搜狐
SOHU.com

搜狐SDL流程与Web应用安全运营实践

董方@sohu. com

About Me

xuammumu@gmail.com

http://weibo.com/vindong

Web安全爱好者，PHPer

提纲

1 信息安全与web应用风险介绍

2 微软SDL流程介绍

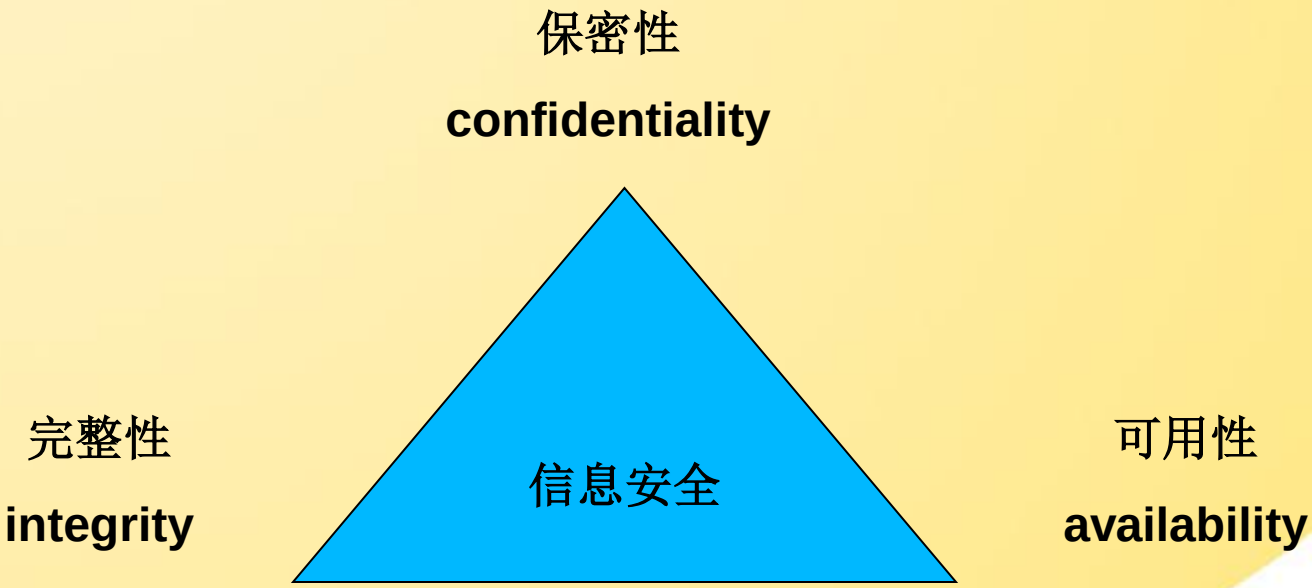
3 搜狐SDL流程介绍

4 搜狐web应用安全运营体系

5 Q&A

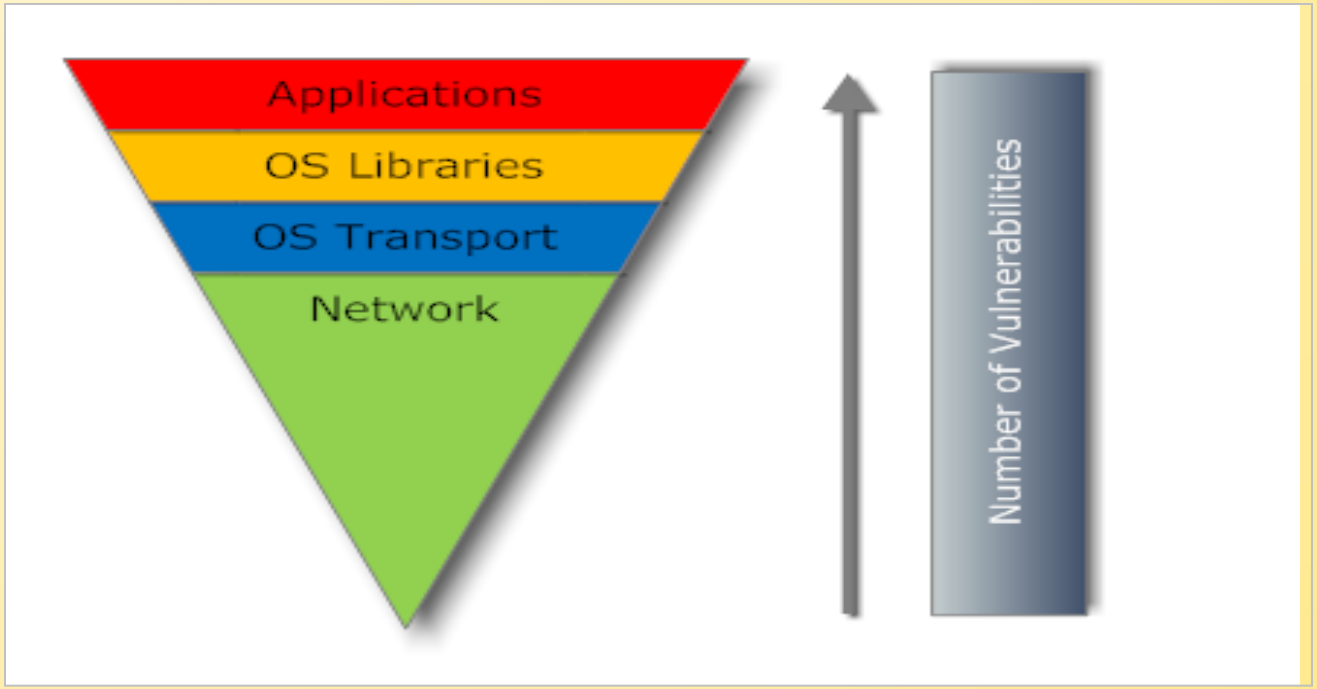
什么是信息安全

- 保护信息系统的硬件、软件及其系统中的数据受到保护，不受偶然或者恶意侵犯而遭到破坏、更改、泄露，保证信息系统连续、可靠、正常地运行。



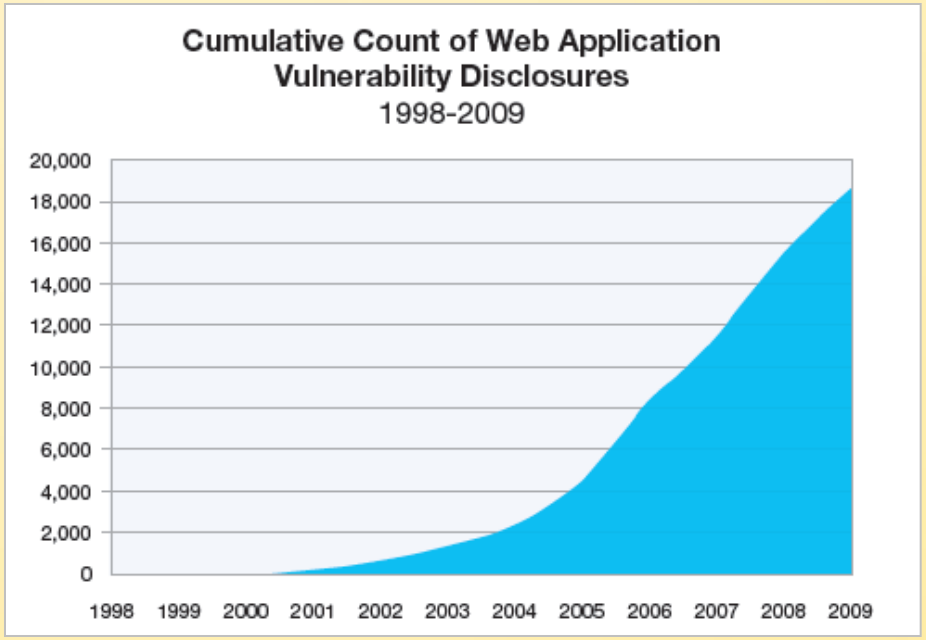
安全风险分层

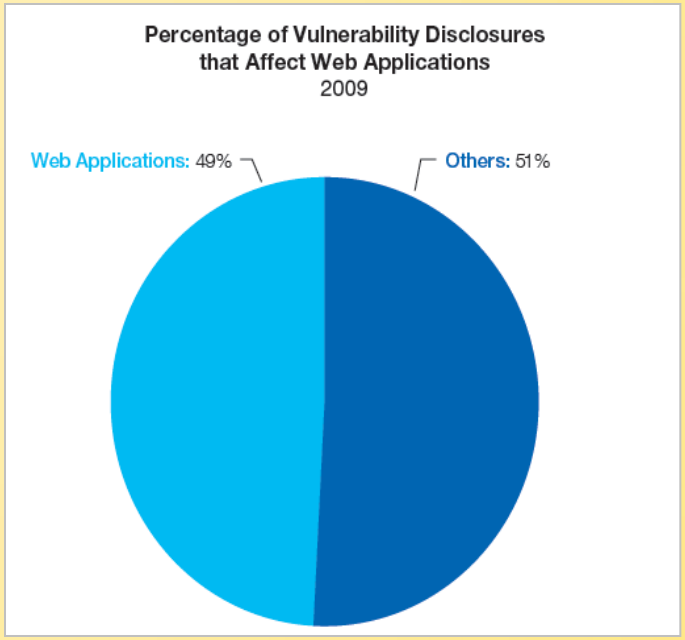
- **SANS**: “***Top Cyber Security Risks - Vulnerability Exploitation Trends***



Web应用风险

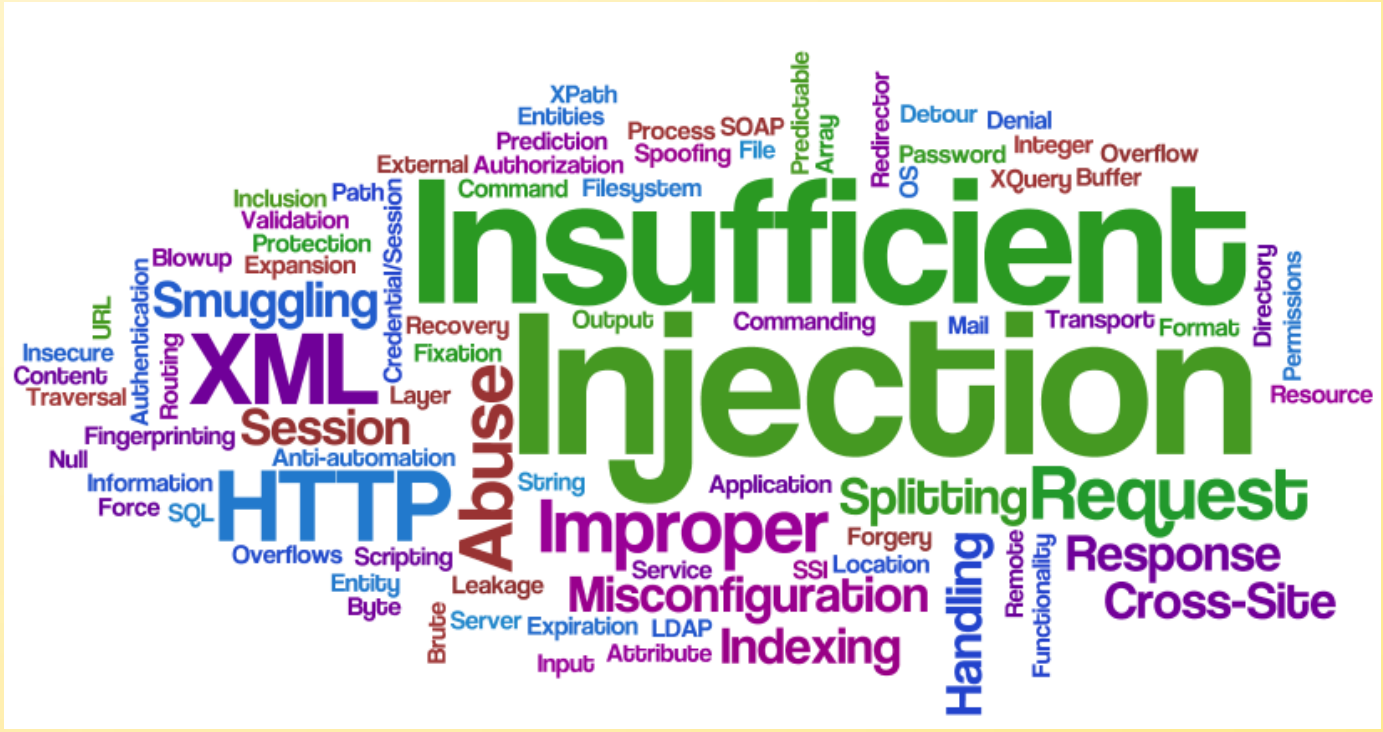
- **IBM**：IBM *X-Force 2009 Trend and Risk Report*





Web应用风险分类

- Web威胁分级标签图



Web应用风险分类

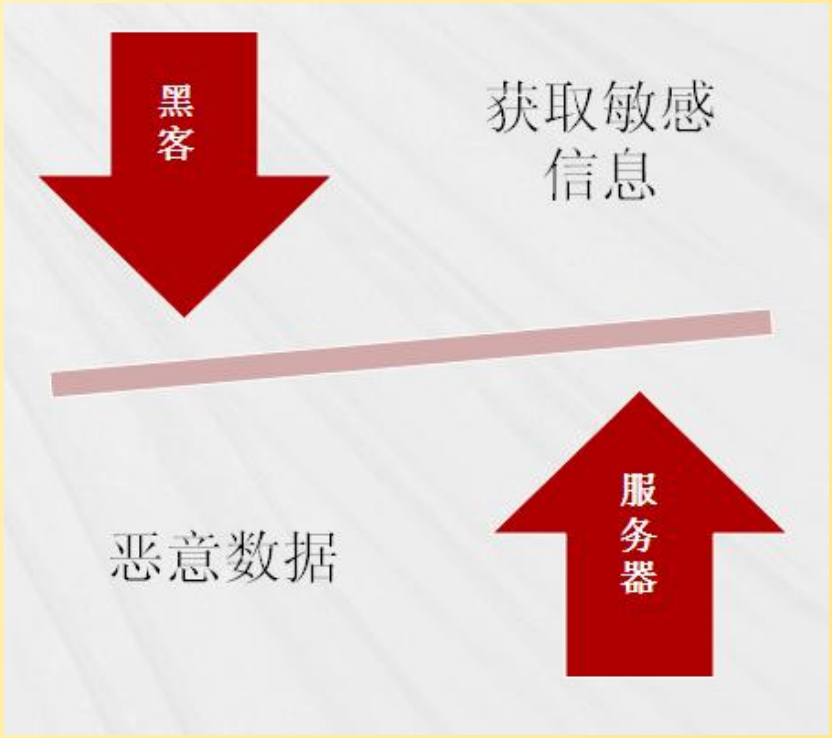
- **OWASP TOP 10**
  - A1: **Injection**
  - A2: **Cross-Site Scripting (XSS)**
  - A3: Broken Authentication and Session Management
  - A4: Insecure Direct Object References
  - A5: **Cross-Site Request Forgery (CSRF)**
  - A6: Security Misconfiguration
  - A7: Insecure Cryptographic Storage
  - A8: Failure to Restrict URL Access
  - A9: Insufficient Transport Layer Protection
  - A10: **Unvalidated Redirects and Forwards**

Web应用风险分类

- 输入/输出数据验证
- 身份验证
- 会话管理
- 授权
- 配置管理
- 敏感数据
- 加密
- 参数操作
- 异常管理
- 审核与记录

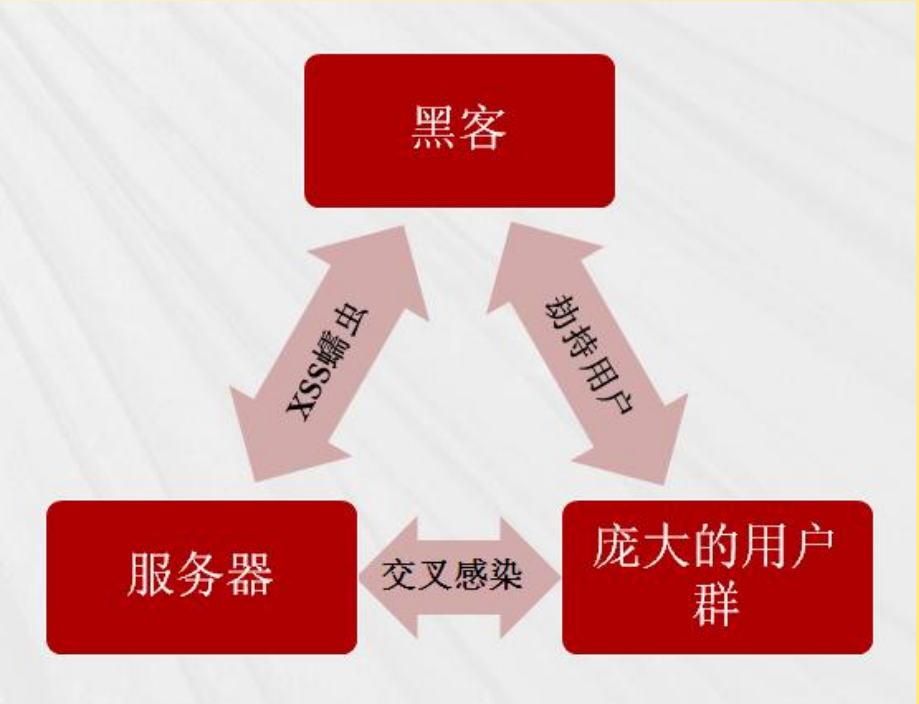
Web攻击模型的演变

Web1.0时期攻击模型



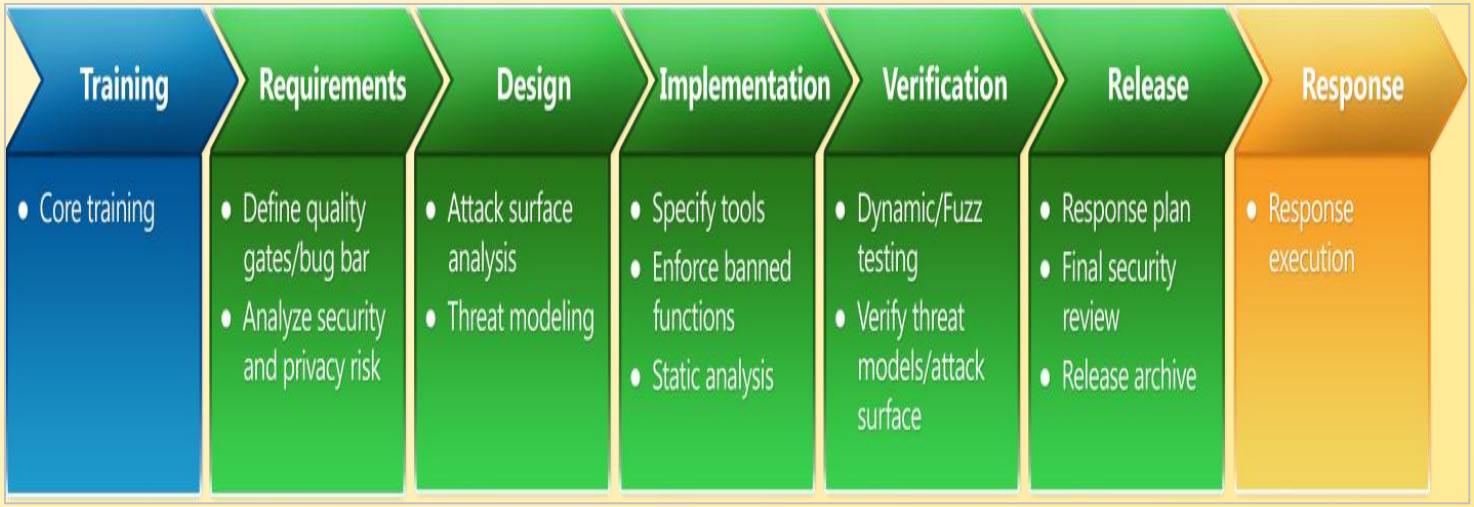
Web攻击模型的演变

Web2.0时期攻击模型



微软SDL流程介绍

- **MS SDL (Security Development Lifecycle)**



安全开发生命周期Security Development Lifecycle(SDL)，起源于微软，是一种专注于软件开发的安全保障流程。

为实现保护最终用户为目标，它在软件开发流程的各个阶段引入安全和隐私问题。

微软SDL流程介绍

- 在SDL流程中，包括了以下七个阶段：
  - 安全培训：推广安全编程意识
  - 需求分析：寻找安全嵌入的最优方式
  - 系统设计：威胁建模
  - 实现：安全开发
  - 验证：黑白盒测试
  - 发布：最后检查确认
  - 响应：应急响应，BUG跟踪

SDL的意义

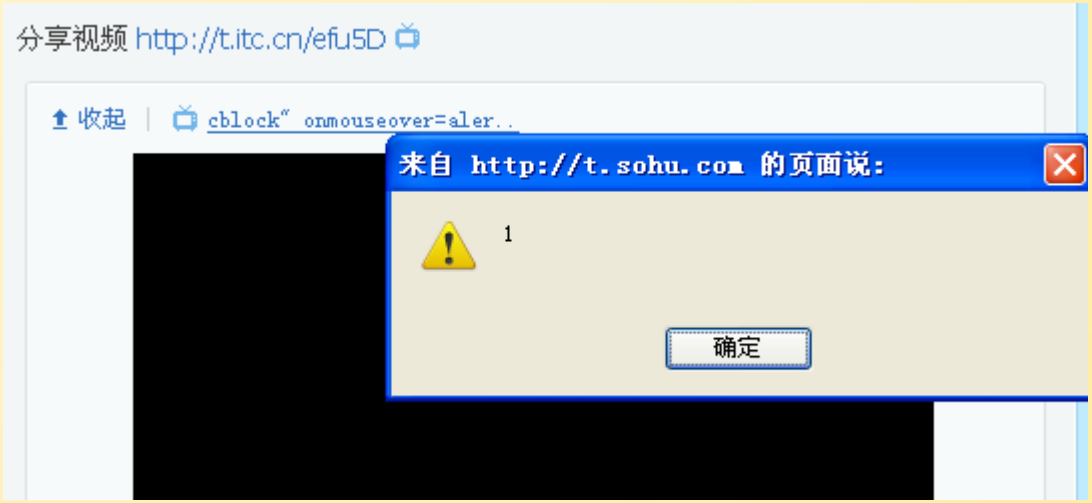
- SDL使设计、代码和文档中与安全相关的漏洞减到最少，在软件开发的生命周期中尽可能早地清除漏洞。
- SDL是一种规范，指导，约束。由人制定，监管，执行。
- SDL不是万能的。

可能导致SDL失败的场景

- 输入的多样化导致威胁建模存在盲点
- 从一切用户的输入都是有害的到任何数据源都是有害的
- 人的因素不可控

微博产品嵌入视频XSS漏洞

- 恶意视频名称叫：xxx” onmouseover=alert(1) “




```
<a class="fuc0
crJs_video_url" onmouseover="alert(1)" title="cblock" target="_blank" href="http://www.tudou.com
/programs/view/69H7K1DC9qc/">
```

微博产品嵌入视频XSS漏洞

- 经过测试，搜狐，新浪，腾讯的微博产品均受影响
- **腾讯微博JSON跨站漏洞**
- http://www.wooyun.org/bugs/wooyun-2010-0508

来自系统的输入

问题：从操作系统获得的信息可以作为可信任的输入么？

你说这系统信息是不可信呢？还是不可信呢？还是不可信呢？

人的因素

- Discuz X2 SQL注入漏洞分析
- forum_attachment.php 14-18行：

```
@list($_G['gp_aid'], $_G['gp_k'], $_G['gp_t'], $_G['gp_uid'], $_G['gp_tableid']) = explode('|', base64_decode($_G['gp_aid']));

if(!empty($_G['gp_findpost']) && ($attach = DB::fetch_first("SELECT pid, tid FROM ".DB::table('forum_attachment')." WHERE aid='$_G[gp_aid]'"))) {
    dheader('location: forum.php?mod=redirect&goto=findpost&pid='.$attach['pid'].'&ptid='.$attach['tid']);
}
```

- base64_decode($_G[‘gp_aid’])//没有过滤只有base64解码
- WHERE aid=‘$_G[gp_aid]’//通过对注入语句进行base64编码完美绕过单引号限制

人的因素

- Discuz X2 SQL注入漏洞分析
- forum_attachment.php 29-31行：

```
$aid = intval($_G['gp_aid']);

$tableid = !empty($_G['gp_tableid']) ? getattachtableid($_G['gp_tableid']) : DB::result_first("SELECT tableid FROM ".DB::table('forum_attachment')." WHERE aid='$aid'");
```

- $aid = intval($_G[‘gp_aid’]);//限制了aid为整型
- WHERE aid=‘$aid‘//之后的数据库查询语句使用$aid变量

- 安全与漏洞之间的距离，只有7行代码！

搜狐SDL流程介绍

- 搜狐web安全面临的问题：
- 项目开发周期短
- 迭代频繁
- 缺乏安全设计
- 缺乏安全编程意识
- 老旧代码难以维护
- 业务线代码风格多变

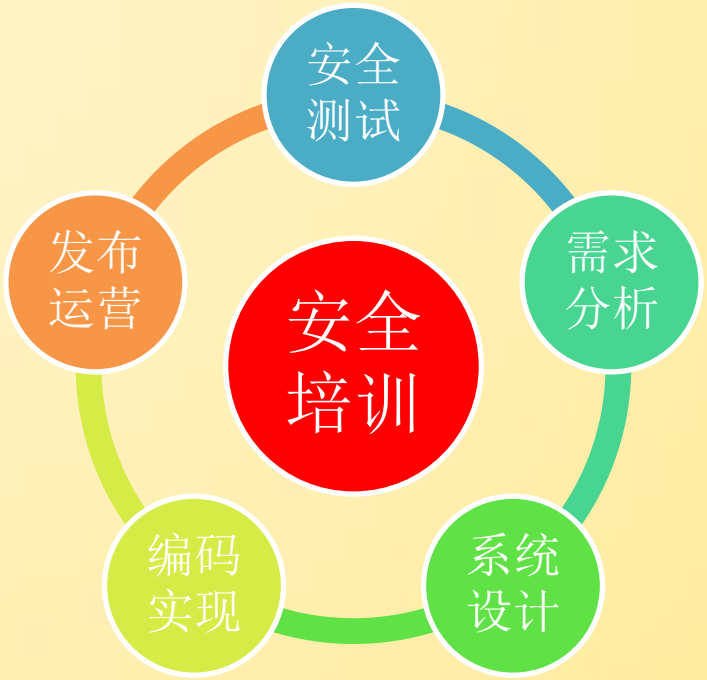
搜狐SDL流程介绍

- 从安全测试入手，事件驱动SDL流程。

安全测试	• 黑盒+白盒测试，构建安全漏洞数据库 • 事件驱动SDL流程
安全培训	• 对常见web漏洞原理以及解决方案进行培训
需求分析	• 识别信息，风险评估，制定安全目标以及最低BUG标准
系统设计	• 威胁建模：系统架构概述，分解应用程序，识别风险，识别漏洞 • 反馈《安全机制调查表》
编码实现	• 使用安全API，源代码审计
发布运营	• 上线审核机制，安全监控，BUG跟踪，漏洞管理

搜狐SDL流程介绍

- 迭代的SDL流程



搜狐SDL流程介绍

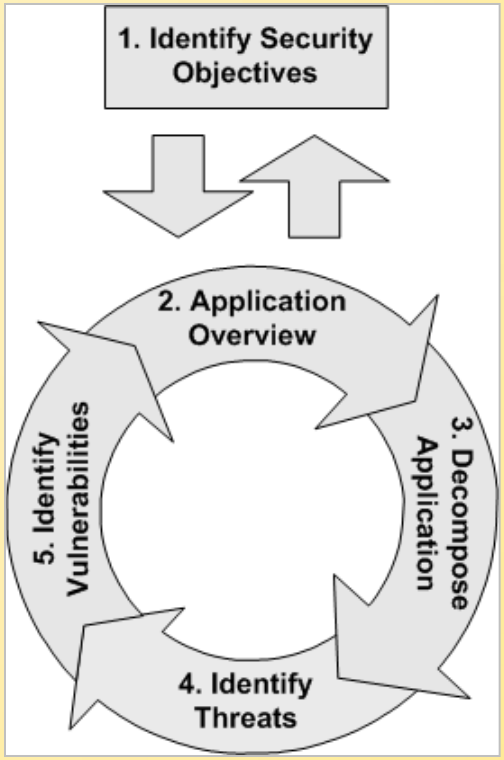
- 需求分析阶段：
  - 识别重要信息（保护对象）
  - 风险评估
  - 安全目标
  - 最低BUG标准
  -

NO

- SQL注入
- XSS 存储型跨站
- 恶意文件上传
- CSRF
- Open Redirect (url跳转)

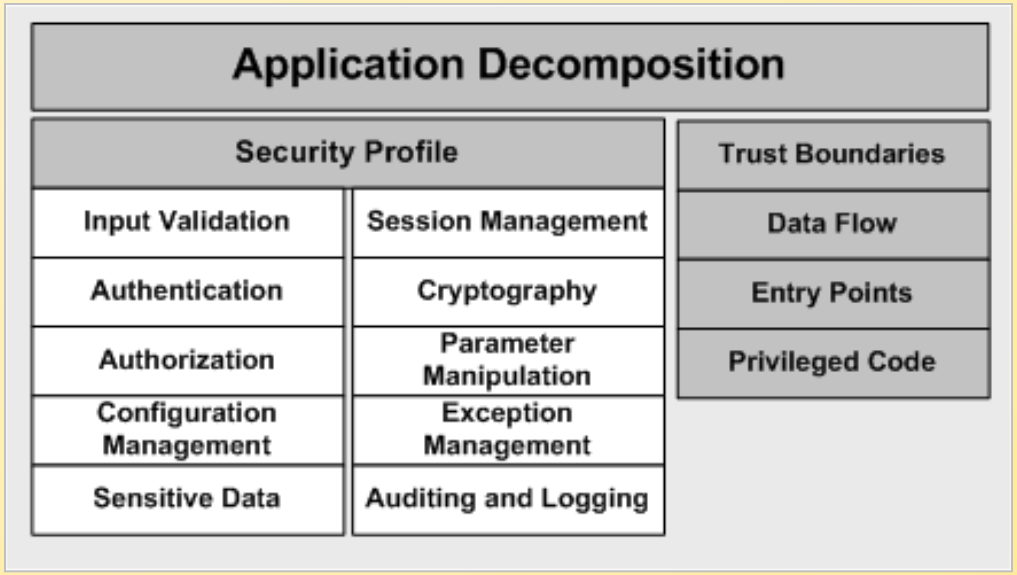
搜狐SDL流程介绍

- 系统设计-威胁建模：
  - 识别安全目标
  - 系统架构概述
  - 分解应用程序
  - 识别威胁
  - 识别漏洞



搜狐SDL流程介绍

- 威胁建模-分解应用程序：
- 《安全机制调查表》：系统架构概述，功能模块介绍，安全机制介绍等
- 功能模块解析



搜狐SDL流程介绍

- 威胁建模-识别威胁&漏洞：
- 分析安全测试数据结果，识别具体漏洞
  - 从功能分析数据流
  - 从数据流分析威胁
  - 确认是否有相应的漏洞
  - 改进安全设计，形成规范文档

搜狐SDL流程介绍

- 编码实现（检测+监测）：
- ESAPI

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validator, Encoder
A2. Injection Flaws	Encoder
A3. Malicious File Execution	HTTPUtilities (Safe Upload)
A4. Insecure Direct Object Reference	AccessReferenceMap, AccessController
A5. Cross Site Request Forgery (CSRF)	User (CSRF Token)
A6. Leakage and Improper Error Handling	EnterpriseSecurityException, HTTPUtils
A7. Broken Authentication and Sessions	Authenticator, User, HTTPUtils
A8. Insecure Cryptographic Storage	Encryptor
A9. Insecure Communications	HTTPUtilities (Secure Cookie, Channel)
A10. Failure to Restrict URL Access	AccessController

搜狐SDL流程介绍

- 编码实现：
- ESAPI

```
function safe_mysql_api($array) {
    if (is_array($array)) {
        foreach ($array as $k => $v) {
            $array[$k] = ESAPI :: getEncoder() -> encodeForSQL(new MySQLCodec(), $v);
        }
    } else if (is_string($array)) {
        $array = ESAPI :: getEncoder() -> encodeForSQL(new MySQLCodec(), $array);
    }
    return $array;
}

function safe_html_api($array) {
    if (is_array($array)) {
        foreach ($array as $k => $v) {
            $array[$k] = ESAPI :: getEncoder() -> encodeForHTML($v);
        }
    } else if (is_string($array)) {
        $array = ESAPI :: getEncoder() -> encodeForHTML($array);
    }
    return $array;
}
```

搜狐SDL流程介绍

- 编码实现（检测+监测）：
- 部署webIDS，记录异常信息

```
HTTP_GET: XSS in GET data : Found string: <script>alert(1)</script> in payload HTTP_GET

Server Data:
```

```
HTTP_GET: SQL injection in GET data : Found string: 1 union select 1,2,3 from admin in payload HTTP_GET

Server Data:
HTTP_ACCEPT */*
HTTP_ACCEPT_LANGUAGE zh-cn
HTTP_UA_CPU x86
HTTP_ACCEPT_ENCODING gzip, deflate
HTTP_USER_AGENT Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.21
```

- 参考资料(Discuz 内置IDS， CodeIgniter内置IDS)
- http://dev.discuz.org/wiki/index.php?title=%E5%AE%89%E5%85%A8%E6%9C%BA%E5%88%B6
- http://codeigniter.org.cn/user_guide/libraries/security.html

搜狐SDL流程介绍

- 有效实施安全开发
  - 高层支持
  - 安全成为目标
  - 需要足够的安全培训
  - 需要有相关流程、技术、工具的支持

  - 困难：
    - 威胁不断变化
    - 人员流动性
    - 周期短、更新频繁
    - 增加工作量
    - 监督执行

搜狐web应用安全运营体系

- 搜狐web应用安全框架
  - 应用架构：业务分离，身份认证，数据加密，日志记录，数据安全，流量监控等
  - 开发过程：SDL
  - 测试：功能测试，压力测试，黑白盒测试
  - 安全响应：安全接口人，安全响应流程，安全事件跟踪
  - 其他：安全交流，安全培训

搜狐web应用安全运营体系

- 安全事件响应平台：
  - 按业务线分类，对日常安全事件进行通报并跟踪处理结果。
  - 通报最新安全漏洞或对最新攻击方式进行预警通知

搜狐web应用安全运营体系

- **Web服务器文件监控机制：**

ID	5
日期	December 17, 2010, 3:54 pm
部门	;
IP	192.168.20.43
内容	文件被修改:/vindong/application/vintest/test.php Line:3:$a = system("uname -a");

查看源代码：

```
<?
echo "hello.world!";
$a = system("uname -a");
?>
```

ID	4
日期	December 17, 2010, 3:43 pm
部门	;
IP	192.168.20.43
	新创建文件/vindong/application/vintest/shell.php Line:51: echo $phpinfo=(!eregi("phpinfo",$dis_func)) ? phpinfo() : "phpinf 新创建文件/vindong/application/vintest/shell.php Line:92:$phpinfo=(!eregi("phpinfo",$dis_func)) ? ""	<a href=\"?action=php 新创建文件/vindong/application/vintest/shell.php Line:101:<title>PhpSpy Ver 2006</title> 新创建文件/vindong/application/vintest/shell.php Line:160:$tb->tdbody('注销会话	PHP环境变量	在线代理 href="?action=shell">WebShell	SQL Query	

- 已经开源：**http://sourceforge.net/projects/webradar/files/**

搜狐web应用安全运营体系

- 日常安全扫描体系：
- 日志扫描
- 网站扫描
- 服务器扫描

- 无论问题最初看起来怎样，它始终是人的问题。

--Gerald M. Weinberg

Q&A

- 谢谢各位☺