Open Security Assessment of Enterprise Solutions

Case Study on Enterprise E-mail (in)Security Solutions
OWASP Security Baseline

Marian Ventuneac
Security Analyst, PhD
Genworth Financial

OWASP
10.6.2011

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

Background

- Security Researcher

  http://www.ventuneac.net

  http://secureappdev.blogspot.com

- OWASP Ireland Dublin
- OWASP Ireland Limerick Chapter

  https://www.owasp.org/index.php/Ireland-Limerick

- Security & Software Engineer, PhD, MEng
  - Data Communication Security Laboratory, University of Limerick
  - Distributed Systems, Technical University of Cluj-Napoca

Agenda

- Enterprise E-mail Security Solutions (anti-spam & anti-virus)
  - Software
  - Hardware/Software Integrated Appliances
  - Virtual Appliances
  - Security-as-a-Service (SaaS)
- A Simple Threat Model
- Risks of Enterprise E-mail (in)Security
- Testing E-mail (in)Security - Case Studies
- OWASP Security Baseline Project (Alpha)

Do We Need E-mail Security Solutions?

- State of spam
  - April 2010, 89.22% of all messages
  - April 2011, 74.81% of all messages
    (source: State of Spam & Phishing, May 2011, Symantec)
- Enterprise E-mail anti-spam and anti-virus solutions
  - Protect against malware, viruses and phishing, e-mail harvesting or denial of service attacks
  - Spam and viruses filtering rate between 95% and 99.x%
  - Ensures business continuity
  - Central to any enterprise's security infrastructure
- Free and commercial webmail offerings often employ enterprise anti-spam and anti-virus solutions

Enterprise E-mail Security Solutions

Overview

- Virtually all security vendors offer e-mail security solutions
- Software
  - Usually built for specific network infrastructures and servers
  - Require pre-configured operating systems
  - Come with a lengthy list of hardware and software requirements
  - Significant effort is required to integrate and configure it
- Hardware/Software Integrated Appliances
  - More robust, providing increased performance and scalability
  - Require less configuration during integration
  - Employ hardened operating systems and pre-configured security software
  - Control-locked by the vendors

Enterprise E-mail Security Solutions

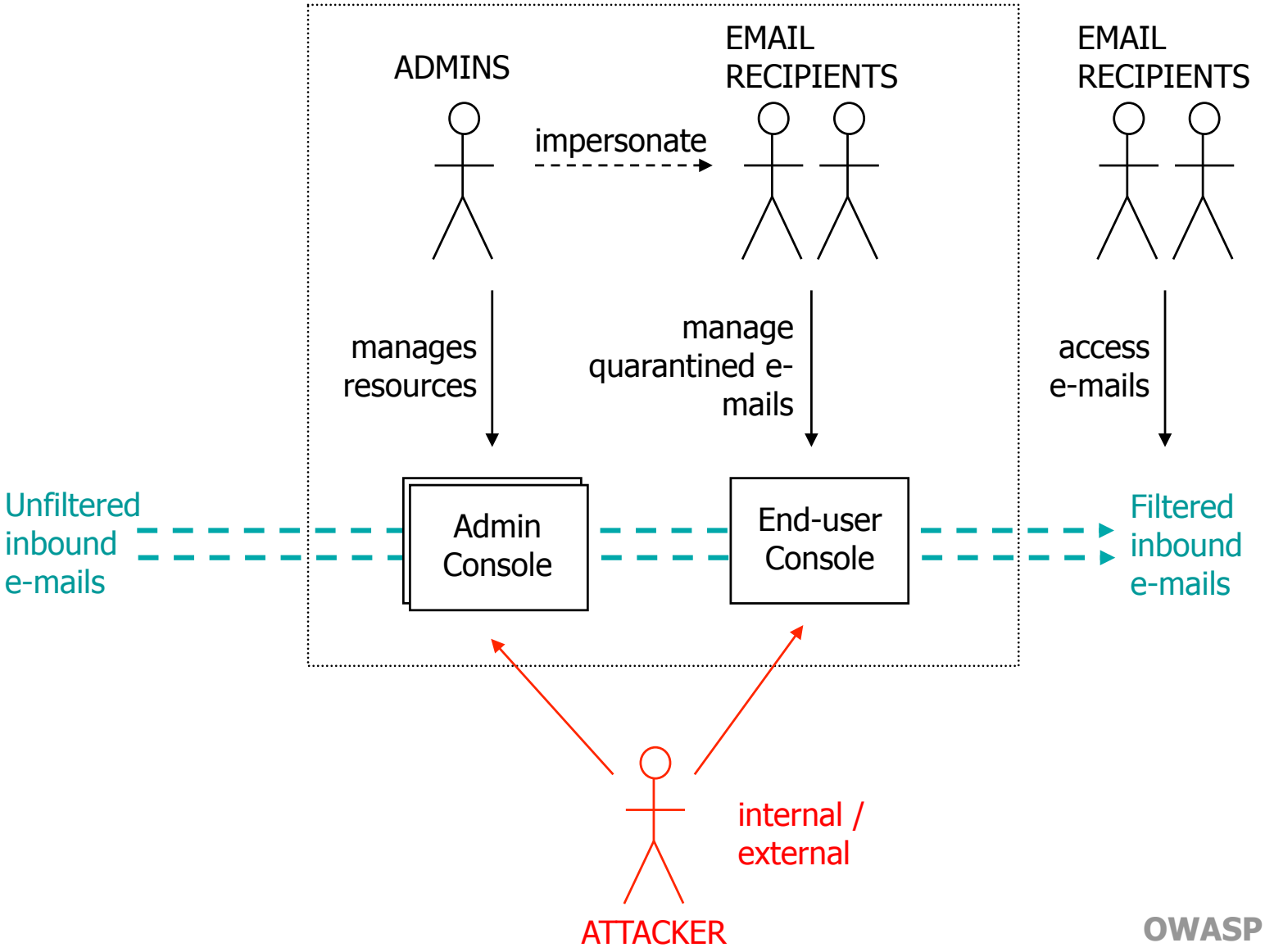
Overview (cont.)

- Virtual Appliances
  - Bundle virtual machines with hardened operating systems and pre-configured security software
  - Require minimal dependency on the hardware, minimal configuration and provide increased service availability
  - Cost-effective alternatives to software and hardware/software solutions
  - Control-locked by the vendors
- Cloud-based Services
  - Private (corporate) clouds
  - Infrastructure-as-a-Service (IaaS) - public clouds
  - Software-as-a-Service (SaaS) - public clouds
    - Requires no hardware or software installation
    - Minimises the administrative costs

Deployment of E-mail Security Solutions

- On-premises solutions usually deployed in the DMZ
- SaaS - public cloud; IaaS - private/public cloud
- No IDS/IPS/WAF deployed to protect such solutions specifically
- Web-based management consoles provided for
  - remote administration of solution's resources (local users, quarantine filters, etc)
  - end-user quarantine management
- Intranet/Internet accessible
- … what could possibly go wrong?

A Simple Threat Model



Risks of E-mail (in)Security Solutions

- Compromise the security of server/appliance
- Bypassing the vendor security controls used to lockdown the appliance
- Gaining and maintaining unauthorised access to appliance/ service administrative settings
- Compromising the service availability

- What about…

Risks of E-mail (in)Security Solutions (cont.)

- **Stealth control of users e-mails**

User A is a Admin AND

User A has access to appliance/service settings, including quarantine filters AND

Attacker B (internal/external) hijacks user A's account

Attacker B can control e-mails for valid users C..Z by falsely classifying it as spam AND

Attacker B can preview/read & release/delete e-mails falsely classified as spam

Risks of E-mail (in)Security Solutions (cont.)

- **Stealth control of users e-mails**

User A is a end-user AND
Attacker B gains access to e-mail filtering settings for user A AND
Attacker B sets tampers the spam filtering settings for user BAND
Spam e-mails are available for preview/full review for user

Attacker A can preview/read & release/delete clean e-mails falsely classified as spam

Risks of E-mail (in)Security Solutions (cont.)

- No timely discovery and mitigation of such attacks
- Vulnerable code is shared between various security solutions
  - attackers can compromise an entire family of products (from software to VA and SaaS solutions)
- Vulnerable IaaS and SaaS solutions could be used to devise attacks against
  - any enterprise (all) using the service
  - the service provider itself

Testing E-mail (in)Security

Case Studies

- Marshal MailMarshal SMTP 2006 (current M86 Security)
- Barracuda Networks - Spam Firewall hardware appliance
- Symantec - Brightmail Security Gateway virtual appliance
- Astaro Security Gateway virtual appliance
- IBM Proventia Mail Security System virtual appliance
- Barracuda Networks - Email Security Service SaaS
- Google Message Security (Postini) SaaS
- …

Marshal - MailMarshal SMTP 2006

MVSA-08-001/CVE-2008-2831 - Multiple XSS

- Ingredients of a large-scale internal attack
  - non-admin user A injects malicious code into his/her SQM account
  - user A enables users B..Z to maintain his account (without previous consent)
  - unsuspecting users B..Z have all reasons to trust A, since is an employee of the same company
  - if users B..Z check A's account (why not?), they become victims of a successful XSS attack
- Attacker A gains control over the victims' SQM console, including what gets classified as spam
- Preview of quarantined e-mails available

Barracuda Networks - Spam Firewall appliance

MVSA-08-003/CVE-2008-1094 - SQL Injection
MVSA-08-002/CVE-2008-0971 - Multiple XSS

- Local admin user A injects malicious SQL code
  - extract information from internal database => information disclosure
  - run SQL heavy queries => DoS attack
- Exploitation of multiple XSS vulnerabilities could lead to Session Hijack
- Barracuda Spam Firewall built-in controls did not allow timely detection and mitigation of such attacks

Symantec Brightmail Gateway

MVSA-09-002/CVE-2009-0063 - Multiple XSS
MVSA-09-001/CVE-2009-0064 - Broken Access Control

- An authenticated underprivileged user could
  - Access to other users' details

```
url_placeholder/administrator/edit.do?userID=1
```

  - Compromise the appliance's network and monitoring settings

```
url_placeholder/setup/SiteSetupAppliance$exec.flo?flowId=0
```

  - Create Admin users
    => gain **full administrative control** of the appliance

- Symantec Brightmail Gateway built-in controls did not allow timely detection of such attacks

IBM Proventia Network Mail Security System

MVSA-10-007/CVE-2010-0152 - Multiple XSS
MVSA-10-006/CVE-2010-0153 - CSRF

- An un-authenticated attacker could
  - Persistently inject malicious scripting code
  - Hijack Admin accounts via malicious scripting code injected into resources accessible to Admin users

  => attacker A could gain **administrative control** of the appliance

IBM Proventia Network Mail Security System

MVSA-10-008/CVE-2010-0154 - Insecure Direct Obj Ref
MVSA-10-009/CVE-2010-0155 - CRLF Injection

- Authenticated user with local admin privileges could perform
  - Path Traversal and Local File Inclusion
  - OS Command execution
    - craft & upload a malicious PHP file onto the appliance
    - execute the malicious PHP file
  - Cookies Injection & External HTTP Redirect

- IBM PNMSS appliance built-in controls did not allow timely detection of such attacks

Astaro Security Gateway

MVSA-11-008/CVE-2009-0044 - SQL Injection
MVSA-11-009/CVE-2009-0045 - Multiple XSS

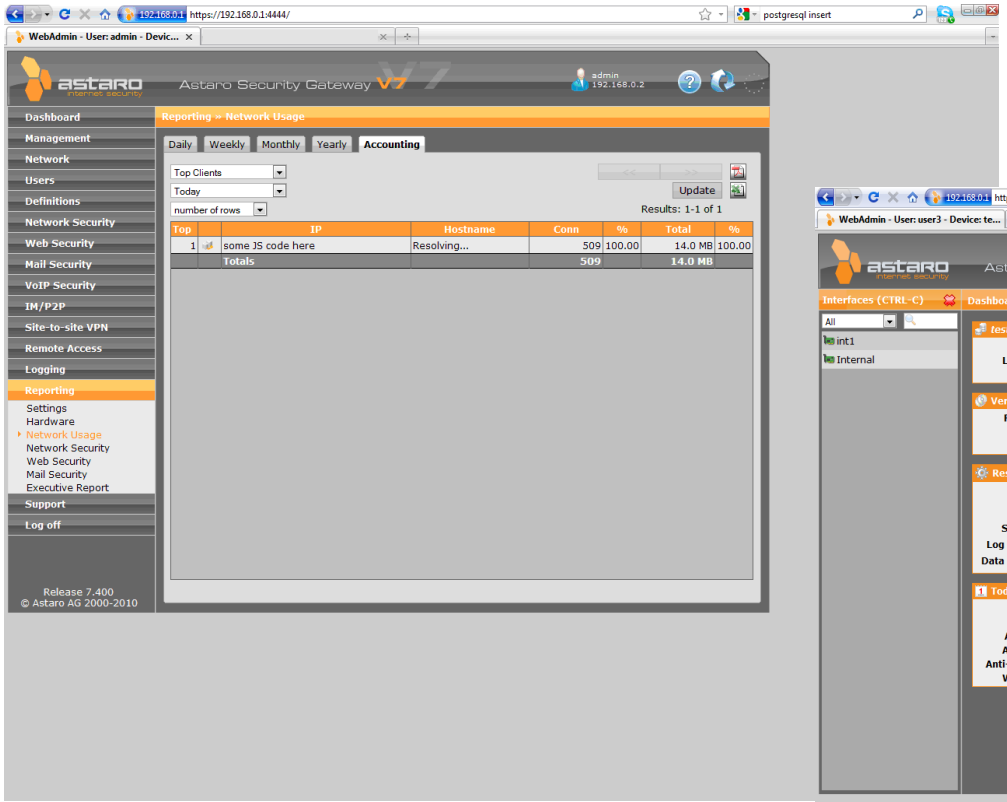
- Underprivileged users performing SQL Injection attacks
  - Information Disclosure
  - Data Alteration and Manipulation
  - Denial of Service
- Local admin user could target other admin users and regular underprivileged users by exploiting multiple XSS vulnerabilities

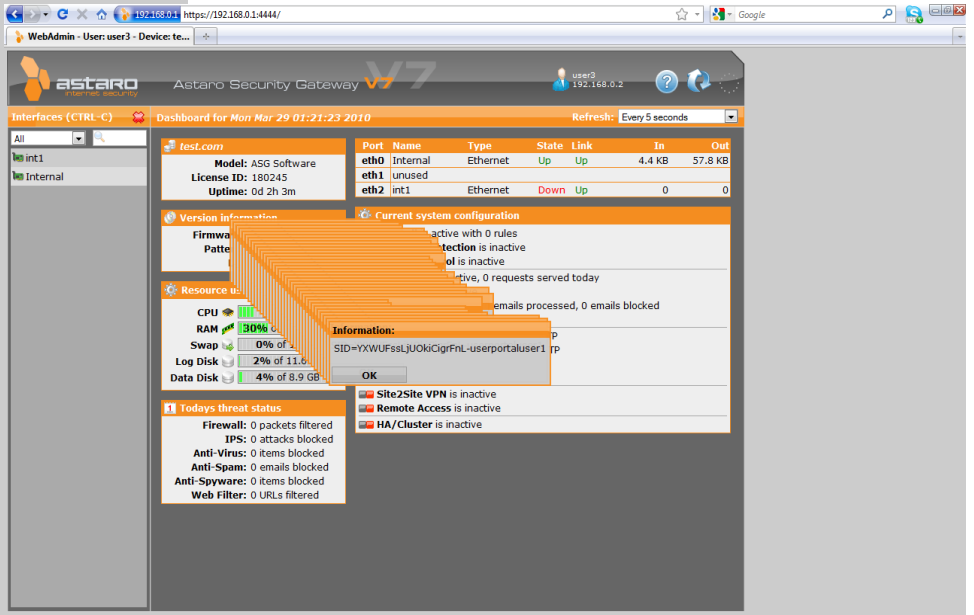
  => session hijack and alteration of account settings

- Astaro Security Gateway built-in controls did not allow timely detection of such attacks

Astaro Security Gateway

MVSA-11-008/CVE-2009-0044 - SQL Injection
MVSA-11-009/CVE-2009-0045 - Multiple XSS






```
CREATE TABLE VMRTMP01(t text);
INSERT INTO VMRTMP01 VALUES ('some JS code
here<script>alert(document.cookie);</script>');
SELECT t FROM VMRTMP01;
```

Barracuda Networks - Email Security Service SaaS

MVSA-10-011 - Admin Console Multiple XSS
MVSA-10-014 - Control Center Multiple XSS

- Email Security Service (Admin Console) - session hijack

  https://ess.barracudanetworks.com

  - Controlling users accounts and settings, users' e-mail quarantine settings
  - Access to filtered e-mails
  - Impersonate end-users & change password

    => hijack end-user account

- Control Center Console - session hijack

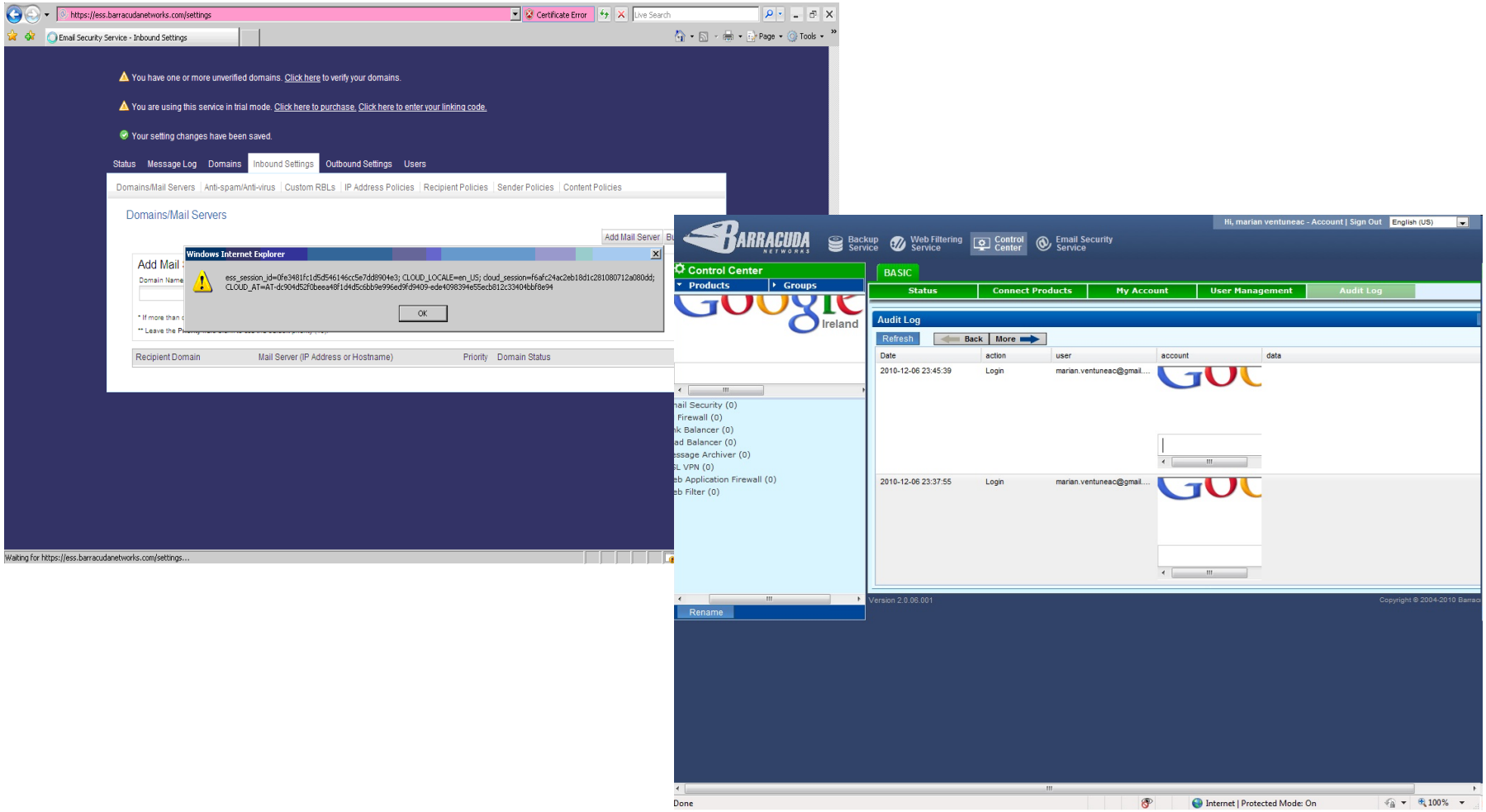
  https://bcc.barracudanetworks.com

  - Controlling settings of various Barracuda appliances, including Spam & Virus Firewall, Web Filter, Web Application Firewall, etc

Barracuda Networks - Email Security Service SaaS

MVSA-10-011 - Admin Console Multiple XSS

MVSA-10-014 - Control Center Multiple XSS



Google Message Security (Postini) SaaS

MVSA-10-001 - SQL Injection (Message Centre II)

- Underprivileged users performing SQL Injection attacks

parameter sort_direction of /junk_quarantine/process and /trash/process

  - Complete SQL error stack trace returned to the client (as HTML comment)
  - Disclosing database information could be valuable in devising database-specific attacks
  - Allowed extraction and manipulation of data from internal database

    => compromise data confidentiality and integrity
  - SQL heavy queries could be handy when the attack is scaled up

    => compromise data availability (DoS)

- Target existing Postini clients & **targeting Google**

Google Message Security - Postini

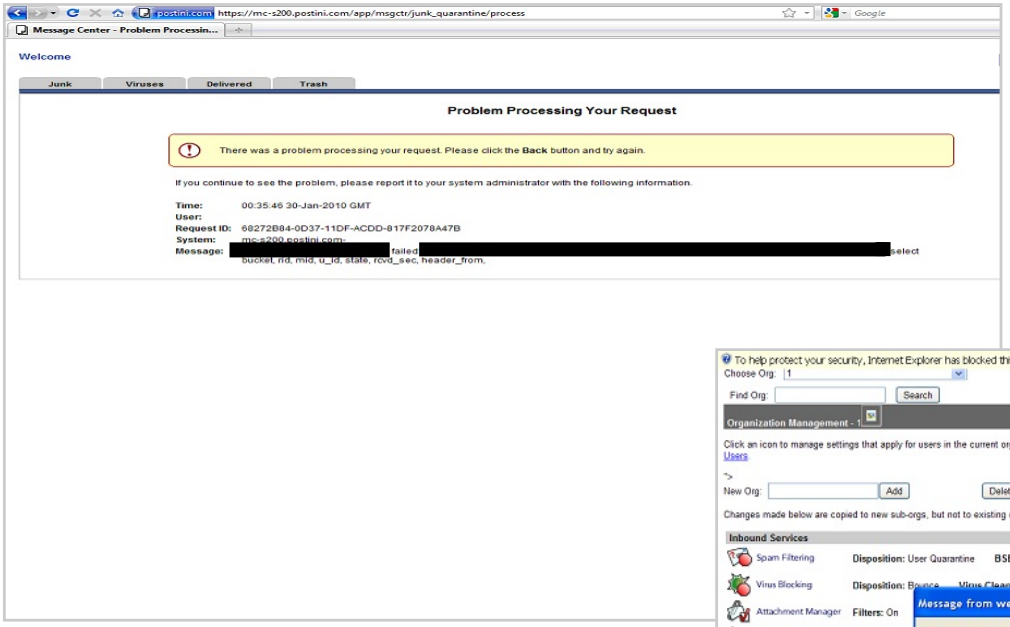
MVSA-10-002 – Multiple Persistent & Reflected XSS
MVSA-10-003 – Improper Error Handling

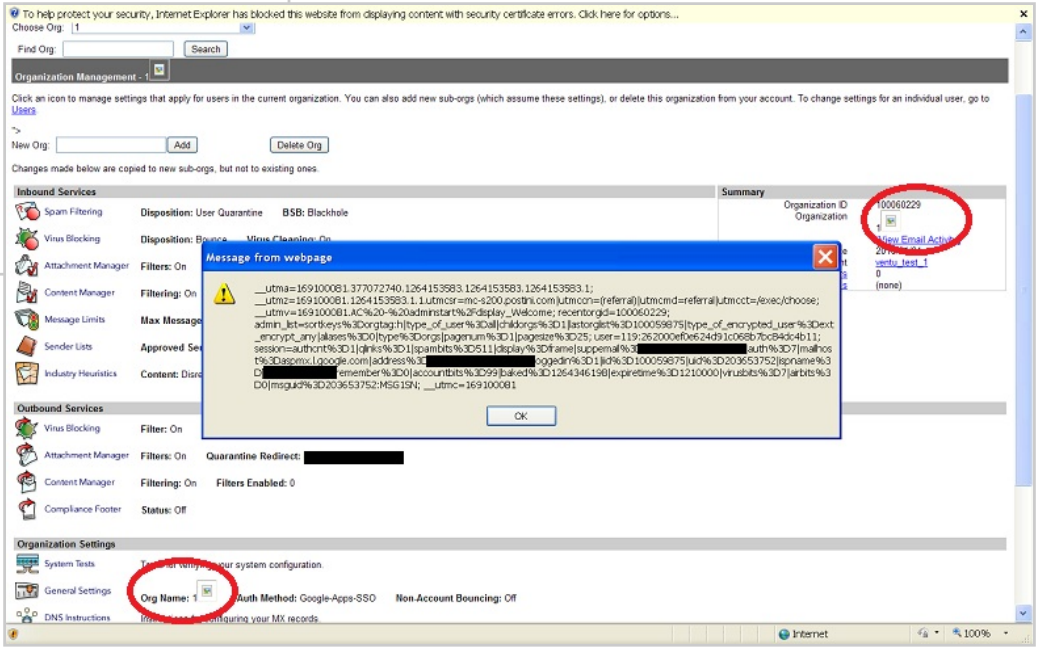
- Security Console
  - An authenticated admin user could exploit persistent XSS
    => target other admin accounts of the parent organizations
    => **target Google**
  - Session Hijack
- Message Centre Classic & Message Centre II
  - Session Hijack
- Security Console and Message Centre II - disclosure of
  - Technology used for services implementation
  - Internal paths for vulnerable resources
  - Database type & vendor & SQL error stack trace

Google Message Security (Postini) SaaS

MVSA-10-001 - SQL Injection (Message Centre II)

MVSA-10-002 - Multiple Persistent & Reflected XSS





Google Message Security - Postini

MVSA-11-010 - Insecure Direct Object Reference
MVSA-11-011 - Cross-Site Request Forgery (CSRF)

- Security Console - authenticated admin for organization A
  - Could enumerate **all Google Apps clients with a Postini subscription** by using various Batch Processing commands
- Exploitation of multiple CSRF vulnerabilities identified in Security Console and Message Centre II console
  - Unauthorized changes to Security Console and Message Centre II console settings (change e-mail filtering settings)
  - When combined with successful exploitation of identified XSS vulnerabilities

    => Session Hijack

    => Potential access to end-user e-mails maliciously re-labeled as spam

Security Testing of E-mail Security Solutions

A Brief Summary

- Exploitation of identified vulnerabilities
  - Often requires low/medium complexity attacks
  - Compromises the solution's security
  - **Could lead to exposure of confidential e-mails**
- Vulnerable code is shared between various security solutions (from software to VA and SaaS)
- Security virtual appliances can be used by attackers
  - to discover vulnerabilities in safe and controlled environments
  - to devise low-footprint attacks

Security Testing of E-mail Security Solutions

A Brief Summary (cont.)

- Security risks for the cloud (Cloud Security Alliance)
  - the misuse of cloud computing
  - the usage of insecure APIs and interfaces
- Vulnerabilities identified in SaaS services could be used to
  - **attack any enterprise using the service**
  - **attack the service provider**
- No controls for timely discovery and mitigation of successful exploitation of such vulnerabilities
- No security baseline for testing such solutions

OWASP Security Baseline (Alpha)

Project Description

- Benchmark security of enterprise products/services against OWASP Top 10 (and other) Security Risks
- Open and comprehensive security assessments of enterprise products/services
- Guidance/support for vendor-independent security verification of enterprise products/services

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

OWASP Security Baseline (Alpha)

Project Goals

- Establishing an OWASP community which actively identifies products/services and devise suitable security test plans
  - actively identify => use/work with/test/research it
- Benchmarking security of tested solutions using
  - OWASP security guidelines and material, tools, etc
  - Open-source testing tools
- Collaborating with various vendors on improving security of assessed frameworks/products/services
- Increasing awareness on available OWASP material and tools

OWASP Security Baseline (Alpha)

Project Roadmap - E-mail Security Solutions Case Study

- Alpha
  - devise testing methodology mapping to OWASP Top 10 Security Risks, including test plan, techniques, tools, etc
  - establish disclosure policy
- Beta
  - publish testing methodology
  - publish major case study
  - gather community support
- Stable
  - assess major products/services and publish the outcome
  - collaborate with vendors to improve security of assessed solutions
  - framework in pace for assessing other classes of products/services
  - coordinate and publish community-validated results

OWASP Security Baseline (Alpha)

Work in Progress

- Testing Methodology & Security Test Plans including
  - OWASP guidelines, cheat sheets, etc
  - manual and semi-automated techniques
  - open source and free tools (OWASP LiveCD, Backtrack, etc)
- Risk Analysis
- Disclosure Policy
- Security Advisories
- …

OWASP Security Baseline

How Can You Contribute?

- Anyone with an interest in improving application security
  - Security Engineers
  - Security Analysts
  - Penetration Testers
  - Security Researchers
  - Software Developers
  - …
- If you find an issue, don't stop! There is a very good chance there are more ☺☺☺
- Contribute to build a comprehensive benchmark of similar products/services

OWASP Security Baseline

Pending Release

- Benchmarking Enterprise Email Security Solutions
- Benchmarking Enterprise Social Networking Platforms
- …

Thank You

marian.ventuneac@owasp.org

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

https://www.owasp.org/index.php/Ireland-Limerick

http://secureappdev.blogspot.com

http://www.ventuneac.net