SecureWorks

Architecting Security In

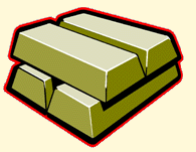
Jon R. Ramsey
Chief Technology Officer
404 486 4417
jramsey@secureworks.com

Security Objectives

- Confidentiality
  - is the need to ensure that information is disclosed only to those who are authorized to view it.
- Integrity
  - the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete
- Availability
  - the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it

http://**www.sans.org/resources/glossary.php**

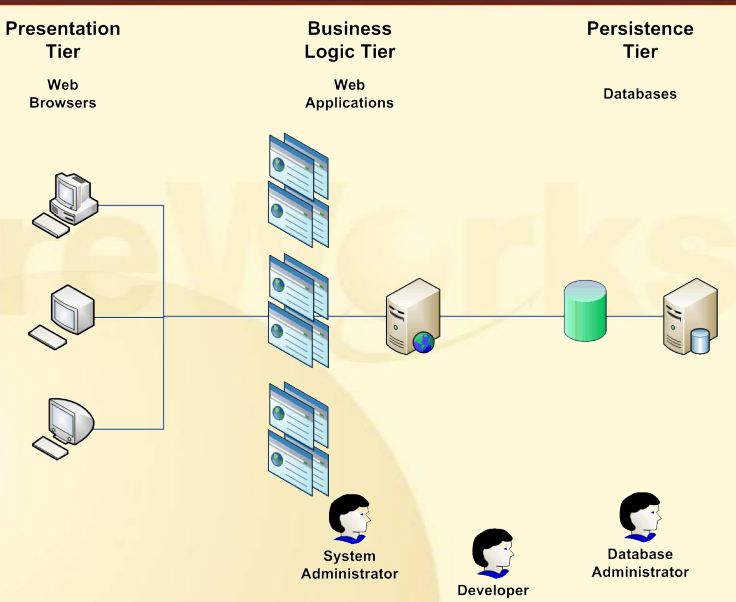
Gold Standard



- **Au**thorization (what)
  - Permission to take some action
- **Au**thentication (who)
  - To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
- **Au**dit (who did what when)
  - The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

http://www.sans.org/resources/glossary.php

Traditional Web Architecture



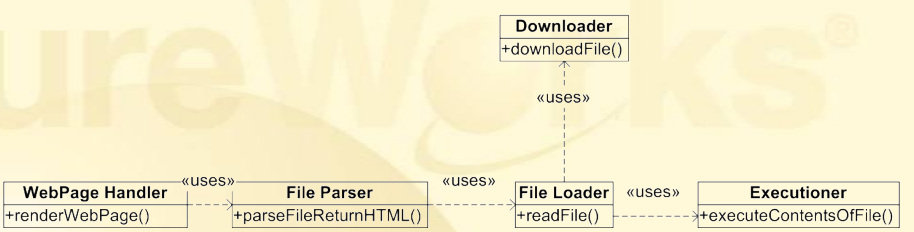
Vulnerabilities in Web Applications – OWASP top 10

- **A1 – Cross Site Scripting (XSS)**
- **A2 – Injection Flaws**
- **A3 – Malicious File Execution**
- A4 – Insecure Direct Object Reference
- **A5 – Cross Site Request Forgery (CSRF)**
- **A6 – Information Leakage and Improper Error Handling**
- **A7 – Broken Authentication and Session Management**
- A8 – Insecure Cryptographic Storage
- **A9 – Insecure Communications**
- **A10 – Failure to Restrict URL Access**

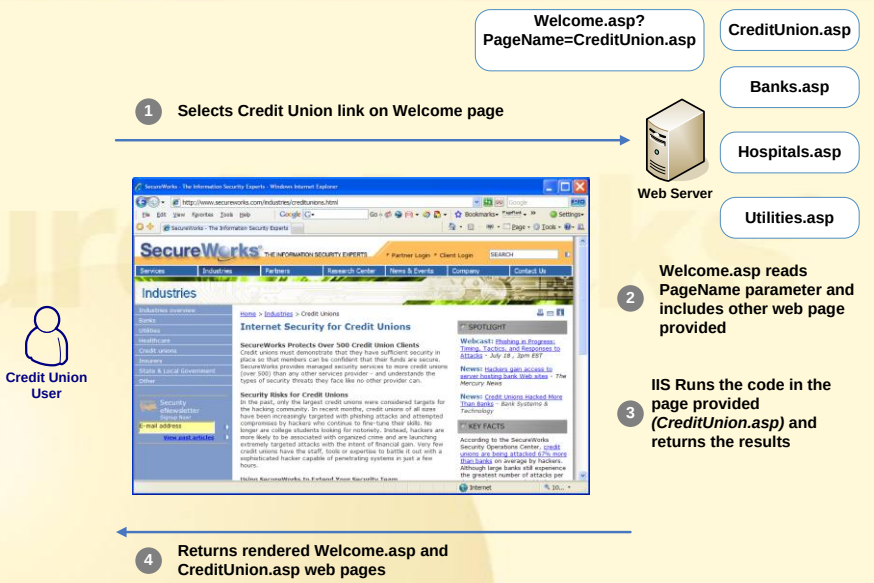
http://www.owasp.org/

File Inclusion Requirement and Design

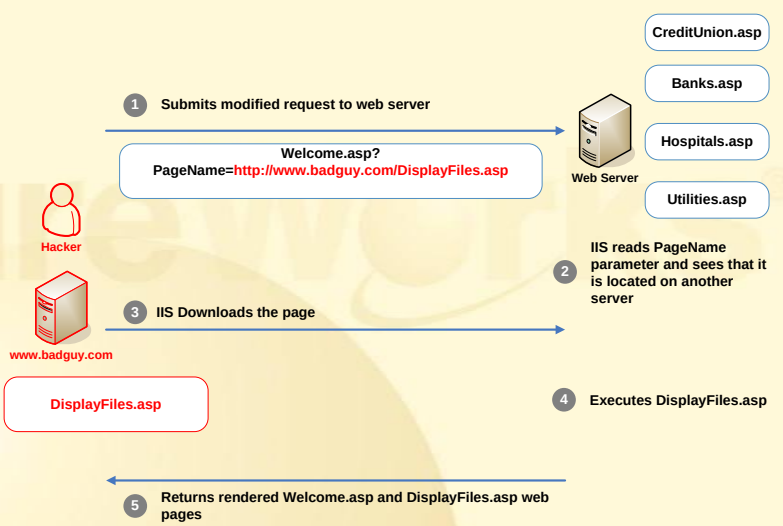
- The server shall be able to include other files located on other servers for execution

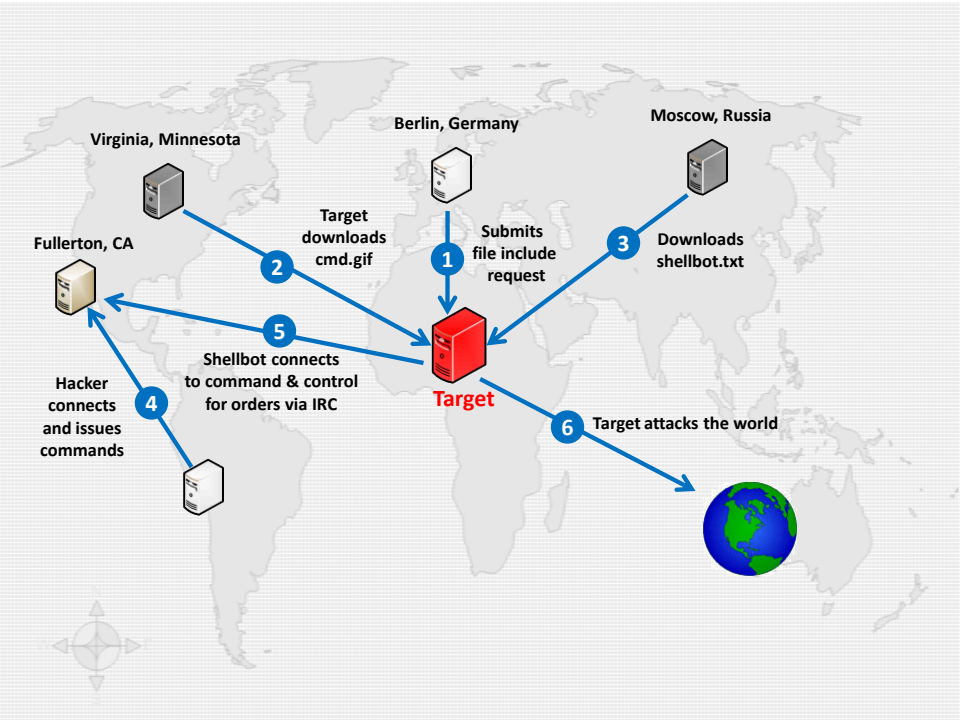


Web Application : File Inclusion - Normal



File Inclusion - Malicious



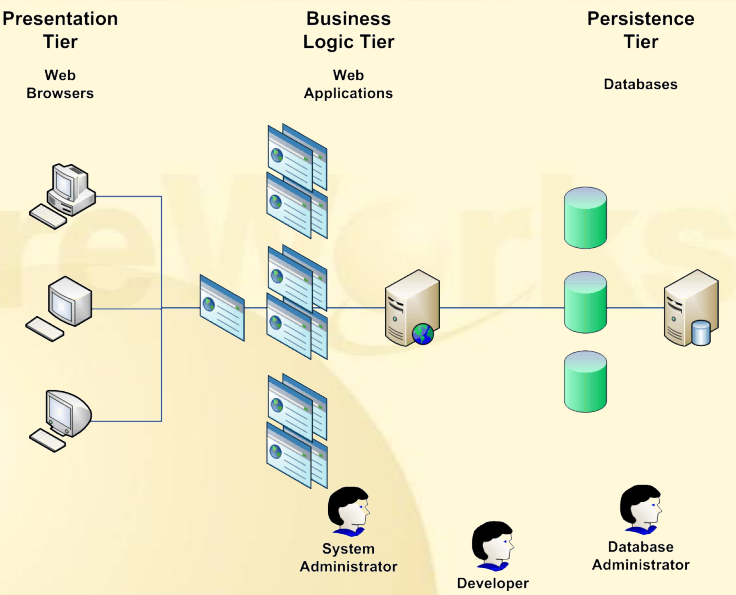


Security Engineering

- Actions should be verifiable
- Always give the least privilege
- Defense in depth
- Audit the system
- Build to contain intrusions
- Fix the weakest link

- http://software.newsforge.com/software/05/11/14/2115222.shtml?tid=78

Secure Architecture



Role of the Security Architect

- Analyze and manage risks to the system's assets
- Define components whose function is essential to security trusted base
- Define design techniques such as layering, strong type languages, least privilege, normalization of attack surface,…
- Document elements of attack surface.
- Protect developers & administrators from themselves ☺
- Keep it simple (complexity is the enemy of security)
- Document and minimize the attack footprint

A Few Ways to Analyze Software Architecture

- Look for the gold standard
  - when where and how is authorization, authentication and auditing accomplished
- Find security design patterns where they are and where they are not
  - Proxy, Factory, Singleton, …
- Find the trust relationships between physical and logical components and validate controls in place
- Model complex systems from varying points of view
  - Confidential data flow and domains
  - Model identities per component in system
- Use formal methods for models (UMLSec, ATAM, …)

Resources

- Security Engineering, A Guide to Building Dependable Distributed Systems (Ross Anderson, Wiley)
- Microsoft Security Development Lifecycle
  - http://msdn2.microsoft.com/en-us/library/ms995349.aspx
- DHS – Security in the Software Lifecycle
  - http://www.stsc.hill.af.mil/Crosstalk/2006/09/0609JarzombekGoertzel.html
- DHS – Building Security In
  - https://buildsecurityin.us-cert.gov/daisy/bsi/547.html

SecureWorks

www.secureworks.com

www.secureworks.com/research

info@secureworks.com

jramsey@secureworks.com

+001 404 – 486 – 4417

