

这十年

2016 FIT 互联网安全创新大会

这十年



Only_guest

2016.1.8

- 关于我

张瑞冬

only_guest

PKAV负责人

双螺旋攻防实验室负责人



为什么选择做安全



Only_guest
2016.1.8

趣事



Only_guest

2016.1.8

网络仲裁者



Only_guest

2016.1.8



破壳网络 pker.in
精英小组

破壳



網絲精英

WWW.PKER.IN

破壳网络 精英小组
PKER.IN

pker.in



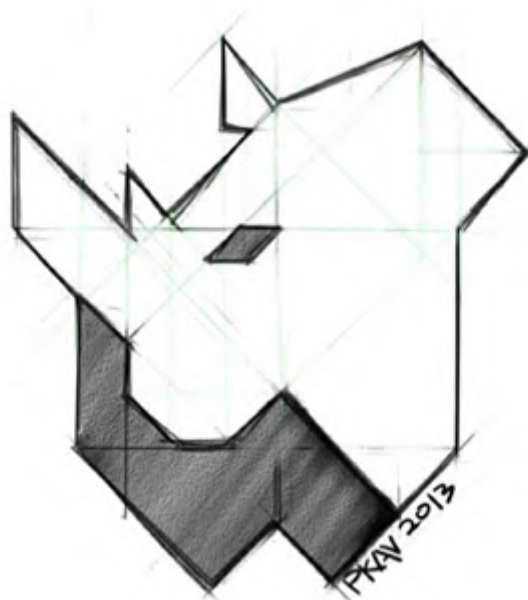
精英小组

破壳网络



Only_guest

2016.1.8



Only_guest
2016.1.8

如何在这条路上快速成长

说：我会。



线下培训

教学模式



教学环境



一楼：教学区 二楼：办公区、休闲区、冥想区



Only_guest

2016.1.8



学员们的 Paper

- 《当 XSS 时长度不够怎么办？Short XSS》
- 《当下最流行的3大黑客 SEO 优化手法大曝光》
- 《浅析现代浏览器安全》
- 《PHP 非字母数字的代码》
- 《Flash CSRF 的原理与 Exp 的编写》
- 《XSS与字符编码的那些事儿》



现在的我和我的团队在干什么



Only_guest
2016.1.8



潮风
Chaofeng

Q 搜索

高级搜索



Only_guest
2016.1.8

寻迹，追寻你的足迹...

邮箱 / 用户名 / 手机号

开始搜索

©PKAV 2015



Only_guest

2016.1.8



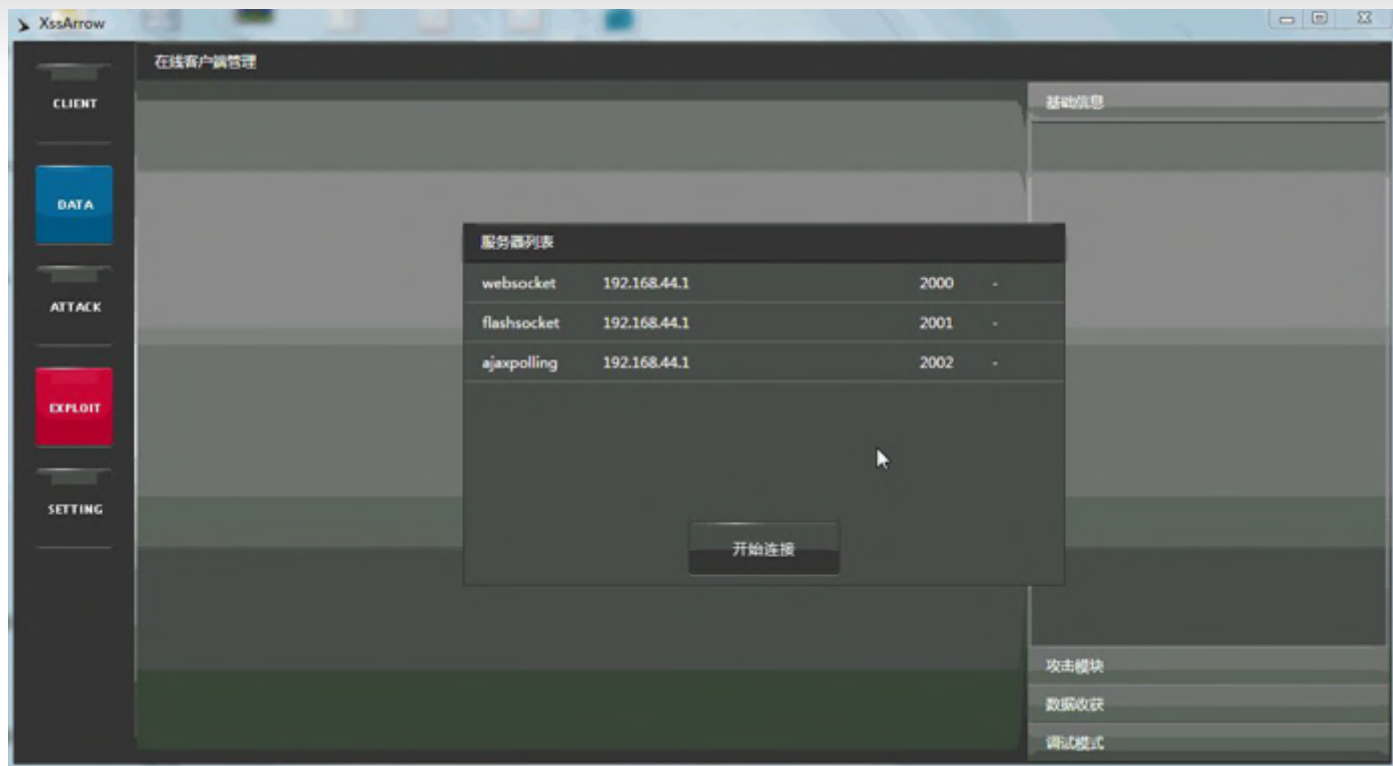


XssArrow

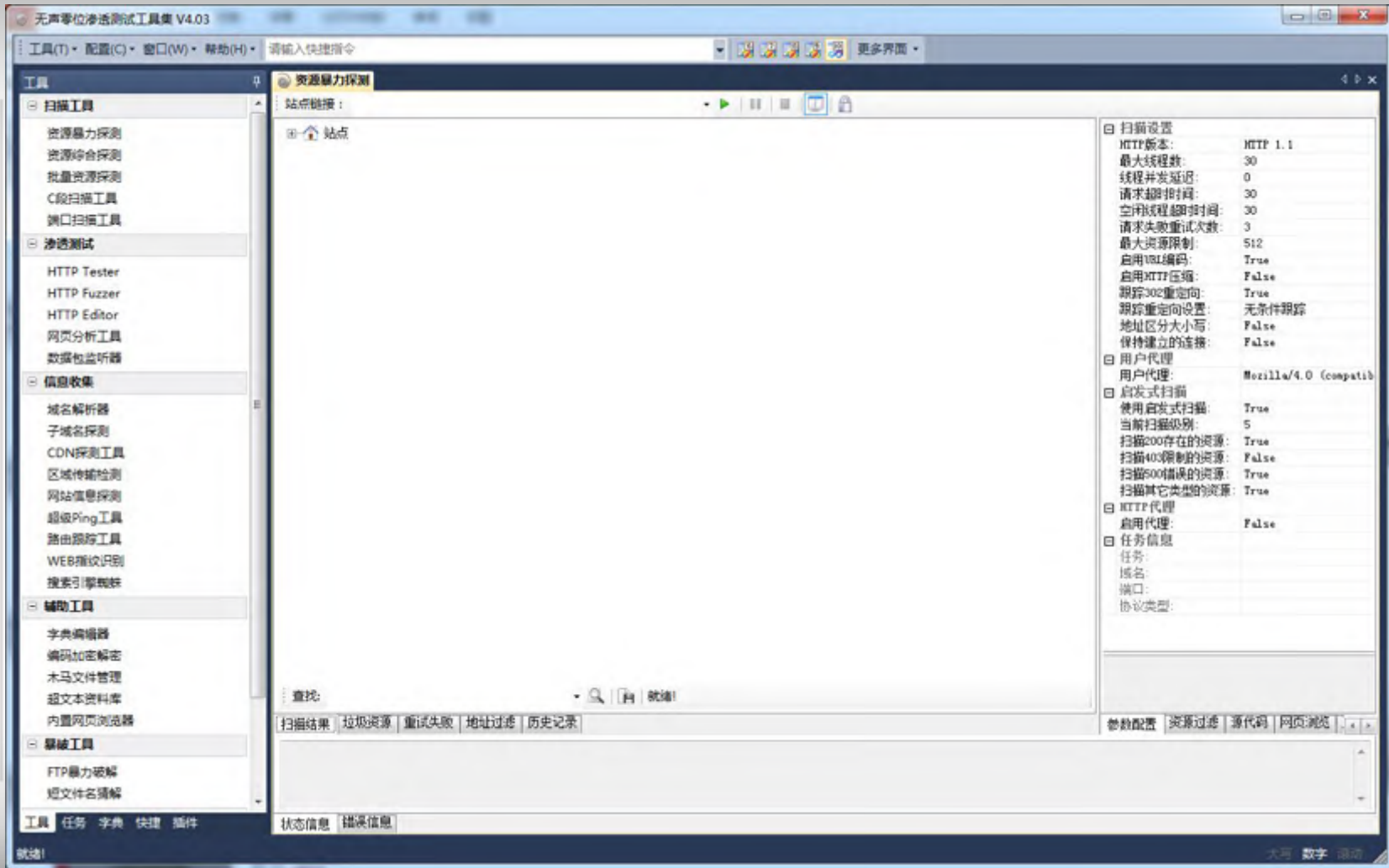
PKAV WEB SECURITY TEAM



Only_guest
2016.1.8



Only_guest
2016.1.8





PKAV HTTP Fuzzer 1.5.3



Only_guest
2016.1.8

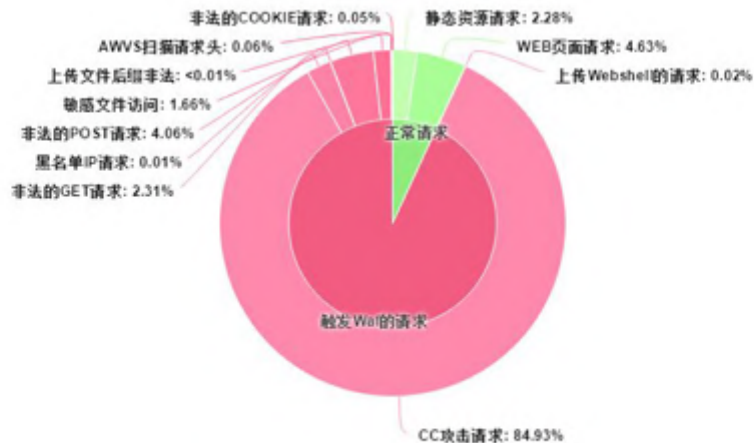
.gov.cn

时间：2015/8/1 上午12:00:00 - 2015/9/17 下午11:59:00

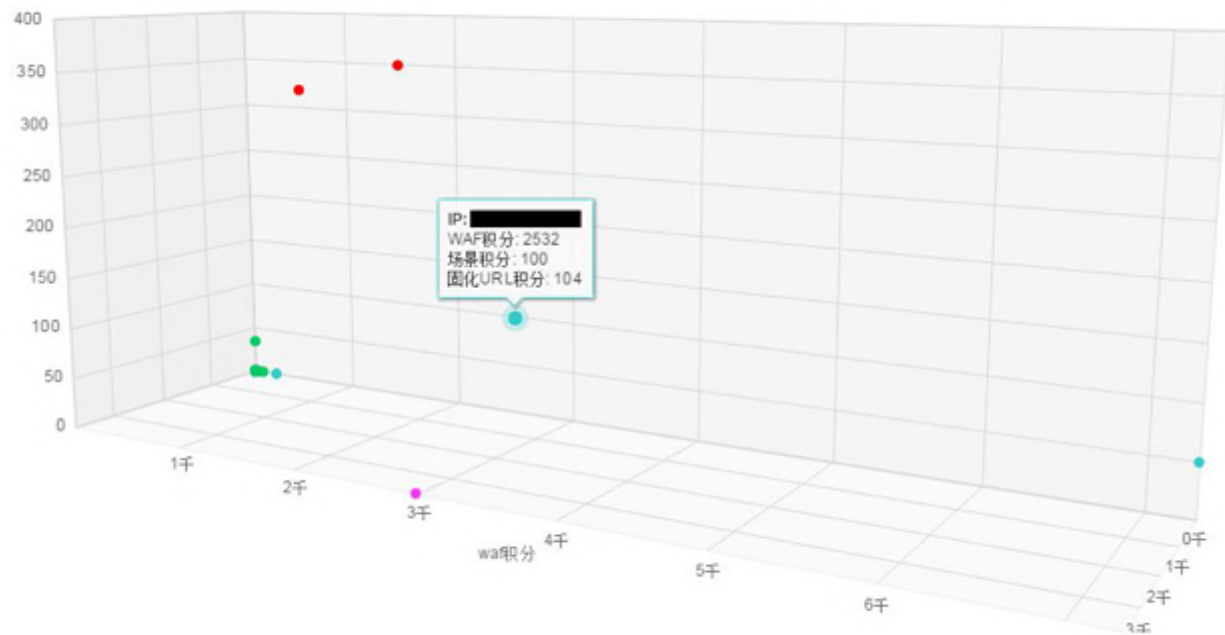
- 整体安全评级：**4**
- 威胁得分基值：374.17

得分
16762.05

访问请求信息

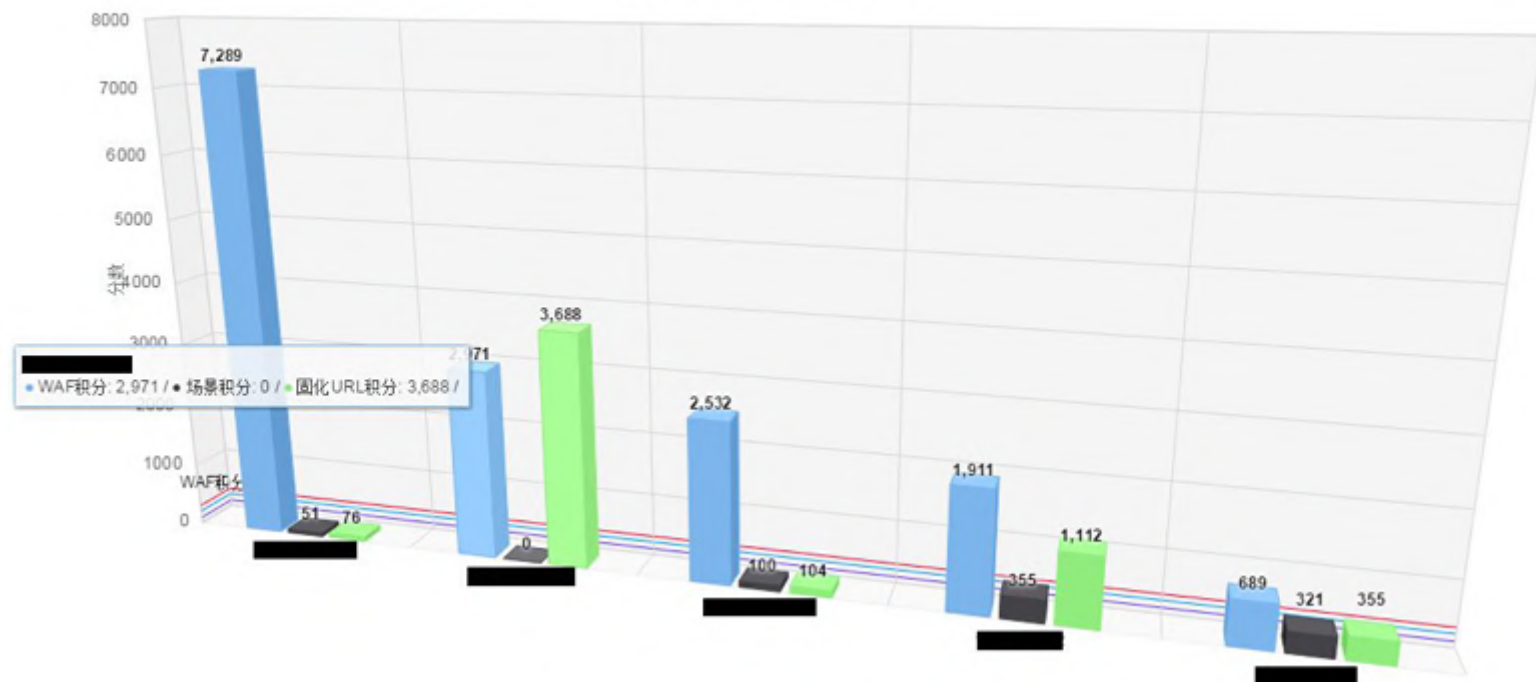
访问总请求
171403正常访问请求
11840疑似攻击请求
159563Only_guest
2016.1.8

(可拖拽视图、单击某点显示该IP详情)



最具威胁的IP统计

(可拖拽视图、单击任意区域显示详细信息)



The Mobile Application Vulnerabilities Evaluation(MAVE)

Definition

- 开放式移动应用安全缺陷评估
- 一个维基式开放交流与安全缺陷评估体系
- 致力于建立规范化移动应用安全缺陷评估体系

Duty

- 维护项目结构
 - 展示窗口
 - 成员组织
 - 软件集合
- 开放式建设
 - 产出移动应用缺陷检测工具
 - 开源
 - 检测点来自移动应用攻击途径检查表
 - 产出行业内移动应用安全报告
 - 来源于成员组织内贡献者
 - 产出移动应用攻击途径检查表
 - 来源于维基式的规范检查体系
 - 追踪与披露恶意移动应用细节
 - 来源于成员组织内贡献者
 - 为移动应用参与节点评估安全缺陷
 - 移动智能设备
 - 主流移动应用
 - 安卓应用市场
- 为通过安全缺陷检测的移动应用颁发安全许可
 - 通过移动应用途径检查表的移动应用
 - 每个通过的应用分配一个hash值
 - 通过hash值可到网站上查阅相关安全检测信息
- 协助移动应用参与节点控制攻击风险
 - 提供专业化的安全解决方案

Architecture

- 展示窗口
 - 网站
 - 展示MAVE工作内容
 - 披露移动应用攻击方法
 - 报道移动应用安全资讯
 - 恶意移动应用追踪报告
 - 报告
 - 移动应用安全评估报告
 - 移动应用攻击途径检查表
 - 移动应用市场安全评估报告
- 成员组织
 - 项目推动事业部
 - BlackHeart
 - 四川无声信息技术有限公司双螺旋安全实验室PKAV团队下属移动安全研究小组
 - 四川大学实验室
 - 第三方贡献者
 - 责任贡献者
 - 高级事业推动成员
- 软件集合
 - 开放式工具集
 - 移动应用缺陷检测工具
 - 专业移动应用安全解决方案

网络仲裁者



Only_guest

2016.1.8

我们在做一切我们喜欢的，有趣的，你也可以加入我们



Only_guest
2016.1.8



以后的我

空闲继续研究各种有趣的技术

做一个优秀的产品经理

做一个优秀的团队负责人

打造一支优秀的网络安全团队



Only_guest

2016.1.8

THANKS