OWASP Dublin Chapter

Alexis FitzGerald

Rits Group
alexis@rits.ie
Skype:fitzgera

OWASP
30th June 2010

The OWASP Foundation
http://www.owasp.org

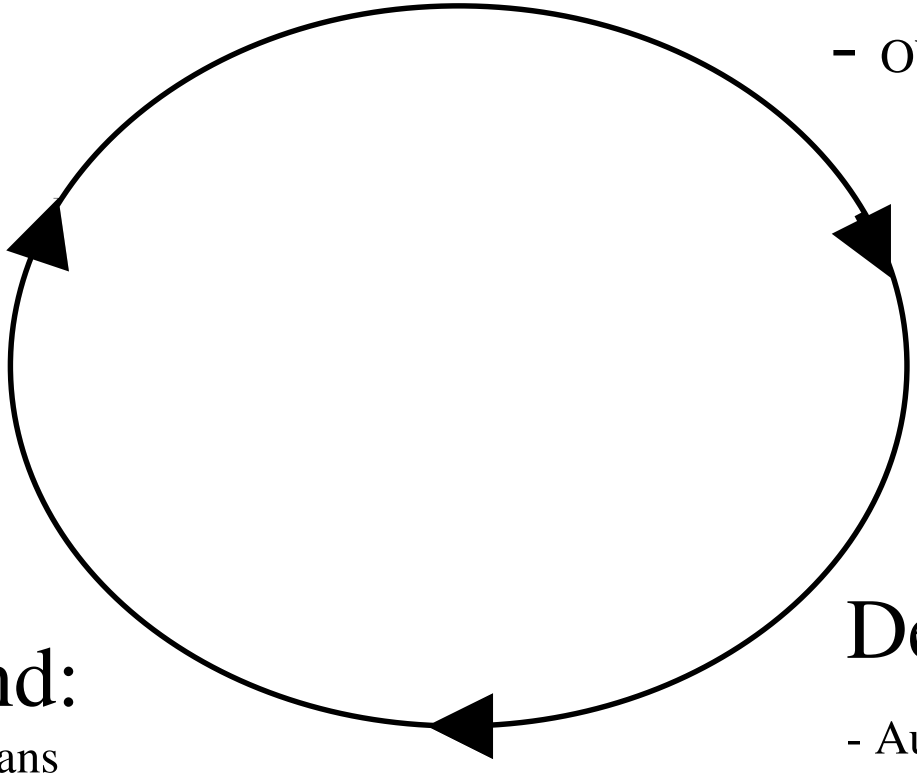
Agenda

- **General Information Security**
- Some OWASP Projects
- State of Application Security
- Data Protection Legislation – What It Says
- Security LifeCycle (Requirements etc.)
- Session Management Good Practices
- User Lifecycle Good Practices

Information Security Pillars

- Confidentiality
  - Prevent disclosure of information
- Integrity
  - Prevent unnecessary modification of data
- Availability
  - Ensure availability of data and systems on a timely basis

Security Model



Protect:

- OWASP Top 10

Detect:

- Audit

- Monitoring

Respond:

- Incident Plans

Agenda

- General Information Security
- **Some OWASP Projects**
- State of Application Security
- Data Protection Legislation – What It Says
- Security LifeCycle (Requirements etc.)
- Session Management Good Practices
- User Lifecycle Good Practices

OWASP Top 10 -I

OWASP

The Open Web Application Security Project

OWASP Top 10 - 2010

The Ten Most Critical Web Application Security Risks

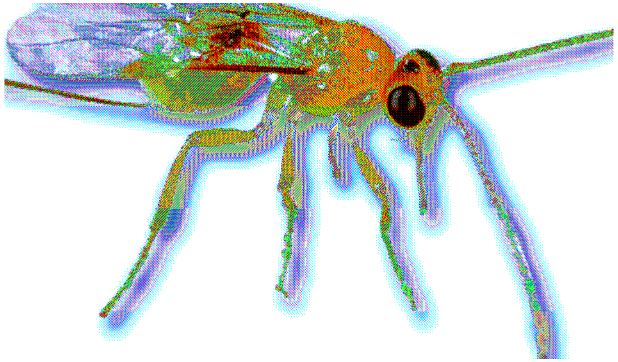
- Risk focused list of the **Top 10 Most Critical Web Application Security Risks**

OWASP Top 10 2010 - II

- 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(NEW)
- A7 –Insecure Cryptographic Storage
- A8 –Failure to Restrict URL Access
- A9 –Insufficient Transport Layer Protection
- A10 –UnvalidatedRedirects and Forwards (NEW)

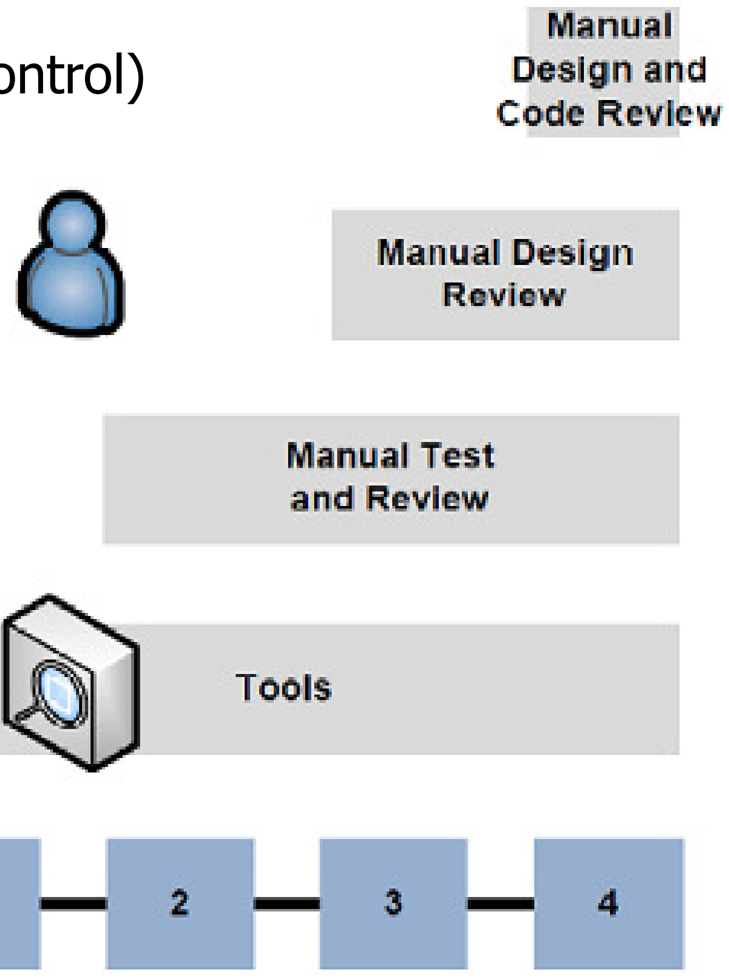
Application Security Verification Standard - ASVS

- This standard can be used to establish a level of confidence in the security of Web applications
  - Use as a metric
  - Use as a yardstick
  - Use during procurement



ASVS Verification Levels

- 1 – Automated (Minimal Security Control)
- 2 – Manual (Personal Transactions)
- 3 – Design (Business 2 Business)
- 4 – Internal (Critical Systems)



OWASP Enterprise Security API - ESAPI

- Free, open source, web application security control library that makes it easier for programmers to write lower-risk applications
- Standard Interfaces
- Reference implementations for different languages e.g. Java EE, .NET, Classic ASP, PHP
- The status for each language is different
- Don’t reinvent the wheel!

OWASP ESAPI II

Includes controls for the following:

- Authentication
- Access control
- Input validation
- Output encoding/escaping
- Cryptography
- Error handling and logging
- Communication security
- HTTP security
- Security configuration

Agenda

- General Information Security
- Some OWASP Projects
- **State of Application Security**
- Data Protection Legislation – What It Says
- Security LifeCycle (Requirements etc.)
- Session Management Good Practices
- User Lifecycle Good Practices

Voice of Reason

- “So over the past 9 years I have performed hundreds of penetration tests and code reviews and have also discovered hundreds of application security issues. Out of all of the issues I have discovered how many could have significant impact on the business or brand. maybe 10-20%? “
  - Eoin http://asg.ie/ 15th Jan 2010

What is the impact?

- Website hacked and passwords compromised in January 2010

- Darragh Doyle, Communications Officer, in an interview on RTE’s Morning Ireland (mostly about Google Buzz). When asked about the aftermath of the hack (2mins 45secs into interview) :
  - –“Reset over 292,000 passwords but we passed the 300,000 user mark yesterday with 17 million hits on the site, **so there's no such thing really as bad publicity**"

- http://www.rte.ie/news/2010/0210/morningireland.html

Opinion

- Given the number of vulnerabilities it’s surprising how few websites are hacked

- Many websites with vulnerabilities seem to survive for years without a problem

Why aren’t applications developed securely?

- Cost of security
  - Time/Money
  - No competitive advantage
  - Functionality over security
- Lack of awareness
  - Developers not aware of issues
  - However business people who commission developments expect them to be secure
- Poor security support in development tools and frameworks

Common Application Security Model

- Prevalent where security isn’t really considered
- Features:
  - Use a password
  - Forgotten password – email out in clear text
  - Maybe use SSL (at least for login)
  - Some other incidental security features

Agenda

- General Information Security
- Some OWASP Projects
- State of Application Security
- **Data Protection Legislation – What It Says**
- Security LifeCycle (Requirements etc.)
- Session Management Good Practices
- User Lifecycle Good Practices

Data Protection Legislation

What does Data Protection Commissioner say about website security and personal information?

ICO (UK) and Websites

- **We collect personal information through our website. Do we have to use an encryption-based transmission system?**
- You are responsible for processing personal information securely. You must adopt appropriate technical and organisational measures to protect the information you collect. **It is difficult to see how you could do this without having a secure, encryption-based transmission system** if the personal information is sensitive or poses a risk to individuals, for example, if it includes credit card numbers. You should be aware that although a secure transmission system will protect the personal information in transit, there is a potentially greater threat to the security of the information when it is decrypted and held on a website operator's server. **Any sensitive personal information, or information that would pose a risk to individuals, should not be held on a website server unless it is properly secured by encryption or similar techniques.**

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf

Data Protection Acts 1988 and 2003: Informal Consolidation

- 2C. Security Measures for Personal Data
- 2C.- (1) In determining **appropriate security measures** for the purposes of section 2(1)(d) of this Act, in particular (but without prejudice to the generality of that provision), where the processing involves the transmission of data over a network, a data controller -
- (a) may have regard to the **state of technological development** and the **cost of implementing the measures**, and
- (b) shall ensure that the measures provide a level of security appropriate to -
- (i) the harm that might result from unauthorised or unlawful processing, accidental or
- unlawful destruction or accidental loss of, or damage to, the data concerned, and
- (ii) the nature of the data concerned.

http://www.dataprotection.ie/viewdoc.asp?DocID=796&ad=1#2A

Data Security Guidance

- General security guidance issued by Data Protection Commissioner
- Some issues discussed:
  - Access Control
  - Encryption
  - Logs and Audit Trails

- http://www.dataprotection.ie/viewdoc.asp?DocID=29

Security Measures for Personal Data:

- More security guidance issued by Data Protection Commissioner
- "Transmission of personal data over a network….such as the internet, should normally be subject to robust encryption"

- http://www.dataprotection.ie/viewdoc.asp?DocID=39

Department of Social & Family Affairs

- Report by Data Protection Commissioner
  - "Data Protection in the Department of Social & Family Affairs"
- Recommendations include:
  - Access Control on a "Need to know basis"
  - Audit "to know who has read an individual's data"
  - Laptop Encryption
  - "Initiate a standardised approach to software development that takes security into account at the beginning of the software development life cycle"
  - Disable USB
- www.welfare.ie/EN/Topics/Documents/ODPCReport.pdf

Department of Finance

- “Protecting the confidentiality of Personal Data” Guidance for Departments
- “Standard unencrypted email should **never** be used to transmit any data of a personal or sensitive nature”
- “With regard to laptops, full disk encryption must be employed regardless of the type of data stored”

- http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

Draft Data Security Breach Code of Practice

- Published by Data Protection Commissioner June 2010
- Must report breaches except:
  - where the personal data was inaccessible in practice due to being stored on encrypted equipment secured to a high standard with a strong password **and** the password was not accessible to unauthorised individuals;
- More than 100 people

http://www.dataprotection.ie/viewdoc.asp?DocID=1077&m=f

Payment Card

- Payment Card Industry - Data Security Standard (PCI DSS)
  - Many relevant requirements
  - Requirement 6 in particular deals with software development
  - Requirement 3 talks about protecting cardholder data

Agenda

- General Information Security
- Some OWASP Projects
- State of Application Security
- Data Protection Legislation – What It Says
- **Security LifeCycle (Requirements etc.)**
- Session Management Good Practices
- User Lifecycle Good Practices

My Disclaimer

- If you already have an SDL then use that
- This approach is minimal

Microsoft Security Development Lifecycle (SDL)

- Awareness/coding guidelines
- Specify security requirements
- Include security reqs in design
- Implement security requirements
- Testing/code reviews etc. (ASVS)
- Secure deployment
- Respond to security issues

http://www.microsoft.com/security/sdl/

Security Development Lifecycle - Training

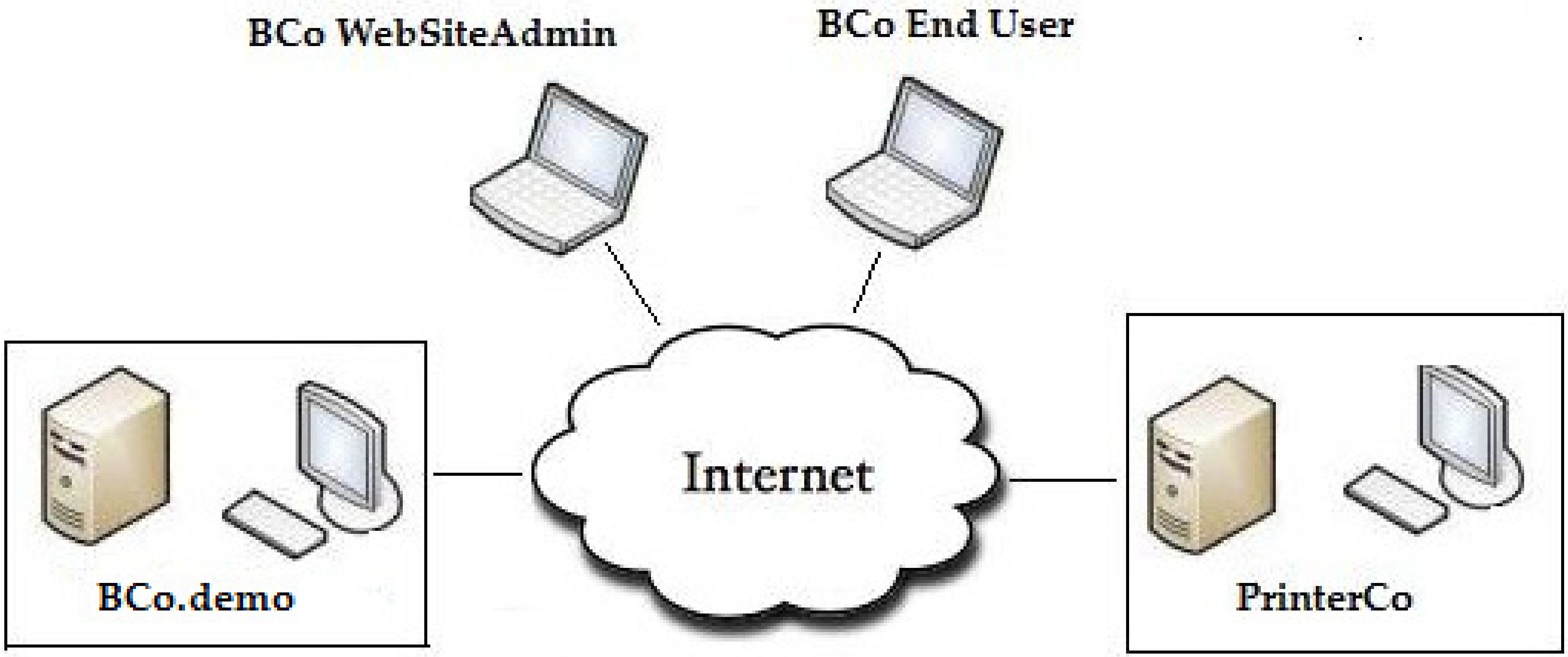
- Awareness/Security Training for developers
- Secure Coding standards especially in relation to OWASP Top 10 for your environment
- OWASP Projects (ESAPI, “cheat sheets”, developer guide)

Useful OWASP Related links

- OWASP Top 10 for .NET developers
  - http://www.troyhunt.com/2010/05/owasp-top-10-for-net-developers-part-1.html
- The OWASP Top Ten and ESAPI (J2EE)
  - http://www.jtmelton.com/2009/01/03/the-owasp-top-ten-and-esapi/
- Using the OWASP PHP ESAPI
  - http://jackwillk.blogspot.com/2010/06/using-owasp-php-esapi-part-1.html

Security Development Lifecycle - Requirements

Website – BrochureCo - BCo.demo



BCo Usage Overview

- BCo.demo End Users signup, enter their postal address and choose a selection of brochures
- Every month BCo.demo Website Admin downloads list of Bco End Users, addresses and brochure selections
- Admin cleans up list of addreses and emails list as spreadsheet to PrinterCo
- PrinterCo sends brochures via snail mail to BCo.demo End Users

OWASP Threats

- Accidental (Discovery)
- Automated Malware
- Curious Attacker
- Script Kiddies
- Motivated Attacker (Insider)
- Organized Crime

- http://www.owasp.org/index.php/Threat_Risk_Modeling

BCo Threats

Probably the first three or four are the main threats:

- **Accidental (Discovery)**
- **Automated Malware**
- **Curious Attacker**
- **Script Kiddies**
- Motivated Attacker (Insider)
- Organized Crime

Possible Data Classifications I

- Public Data (Standard Websites)
  - Static HTML (A6 –Security Misconfiguration)
  - DB Driven (Input validation etc.)
- Personal Data
  - Data Protection Legislation

Possible Data Classifications II

- Money (Online Banking)
  - Authentication
  - End user computer problems
- Payment Cards
  - PCI DSS – Avoid if possible
- Intellectual Property
  - Corporate Governance Rules

Choose Data Classification

- BCo.demo processes Personal Data

- BCo.demo is Data Controller
- PrinterCo is Data Processor

- BCo.demo is responsible for ensuring that PrinterCo has proper security measures in place

Security Drivers I

- Personal Data:
  - Data Protection Legislation

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Every organization who collect, owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

Security Drivers II

- Money
  - FDIC – Two Factor Authentication
  - Money Laundering
- Payment Card
  - PCI DSS
- Intellectual Property
  - Corporate Governance
- Information Security Policy (e.g all personal data must be encrypted)

Choose Bco.demo Security Driver

- BCo.demo processes Personal Data
- The main security driver is therefore Data Protection Legislation.
- BCo.demo needs to comply with the legislation

Choose ASVS Level for verification

- What level of ASVS should the application be verified to.
  - 1 – Automated (Minimal Security Control)
  - 2 – Manual (Personal Transactions)
  - 3 – Design (Business 2 Business)
  - 4 – Internal (Critical Systems)
- BCo.demo is probably at level 2

Data Flow Diagrams

- Identify Data Flows
- Identify Trust Boundaries
  - Where data crosses trust boundaries
  - Internal and External
- Identify Data Storage
  - Database
  - USB
  - Laptops

Data Flow Security

- For Data Flows/Trust Boundaries decide what security measures depending on classification:
  - For networks consider implementing SSL/TLS
  - Authentication and Data Validation
  - Personal data over public networks should be encrypted.
  - Internal networks? If large internal network then should consider encryption
  - End to end encryption???

BCo.demo Data Flows Security

- Data between end users and BCo.demo needs to be secured (typically SSL/TLS) etc.
- Data between website admins and BCo.demo needs to be secured (typically SSL/TLS) etc.
- Spreadsheet Email between website admin and PrinterCo needs to be secured (typically AES encryption based)

- These requirements are driven by Data Protection Legislation

Data Storage Security

- For Data Storage Location decide on security measures depending on classification:
  - Personal data on PCs, portable devices etc. should be encrypted
  - Personal data on DBs/Servers????
  - For payment card confidentiality look at PCI Requirement 3 - but it should always be protected

Other Data Storage Issues

- How to handle test data. Be careful about using a copy of production personal data as test data. It still falls under “Data Protection” regulations.
- Data produced as a result of trouble-shooting problems
- Backup data

BCo.demo Data Storage Security

- The data on the website admin laptops should be encrypted.
- Typically use hard-disk encryption

- What about storage on BCo.demo databases???

Data Retention

- How long is data to be retained?
  - "Retain it no longer than is necessary for the specified purpose or purposes”
    - Data Protection Principle 7
  - “Details of individual transactions must be retained for 6 years after the date of the transaction”
    - Consumer Protection Code

BCo.demo Data Retention

- Personal Data
  - "Retain it no longer than is necessary for the specified purpose or purposes”
- Ability for user to delete account.
- Delete accounts from backup???

Availability

- One area where InfoSec can actually save money
- “Are you ready to pay for 99.999% availability?”
- Can you live with website not being available for a day or so while service is restored?

BCo.demo Availability

- Probably the ability to restore from backup
- And rebuild the website

Define Roles/Users

- Website Roles
  - BCo.demo Website Administrator
  - Bco.demo end user (authenticated)
  - Public/Unauthenticated User

- Operational Roles
  - DBA
  - Server Network/Admin
  - Insider threat considerations

Roles/User Lifecycle

- For each role specify:
  - Identification
    - Banking – Money Laundering (Utility bills etc.)
  - Registration/Enrolment
  - Authentication/Logon
    - Passwords (Will they still be as popular in 2020?)
    - Banking - 2 Factor
  - Logoff
  - Forgotten/Lost Credentials
  - Account Disable/Lockout
  - Account Deletion

Authorisation/Access Control

- How to ensure that users can only do what they are allowed to do
  - Coarse – e.g a normal user should not be able to view the list of users
  - Fine – e.g a user should only be able to see his accounts – but not accounts of other users
  - Business logic rules

Audit Trail I

- Decide how audit trail to be implemented
- Not really covered in OWASP
- Important for detection, troubleshooting, problem resolution, forensics, litigation
- Data Protection Commissioner talks about it

Audit Trail II

- For example PCI Requirement 10.3 requires
  - User ID, type of event, timestamp, success/failure
- Suggest having a simple global Audit API which writes to (e.g):
  - Syslog Server
  - DB Table (via Stored Procedure naturally!)
- Define audit events
- Call Audit API from application

Security Development Lifecycle – Design

Design

- In design phase, incorporate the security decisions made in requirements phase
  - E.g Encryption, SSL/TLS
  - OWASP Top 10
  - Backup
  - Etc.
- A number of the chosen security controls may depend on framework configuration settings

Security Development Lifecycle –Implementation

- Implement security controls as designed in previous phases:
  - OWASP Top 10 etc.

Security Development Lifecycle –Verification

- Hopefully it should only be to confirm that the security requirements have been implemented properly
- Determine what ASVS level the application should be verified as
- OWASP Testing and Code Review Projects
- Verification based on ASVS level. Combination of:
  - Automated scans
  - Manual application testing
  - Code Reviews

Security Development Lifecycle –Release

- Deploy securely
- Remove unnecessary resources (tutorials, demos etc.)
- Web/App Server/DB hardening checklists
- Some of the security controls (e.g. authorisation) may depend on settings in the framework.

Security Development Lifecycle –Response

- Respond to security incidents
- Updated versions of libraries, frameworks:
  - Responsibility for this tends to fall between the cracks
- For example recent critical vulnerability discovered in Spring Framework. Make sure to apply appropriate patch

Agenda

- General Information Security
- Some OWASP Projects
- State of Application Security
- Data Protection Legislation – What It Says
- Security LifeCycle (Requirements etc.)
- **Session Management Good Practices**
- User Lifecycle Good Practices

Session Management - Good Practices I

- Mark session cookies as secure
- New session cookie on authentication
- HTTPOnly – Script cannot access cookies
- Logout button on all pages when logged in. Terminate session.
- AUTOCOMPLETE set to off on sensitive fields/forms
  - <INPUT NAME="name" AUTOCOMPLETE=OFF>

Session Management - Good Practices II

- http meta refresh for browser timeouts
  - <meta http-equiv="refresh" content="300;url=timeoutpage " />
- Caching parameters to prevent sensitive data from being left on browser
  - Pragma: no-cache
  - Cache-Control: no-cache
  - Expires: -1

Session Management - Good Practices III

- New Headers
  - Supported only on new browsers - maybe
  - Secure Transport Security (STS)
    - Prevent Man In The Middle (MITM)
    - Forces use of SSL – Introduced by Paypal
    - Google Chrome or Firefox NoScript
    - Info: en.wikipedia.org/wiki/Strict_Transport_Security
  - X-Frame-Options: DENY or SAMEORIGIN
    - Prevents Framing
    - Aimed at clickjacking type attacks
    - IE8, Safari, Chrome, Firefox, with the NoScript addon

Agenda

- General Information Security
- Some OWASP Projects
- State of Application Security
- Data Protection Legislation – What It Says
- Security LifeCycle (Requirements etc.)
- Session Management Good Practices
- **User Lifecycle Good Practices**

User Life Cycle – Identification

- Some applications (e.g. banking) may require formal identification for anti money laundering purposes
  - Proof of identity (e.g. passport)
  - Proof of address (e.g. utility bills)

User Life Cycle – Registration Step I

- Based on password authentication.
  - Secure enough for your application? Depends on classification.
- User enters email address
  - Check if email address already entered
- Send link to user's email address
  - Link should be time-limited (e.g. 24 hours)
  - Risk of automated scripted attacks
- User clicks link and goes back to registration page
- Enters password (and confirm password)
  - Enforce appropriate complexity
- Utility companies sometimes send some credential with normal mail (e.g. statement)

User Life Cycle – Registration Step II

- Prepare for forgotten password mechanism
- User chooses secret questions:
  - www.goodsecurityquestions.com
  - User must choose something like 3 from 10
  - Could also use something which is specific to the application (e.g. utility account number)
- Disable link that was emailed, so it cannot be reused.

User Life Cycle – Registration Step III

- User logs on and completes profile depending on application requirements.

- Password Principles:
  - Passwords should never be in cleartext
  - Salted and hashed when stored
  - Transmitted over SSL/TLS
  - DO NOT email passwords

User Life Cycle – Logon

- User enters username/email address and password
- If successful then continue and display timestamp for previous successful logon
- To help prevent brute-force automated attacks, allow a login attempt every 2 to 3 seconds. User will not notice delay
- After a few unsuccessful logon attempts (e.g.5), disable account for a few minutes (e.g 5).

User Life Cycle – Forgotten Password I

- Remember that forgotten password is an alternate logon mechanism (ask Sarah Palin)
- Email link to user – time limited (24 hours?)
- User clicks link and goes back to website
- Display secret questions.
- If user enters answers correctly, then goto password entry page.
  - User must enter password and confirm password as normal.
  - Disable email link so can't be reused

User Life Cycle – Forgotten Password II

- Allow a limited number of forgotten password attempts
- Then force user to restart complete mechanism

- When user goes through forgotten password mechanism, then delete any sensitive info held in profile (e.g payment info)

User Life Cycle – Logoff / Account Deletion

- Logoff
  - Delete Session
  - Good Session Management Practices
- Account Deletion
  - Depends on legislation, privacy
  - Have ability to delete accounts completely (including backups etc)

Password Paper

“The password thicket:technical and market failures in human authentication on the web”

Joseph Bonneau and Sören Preibusch

“We report the results of the first large-scale empirical analysis of password implementations deployed on the Internet”

The End

- Questions?
- Email me:
  - alexis@rits.ie