




2016 杭州·云栖大会  
THE COMPUTING CONFERENCE

云栖社区  
yq.aliyun.com

# 云盾为视频系统筑建安全堡垒

2016  
The Computing Conference

主办单位:  杭州

 Alibaba Group  
阿里巴巴集团

战略合作伙伴: 

宽夫  
阿里云安全事业部架构师



扫码观看大会视频

---

# 目录

## content

---

1. 视频行业安全诉求
2. 下注云盾，启动安全护航
3. 共建直播行业安全标准



《关于

尊敬的

7月19

一次恶

云计算

已恢复

有再次

公司已启

严重和

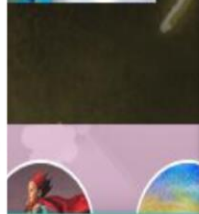
公安机

争,又

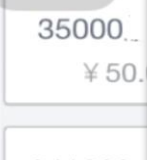
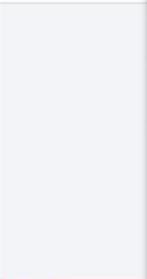
击者必



扫一扫



●●●●● 中国



售价:¥6.0

漏洞标题: 某海个人网盘泄露公司敏感信息

漏洞等级: 低危

漏洞URL: <http://yunpan.360.cn>

简要描述(说明影响):

某海个人网盘中上传了公司敏感信息,造成公司大量敏感信息泄露,其中包括网站后台等

详细说明(详细说明漏洞发现的过程,提供截图;有POC提供POC):

某海个人网盘中上传了公司敏感信息,造成公司大量敏感信息泄露,其中包括网站后台等

360云盘

网盘 网络相册 云收藏 更多

所有文件

上传

新建文件夹

所有文件

原型html

数据需求.xlsx

原型.zip

原型.html.zip

数据后台原型0625

来自-手机M60-L11

数据分析

运维工作

临时

名称	修改日期	类型
原型html	2016/3/26 14:05	文件夹
数据需求.xlsx	2016/3/26 4:03	Microsoft Excel 工...
原型.zip	2016/3/26 3:25	WinRAR ZIP 压缩文...
原型.html.zip	2016/3/26 3:47	WinRAR ZIP 压缩文...

扫码观看大会视频

部

标题

作者

最新回复

点击 回复 回复时间 ↓

③ 收shell的php要一手的骗子滚

169 004

a5

311 1 08-28 14:50

③ 买shell, 要一手的。。能长期合作的联系。骗子滚。

169 004

a5

393 1 08-28 14:50

③ 国内著名黑客联系

a5

a5

48 0 08-28 14:43

③ 5万求拿某站服务器权限, 有的私聊, 要定金免开尊口。

Ch

Ch

85 0 08-04 20:20

③ 所有webshell提权服务器网站统统收购! 加Q602235144

webshell 推

推

185 2 07-25 17:50

③ 批量出售webshell。。。。

甲 推

推

2899 3 07-25 17:48

③ 出售高权重一手webshell, 现拿现卖, 诚信合作QQ: 1841243696

82012 推

推

857 4 07-25 17:35

③ 出售群站服务器

4471 ws

ws

137 0 05-22 11:09

③ 收购权重3以上的shell要收一手的, 长期收购流量。

22330 qq

qq

354 0 01-27 15:31

③ 公布一个骗子QQ137531634淘宝ID: 龙出云6563

oi

oi

373 2 10-19 20:41

③ 长期大量收购网站shell!!!

sa

sa

409 0 10-16 10:59

③ 长期出售webshell, 联系: 1841243696

82012 wo

wo

368 1 10-07 19:32

③ webshell出售, 各种蜘蛛劫持程序。诚信QQ: 811248461

56abc ab

ab

348 0 09-25 14:17

③ 收shell的php要一手的骗子滚

169 004

169

157 0 09-23 13:42

③ 收shell的php要一手的骗子滚

169 004

169

171 0 09-23 13:37

③ 及地方广告早

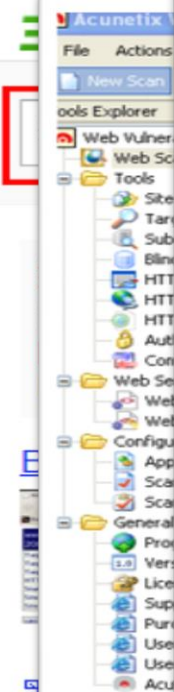
56 756

56

137 0 09-23 13:37



扫码观看大会视频

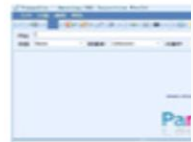


360

sql注入

详解 sql  
学sql注入。  
<http://www>

Pangolin



Pangolin



## 某业务信息泄露(用户手机号&主播敏感信息)

0:25 166

漏洞标题	某业务信息泄露(用户手机号&主播敏感信息)
相关厂商	
漏洞作者	DloveJ
提交时间	2015-10-28 21:51
公开时间	2015-12-10 10:04
漏洞类型	账户体系控制不严
危害等级	高
自评Rank	15
漏洞状态	厂商已经确认
Tags标签	敏感功能直接对外,用户敏感信息泄露



扫码观看大会视频

1

## 快速爆发期，流量安全隐患

直播网站（PC+移动）+房间服务api++聊天/弹幕消息api

2

## 注册、登录、找回密码接口漏洞，粉丝漏洞售卖

新注册用户，恶意调用粉丝接口，获得vip权限

3

## APP端的破解，核心源码泄露

使用模拟器注册客户端，造成运营数据不准及接口乱刷

4

## 运营数据泄露，公司资产损失

服务器及数据库权限暴力破解

5

## 直播内容违规

大量截帧的图片涉黄、涉恐识别



---

# 目录

## content

---

1. 视频行业安全诉求
2. 下注云盾，启动安全护航
3. 共建直播行业安全标准





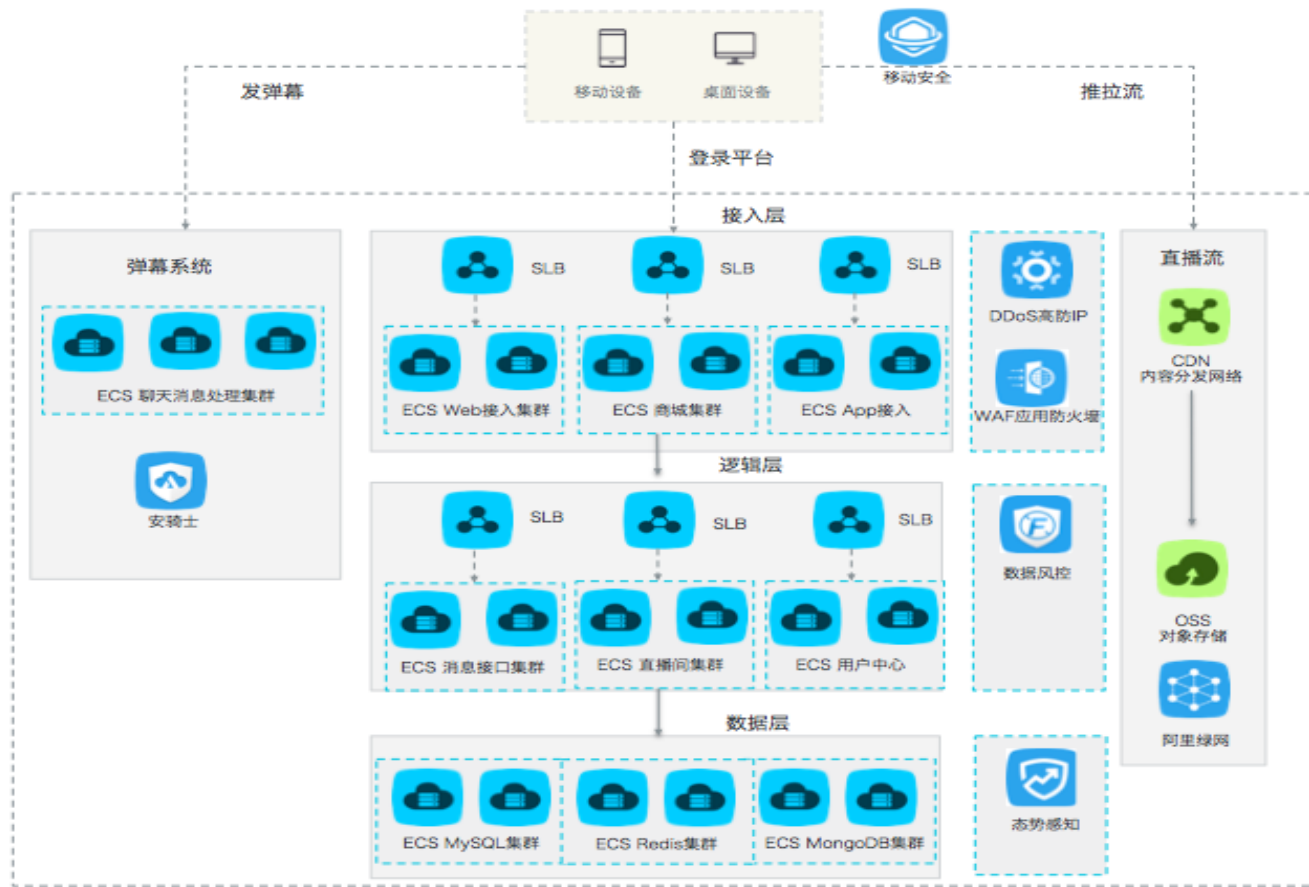
DDoS高防IP

Web应用防火墙

安骑士

态势感知

移动安全



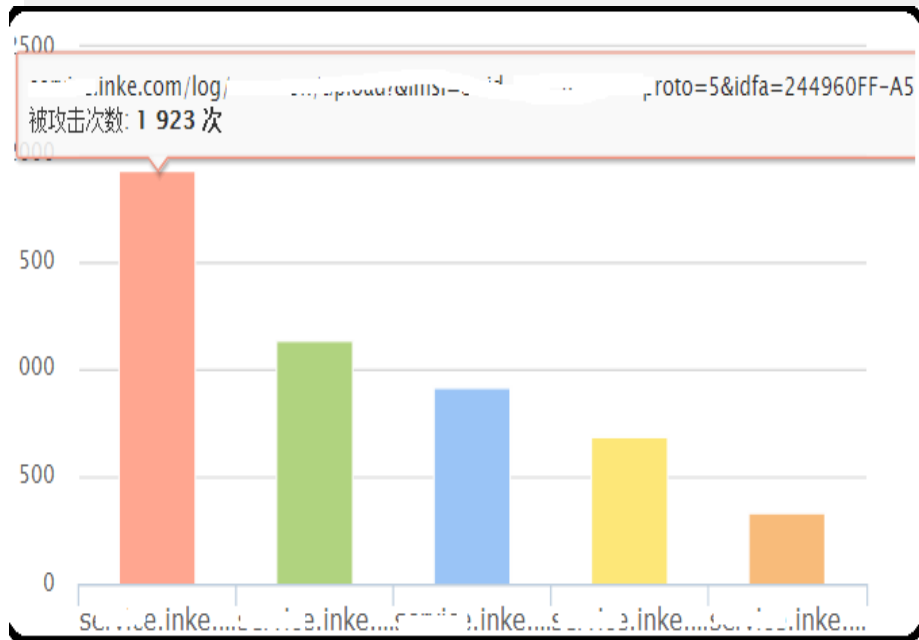
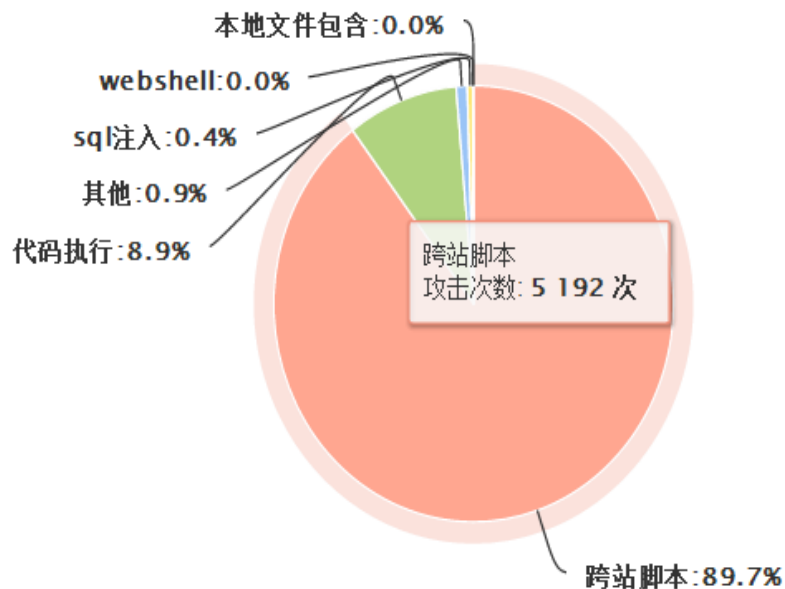
扫码观看大会视频



## DDOS高防IP服务以下站点四层攻击

PC/手机域名：www.\*\*.com

下载域名：live.\*\*.com



扫码观看大会视频

- 业务漏洞

## Request

Raw Params Headers Hex

```
POST /...ml HTTP/1.1
Host: ...com
Content-Length: 95
Accept: */*
Origin: http://...com
Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 6P Build/MDB08K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/44.0.2403.117 Mobile Safari/537.36kesudai kesuApp
asuAndroid
```

```
Content-Type: application/javascript; charset=utf-8; type=urlencoded
Referer: http://www.163.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,en-US;q=0.8
```

ookie: kesucorp=; s=314L\_\_\_\_\_

```
ary=a7a28957bde0bf1a11d3ea^ ^ ^ ^ - - = - : . _ a
```

[GALLERY][FILTER]=nofilter

```
lowtype=list&page=&orderBy=price%20asc.1-if(1=1 and 1=1.1.(select 1 union select 2))&cat id=19
```

```
python sqlmap.py -r sk --tech B --databases mysql --delay 0.3 -D ...
```

搜索字段中含有: 的字段

Columns like 'r' were found in the following databases:

Database:

Table: sdb pam account

[1 column]

| Column |

```
| login_password |
```

Database: i

Table: [L2L3\\_L4 - numbers](#)

行加密处理, token动态更新



扫码观看大会视频

JEB - /Users/mzf/Downloads/com.meelive.ingkee.apk

编译语言 反编译的Java 字符串 常量 注释

```

.class public StubApplication
.super Application
.source "StubApplication.java"

.method static constructor <clinit>()V
    .registers 9
    .prologue
00000000 const-string        v1, ""
    :4
    .local v1, "arch":Ljava/lang/String;
00000004 const-string        v5, "android.os.SystemPropert
00000008 invoke-static        Class->forName(String)Class,
0000000E move-result-object   v2
    .local v2, "clazz":Ljava/lang/Class;
00000010 const-string        v5, "get"
00000014 const/4             v6, 1
00000016 new-array            v6, v6, [Class
0000001A const/4             v7, 0
0000001C const-class          v8, String
00000020 aput-object          v8, v6, v7
00000024 invoke-virtual        Class->getDeclaredMethod(Str
0000002A move-result-object   v4
    .local v4, "get":Ljava/lang/reflect/Method;
0000002C const/4             v5, 1
0000002E new-array            v5, v5, [Object
00000032 const/4             v6, 0
00000034 const-string        v7, "ro.product.cpu.abi"
00000038 aput-object          v7, v5, v6
0000003C invoke-virtual        Method->invoke(Object, [Obj
00000042 move-result-object   v5
00000044 move-object          v0, v5
00000046 check-cast          v0, String
0000004A move-object          v1, v0
    
```

libe 304.so  
libe 304ex.so  
libe  
libi s.so  
libi o  
libi io  
libi  
libi  
libi t2.so  
libi e.so  
libi xg.so  
libi r.so  
libi  
libi pipeline.so  
libi simageeffect.so  
libi video.so  
libi unk.so  
libi ni1.1.0.so  
libi 64.so  
libi ls...if\_surface.so  
libi lsonroids\_gif.so  
libi lpload.so  
libi io  
libi  
libi shared.so  
libi th.so  
libi o  
libi age.so  
libi dkcore.so

好

用jeb反编译java代码的话，现在只能看到我们壳的代码，真正的代码逻辑被隐藏掉了。

然后，so的话，加固的是lib...so

你们先看看，有问题再搞起~~

好的





欢迎致电：400-818-8880 (09:00-18:00)



[关于我们](#) [帮助中心](#) [资讯中心](#) [下载手机端](#) [登录](#) | [注册](#)

欢迎致电：400-818-8880 (09:00-18:00)



[关于我们](#) [帮助中心](#) [资讯中心](#) [下载手机端](#) 156\*\*\*\*6020 | [退出](#)

[返回首页](#)



您已经完成注册!

完成



扫码观看大会视频



业务量：某客户直播路1万路，每5S截一帧图片，日图片量3000万；

解决方案：

第一层：自有系统过滤（使用md5进行过滤，如果命中黑样本直接删除）第二层：使用绿网过滤；第三层：人工审核，发现问题在回拉视频判断



扫码观看大会视频

场景	安全解决方案
移动App漏洞、仿冒	移动安全方案：安全加固，安全组件
被DDoS攻击导致业务瘫痪	防DDoS方案：DDoS高防
被频繁爆漏洞引发公共危机 被黑客入侵导致数据泄露、资金损失	防入侵方案：WAF、安骑士、先知计划、态势感知、安全专家服务
网站内容需要加密传输，防钓鱼、防流量劫持 敏感数据需要加密存储	数据加密方案：证书服务、加密服务
因为垃圾注册、拖库撞库、营销作弊导致业务损失	业务风控方案：反欺诈
因为文字、图片、视频内容违规导致监管风险	内容安全方案：绿网



---

# 目录

## content

---

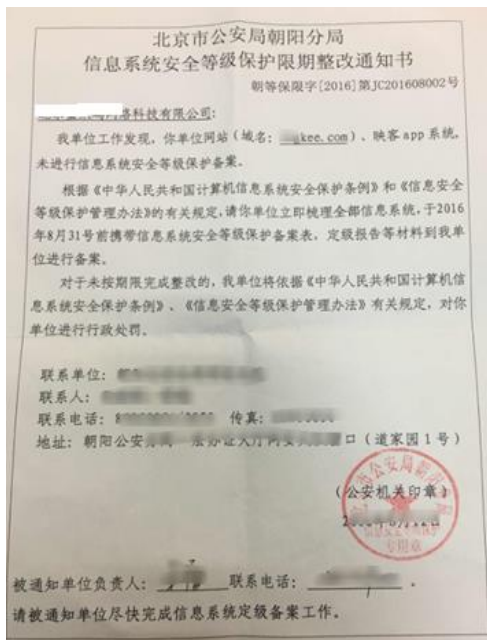
1. 视频行业安全诉求
2. 下注云盾，启动安全护航
3. 共建直播行业安全标准





## 解决视频客户等保合规

为了便于阿里云云上系统能够快速满足等保合规的要求，阿里云通过建立“等保合规生态”，联合阿里云合作伙伴咨询厂商、各地测评机构和公安机关，提供一站式、全流程等保合规解决方案。



## 系统定级

## 系统备案

## 建设整改

## 等级测评

## 监督检查

运营单位

确定信息系统安全保护等级

准备备案材料，到当地公安机关备案

建设符合等级要求的安全技术体系和管理体系

准备和接受测评机构测评

接受公安机关的定期检查

咨询厂商

协助运营单位准备定级报告，并组织专家评审（三级）

协助运营单位准备备案材料

协助运营单位进行系统安全加固和制定安全管理制度

协助运营单位参与等级测评过程并进行整改

协助运营单位接受检查和进行整改

阿里云

提供符合等级要求必须的安全产品和服务

提供云服务商安全资质、云平台通过等保的证明材料

测评机构

测评机构对系统等级符合性状况进行测评

公安机关

当地公安机关审核受理备案材料

公安机关监督检查运营单位开展等级保护工作



2016 The  
Computing  
Conference  
**THANKS**

