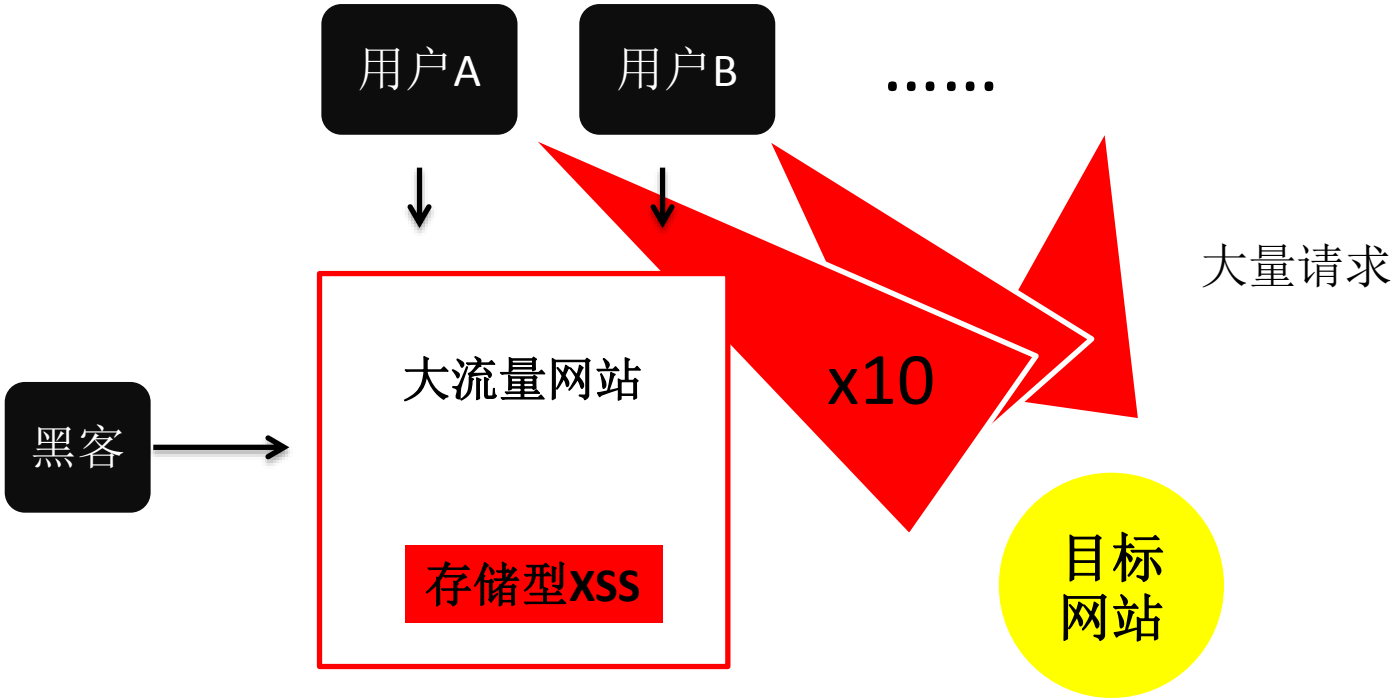

HttpOnly
vs
XSS窃取
cookies
XSSER.ME
403 条记录
XSS
盲打
XSS
XSS
蠕虫
277 条记录
XSS
水坑
XSS
DDoS

Xss攻击放大化 之 xss 蠕虫



实际案例： 新浪微博、 百度贴吧

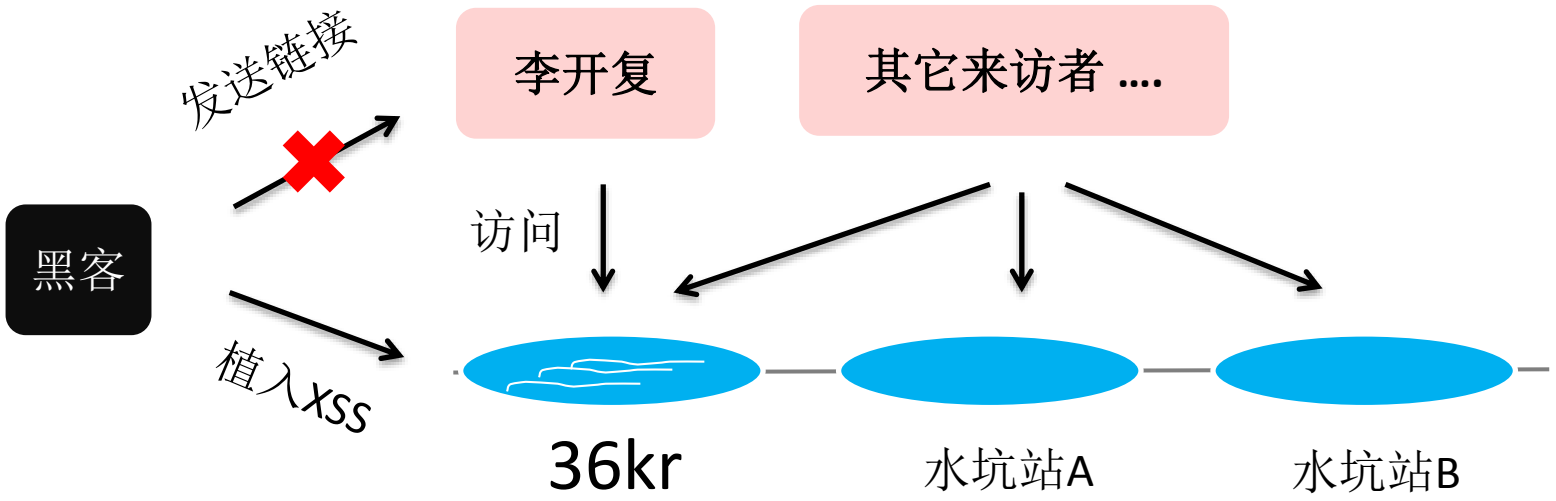
Xss攻击放大化 之 XSS DDoS



实际案例：利用**搜狐视频**的存储型XSS漏洞对目标网站进行DDoS

（网站用户多，流量大，用户在视频页停留时间长）

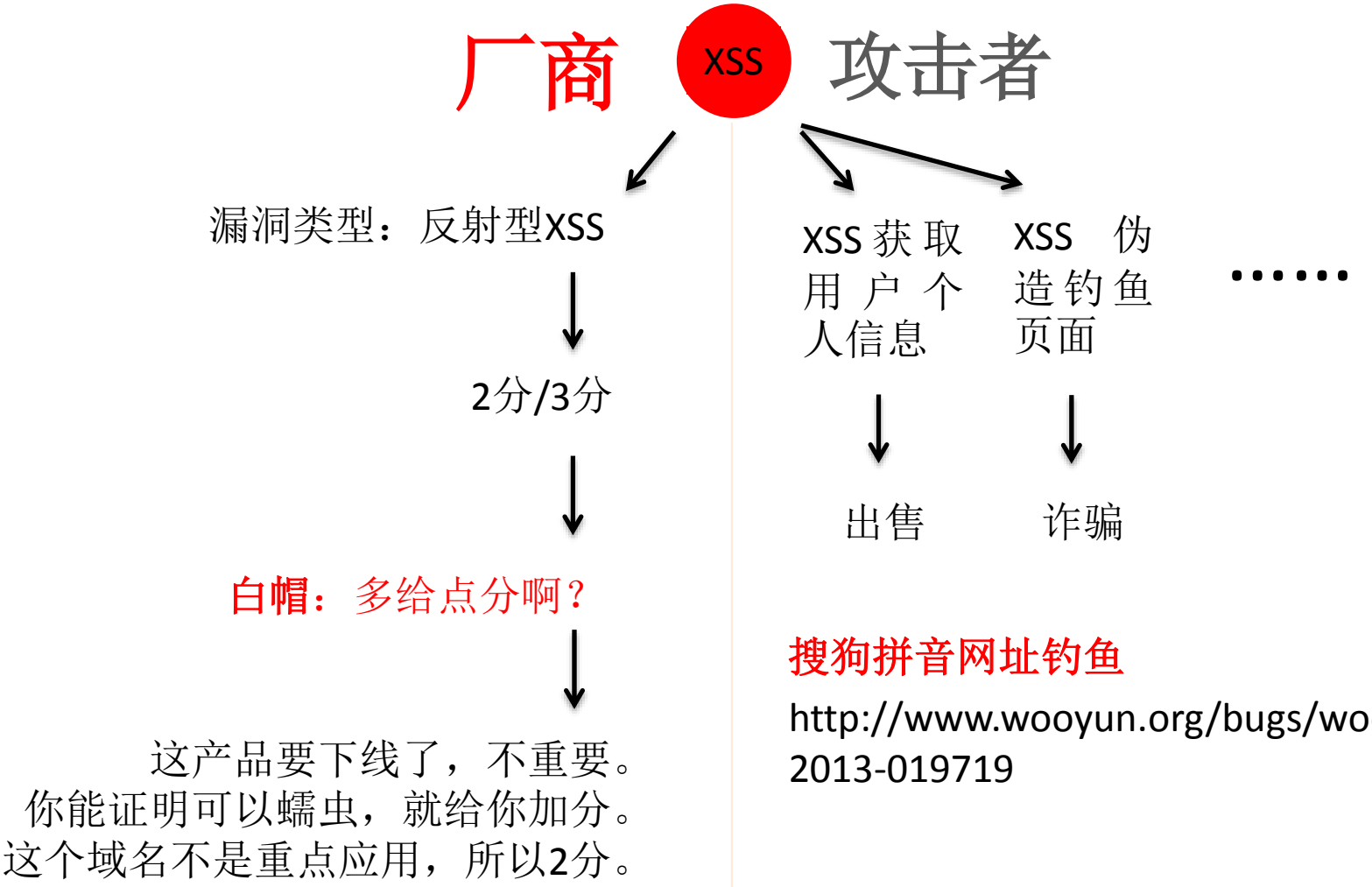
Xss攻击放大化之 xss 水坑攻击



实际案例：

每天早晨起来，把36kr新发布的文章评论中插入QQ的XSS代码，数天后，劫持李开复的腾讯微博，并让其关注了乌云漏洞报告平台。

1. 文章评论插件采用第三方插件，漏洞为第三方插件漏洞
2. 36kr网站只是充当了一个流量载体，攻击者并不关心36kr网站自身的用户数据


厂商
XSS
攻击者
漏洞类型：反射型XSS
2分/3分
白帽：多给点分啊？
这产品要下线了，不重要。
你能证明可以蠕虫，就给你加分。
这个域名不是重点应用，所以2分。
XSS 获取用户个人信息
XSS 伪造钓鱼页面
……
出售
诈骗
搜狗拼音网址钓鱼
http://www.wooyun.org/bugs/wooyun-2013-019719

对于**攻击者**来说，
任何一个看似很小的漏洞，
都能被充分利用。

一个被忽略的漏洞。。。。

缺陷编号： **WooYun-2013-39670**
漏洞标题： 优酷分站一个存储型XSS漏洞
相关厂商： **优酷**
漏洞作者： neobyte

漏洞原理见乌云**drops**: http://drops.wooyun.org/papers/1426


http://v.youku.com/v_show/id_XNjIwNDI2NDI0.html?f=20383529&ev=1
重阳节老人视频集锦—专辑：《重阳节特辑：人...
YOUKU 优酷
首页
频道
搜库
资讯频道 > 资讯专辑 > 重阳节特辑：人老心不老 活出童趣活在阳光
重阳节老人视频集锦
广告剩余 6 秒
静音
Message from webpage
youku.com
OK
www.wooyun.org

为什么被忽略？

1. 因为缺陷文件的域名不是 ***.youku.com**？

   http://irs01.net/MTFlashStore.swf

   但实际上此XSS代码所影响的域确实是优酷的域名。

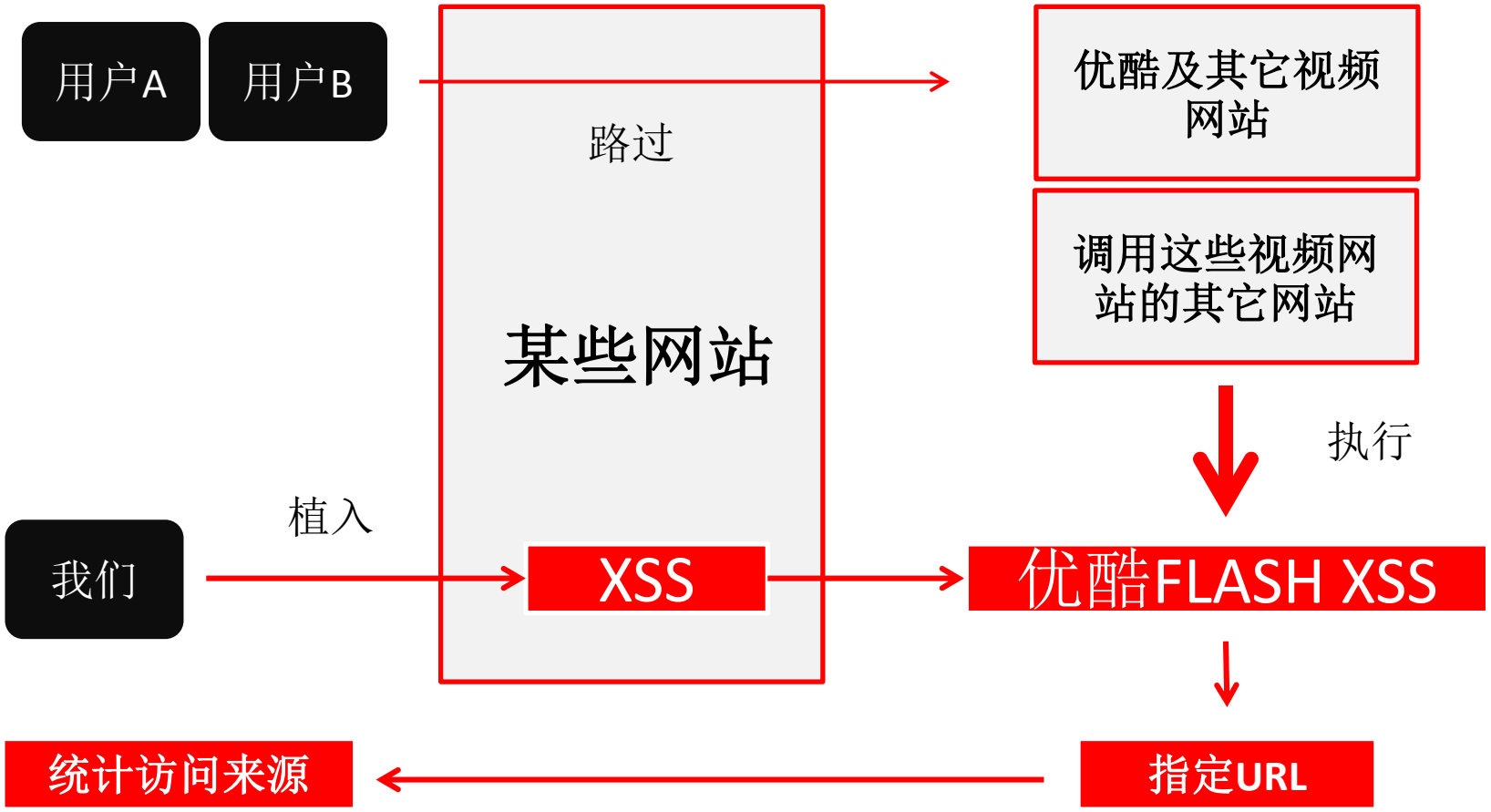
2. 既然该第三方文件的XSS能影响到自身域名，为什么没有通知第三方进行修复？

   这是一种“反正不是我们自己文件所造成的缺陷”的心态么？

漏洞被**忽略**，会有什么后果呢？

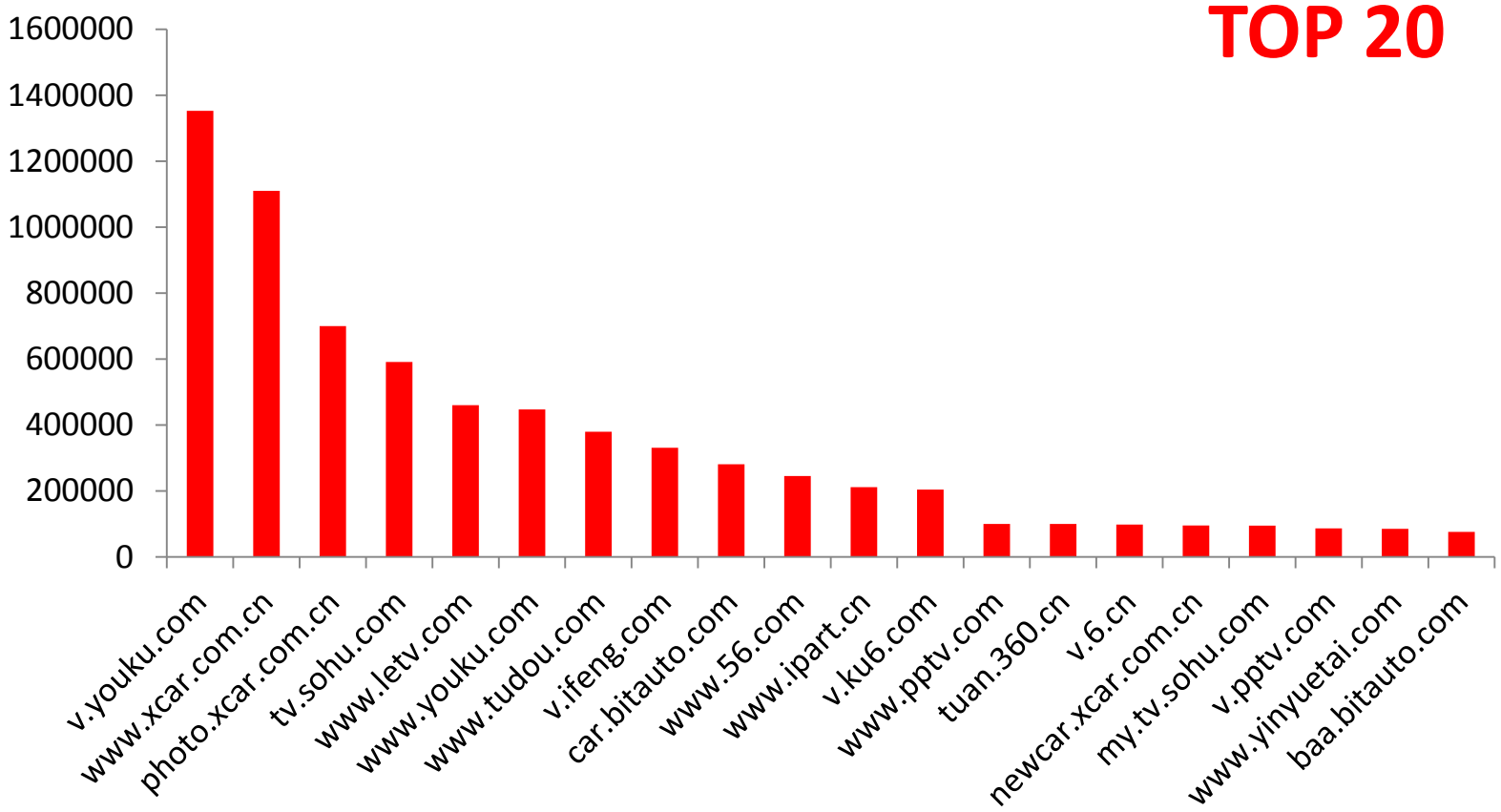
视频录像 0x01

问题1：到底有多少网站受这个漏洞影响？



统计结果：

- 2.39 GB 访问日志
- 9513830次 带有请求来源的访问请求
- 2831 个 域名



问题2：你弹个窗有什么用？

从

alert("ok")

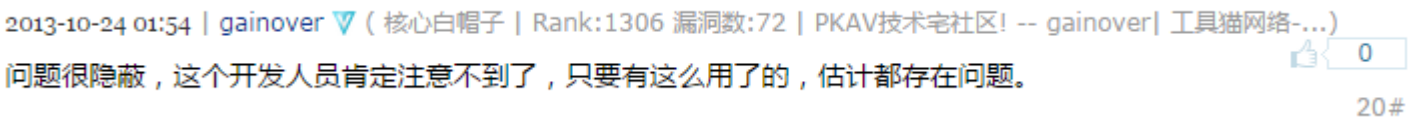
到

真实数据的泄漏

视频录像 0x02

就这样完了吗？？？

当然，不仅仅是这一个漏洞！



2013-10-24

问题很隐蔽，这个开发人员肯定注意不到了，只要有这么用了的，估计都存在问题。

还有**哪些**呢？

乌云上已公开案例

2013-11-14

新浪博客存储型XSS（**全部博客可留后门**）

2014-02-21

一个可大规模悄无声息**窃取淘宝/支付宝账号与密码**的漏洞

2014-03-20

我是如何实现批量种植rootkit**窃取阿里云账号密码**的

暂未公开案例

视频录像 0x03

（电商案例）

视频录像 0x04

（社交网络应用案例）

漏洞特点与XSS僵尸网络

隐蔽性

对用户

用户说：钓鱼网站我都分不清！

对厂商

恶意代码存储在用户电脑中，
从厂商角度，网站无任何异常！

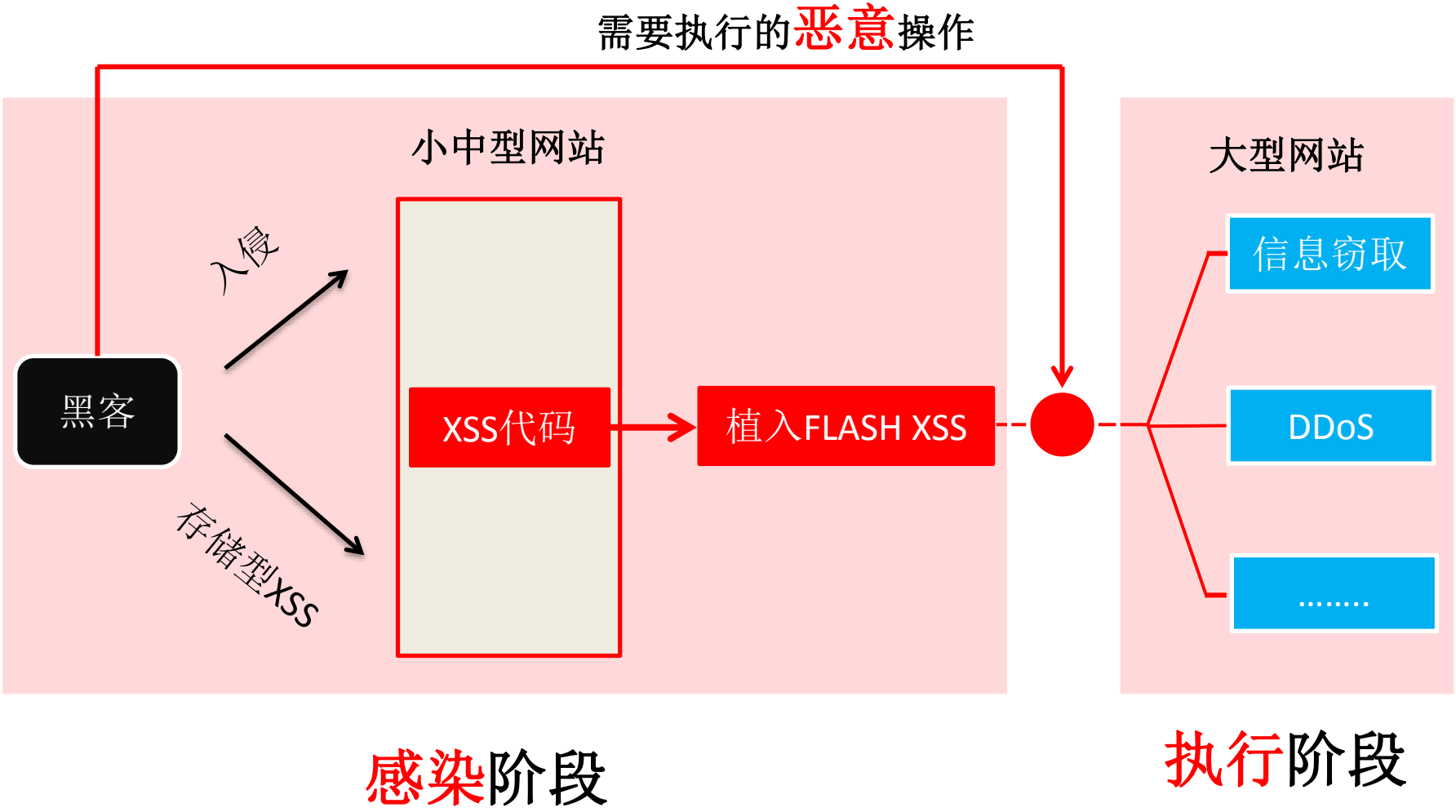
持久性

长期存在于用户电脑中，
且**不易清理**，
每次用户打开存在漏洞网站均会触发。

流量大

受影响网站用户量大，
用户在页面停留时间长。
使得XSS的利用代码
可以**获得更长的执行时间**。

XSS僵尸网络的构建


需要执行的恶意操作
小中型网站
大型网站
入侵
黑客
XSS代码
植入FLASH XSS
存储型XSS
信息窃取
DDoS
.....
感染阶段
执行阶段

欢迎提问

成都*PKAV*团队招人

如有意向者

请将简历发送至 ***g_@live.com***

谢谢大家!