非传统型威胁

社交网络安全

OWASP 中国

The Open Web Application Security Project

关于我

OWASP 中国
The Open Web Application Security Project

- 刘丹
- 人人网 安全中心

- Daniel Liu
- Renren Inc. Security Center
- Dan.liu@renren-inc.com

摘要

OWASP 中国
The Open Web Application Security Project

- 我们面临的威胁
- 如何定义这些威胁
- 威胁背后的利益
- 如何处理这些威胁
- 趋势和案例分析

我们面临的威胁

OWASP 中国
The Open Web Application Security Project

- 我们面临的威胁
  - 传统web攻击:XSS、CSRF、SQL Injection
  - 社交营销:发布垃圾信息
  - 帐号攻击:暴力破解帐号
  - 虚假帐号:僵尸帐号
  - 数据收集:恶意索引SNS数据

- 如何定义这些威胁
  - 特征
    - 传统-失能：业务功能遭到攻击，导致无法正常提供服务
    - 非传统-异常：寄生在业务中的非法数据流
  - 定义：
    - 传统：系统功能失常，无法提供服务
    - 非传统：打破正常秩序，非授权利用系统特性，影响服务质量
  - 分类
    - 传统型：基于系统设计缺陷产生的威胁，单一的攻击
    - 非传统型：基于系统的正常功能产生的威胁，组合型攻击

OWASP 中国
The Open Web Application Security Project

中毒/外伤

- 特征突出
- 反应强烈
- 迅速致命

寄生体/毒瘤

- 不易被发现
- 症状舒缓
- 慢性死亡

威胁背后的利益

OWASP 中国
The Open Web Application Security Project

- 传统攻击
  - 利益诉求急促
  - 快速，周期短
  - 危害易于发现
- 非传统攻击
  - 利益长尾效应
  - 进行全面
  - 隐蔽的攻击

威胁背后的利益

OWASP 中国
The Open Web Application Security Project

- 传统攻击：挂马，SEO，获取系统权限
  - 利益薄，风险大
  - 防御容易
- 非传统攻击：将电子邮件营销的方式移植到社交网络，本质相同，都是基于关系的营销策略：“关系营销”
  - 高回报
  - 难于发现甄别
  - 风险低
  - 防御困难
  - 成本和门槛极低

如何处理这些威胁

OWASP 中国
The Open Web Application Security Project

- 传统型:
  - 加强安全规范的实施
  - 加强线上扫描和监控
  - 内网布控

如何处理这些威胁

OWASP 中国
The Open Web Application Security Project

- 非传统型:
  - 行为监控分类
  - 严格给出定义，区分正常和非正常行为
  - 按照业务布控
  - 分析攻击链条，多点打击
  - 基于统计学和机器学习的行为分析系统

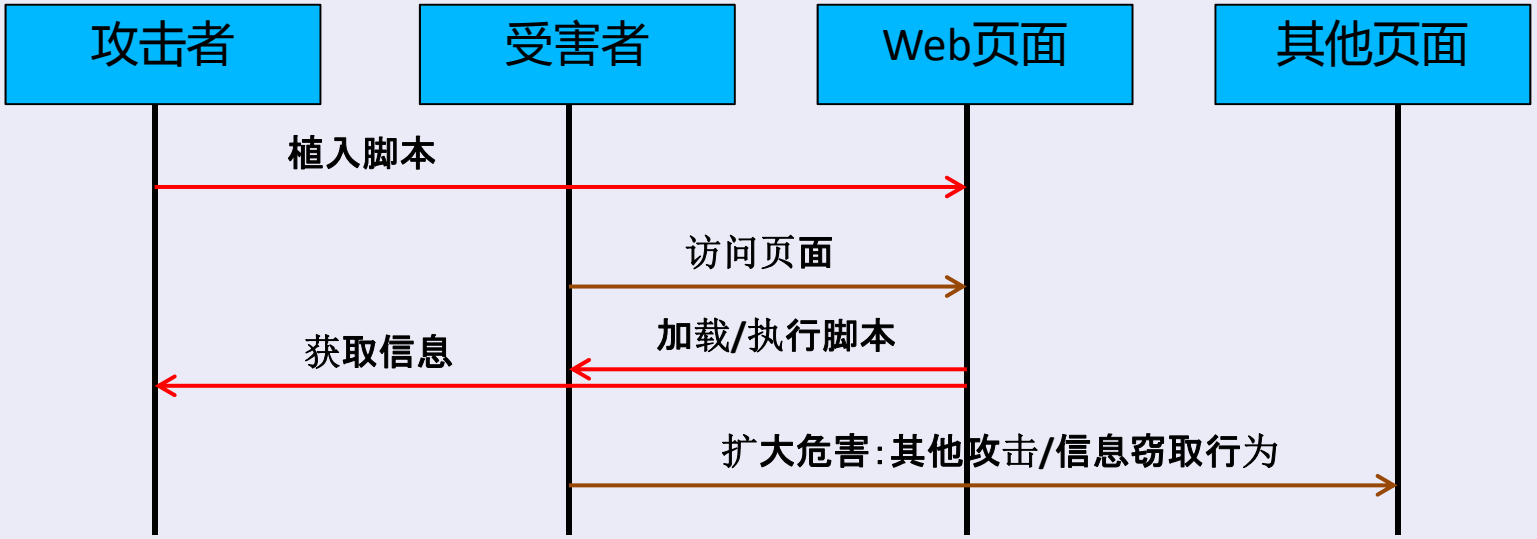
案例和趋势分析

OWASP 中国
The Open Web Application Security Project

- 传统型安全案例
- 非传统型安全案例
- 结合型案例

OWASP 中国
The Open Web Application Security Project

- 案例一
  - XSS攻击：偷取信息劫持用户
  - CSRF攻击：劫持用户



案例和趋势分析

OWASP 中国
The Open Web Application Security Project

- 案例二
  - 注册恶意帐号
  - 垃圾信息发布
  - 恶意加粉丝
  - 刷浏览量

- 案例三：混合型攻击
  - 基于传统攻击
  - 将两种攻击有机结合
  - 针对新的机器学习系统，可以绕过，增加识别难度
  - 隐蔽，可控性强，利益明显
  - 互为补充缺点，诱使系统误判，无法采取正常手段防御

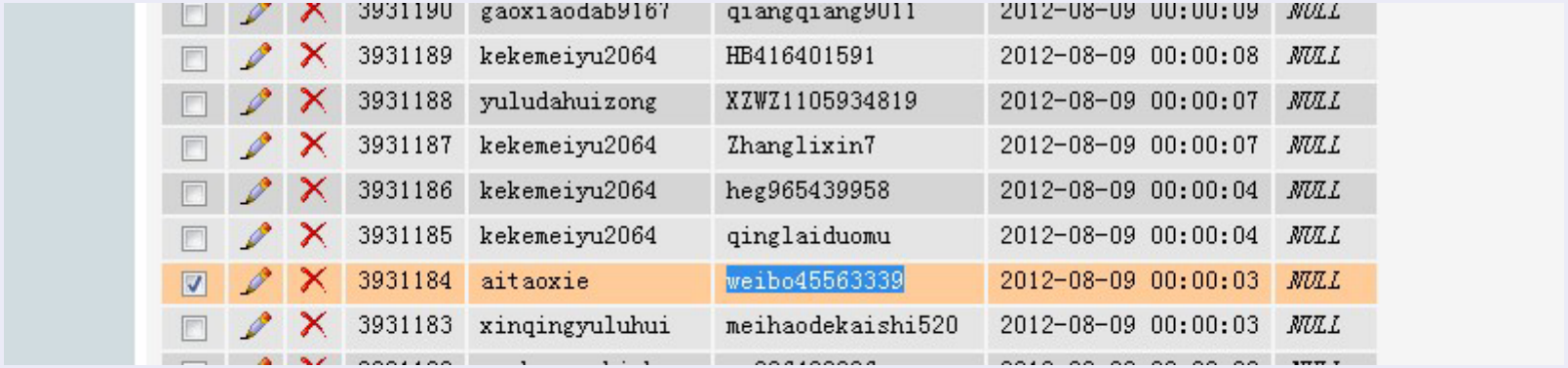
案例和趋势分析

OWASP 中国
The Open Web Application Security Project

id	Type	UrlReferrer	Domain	IP	Timer	Accredit	trigger	Cookies
13841498	ad2	NULL	adsfile.qq.com	116.28.102.218	2012-08-09 00:36:46	1	0	NULL
13841497	ad2	NULL	adsfile.qq.com	112.95.126.188	2012-08-09 00:24:27	1	0	NULL
13841496	ad2	NULL	adsfile.qq.com	58.254.59.213	2012-08-09 00:23:55	1	0	NULL
13841495	ad2	NULL	adsfile.qq.com	121.15.135.209	2012-08-09 00:08:08	1	0	NULL
13841494	ad2	NULL	adsfile.qq.com	125.91.128.73	2012-08-09 00:06:03	1	0	NULL
13841493	ad2	NULL	adsfile.qq.com	121.10.176.202	2012-08-09 00:04:48	1	0	NULL
13841492	ad2	NULL	adsfile.qq.com	222.50.13.206	2012-08-09 00:04:32	1	1	NULL
13841491	ad2	NULL	adsfile.qq.com	58.255.126.2	2012-08-09 00:03:20	1	1	NULL
13841490	ad2	NULL	adsfile.qq.com	119.130.77.63	2012-08-09 00:01:59	1	0	NULL
13841489	ad2	NULL	adsfile.qq.com	119.122.187.249	2012-08-09 00:01:40	1	1	NULL

案例和趋势分析

OWASP 中国
The Open Web Application Security Project



			3931190	gaoxiaodab9167	qiangqiang9011	2012-08-09 00:00:09	NULL
			3931189	kekemeiyu2064	HB416401591	2012-08-09 00:00:08	NULL
			3931188	yuludahuizong	XZWZ1105934819	2012-08-09 00:00:07	NULL
			3931187	kekemeiyu2064	Zhanglixin7	2012-08-09 00:00:07	NULL
			3931186	kekemeiyu2064	heg965439958	2012-08-09 00:00:04	NULL
			3931185	kekemeiyu2064	qinglaiduomu	2012-08-09 00:00:04	NULL
☑			3931184	aitaoxie	weibo45563339	2012-08-09 00:00:03	NULL
			3931183	xinqingyuluhui	meihaodekaishi520	2012-08-09 00:00:03	NULL

案例和趋势分析


OWASP 中国
22
23
24
public function addqq(param1)
var e:* = event;
phpMyAdmin
localhost ▸ weibo
结构 SQL 搜索 查询 导出 导入 操作 权限 删除
数据库
(10)
(10)
hetie
dom
ip
log
mallog
bo
bo3
表 操作 记录数 1 类型 整理 大小 多余
cachetie 0 MyISAM utf8_general_ci 1.0 KB -
dom 3 MyISAM utf8_general_ci 3.1 KB -
errdom 0 MyISAM utf8_general_ci 1.0 KB -
errip 21,585 MyISAM utf8_general_ci 1.5 MB -
errlog 93,114 MyISAM utf8_general_ci 17.0 MB -
normallog 13,841,498 MyISAM utf8_general_ci 1.2 GB -
qq 114,787 MyISAM utf8_general_ci 11.4 MB 4.6 MB
qq2 2,818,840 MyISAM utf8_general_ci 229.3 MB -
weibo 19,760 MyISAM utf8_general_ci 740.3 KB -
weibo3 0 MyISAM utf8_general_ci 1.0 KB -
10 个表 总计 16,909,587 MyISAM utf8_general_ci 1.4 GB 4.6 MB
catch (e)
50
51
52
执占搜索推荐
posturl("http://radio.t.qq.com/mini/follow.php", "u=" + addqq + "&uin=" + qqnum

声明

OWASP 中国
The Open Web Application Security Project

- 本讲稿涉及公司和内容的最终解释权归其所有
- 所涉及的案例图片未经许可禁止转载

OWASP 中国

The Open Web Application Security Project

感谢