Secure development and the SDLC

Presented By Jerry Hoff
@jerryhoff

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Agenda

- Part 1: The Big Picture
- Part 2: Web Attacks
- Part 3: Secure Development
- Part 4: Organizational Defense

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Part 1: The Big Picture

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Non stop hacking…

United States Postal Service Hacked

Posted Nov 10, 2014 by Greg Kumparak (@grg)

1,523 SHARES

It seems like 2014 has been one endless series of massive hacks. Home Depot. Target. Neiman Marcus. Michaels. JPMorgan Chase. It's been one hack after the other, each du anything from customer credit card numbers to mailing addresses into the wild.

The latest one is a big one: the United States Postal Service.

Here's what we know:

- The hack was seemingly focused not on nabbing customer credit cards, but on emp data. The hackers likely had access to confidential data on all 800,000 USPS employ That includes names, Social Security numbers, addresses, and pretty much anythir you'd put on a job application.
- Customer credit card information seemingly wasn't exposed. However, anyone wh USPS customer support from January 1st to August 16th of 2014 might have had information stolen, depending on what information they provided to the CS rep: names, addresses, telephone numbers and email addresses.
- The intrusion was first detected in mid-September, nearly 2 full months before being disclosed. The USPS says this delay was because "communicating the breach immediately would have put the remediation actions in jeopardy..."

Officials warn 500 million financial records hacked

Erin Kelly, USA TODAY 8:10 p.m. EDT October 20, 2014

(Photo: David Goldman, AP)

f 9269 CONNECT | 1303 TWEET | in 1018 LINKEDIN | 95 COMMENT | EMAIL | MORE

WASHINGTON — Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building.

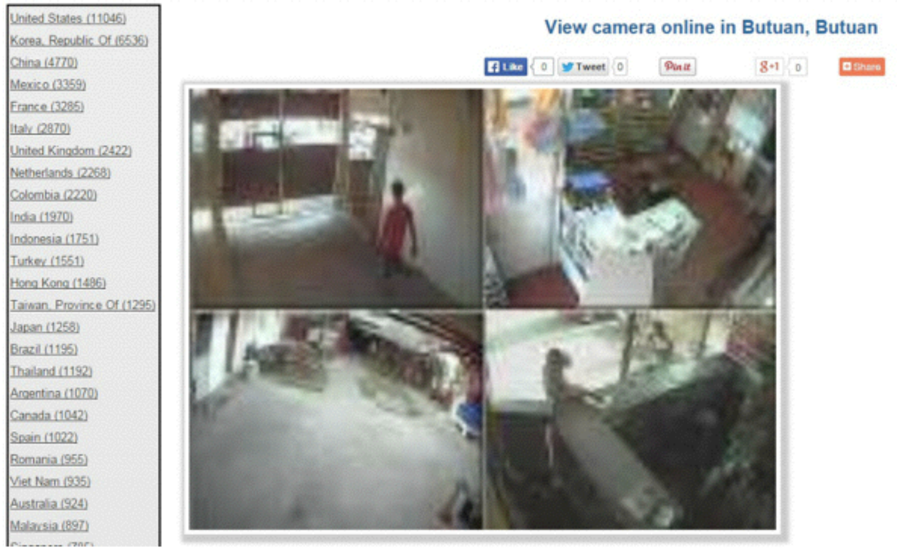
"We're in a day when a person can commit about 15,000 bank robberies sitting in their basement," said Robert Anderson, executive assistant director of the FBI's Criminal Cyber Response and Services Branch.

The U.S. financial sector is one of the most targeted in the world, FBI and Secret Service officials told business leaders at a cybersecurity event organized by the Financial Services Roundtable. The event came in the wake of mass hacking attacks against Target, Home Depot, JPMorgan Chase and other financial institutions.

"You're going to be hacked," Joseph Demarest, assistant director of the FBI's cyberdivision, told the business leaders. "Have a plan."

Hundreds of PHL security cams hacked, posted online

November 11, 2014 12:37pm



Sample screen grab of just one of hundreds of hacked webcams across the Philippines.

Here's one more reason for owners of security cameras to change their devices' default passwords: their private lives could be made public by a hacker's website.

The Cybercrime Economy

U.S. weather system hacked, affecting satellites

By Jose Pagliery @Jose_Pagliery November 12, 2014: 2:34 PM ET

The scary reality of hacking infrastructure

699 TOTAL SHARES

505 106 62 26

NEW YORK (CNNMoney)

Hackers attacked the U.S. weather system in October, causing a disruption in satellite feeds and several pivotal websites.

The National Oceanic and Atmospheric Administration, NOAA, said that four of its websites were hacked in recent weeks. To block the attackers, government officials were forced to shut down some of its services.

Hacking Tops List of Crimes Americans Worry About Most

by Rebecca Riffkin

Story Highlights

- *Theft of one's credit card info from stores is most common worry*
- *62% of Americans worry about computer and smartphone hacking*

WASHINGTON, D.C. -- As the list of major U.S. retailers hit by credit card hackers continues to grow this year, Americans are more likely to worry about having credit card information they used in stores stolen by computer hackers than any other crime they are asked about. Sixty-nine percent of Americans report they frequently or occasionally worry about this happening to them. Having a computer or smartphone hacked (62%) is the only other crime that worries the majority of Americans.

Crime Worries in U.S.

How often do you, yourself, worry about the following things -- frequently, occasionally, rarely or never? How about ...

U.S. Hacked Despite $10B Spent Yearly on Security

Billions wasted, secrets exposed by federal employees' carelessness & online playtime

November 11, 2014

The Intelligencer / Wheeling News-Register

Save | Comments (9) | Post a comment |

They have clicked links in bogus phishing emails, opened malware-laden websites and been tricked by scammers into sharing information.

Federal employees and contractors scattered across more than a dozen agencies, from the Defense and Education departments to the National Weather Service, are responsible for at least half of federal cyberincidents each year since 2010, according to an Associated Press analysis of records.

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

why?

warum?

perche?

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Web Site / Web Application

Custom Code

Frameworks & Libs

Language Support

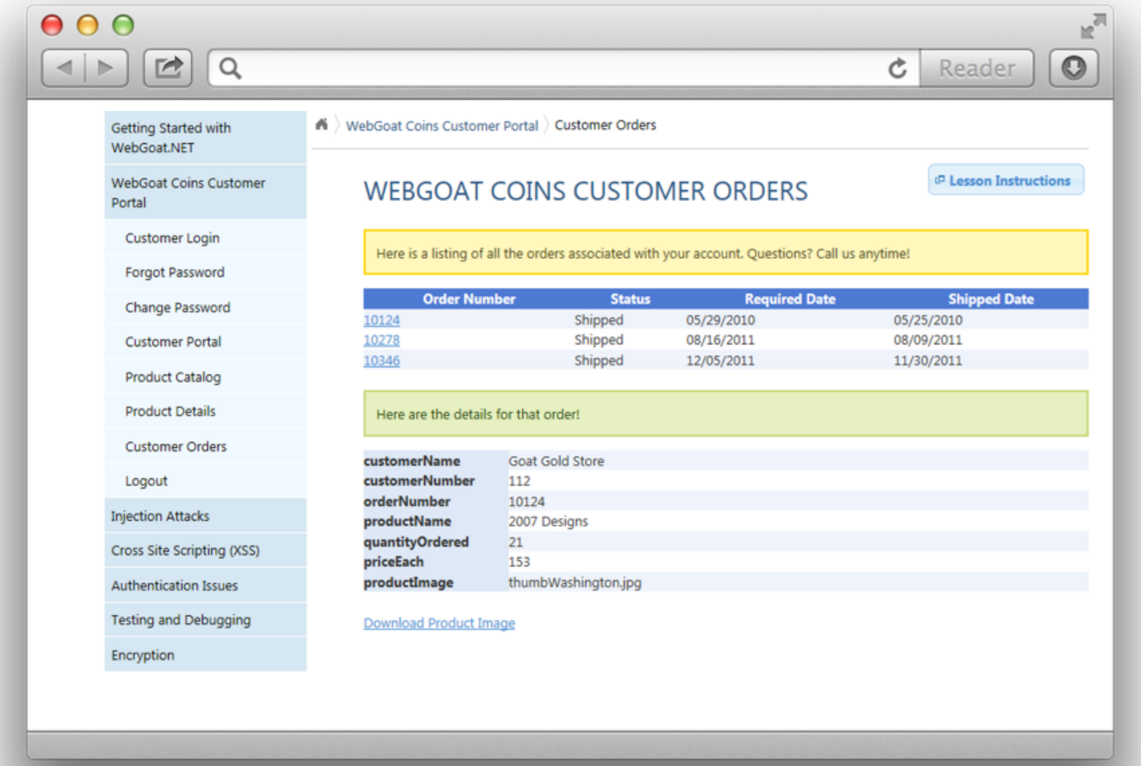
Application Server

Web Server

Operating System

HTTP, HTML, JavaScript, CSS
Cookies, SVG, Plugins, Add-ons
iFrames, Flash, WebSockets
Client side database…

20 year old legacy!
Browsers inconsistent



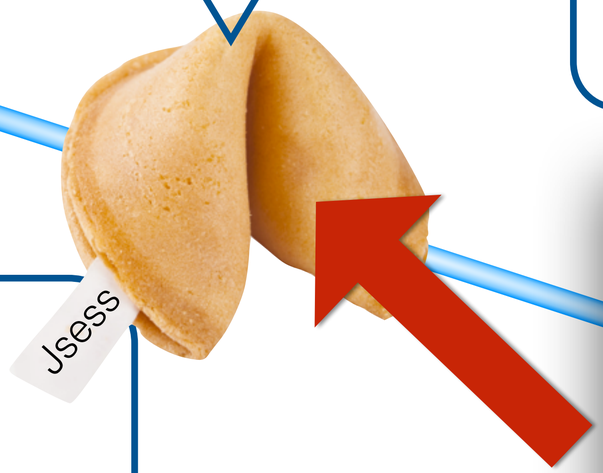
OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Vulnerability

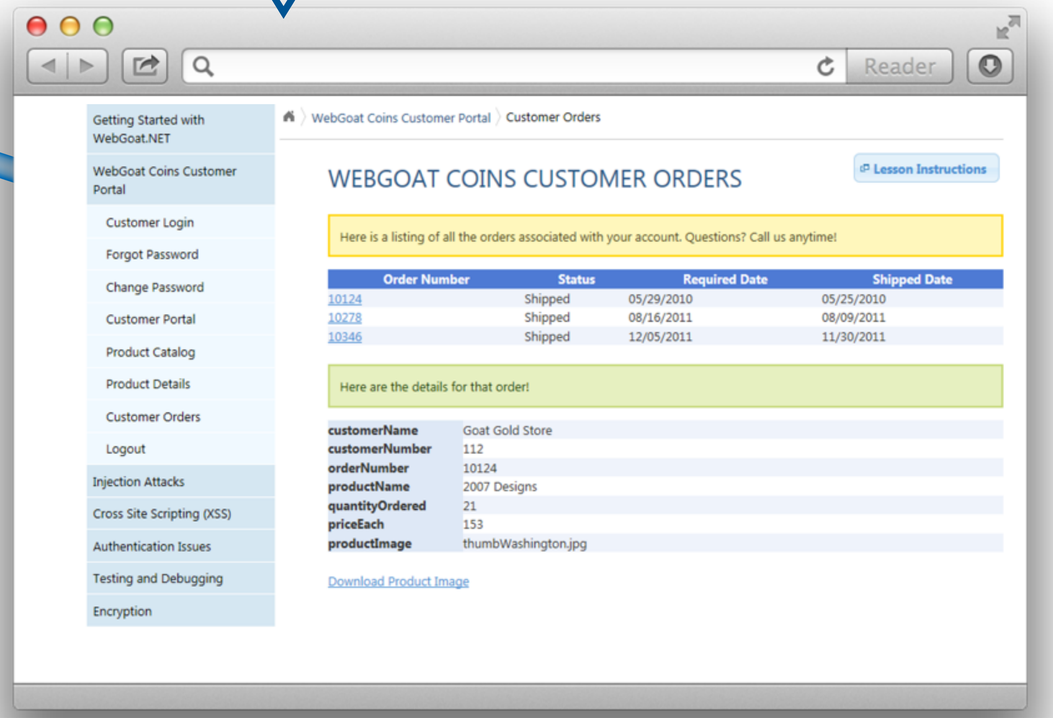
- Weakness that can be exploited to cause harm
- Each vulnerability has a “impact”
- Each vulnerability has a “‘likelihood”

Email: **jerry@owasp.org** Twitter: **@jerryhoff**

Steal Cookie
Guess Cookie
Reuse Cookies
Steal Data



Malicious JavaScript (XSS)
Generate Forged Requests
Stolen Clicks (ClickJacking)



Injection
Authentication
Access Control
Vulnerable Libraries
Forge HTTP Headers
Abuse Business Logic
Security Configuration
Accept Forged Requests

OWASP Top 10 2013

- Big daddy of all web risk documents
- Do not base your security program on a “Top 10” list - **Hoff’s Law**
- http://www.owasp.org

Current “Top 10”

A1 Injection
A2 Broken Auth and Session Management
A3 Cross-Site Scripting (XSS)
A4 Insecure Direct Object References
A5 Security Misconfiguration
A6 Sensitive Data Exposure
A7 Missing Function Level Access Control
A8 Cross-Site Request Forgery (CSRF)
A9 Using Known Vulnerable Components
A10 Unvalidated Redirects and Forwards

OWASP ASVS

- Application Security Verification Standard (2014)
- Superb checklist
- **DOWNLOAD THIS NOW** (your homework)

https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf

V2. **Authentication**
V3. **Session Management**
V4. **Access Control**
V5. **Malicious Input Handling**
V7. **Cryptography at Rest**
V8. **Error Handling and Logging**
V9. **Data Protection**
V10. **Communications**
V11. **HTTP**
V13. **Malicious Controls**
V15. **Business Logic**
V16. **File and Resource**
V17. **Mobile**

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Risk

- Risk = vuln likelihood * vuln impact
- Typically ranked “critical” through “low”
- Risk based approach = assign each risk a $$ amount

Security Control

- Mitigates an vulnerability
- For each major vulnerability, there is a corresponding security control
- Examples: cookie flag, http header, encoders, ORM, validation….

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

End of Part 1: The Big Picture

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Part 2:
Web Attacks
Finding and Exploiting Victims

Email: **jerry@owasp.org** Twitter: **@jerryhoff**

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

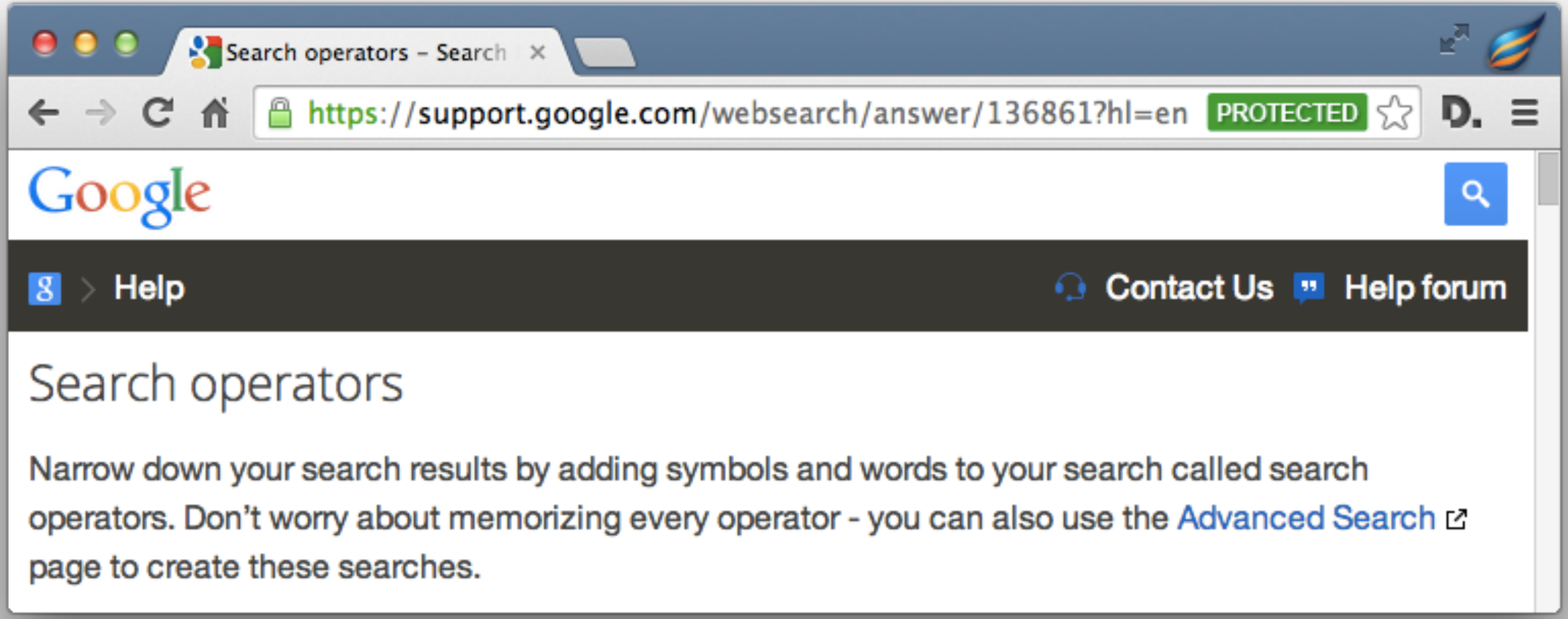
Am I Secure?

bin ich sicher?

sono sicuro?

Advanced Google Search

about: link: site: filetype: inurl:



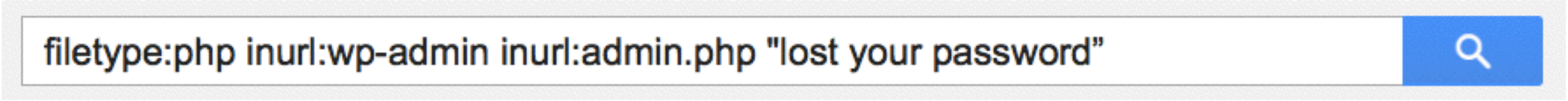
OWASP
German OWASP Day 2014
9. Dezember
Hamburg

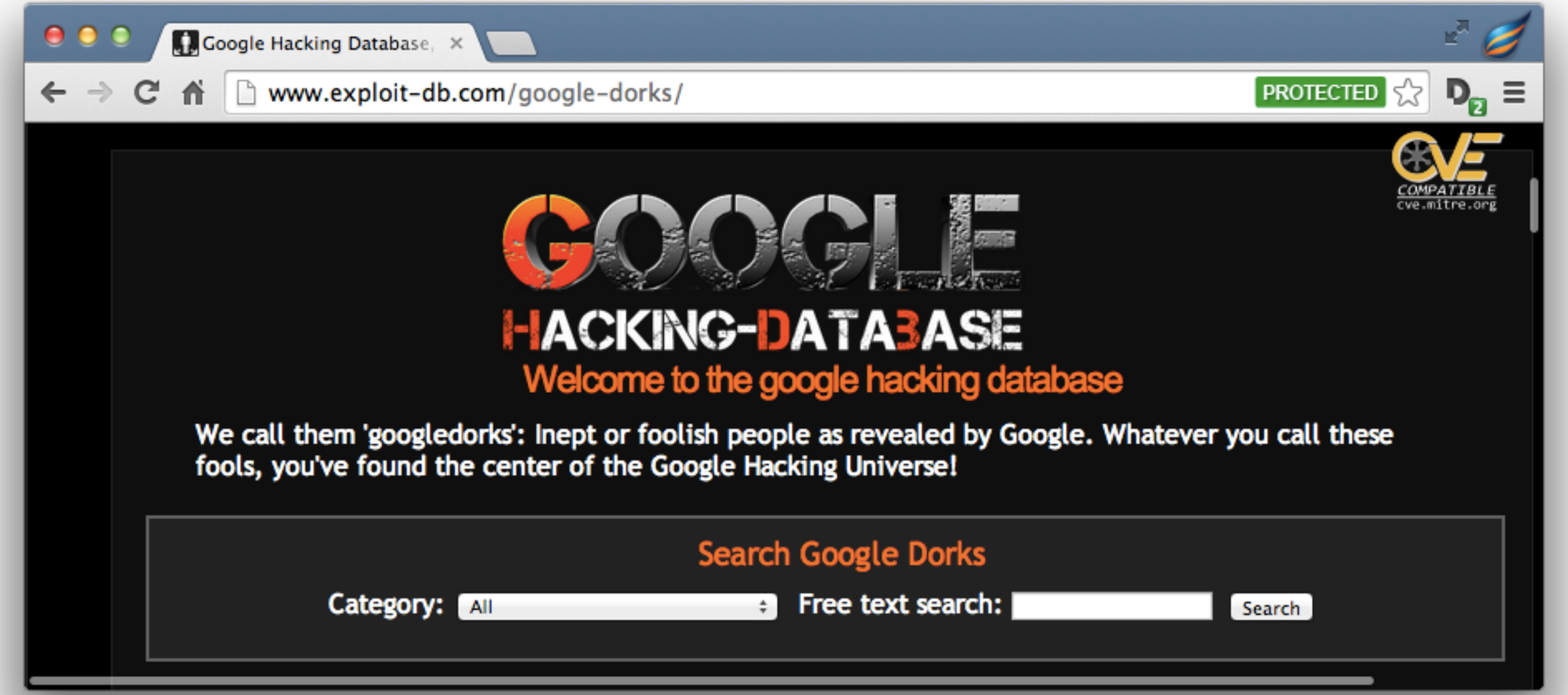
Finding file types

- site:example.com filetype:___
- Sometimes determine technologies (asp, php, jsp, aspx, cfm, pl)
- find interesting file types (.pdf, .docx, .xlsx, .txt, .readme)
- find very interesting file types (.log, .old)

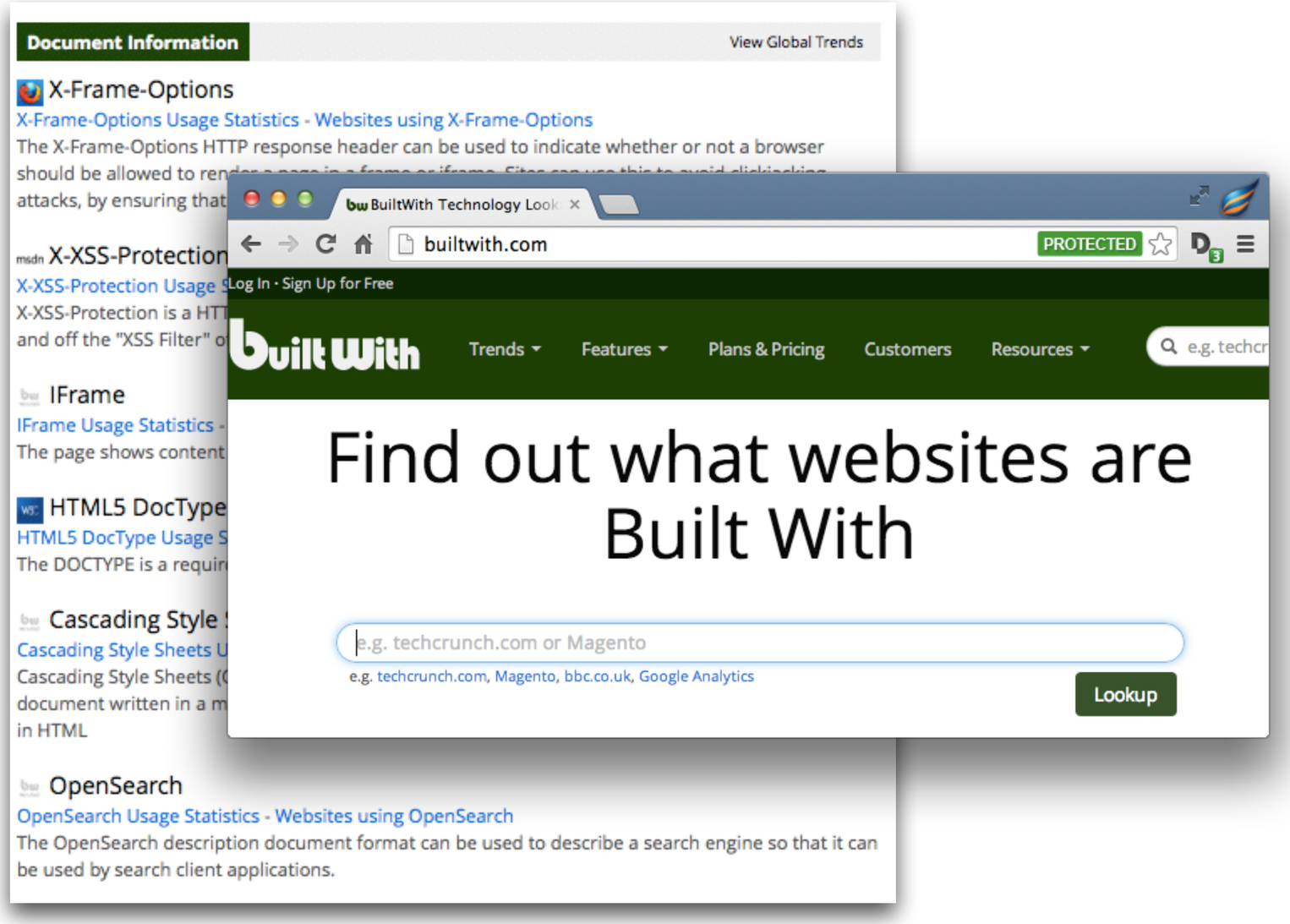
Getting more specific

- inurl:
- Searches for keywords in URL
- Use this to find all “wordpress” login screens…



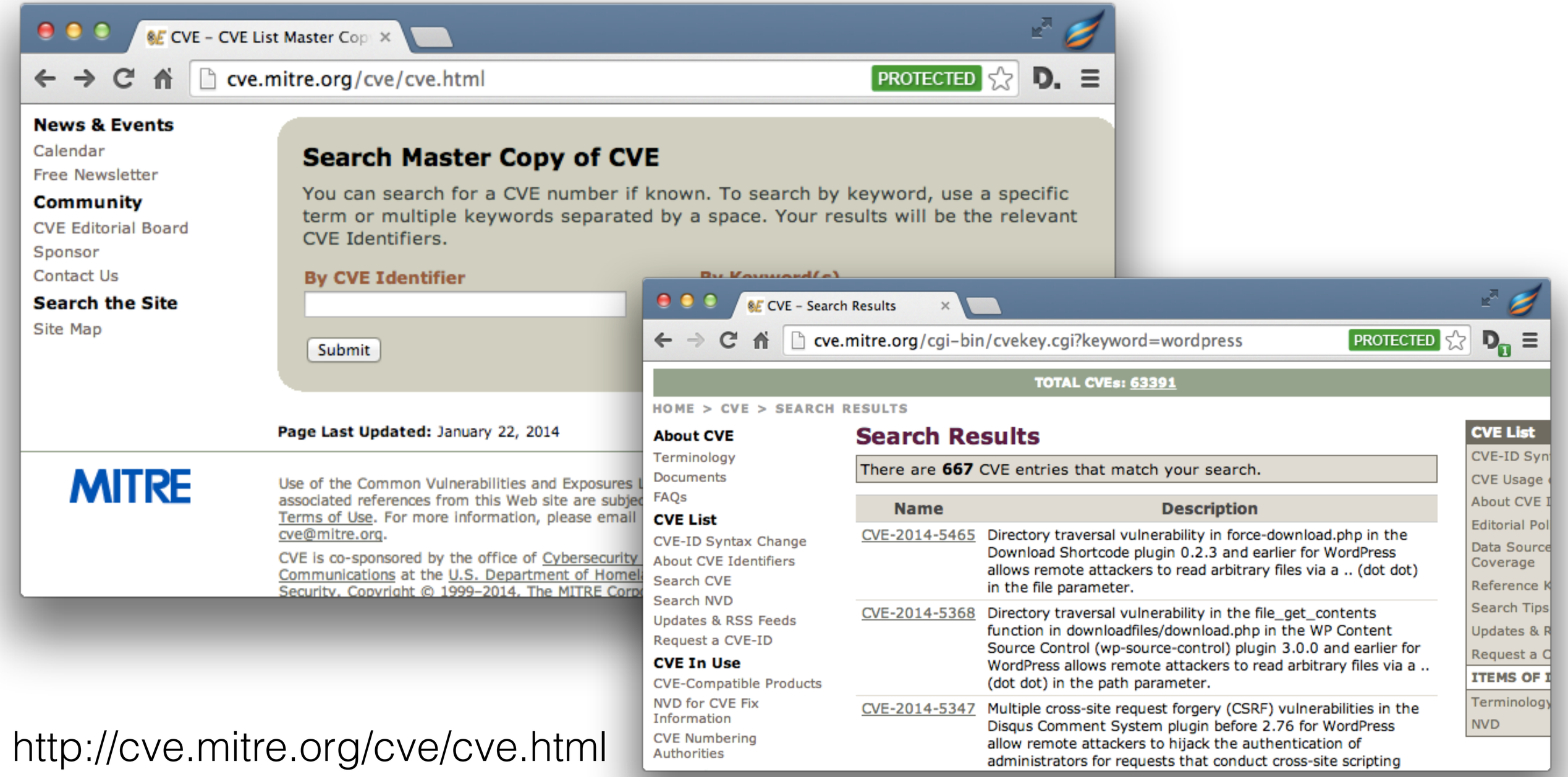


http://www.exploit-db.com/google-dorks/



- Web Server
- SSL
- Namespace Provider
- Email
- Hosting
- CMS
- Analytics & Tracking
- JavaScript Library
- Document Info
- Encoding
- Server Information

http://builtwith.com/



http://cve.mitre.org/cve/cve.html

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

End of Part 2:

Web Attacks

Finding and Exploiting Victims

Email: **jerry@owasp.org** Twitter: **@jerryhoff**

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Part 3:
Secure Development

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

This is a big topic…

großes Thema…

grande tema…

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Just for starters…

Authentication	Centralize! Shiro / Spring Security Active Directory Single Sign On / Access Management
Authorization	Centralize! External / URL based (Siteminder) Application / URL based (Filters) Authorization Annotations
Session Management	Protection Session Cookie (httponly, secure, timeouts, cryptographically strong)
Database / SQL Injection	Parameterization / ORM
Injection	Input validation / Encoding

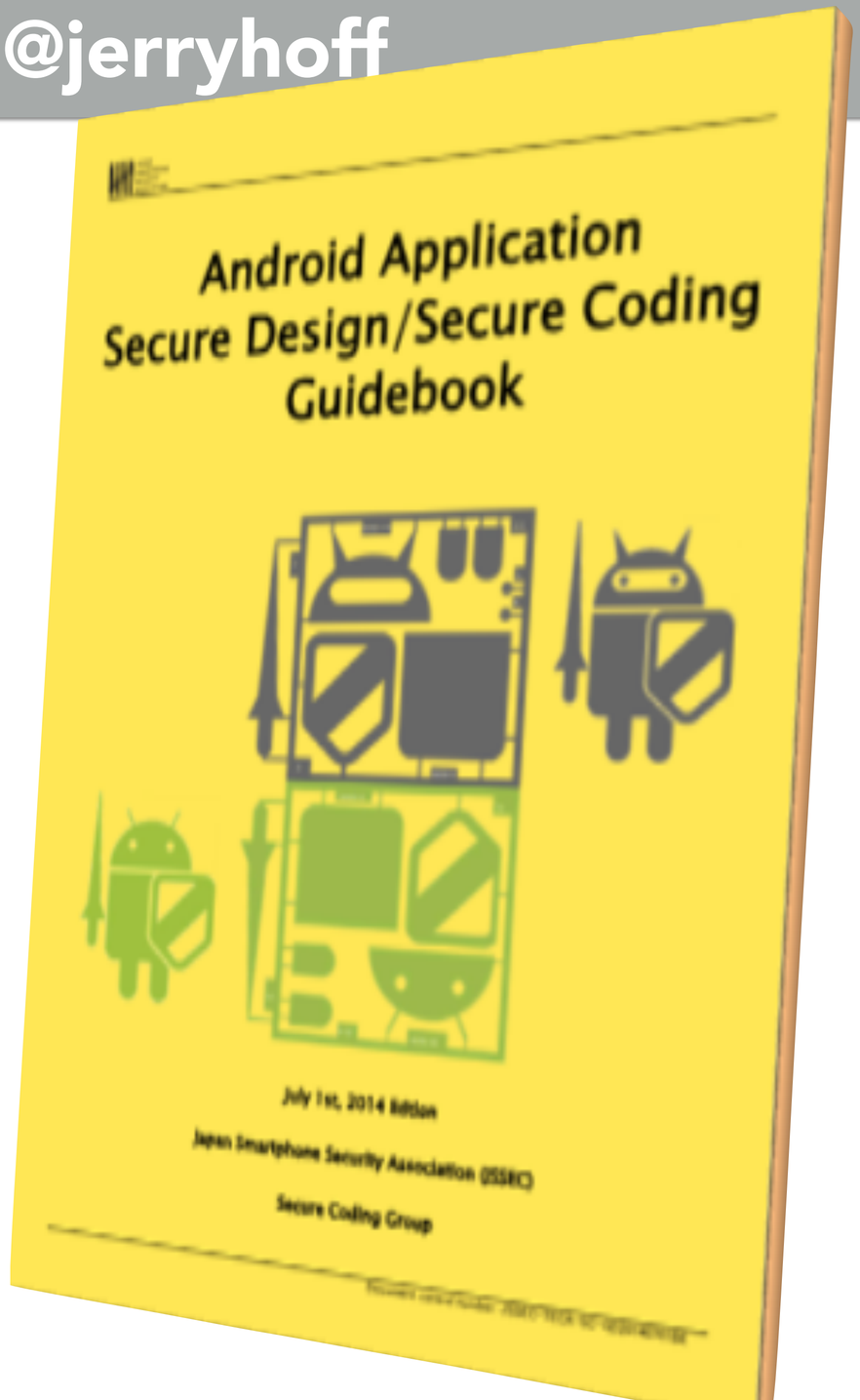
Malicious Input	Centralized, standardized input validation Contextual encoding of all untrusted input
Crypto	Hashing: SHA-2 (soon SHA-3) Symmetric: AES Asymmetric: RSA, ECC Protect Keys: Don't store in DB, use file system protections, read only, key rotation policy
Error Handling / Logging	No details in error messages Log all the things!
Data Protection	No Cache No Autocomplete
Communcation	HTTPS all the things (appropriately configured)
3rd Party Libraries	Track all 3rd party libs in deployment Check for known vulns, CVEs, etc..

OWASP
German OWASP Day 2014
9. Dezember
Hamburg

Know thy frameworks…

Android

- Android Application Secure Design / Secure Coding Guidebook
- July 2014
- 450+ page document
- Japan Smartphone Security Association (JSSEC) Secure Coding Group



Struts 1: cleartext password in datasource config
Struts 2: using auto-executed plugins that are picked up from the classpath
Android custom permission, exported receiver/provider/service, insecure version, touchjacking)
Hibernate: cleartext password in connection config
JSF: client state saving config
JSF: developer mode enabled config
JPA: cleartext password in connection config
J2EE: auto-executed web fragments
J2EE: verb tampering (HTTP Verb bypass)
J2EE: session expiration
J2EE: secure / httponly flags
J2EE: error page
J2EE: url rewriting
WebSphere: serve servlets by class name

…… hundreds of platform specific configuration rules ……

Browser Security

- Strict-Transport-Security: Enforces HTTPS
- X-Frame-Options: Anti-clickjacking
- X-XSS-Protection: Anti-Reflected XSS
- Content-Security-Policy: Anti-XSS, etc..
- X-Content-Type: “nosniff”, prevents browser from guessing a content-type

https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Part 4:
Organization Defense

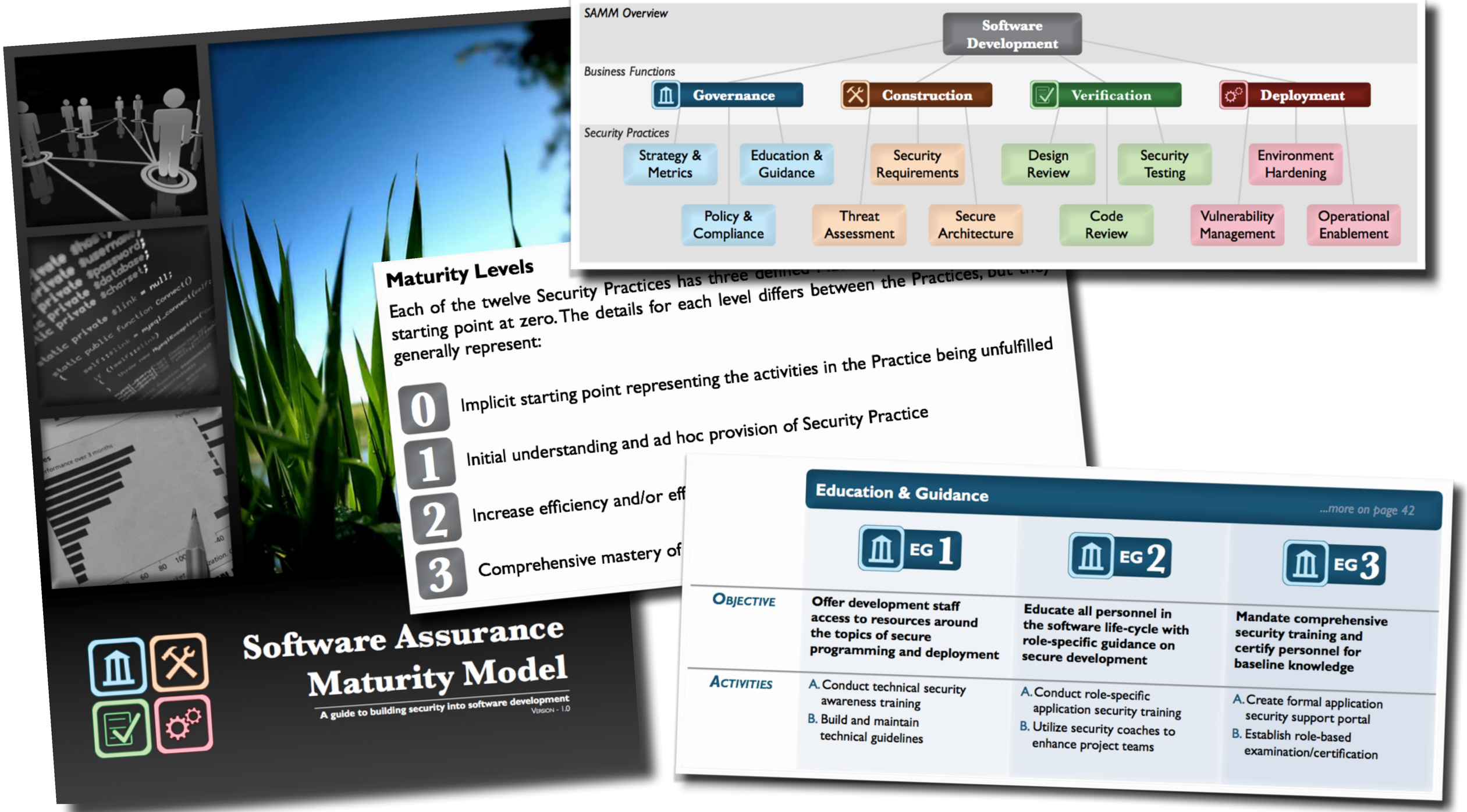
Microsoft

Microsoft®
Security Development Lifecycle

Simplified Implementation of the Microsoft SDL

Updated November 4, 2010

For the latest information, please see http://www.microsoft.com/sdl.


SAMM Overview
Software Development
Business Functions
Governance
Construction
Verification
Deployment
Security Practices
Strategy & Metrics
Education & Guidance
Security Requirements
Design Review
Security Testing
Environment Hardening
Policy & Compliance
Threat Assessment
Secure Architecture
Code Review
Vulnerability Management
Operational Enablement
Maturity Levels
Each of the twelve Security Practices has three defined
starting point at zero. The details for each level differs between the Practices, but they
generally represent:
0 Implicit starting point representing the activities in the Practice being unfulfilled
1 Initial understanding and ad hoc provision of Security Practice
2 Increase efficiency and/or eff
3 Comprehensive mastery of
Education & Guidance
...more on page 42
EG 1
EG 2
EG 3
OBJECTIVE
Offer development staff access to resources around the topics of secure programming and deployment
Educate all personnel in the software life-cycle with role-specific guidance on secure development
Mandate comprehensive security training and certify personnel for baseline knowledge
ACTIVITIES
A. Conduct technical security awareness training
B. Build and maintain technical guidelines
A. Conduct role-specific application security training
B. Utilize security coaches to enhance project teams
A. Create formal application security support portal
B. Establish role-based examination/certification
Software Assurance Maturity Model
A guide to building security into software development
Version - 1.0

Maturity

- Assess your organization based on a maturity model
- Pick a target level based on organizational risk tolerance
- Plan a path to achieve the target level
- Direction: top-down (C-Level) - cascade to BA, Architects, Developers, QA, Deployment…

https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Often overlooked…

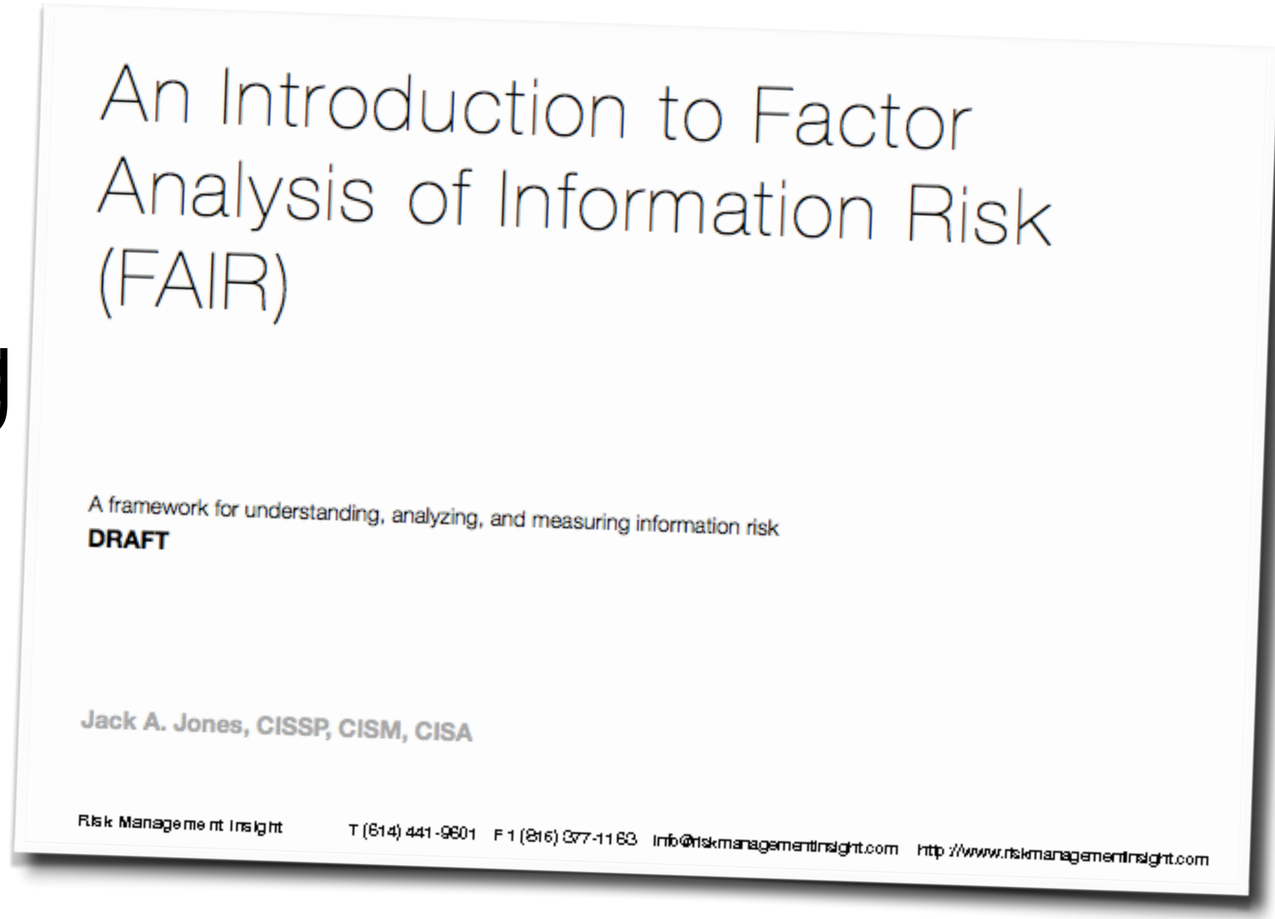
- Standardized security controls
- Secure coding guidelines
- Dependency management
- Framework-specific security training

Example: Mozilla Playdoh

https://playdoh.readthedocs.org/en/latest/

Backlog

- What about existing applications?
- Quantify the risk (risk-based approach)


An Introduction to Factor Analysis of Information Risk (FAIR)

A framework for understanding, analyzing, and measuring information risk
DRAFT

Jack A. Jones, CISSP, CISM, CISA

Risk Management Insight T (614) 441-9601 F 1 (816) 377-1163 info@riskmanagementinsight.com http://www.riskmanagementinsight.com

http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

That's it!

Questions? Fragen? Domande?

@jerryhoff

jerry@owasp.org

https://www.youtube.com/user/AppsecTutorialSeries

http://www.computerworld.com/author/jerry-hoff/