Security Bulletin Publication at AusCERT using “EzESB”

Robert Lowe and Matthew Braid

Computer Security Analysts

AusCERT – who are we

AusCERT
Australian Computer Emergency Response Team

- Australia's National CERT
- Funded primarily by member subscriptions
- Security bulletins
  - Redistribution of external security bulletins (ESBs), with permission
  - Advisories or updates, authored by AusCERT
  - A recent member survey rated this service as our most valued
    - 68% rated security bulletin publication as essential
    - 32% rated it useful
  - Filtering based on member profiles
  - SMS alerts of important bulletins
  - RSS feeds

The Problem

- Many sources of security bulletins – each with their own format
  - Original content retained, but wrapped in AusCERT's "meta-format" with consistent header fields
- Several bulletins to be redistributed on most days
  - 873 ESBs in 2003
  - 827 ESBs in 2004
- Repetitive, tedious task
- Staff rotation can result in inconsistencies across bulletins

Requirements

- Efficient
  - Bulletin redistribution should be quick and simple
- Standardised
  - Consistent use of summary fields
  - A well defined creation process (including peer review)
  - Automatically generate as much information as possible
- Auditable
  - Keep track of all previous bulletins with important compilation steps

Requirements (cont)

- Flexible
  - – Publish bulletins via email, SMS and website
  - – New or changed external bulletins and publication methods
- Stable and Storable
  - – Bulletins can be saved in state for later completion or to be passed on to another staff member
- Integrated
  - – Must work with our current internal tools

The Tool – EzESB 1.0

- Originally built in an ad-hoc manner to fast-track creation of header information and inclusion of standard footers – EzESB 1.0
- Did the job, but inflexible
  - Changes to procedure required code updates
- Ugly, and a big change for some staff
  - Move from command line editor to a GUI
  - Earned the title ‘HardESB’ from some

EzESB 2.0

- Value of EzESB was recognised and resourced as a development project
- GUI improvement – more intuitive and attractive
- PGP integration – signature checking and creation
- Use of configuration files – procedure updates did not require code updates
- Integration to AusCERT's web content management system
  - Automatic uploads
  - Content metadata adjustable within EzESB itself

EzESB 2.0 (cont)

- Tied into our email client exmh
- "Check Points" to save and restore work
- Fields could be automatically extracted from the original bulletin
  - Guesswork rules still hard coded
- Vast improvement, but some things were still too manual
  - Sending of email and update of website was two separate actions

EzESB 2.0 - Outpaced

- During 2003, internal tools underwent a major update
  - Previous flat-file database system replaced with RDBMS and integrated tracking tools – IMS
  - New extensible mailing list software built – IMSML (aka ‘Major Tom’)
- New services added
  - Early Warning SMS
  - Member Profile Email – bulletin filtering
- EzESB 2.0 no longer up to scratch

EzESB 3.0

- EzESB 3.0 merged into the new IMS
- Improved GUI
  - Large friendly buttons for common tasks
    - Menus rarely needed any more
  - Wizard-like sequential actions
- Improved flexibility
  - Guesswork rules moved to configuration files
  - Personal configuration files
  - Bulletin type (ESB, Alert, Advisory, Update) can be changed with a single mouse-click

EzESB 3.0 (cont)

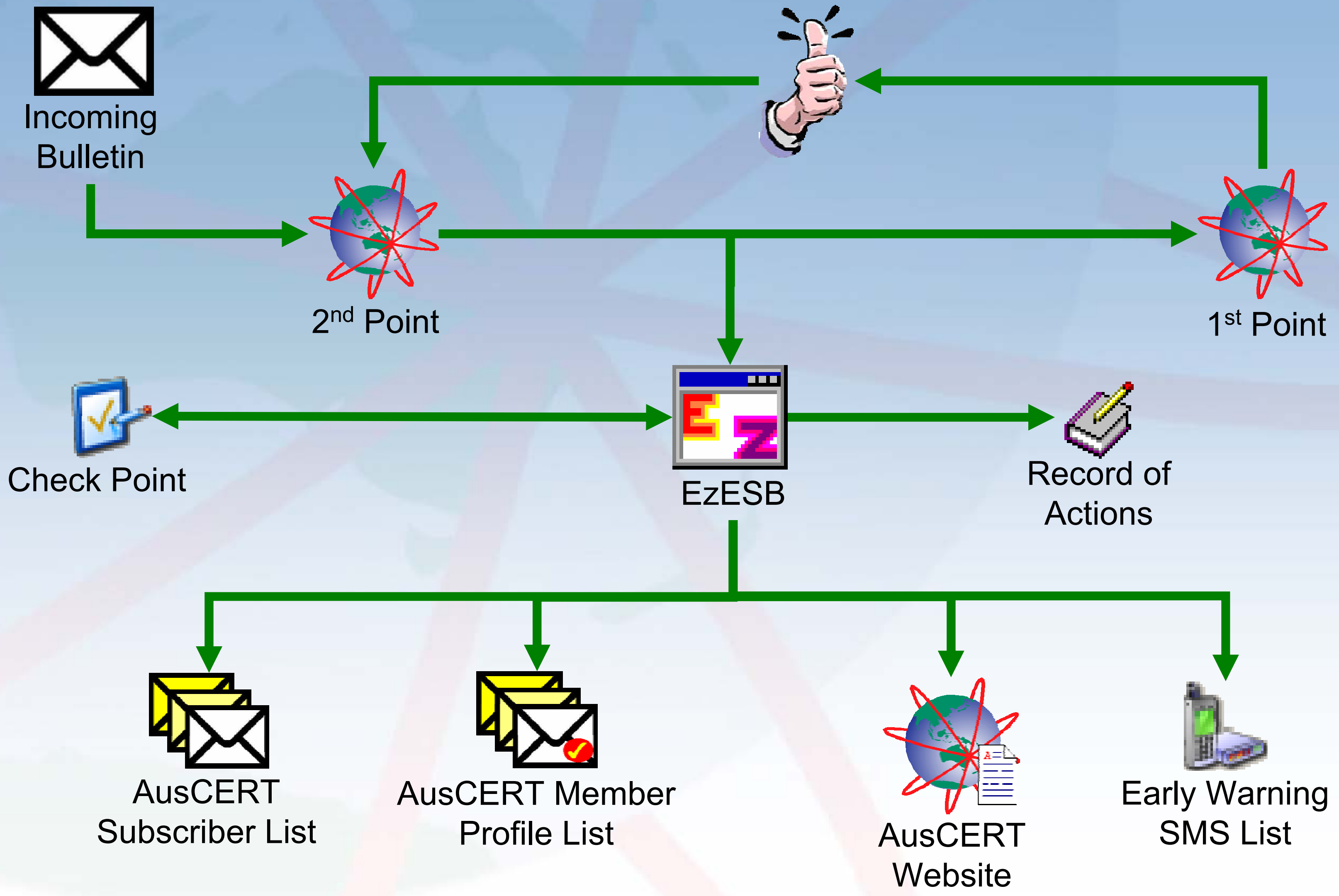
- Guesswork improved
  - WCMS metadata guessed
  - More fields guessed depending on bulletin type
- More common tasks automated or ‘buttonised’
  - Strip out email headers and non-PGP-signed content
  - Built-in spell checking
  - Common tasks grouped together
- Increase in the bulletin types supported. Including: Apple, CIAC, Cisco, Core, Debian, eEye, FreeBSD, HP, iDEFENSE, ISS, MacroMedia, Microsoft, NetBSD, Red Hat, Sun, SGI, UNIRAS, US-CERT

EzESB 3.0 (cont)

- Early Warning SMS and Member Profile Email integration
  - Combined with email as a single ‘Send’ action
- Email destinations modifiable
  - Can send to extra addresses or lists if desired
- Peer review email expanded
  - Includes data on WCMS and SMS settings
- Check Points rewritten to use IMS for storage
  - Integrated search functions

Work Flow

AusCERT
Australian Computer Emergency Response Team



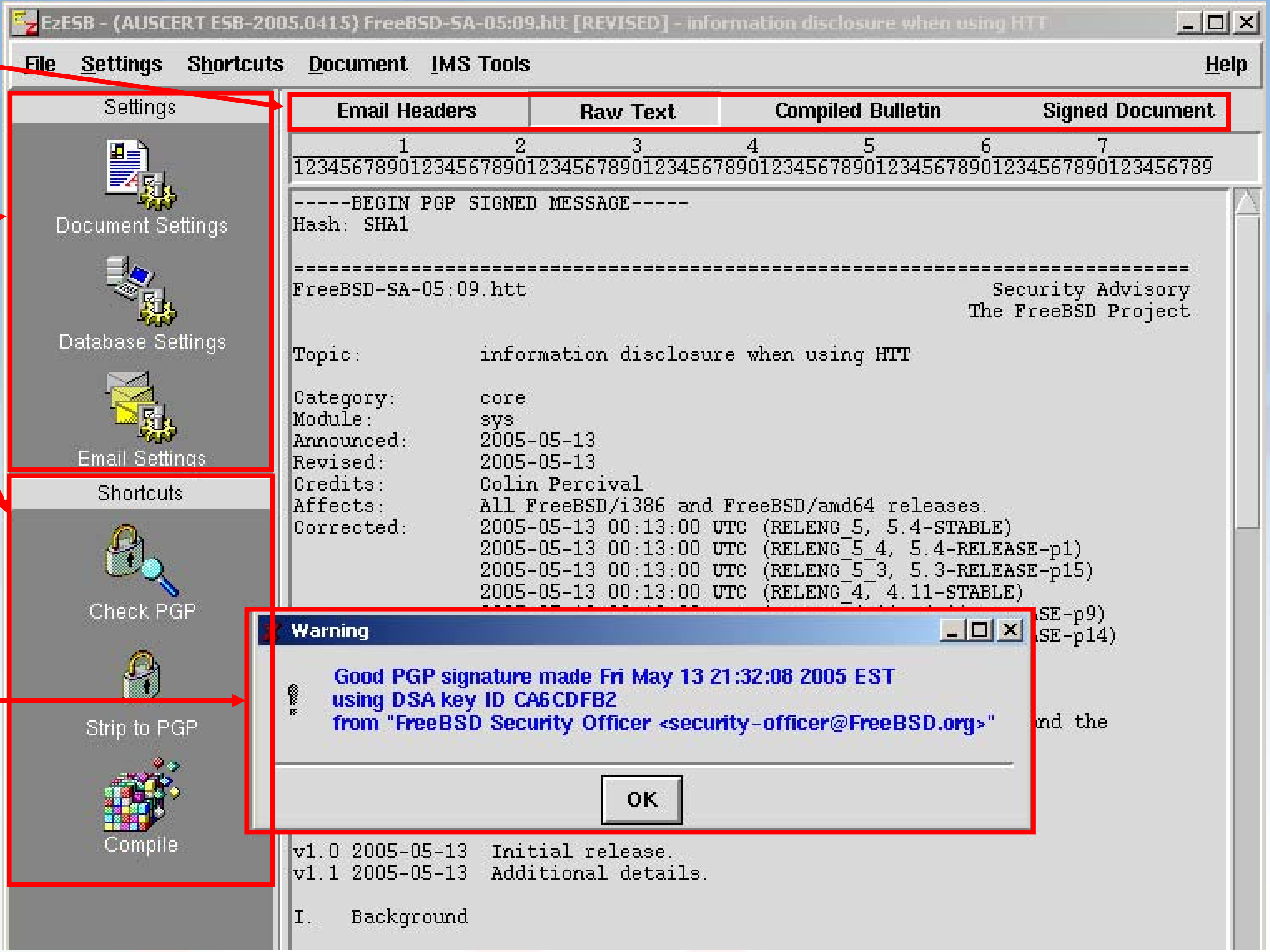
Screenshots

Bulletin Progression

Shortcuts to the Settings Dialogs

Stage-specific Shortcuts

This bulletin's PGP Signature is correct



```
         1         2         3         4         5         6         7
1234567890123456789012345678901234567890123456789012345678901234567890123456789
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=============================================================================
FreeBSD-SA-05:09.htt                                        Security Advisory
                                                          The FreeBSD Project

Topic:          information disclosure when using HTT

Category:       core
Module:         sys
Announced:      2005-05-13
Revised:        2005-05-13
Credits:        Colin Percival
Affects:        All FreeBSD/i386 and FreeBSD/amd64 releases.
Corrected:      2005-05-13 00:13:00 UTC (RELENG_5, 5.4-STABLE)
                2005-05-13 00:13:00 UTC (RELENG_5_4, 5.4-RELEASE-p1)
                2005-05-13 00:13:00 UTC (RELENG_5_3, 5.3-RELEASE-p15)
                2005-05-13 00:13:00 UTC (RELENG_4, 4.11-STABLE)
                                                            SE-p9)
                                                            SE-p14)

                                                              nd the

v1.0 2005-05-13   Initial release.
v1.1 2005-05-13   Additional details.

I.   Background
```

Good PGP signature made Fri May 13 21:32:08 2005 EST
using DSA key ID CA6CDFB2
from "FreeBSD Security Officer <security-officer@FreeBSD.org>"

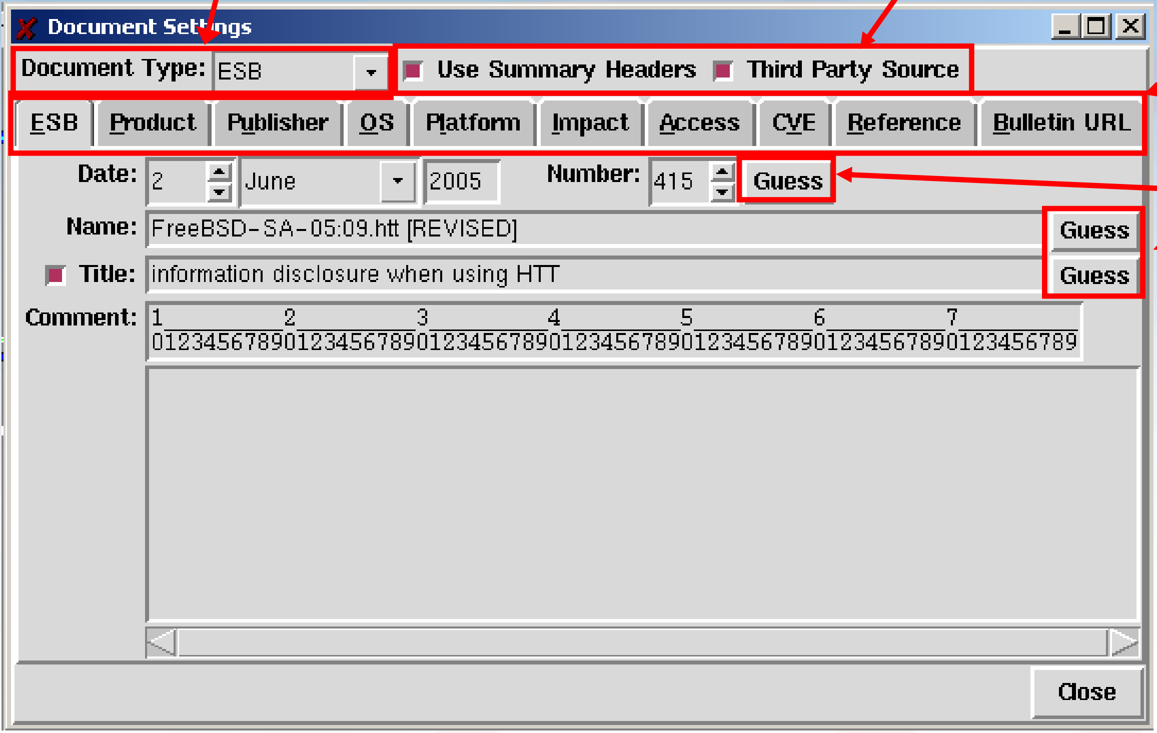
Screenshots

Change the document type if necessary

Changes header format and default footer

Set header field values

Revert to Guessed values



Document Type: ESB

☒ Use Summary Headers ☒ Third Party Source

Date: 2 June 2005 Number: 415 Guess

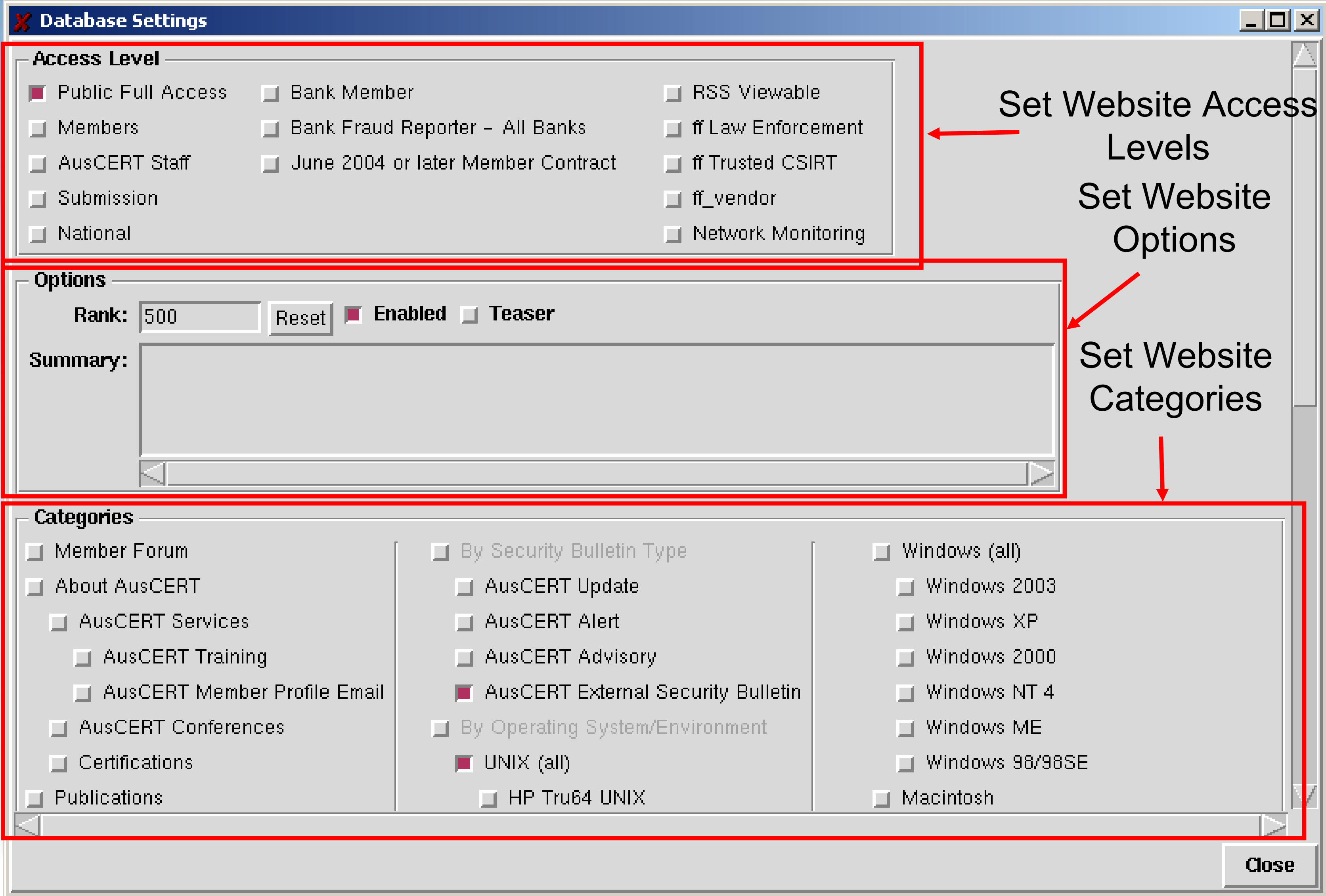
Name: FreeBSD-SA-05:09.htt [REVISED] Guess

☒ Title: information disclosure when using HTT Guess

Comment:

```
1         2         3         4         5         6         7
0123456789012345678901234567890123456789012345678901234567890123456789
```

Screenshots



Database Settings

Access Level

☒ Public Full Access
□ Members
□ AusCERT Staff
□ Submission
□ National

□ Bank Member
□ Bank Fraud Reporter – All Banks
□ June 2004 or later Member Contract

□ RSS Viewable
□ ff Law Enforcement
□ ff Trusted CSIRT
□ ff_vendor
□ Network Monitoring

Options

Rank: 500 Reset ☒ Enabled □ Teaser

Summary:

Categories

□ Member Forum
□ About AusCERT
  □ AusCERT Services
    □ AusCERT Training
    □ AusCERT Member Profile Email
  □ AusCERT Conferences
  □ Certifications
□ Publications

□ By Security Bulletin Type
  □ AusCERT Update
  □ AusCERT Alert
  □ AusCERT Advisory
  ☒ AusCERT External Security Bulletin
□ By Operating System/Environment
  ☒ UNIX (all)
    □ HP Tru64 UNIX

□ Windows (all)
  □ Windows 2003
  □ Windows XP
  □ Windows 2000
  □ Windows NT 4
  □ Windows ME
  □ Windows 98/98SE
□ Macintosh

Set Website Access Levels

Set Website Options

Set Website Categories

Possible Future Enhancements

- The ability to deduce more information from a wider variety of external security bulletins
- Integration with AusCERT’s mailing list application, enabling targeted bulletins to specific (possibly encrypted) mailing lists
- A better process for the handling of updates and revisions of bulletins
- A structured revision history of bulletins
- Migration of all AusCERT public communications to EzESB
- Templating for AusCERT authored publications (advisories and updates)
- Automatically “timing out” member advisories to be publicly viewable after a predefined period

Questions and live demo

Questions and live demonstration

(time and technology permitting)