STI · INNSBRUCK

Web Engineering
Web Application Security Issues

Dec 14 2009

Katharina Siorpaes

What is Web Application Security?

STI · INNSBRUCK

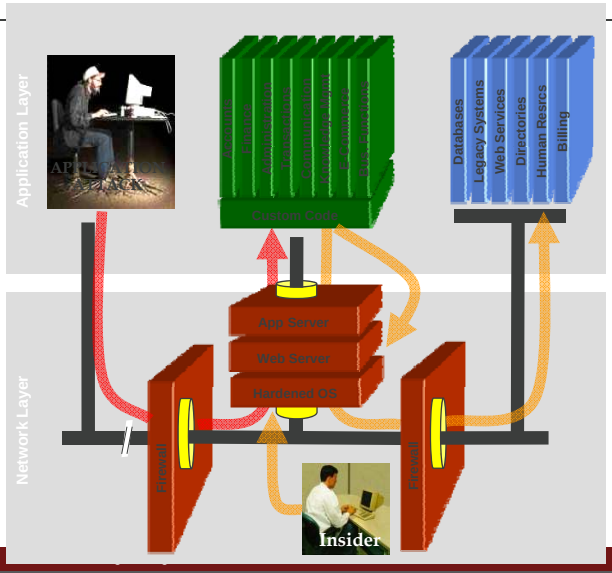
It is NOT Network Security

It is securing:

- "Custom Code" that drives a web application
- Libraries
- Backend Systems
- Web and Application servers

Problem Illustration

STI · INNSBRUCK

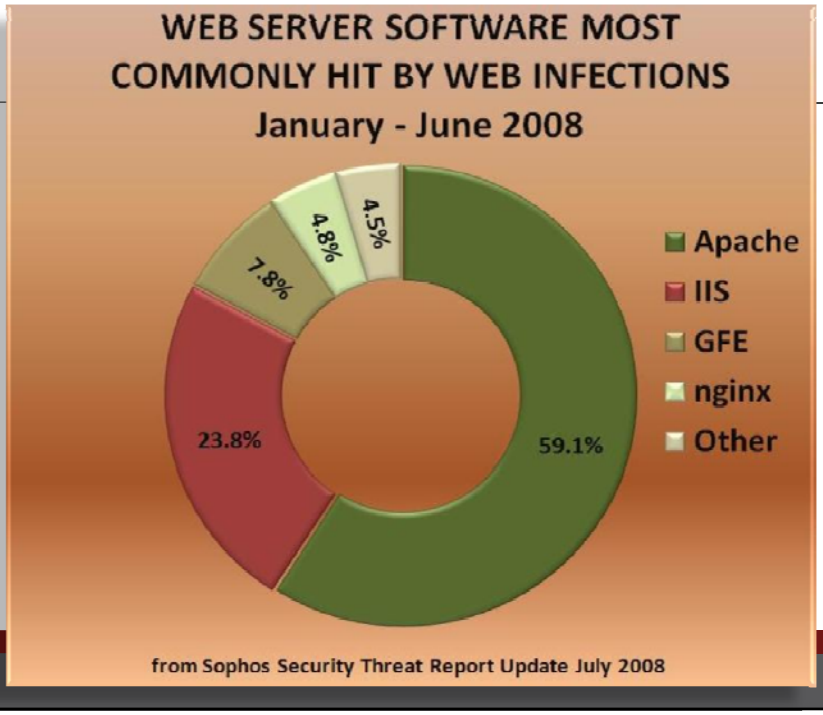


Application Layer

- Attacker sends attacks inside valid HTTP requests
- Your custom code is tricked into doing something it should not
- Security requires software development expertise, not signatures

Network Layer

- Firewall, hardening, patching, IDS, and SSL cannot detect or stop attacks inside HTTP requests.
- Security relies on signature databases



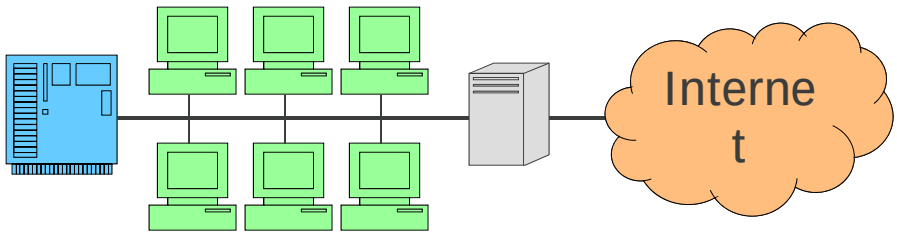
Need for Securing Web Sites / Applications

STI · INNSBRUCK

- Defaced Sites Reported on the Internet
- Defacement reasons
  - Application Vulnerability
  - Site owner authored (accidental/intentional)
  - Web Server Misconfiguration

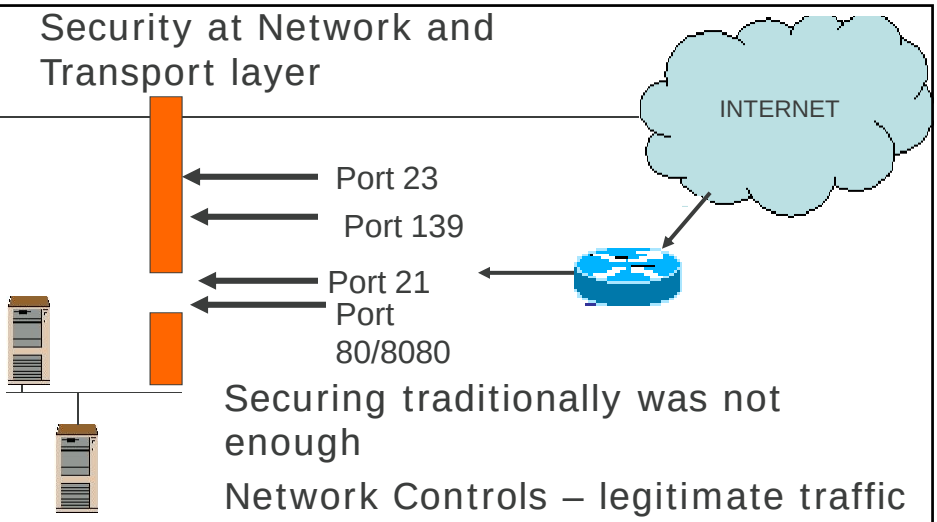
STI · INNSBRUCK

Corporate Security



Server (Data) | **Workstations (Green Segment)** | **Firewall !!!!!!!!!!!** | **Wild Wild West**

Security at Network and Transport layer



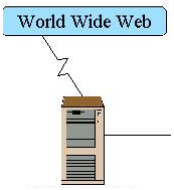
Securing traditionally was not enough

Network Controls – legitimate traffic

Above 70% attacks at the application level

STI - INNSBRUCK

Web Application



- A web application is generally comprised of a collection of scripts , that reside on a web server and interact with a database and other sources of dynamic content.
- Runs generally at port 80/8080

Attacks Undetected

- Data as part of legitimate traffic on port 80/8080 go undetected.
- Conventional Network devices and Firewalls cannot distinguish bad data from the genuine data

Web Application Security

STI - INNSBRUCK

- Refers to the combination of People, Processes and Technology
- Identify, Measure and Manage the risks
- Presented by Open source and custom web applications

Risks identified in applications

STI - INNSBRUCK

- A malicious user can log in without a valid account.
- An unauthorised user view, add, update, delete data.
- An authenticated user can Add/Update data as another user.
- A malicious user can upload malicious contents.
- A malicious user can steal user credentials.

People Processes Technology

STI - INNSBRUCK

•Awareness	•Training	•Guidelines
•Secure Development	•Secure code Review	•Security Testing
•Secure Configuration	•Application Firewalls	•Automated Scanners

Web Application Security Standards

STI - INNSBRUCK

- OWASP (Open Web Application Security Project)
- WASC (Web Application Security Consortium)

OWASP

STI · INNSBRUCK

The Open Web Application Security Project is a project dedicated to sharing knowledge and developing open source software that promotes understanding of web application security.

For more info see http://www.owasp.org

✓ OWASP Top 10

WASC

STI · INNSBRUCK

Is an international group of experts, practitioners and organizational representatives who produce open source and widely agreed upon best practice security standards for the world wide web.

http://www.webappsec.org

✓Web Hacking Incidents Database

✓Web Security Threat classification

OWASP Top Ten Project

STI - INNSBRUCK

- ✓ It Provides a minimum standard for web application security.
- ✓ The OWASP top ten represents a broad consensus about what the most critical web applications vulnerabilities are.
- ✓ Adopter
  - ✓ US Federal Trade commission, US DOD , VISA
  - ✓ Other companies including Sprint, IBM etc..

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI - INNSBRUCK

- ✓ A1 - Unvalidated Input
  Information from Web requests is not validated before being used by a Web application. Attackers can use these flaws to attack backend components through a Web application.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A2 -Broken Access Control
  Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A3 - Broken Authentication and Session Management
  Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A4 - Cross Site Scripting (XSS) Flaws
  The Web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A5 - Buffer Overflow
  Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and Web application server components.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A6 - Injection Flaws
  Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- A7 - Improper Error Handling
  Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI - INNSBRUCK

- ✓ A8 - Insecure Storage
  Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI - INNSBRUCK

- ✓ A9 - Denial of Service
  Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

OWASP Top Ten Most Critical Web Application Vulnerabilities

STI · INNSBRUCK

- ✓ A10 - Insecure Configuration Management
  Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

The Developer's Role in Application Security

STI · INNSBRUCK

Developers must:

- Work with solution architects and systems administrators to ensure application security
- Contribute to security by:
  - Adopting good application security development practices
  - Knowing where security vulnerabilities occur and how to avoid them
  - Using secure programming techniques

Holistic Approach to Security

STI · INNSBRUCK

Security must be considered at:

- All stages of a project
  - Design
  - Development
  - Deployment
- All layers
  - Network
  - Host
  - Application

“Security is only as good as the weakest link”

Resources

STI · INNSBRUCK

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

http://confluence.ltc.arizona.edu/confluence/display/WEBPRACTICES/Web+Application+Best+Practices

http://www.webappsec.org/

http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=84B3AA98-A1E5-4A74-A56B-7ADDBDED79CC&displaylang=en

http://security.arizona.edu/appdev

Questions?

STI · INNSBRUCK