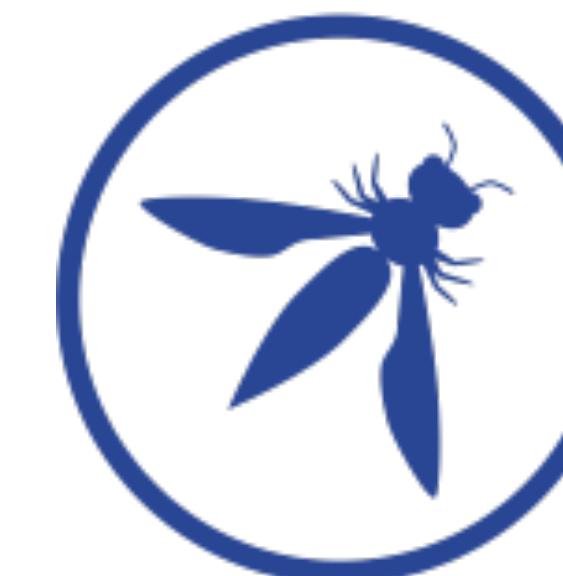


Secure development and the SDLC

Presented By Jerry Hoff
@jerryhoff



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

Email: jerry@owasp.org Twitter: @jerryhoff



Part 1: The Big Picture

Email: jerry@owasp.org Twitter: @jerryhoff



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 due 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 employee data. The hackers likely had access to confidential data on all 800,000 USPS employees. That includes names, Social Security numbers, addresses, and pretty much anything you'd put on a job application.
- Customer credit card information seemingly wasn't exposed. However, anyone who used USPS customer support from January 1st to August 16th of 2014 might have had their 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 **t** 1303 TWEET **in** 1018 LINKEDIN **95** COMMENT **e** 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."

USA NOW



Obama's climate change plan: destined to fail? | USA NOW
Nov 12, 2014

Hundreds of PHL security cams hacked, posted online

November 11, 2014 12:37pm

[Facebook Recommend](#) 923 [Share](#) 1827 [Tweet](#) 85 [Email](#) 0 [ShareThis](#) 2165 [G+1](#) 0

United States (11046)
Korea, Republic Of (6536)
China (4770)
Mexico (3359)
France (3285)
Italy (2870)
United Kingdom (2422)
Netherlands (2268)
Colombia (2220)
India (1970)
Indonesia (1751)
Turkey (1551)
Hong Kong (1486)
Taiwan Province Of (1295)
Japan (1258)
Brazil (1195)
Thailand (1192)
Argentina (1070)
Canada (1042)
Spain (1022)
Romania (955)
Viet Nam (935)
Australia (924)
Malaysia (897)



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

[Facebook Recommend](#) 1.6k

[Reddit](#) [P](#) [g+](#) [Print](#)

The scary reality of hacking infrastructure

699
TOTAL SHARES

505 [Facebook](#) 106 [Twitter](#) 62 [LinkedIn](#) 26 [Email](#)

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.

why?
warum?
perche?

Email: jerry@owasp.org Twitter: @jerryhoff



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**

The screenshot shows a web browser window displaying the 'WebGoat Coins Customer Portal'. The left sidebar contains a navigation menu with links like 'Customer Login', 'Forgot Password', 'Change Password', 'Customer Portal', 'Product Catalog', 'Product Details', 'Customer Orders', 'Logout', 'Injection Attacks', 'Cross Site Scripting (XSS)', 'Authentication Issues', 'Testing and Debugging', and 'Encryption'. The main content area shows a table of 'WEBGOAT COINS CUSTOMER ORDERS' with three entries:

Order Number	Status	Required Date	Shipped Date
10124	Shipped	05/29/2010	05/25/2010
10278	Shipped	08/16/2011	08/09/2011
10346	Shipped	12/05/2011	11/30/2011

Below the table, a green box displays the details for the first order:

customerName	Goat Gold Store
customerNumber	112
orderNumber	10124
productName	2007 Designs
quantityOrdered	21
priceEach	153
productImage	thumbWashington.jpg

A link 'Download Product Image' is also present.

Vulnerability



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

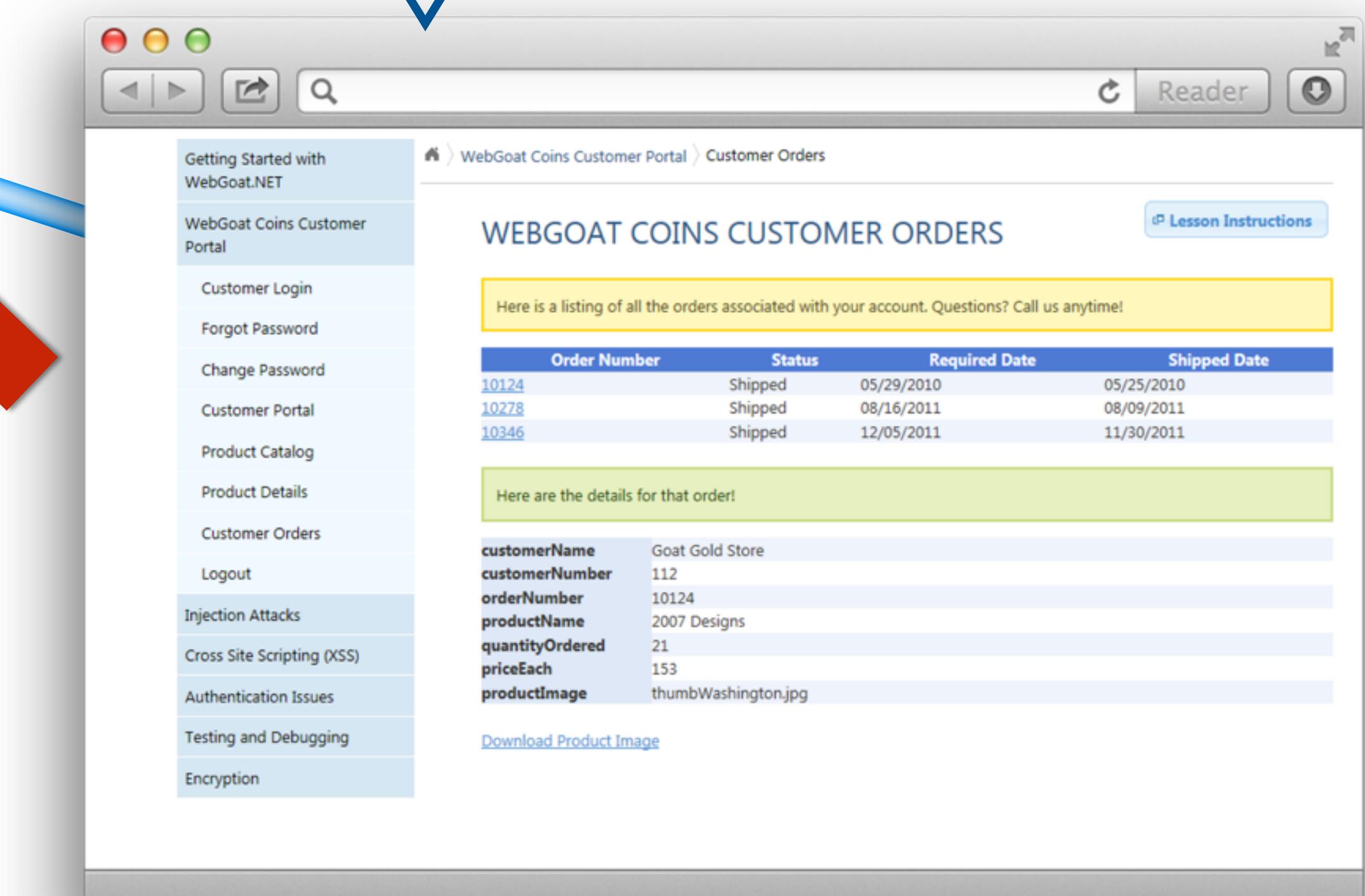


Injection
Authentication
Access Control

Vulnerable Libraries
Forge HTTP Headers
Abuse Business Logic
Security Configuration
Accept Forged Requests

Steal Cookie
Guess Cookie
Reuse Cookies
Steal Data

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



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**

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....

End of Part 1:
The Big Picture

Email: jerry@owasp.org Twitter: @jerryhoff



Part 2: Web Attacks

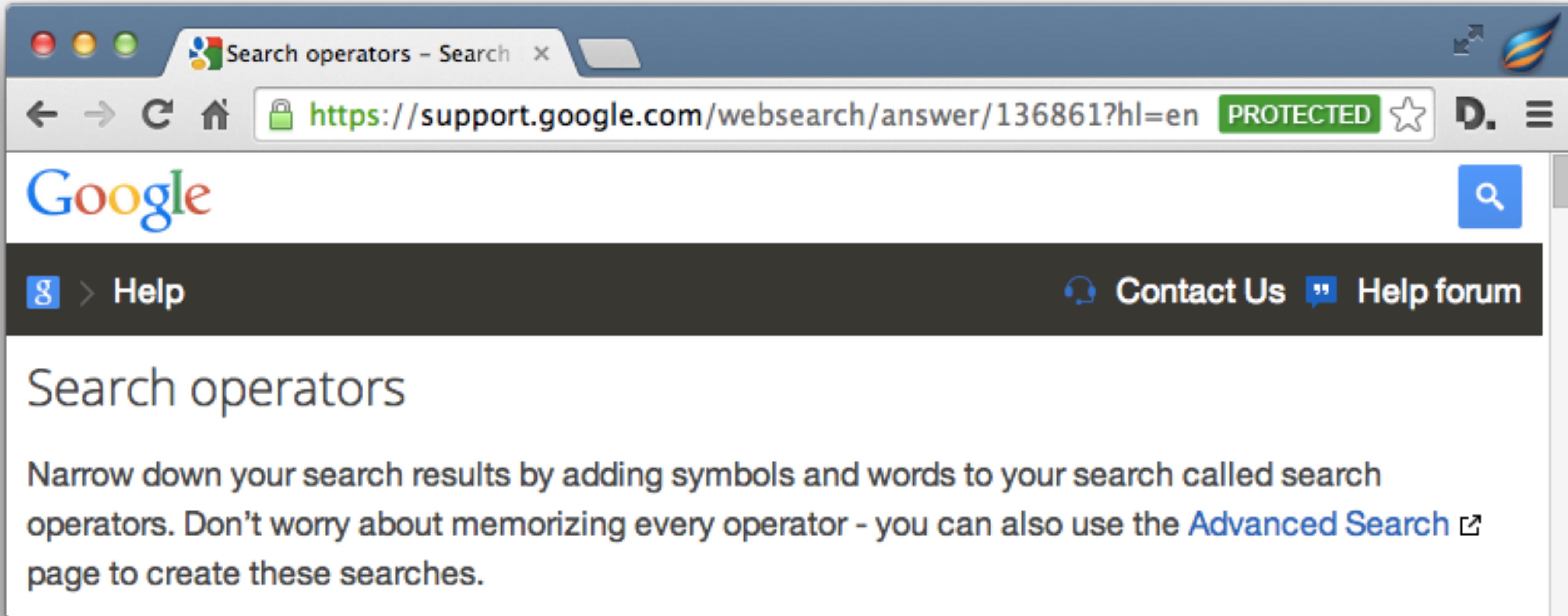
Finding and Exploiting Victims

Am I Secure?

bin ich sicher?
sono sicuro?

Advanced Google Search

about: link: site: filetype: inurl:



The screenshot shows a web browser window with the title bar "Search operators - Search". The address bar displays a secure connection to "https://support.google.com/websearch/answer/136861?hl=en" with a "PROTECTED" badge. The main content area is a Google search results page titled "Search operators". The text on the page reads: "Narrow down your search results by adding symbols and words to your search called search operators. Don't worry about memorizing every operator - you can also use the Advanced Search page to create these searches." Navigation links for "Help" and "Contact Us" are visible at the bottom.

Finding file types

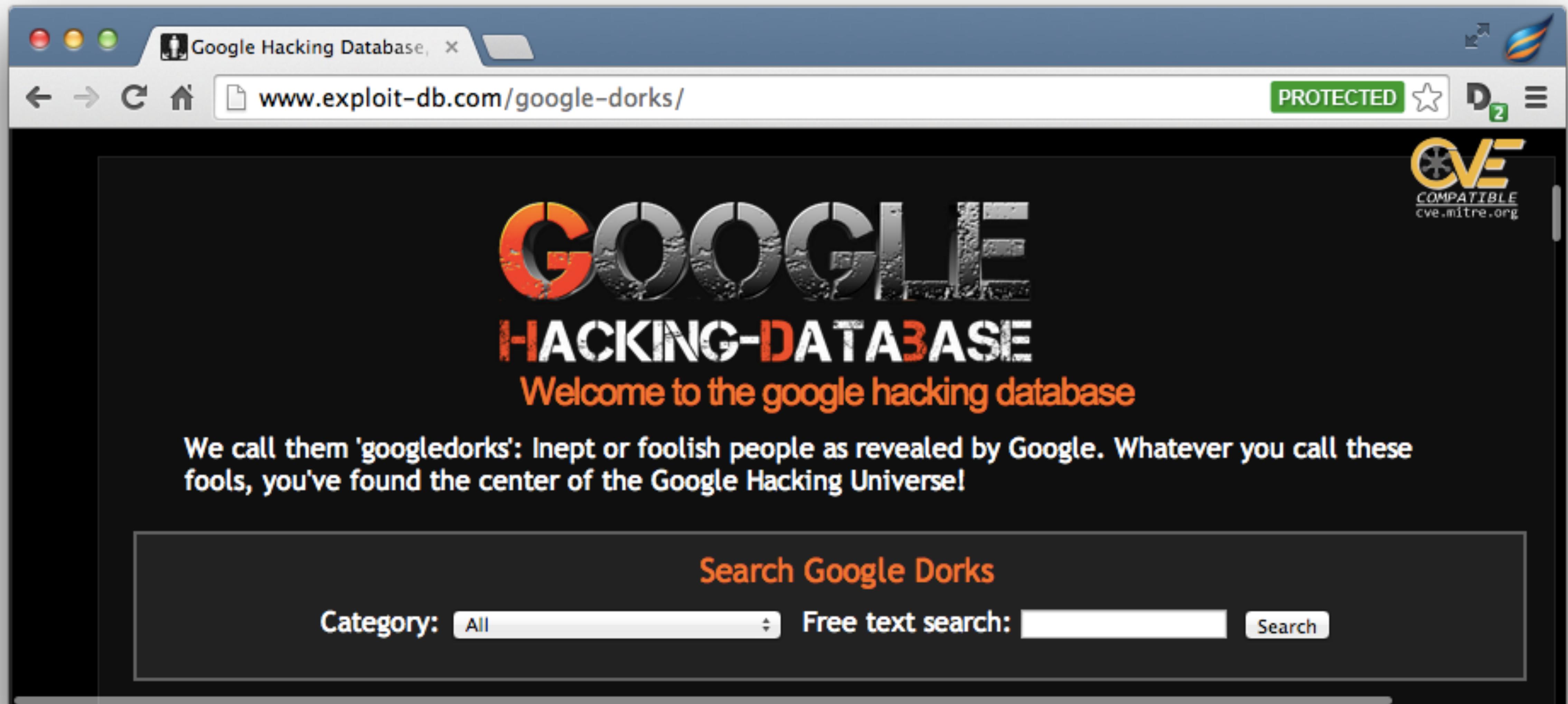
- site:example.com filetype:__
- Sometimes determine technologies (asp, php, jsp, aspx, cfm, pl)
- find interesting file types (.pdf, .docx, .xlsx, .txt, .readme)
- find very interesting file types (.log, .old)

Getting more specific

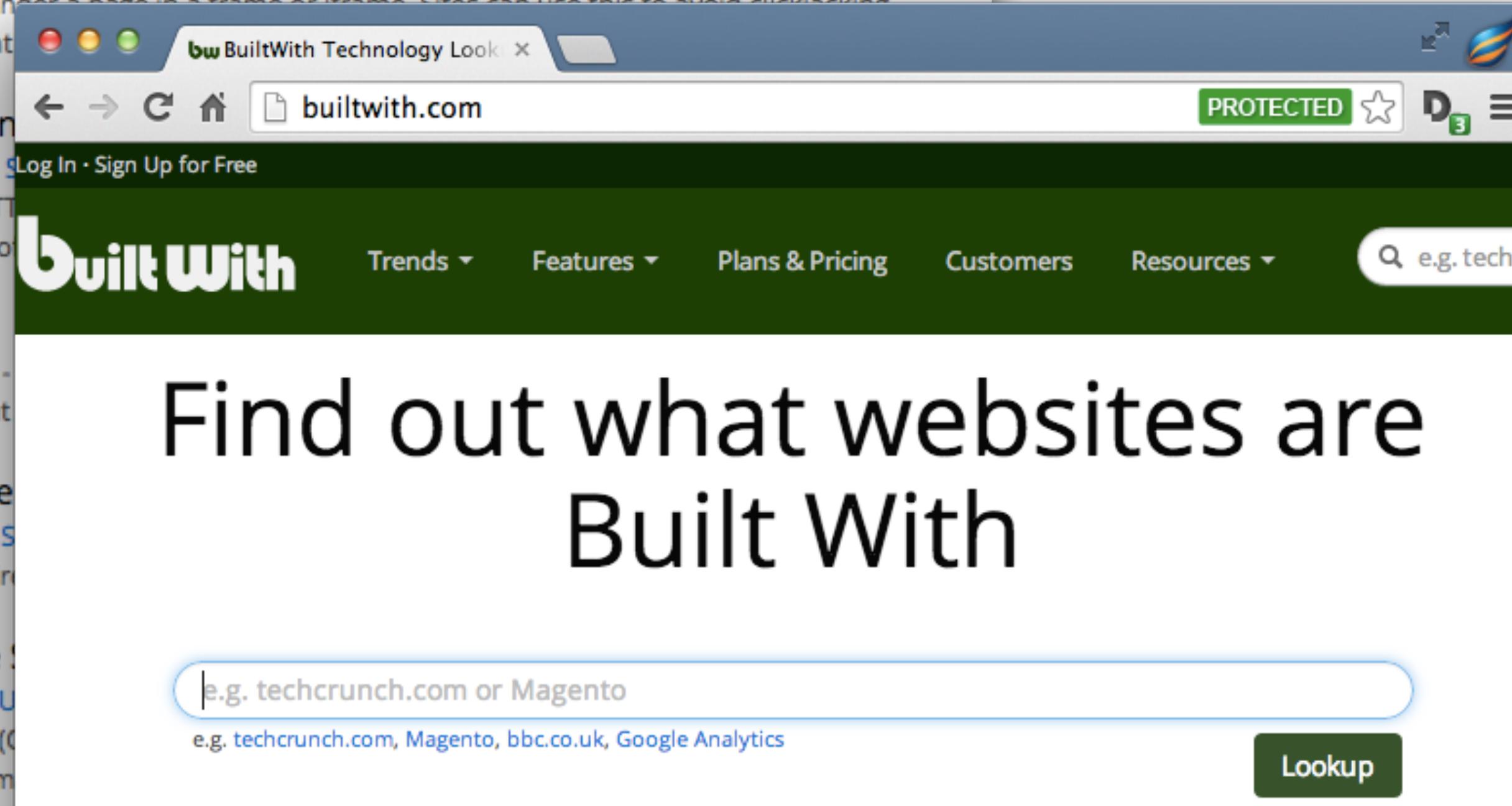
- inurl:
- Searches for keywords in URL
- Use this to find all “wordpress” login screens...

filetype:php inurl:wp-admin inurl:admin.php "lost your password"





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



The screenshot shows a browser window displaying the BuiltWith Technology Lookup website. The URL in the address bar is builtwith.com. The page header includes the BuiltWith logo and navigation links for Trends, Features, Plans & Pricing, Customers, and Resources. A search bar at the top right contains the placeholder "e.g. techcrunch". Below the search bar, there is a large text area with the heading "Find out what websites are Built With". A text input field below the heading has the placeholder "e.g. techcrunch.com or Magento". To the right of this input field is a green "Lookup" button. The main content area of the page discusses various web technologies and their usage statistics.

Document Information

X-Frame-Options
[X-Frame-Options Usage Statistics - Websites using X-Frame-Options](#)
The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a frame or iframe. This can be used to avoid clickjacking attacks, by ensuring that

X-XSS-Protection
[X-XSS-Protection Usage Statistics - Websites using X-XSS-Protection](#)
X-XSS-Protection is a HTTP response header that can be used to prevent XSS attacks, and off the "XSS Filter" on

IFrame
[IFrame Usage Statistics - Websites using IFrame](#)
The page shows content

HTML5 DocType
[HTML5 DocType Usage Statistics - Websites using HTML5 DocType](#)
The DOCTYPE is a required part of an HTML document, and it defines the rules that the browser should use to interpret the document written in a markup language like

Cascading Style Sheets
[Cascading Style Sheets Usage Statistics - Websites using Cascading Style Sheets](#)
Cascading Style Sheets (CSS) is a style sheet language used to describe the presentation of a document written in a markup language like

OpenSearch
[OpenSearch Usage Statistics - Websites using OpenSearch](#)
The OpenSearch description document format can be used to describe a search engine so that it can be used by search client applications.

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

<http://builtwith.com/>

The screenshot shows a web browser window with the title "CVE - CVE List Master Cop..." and the URL "cve.mitre.org/cve/cve.html". The page has a sidebar with links for "News & Events", "Community", and "Search the Site". The main content area is titled "Search Master Copy of CVE" and contains instructions for searching by CVE Identifier or Keyword(s). There is a search form with fields for "By CVE Identifier" and "By Keyword(s)".

The screenshot shows a web browser window with the title "CVE - CVE List Master Cop..." and the URL "cve.mitre.org/cve/cve.html". The page has a sidebar with links for "News & Events", "Community", and "Search the Site". The main content area is titled "Search Master Copy of CVE" and contains instructions for searching by CVE Identifier or Keyword(s). There is a search form with fields for "By CVE Identifier" and "By Keyword(s)".

Page Last Updated: January 22, 2014

MITRE

Use of the Common Vulnerabilities and Exposures is subject to the [Terms of Use](#). For more information, please email cve@mitre.org.

CVE is co-sponsored by the office of [Cybersecurity Communications](#) at the [U.S. Department of Homeland Security](#). Copyright © 1999–2014, The MITRE Corporation.

The screenshot shows a web browser window with the title "CVE - Search Results" and the URL "cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress". The page displays a search results summary with "TOTAL CVEs: 63391" and a breadcrumb trail "HOME > CVE > SEARCH RESULTS". The main content area is titled "Search Results" and states "There are 667 CVE entries that match your search." A table lists three CVE entries with their names and descriptions.

Name	Description
CVE-2014-5465	Directory traversal vulnerability in force-download.php in the Download Shortcode plugin 0.2.3 and earlier for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter.
CVE-2014-5368	Directory traversal vulnerability in the file_get_contents function in downloadfiles/download.php in the WP Content Source Control (wp-source-control) plugin 3.0.0 and earlier for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the path parameter.
CVE-2014-5347	Multiple cross-site request forgery (CSRF) vulnerabilities in the Disqus Comment System plugin before 2.7.6 for WordPress allow remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting.

CVE List

- CVE-ID Syn
- CVE Usage
- About CVE I
- Editorial Pol
- Data Source
- Coverage
- Reference K
- Search Tips
- Updates & R
- Request a C

ITEMS OF I

- Terminology
- NVD

End of Part 2: **Web Attacks** **Finding and Exploiting Victims**

Part 3: Secure Development

This is a big topic...
großes Thema...
grande tema...

Email: jerry@owasp.org Twitter: @jerryhoff



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
Communication	HTTPS all the things (appropriately configured)
3rd Party Libraries	Track all 3rd party libs in deployment Check for known vulns, CVEs, etc..

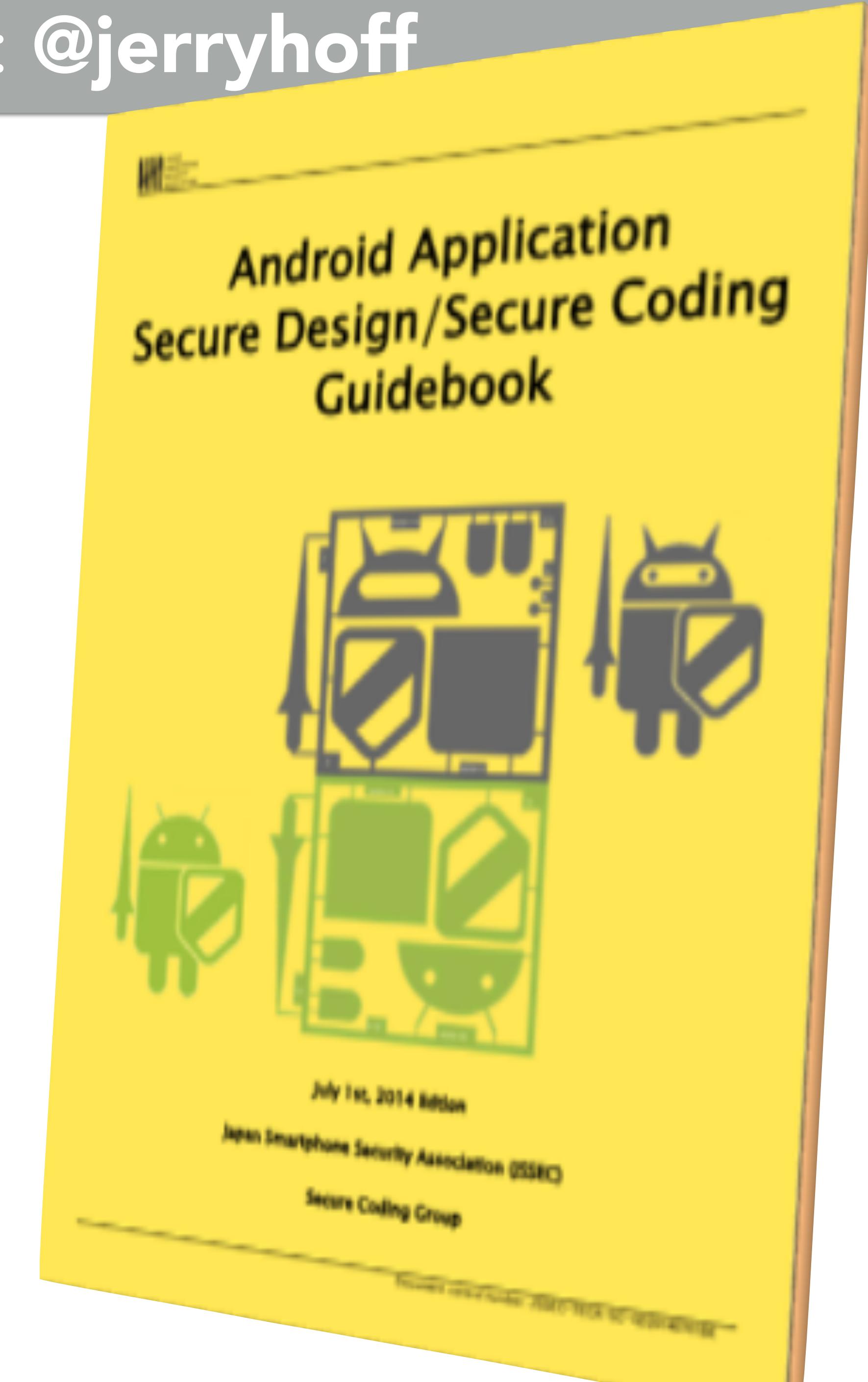
Email: jerry@owasp.org Twitter: @jerryhoff



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

Part 4: Organization Defense

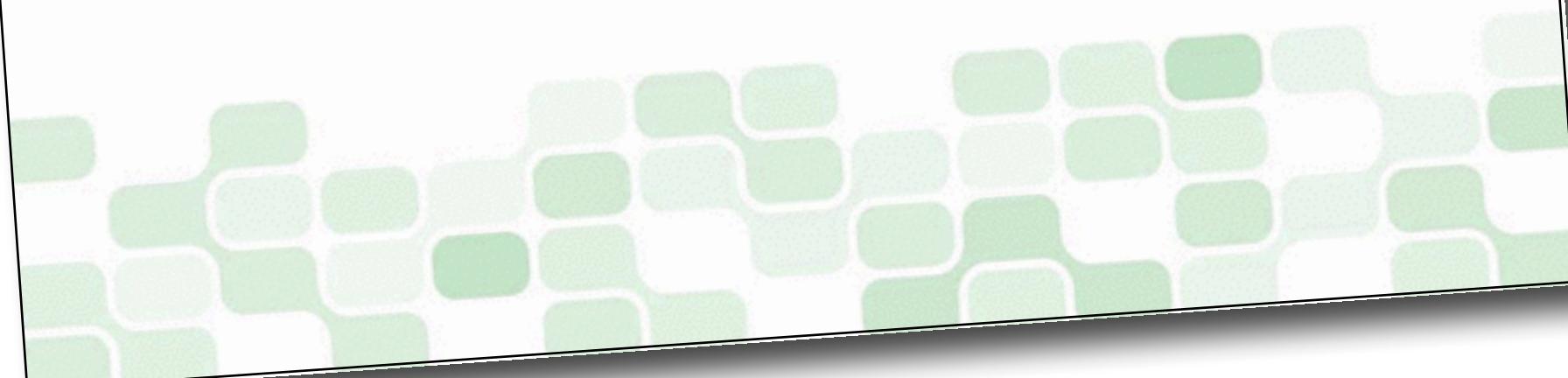


Microsoft® Security Development Lifecycle

Simplified Implementation of the Microsoft SDL

Updated November 4, 2010

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



The slide features a collage of images: a network diagram with people icons, a snippet of C++ code showing database connection logic, a bar chart titled 'Performance over 3 months' with values 0.5, 0.6, 0.7, 0.8, 0.9, and 1.0, and a close-up photograph of green grass growing in water. At the bottom left are four icons: a blue square with a white building, an orange square with a white wrench, a green square with a white checkmark, and a red square with a white gear. The title 'Software Assurance Maturity Model' is at the top right, followed by the subtitle 'A guide to building security into software development' and 'VERSION - 1.0'.

Software Assurance Maturity Model

A guide to building security into software development
VERSION - 1.0

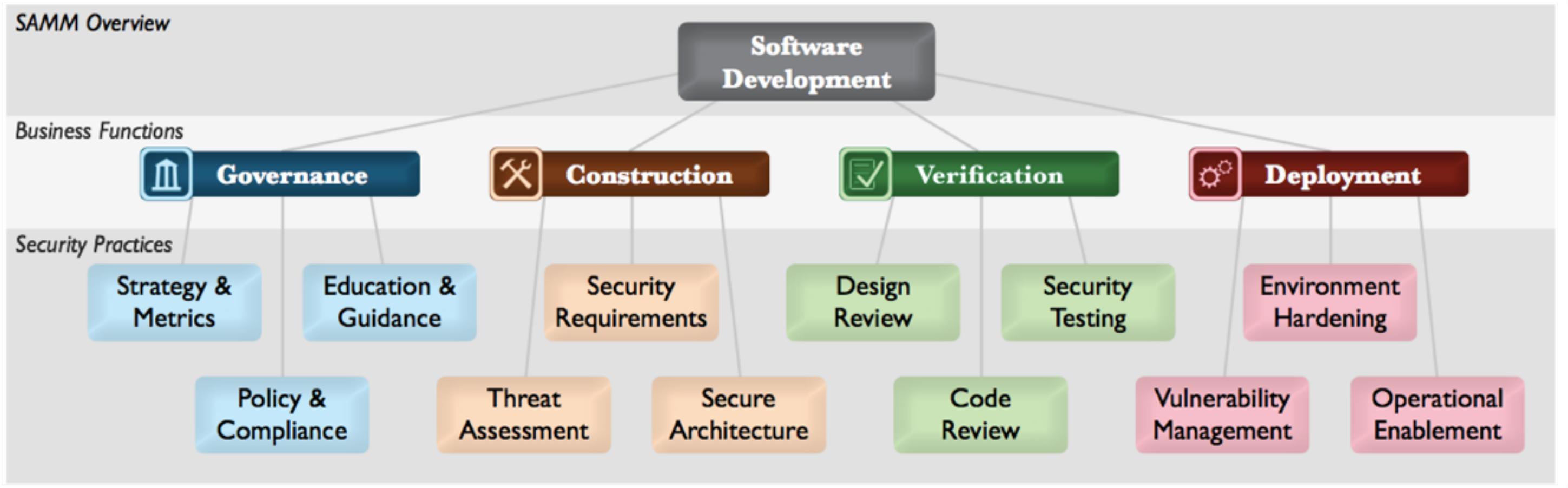


Software Assurance Maturity Model

A guide to building security into software development
VERSION - 1.0



SAMM Overview



Maturity Levels

Each of the twelve Security Practices has three defined levels of maturity, starting point at zero. The details for each level differs between the Practices, but the 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 effectiveness
- 3** Comprehensive mastery of the practice

Education & Guidance



EG 1



EG 2



EG 3

...more on page 42

OBJECTIVE	ACTIVITIES		
<p>Offer development staff access to resources around the topics of secure programming and deployment</p> <p>Educate all personnel in the software life-cycle with role-specific guidance on secure development</p> <p>Mandate comprehensive security training and certify personnel for baseline knowledge</p>	<p>A. Conduct technical security awareness training</p> <p>B. Build and maintain technical guidelines</p> <p>A. Conduct role-specific application security training</p> <p>B. Utilize security coaches to enhance project teams</p> <p>A. Create formal application security support portal</p> <p>B. Establish role-based examination/certification</p>		

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...

Often overlooked...



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

Example: Mozilla Playdoh

The screenshot shows a dark-themed documentation page for 'Playdoh'. On the left, a sidebar lists various sections: 'Getting started', 'User Guide' (which is currently selected), 'Maintaining playdoh, playdoh-lib, playdoh-docs and funfactory', 'pip and friends: Packaging', 'Operations', 'Best Practices', 'Monkey patches', 'Troubleshooting', and 'Getting help and contacting playdoh devs'. The main content area has a light background and features a large title 'Playdoh' in bold. Below it, a paragraph explains that Mozilla's Playdoh is a web application template based on Django. It then describes Django as a high-level Python Web framework and notes that Playdoh is a pre-configured Django project with specific goals. A bulleted list at the bottom outlines these goals.

Playdoh

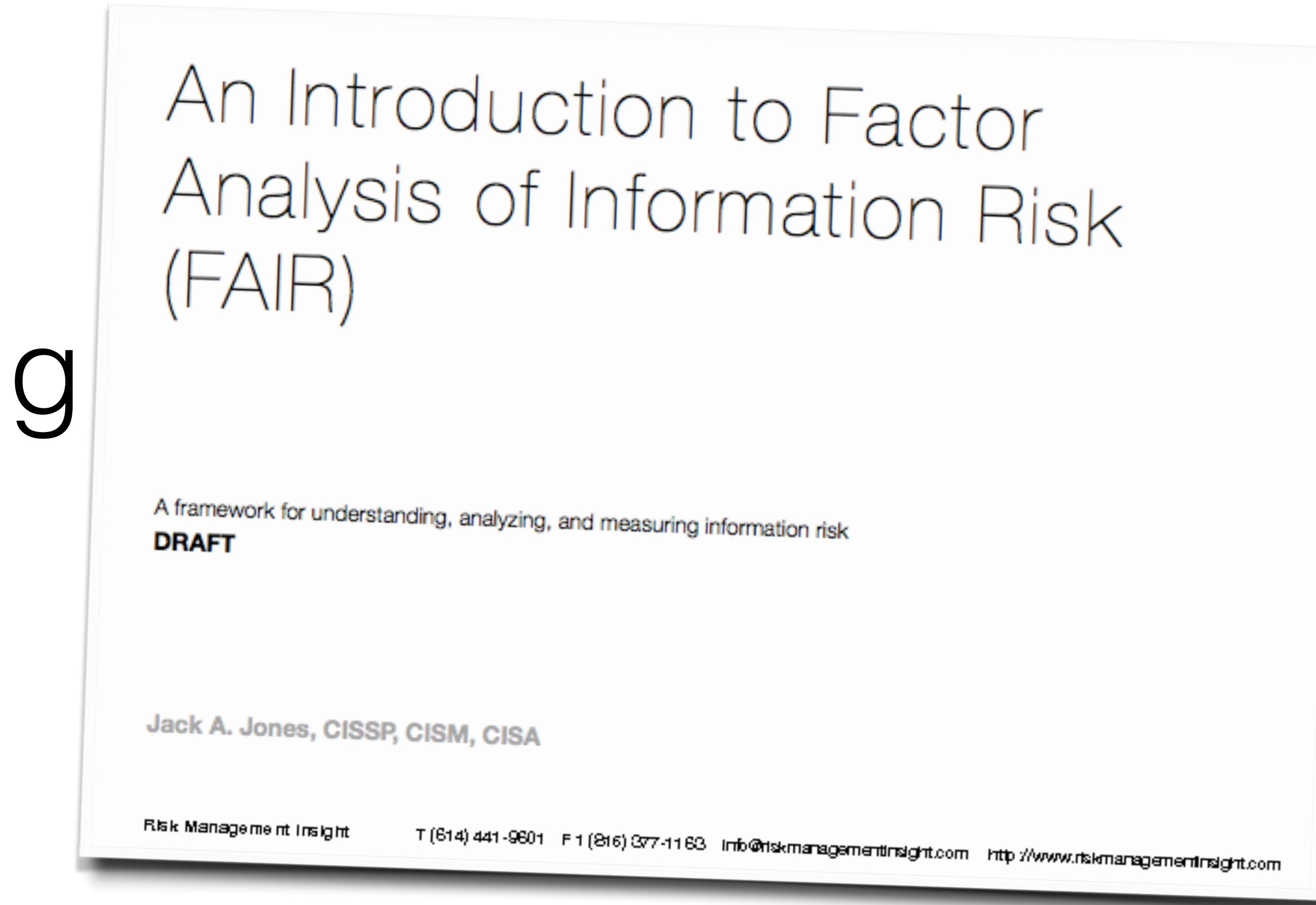
Mozilla's Playdoh is a web application template based on [Django](#).

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Playdoh is simply a pre-configured Django project that adds some essential modules and middleware to meet the following goals:

- Enhance the **security** of your application and its data
- Achieve optimal **performance** in the face of high traffic
- **Localize** content in multiple languages using [Mozilla's L10n standards](#)
- Use the best tools and best practices to make development **fun and easy**

Backlog

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



That's it!

Questions? Fragen? Domande?



@jerryhoff



jerry@owasp.org



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



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