[redacted]

Application Security Assessment Report

[redacted] Online Magazine

Version 0.2 - 20 October 2010

COMMERCIAL-IN-CONFIDENCE

Table of contents

1 Executive Summary

1.1 Overview

[redacted] has recently commenced publishing an online edition of the [redacted] using the Realview platform. As part a due diligence exercise [redacted] was engaged to conduct an application security assessment of the newly adopted system.

Testing comprised of an application security assessment to gauge the security of the platform from the perspective of an anonymous attacker, and to identify issues which could result in reputational damage to [redacted]

The review was conducted without credentials, externally over the internet, on the 10th October 2010. Retesting was subsequently performed on the 16 October 2010 after some remediation activities were completed.

1.2 Key findings

Overall, the security posture of the application was found to be below industry best practice.

The key findings of the assessment include:

- The application was found to suffer from reflected cross-site scripting. As a result an attacker could craft and distribute links to the site, which when followed, cause the victim user to view a defaced version of the site. The defacement could cause the site to request advisor credentials and transmit them to the attacker, or display content which is offensive or misleading.
- The application displays detailed error messages to users, disclosing system information which may assist an attacker in crafting an attack.
- During initial testing the application was found to suffer from SQL injection, which could have permitted an attacker to modify backend data stores directly. However this issue was later resolved and verified to longer be exploitable.

The following chart and table provide an indication of the risks and vulnerabilities identified:

Review component	Extreme	High	Moderate	Low
[redacted]	0	0	1	1
Total	**0**	**0**	**1**	**1**

1.2.1 Risk exposure

[redacted] considers the [redacted] application (Realview platform) to pose a **LOW** risk to [redacted] This rating acknowledges the small risk posed by cross-site scripting vulnerabilities on a [redacted] branded website.

2 Schedule of recommendations

The following schedule incorporates all risks and recommendations identified in this deliverable as a result of test cases carried out. Ratings are in line with AS 4360. Further detail on the risk rating can be found in Appendix C - Risk rating scheme. The numbering scheme references the full recommendation, as provided within the report.

Domain references are as follows: [redacted] application (hosted by Realview) [**FTO**].

Consequence ratings are as follows: Very Low [**VLO**]; Low [**LOW**]; Medium [**MED**]; High [**HIGH**]; Very High [**VHI**].

Consequence ratings are as follows: Insignificant [**INS**]; Minor [**MIN**]; Moderate [**MOD**]; Major [**MAJ**]; Catastrophic [**CAT**].

Risk Ratings are as follows: Extreme [**EXT**], High [**HIGH**], Moderate [**MOD**]; Low [**LOW**].

Ref.	Issue / risk	Like.	Cons.	Risk	Recommendation	Status
FTO-03 (p.16)	The application suffers from cross-site scripting. By coercing users into visiting a malicious link or website, an attacker could hijack user sessions, and cause victims to view a defaced .version of the website	RARE	LOW	**LOW**	Apply HTML entity encoding or URL encoding to all untrusted data (preferably all data values) before rendering within application output.	**Open**
FTO-01 (p.13)	The application was found to display detailed error messages, which disclose system which may assist an attacker in crafting an attack.	RARE	VLOW	**LOW**	Implement generic error messages throughout the application.	**Open**

Table 1: Schedule of recommendations

3 Review approach

[redacted] conducted an application penetration test of the following systems using a structured verification approach.

3.1 Tested environments & timing

The URLs provided for the application security assessment are shown below:

- [redacted] (hosted by Realview)
  [redacted]
  (210.87.32.80)

Testing was conducted on the following dates:

- 10 October 2010
- 18 October 2010 (Retesting)

3.2 Test cases

Application penetration testing comprised of application familiarisation followed by in-depth assessment using the following test cases as a starting point for response and behaviour analysis:

- **TCA-01 - Information gathering**
  Information gathering is the most fundamental step in application security testing. It allows the tester to become familiar with the application and to identify all the components, entry points and thus potential attack vectors. Subsequently, the tester is able to prioritise testing effort based on the highest risk areas of the system.

- **TCA-02 - Information disclosure**
  A common vulnerability in web applications is the accidental disclosure of sensitive information either directly or implicitly through application behaviour. This includes both confidential information, such as user data or company secrets, and internal application details which may aid an attacker in identifying vulnerabilities including application debug output, source code, application API versions, directory structure and network layout.

- **TCA-03 - Authentication and authorisation**
  If authentication is not conducted robustly, an attacker may be able to access application functionality without identifying themselves to the system or may be able to supply a fraudulent identity when performing application actions. It may also be possible for an attacker to masquerade as a legitimate user – accessing private information or executing

actions on behalf of the victim. The failure of authorisation and access controls may allow an attacker to view data or perform actions which they are not entitled to access.

- **TCA-04 - Session management**
  It is common for applications to track an individual's navigation through the use of stored session information, especially when authentication is involved. Session management is closely linked to authentication, as sessions are typically used to prevent the need for a user to provide authentication credentials for every request. This means an attacker who successfully hijacks a valid user session or otherwise subverts session functionality, can access the web application as if they were the session's rightful owner.

- **TCA-05 - Data validation**
  Appropriate data validation within an application allows it to detect and handle incorrect, malformed or unexpected inputs before passing such data to subsystems for processing or execution. Insufficient or inappropriate data validation within an application may allow an attacker to supply unauthorised or malicious commands or parameters to subsystems which may affect the results of processing or cause unauthorised actions to be performed. Data validation issues may occur directly or may arise indirectly through second-order injection attacks where previously stored values are used without validation.

- **TCA-06 - Use of cryptography**
  Failing to secure application data or communications may result in information disclosure or data compromise. Cryptography often provides a means of securing an application and its data however it is notoriously complex to design, implement, and configure securely. Issues with cryptography often result in the compromise of data held within the system as protections are usually applied to important components.

- **TCA-07 - Business logic**
  An individual application contains workflows and implements business rules and policies specific to that application. Business logic can be susceptible to flaws which allow for actions outside these workflows and business rules to be performed. Such issues impact applications in ways specific to their individual context. Certain functionality, by its very nature, may also pose a risk and weak implementations may provide a vector for system or data compromise.

- **TCA-08 - Denial of service**
  Denial of service attacks seek to disrupt the business function being provided an application. There are many forms of denial of service attacks however all target ability of an application to achieve its intended goal are therefore analysed in terms of the applications context.

- **TCA-09 - Auditing and logging**
  Logs are a fundamental component of the intrusion detection process and often form

much of the audit trail. In many applications all non-repudiation is provided by logs. Testing of log mechanisms seeks to verify that the data stored can be tampered with, disguised, or otherwise manipulated. Furthermore, it seeks to ensure that logs store a complete and thorough record of events.

The [redacted] application security test case to OWASP Top Ten mapping is provided below.

OWASP Vulnerability	[redacted] Test Case								
	TCA-01 Information Gathering	TCA-02 Information Disclosure	TCA-03 Authentication and Authorisation	TCA-04 Session Management	TCA-05 Data Validation	TCA-06 Use of Cryptography	TCA-07 Business Logic	TCA-08 Denial of Service	TCA-09 Auditing and Logging
A1. Injection					✓				
A2.Cross-Site Scripting (XSS)					✓				
A3. Broken Authentication & Session Management			✓						
A4. Insecure Direct Object Reference		✓	✓						
A5. Cross Site Request Forgery (CSRF)				✓					
A6. Security Misconfiguration		✓							
A7. Insecure Cryptograhic Storage			✓			✓			
A8. Failure to Restrict URL Access			✓						
A9. Insufficient Transport Layer Protection						✓			
A10. Unvalidated Redirects and Forwards			✓						

Table 2: OWASP Top Ten test case mapping

3.3 Best practice framework

The applications and infrastructure were reviewed in accordance with generally accepted security best practice principles (Confidentiality, Integrity, Availability, Authentication, Accountability, Least Privilege and Defence-in-Depth) and recognised industry standards. These standards include, but are not limited to:

- OWASP Guide to Building Secure Web Applications and Web Services
- OWASP Top Ten Most Critical Web Application Security Risks
- Web Application Security Consortium Threat Classification

3.4 Assumptions and limitations

Penetration tests are designed to identify security deficiencies and evaluate the effectiveness of safeguards by mimicking the actions of real-life attackers, using the same processes and tools a genuine attacker would use to infiltrate information systems.

The approach to testing application security is distinct from functional, technical, or user acceptance testing. For the latter a test scenario has an expected response, and when that response is received the test can be deemed a success, security testing requires that a different method be used. Specifically, functional testing is based on use cases that are known and well defined, however security testing requires "misuse cases", the entire set of which cannot be defined as a system can potentially be misused in an infinite number of unpredictable ways.

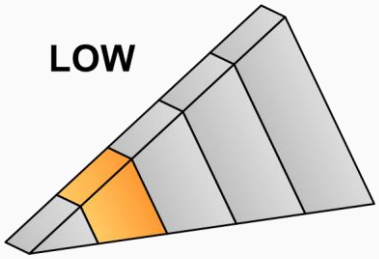
The nature of such testing, and the agreed project scope, presented the following limitations:

- The assessment scope was limited by the available time allocated to the assessment. [redacted] prioritised tests based on our experience, and likely vulnerable areas in the systems. The tests sought to identify systemic issues as opposed to provide a complete list of weaknesses for resolution. Where point-issues are identified, it is possible (and in some cases likely) that additional such issues exist in the application. The proposed 'recommendations' are to be applied throughout the application unless otherwise noted.
- This assessment was a penetration test simulating a malicious attacker; and as such did not include a source code review in parallel with testing. Certain types of vulnerabilities that are more readily identifiable from source code review, may not have been able to be identified through this assessment. If significant vulnerabilities were identified via testing, it is recommended that [redacted] conduct a thorough code review to ensure these issues are fully understood and mitigated.
- Internet, network and application security are continually growing and evolving fields, and vulnerability assessment by [redacted] does not mean that [redacted] systems are secure from every form of attack. Particularly, the assessment was completed on a specific configuration of the target system, as specified in this report, and at a specific point in time. Future development and system changes may introduce new vulnerabilities not currently identified; and advancement in attack techniques may introduce additional avenues for compromise that are not currently known.

In addition to these general limitations, the following specific assumptions and limitations were encountered during testing:

- Testing was performed against a production environment. At [redacted] request destructive and invasive tests were not performed.
- As testing was commissioned by [redacted] risk ratings and attack scenarios have been provided from a [redacted] perspective. This report does not consider the risk posed to the third party vendor Realview.

4 Application assessment

Test description	Business risk exposure
The [redacted] hosted at the following location: • [redacted] (210.87.32.80)	

4.1 Summary

The application provides an online version of the [redacted] A small number of security issues were identified during testing, one of which has since been resolved.

4.1.1 Test case findings summary

The following table is a summary of the security posture of the application with reference to the [redacted] Test Cases. A green tick indicates no issues were found, while a red cross indicates at least one issue was identified.

Ref.	Test case	Result
TCA-01	Information gathering	✓
TCA-02	Information disclosure	✗
TCA-03	Authentication and authorisation	✓
TCA-04	Session management	✓
TCA-05	Data Validation	✗
TCA-06	Use of cryptography	✓
TCA-07	Business logic	✓
TCA-08	Denial of service	✓
TCA-09	Logging manipulation	✓

Figure 1: Test case results

4.1.2 OWASP Top Ten summary

The Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks serves as a security benchmark for typical applications. While developers of applications with stringent security requirements may wish to also address other areas, it is generally accepted within the security industry that most organisations should strive to protect against the OWASP Top Ten.

The following table is a summary of the security posture of the application with reference to the OWASP Top Ten. A green tick indicates no issues were found, while a red cross indicates at least one issue was identified.

Ref.	Risk	Result
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	✓
A7	Insecure Cryptographic Storage	✓
A8	Failure to Restrict URL Access	✓
A9	Insufficient Transport Layer Protection	✓
A10	Unvalidated Redirects and Forwards	✓

Figure 2: OWASP Top Ten results

4.1.3 TCA-01 Information gathering

Information gathering is the most fundamental step in application security testing. It allows the tester to become familiar with the application and to identify all the components, entry points and thus potential attack vectors. Subsequently, the tester is able to prioritise testing effort based on the highest risk areas of the system.

Server technology identification	Informational
The first step towards attacking any web application is determining which technologies it has been created with and is currently running on. The Realview application was found to comprise the following technologies:	

- Web server: Microsoft-IIS/6.0
- Application platform: ASP/ ASP.NET
- Application server: AspNet 2.0.50727
- Database server: Microsoft SQL Server

This is an informational item only and no risk is associated with this finding.

Shared hosting environment	Informational

The assessed application is hosted on a server which also hosts websites belonging to other organisations. These virtual servers were not examined during the assessment, however may increases the hosts overall attack surface. This may be of particular significance if the hosting is shared with an organisation which is frequently targeted by attacks or activism.

A list of the domains identified is contained in Appendix B - Technical appendix .

This is an informational item only and no risk is associated with this finding.

Directory and file enumeration	Informational

In some web applications and web servers there are sensitive and/or vulnerable files and directories which are not linked to from the main site, or for which the links are not displayed to users, these files are usually security sensitive, and as such automated scanning and crawling of the application was performed.

While no sensitive files were identified, the application was found to comprise the following primary components:

- /default.aspx
- /djvu/
- /global/
- /global/adserver/
- /global/content/
- /global/content/Captcha.ashx
- /global/content/getimage.aspx
- /global/content/GetPageLinks.aspx
- /global/css/
- /global/images/
- /global/javascript/
- /global/lib/
- /global/loadconfig.aspx
- /global/logging/
- /global/logging/log.aspx
- /global/search/

- /global/sound/
- /global/subscribe/
- /global/subscription/
- /global/survey/
- /global/survey/survey.asp
- /global/template/
- /global/v2/
- /ipad/
- /skins/realview/
- /skins/realview/rvweb/
- /test/

This is an informational item only and no risk is associated with this finding.

4.1.4 TCA-02 Information disclosure

A common vulnerability in web applications is the accidental disclosure of sensitive information either directly or implicitly through application behaviour. This includes both confidential information, such as user data or company secrets, and internal application details which may aid an attacker in identifying vulnerabilities including application debug output, source code, application API versions, directory structure and network layout.

FTO-01	Detailed error messages	Low Risk

Information disclosure through error messages is one of the most prevalent issues in modern web applications. While in the majority of cases they do not provide a direct means of compromise, they can offer a great source of information to a potential attacker through which further issues can be identified.

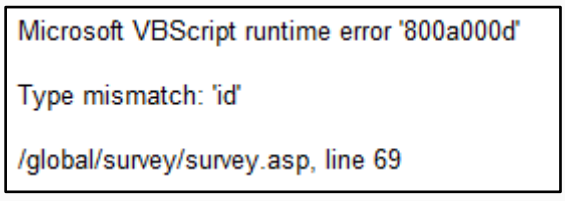
Retest findings

Parts of the application do not handle exceptions gracefully and disclose detailed information through error messages. The issue detail has been updated below to reflect the retest findings, as the behaviour of the URL previously provide has changed

Issue details

Whilst the majority of the site appears to handle exceptions without disclosing technical details to end users, the following page was found to disclose detailed error messages:

- [redacted]/global/survey/survey.asp?id=%3CA%3E (Shown below)



Classification

- [redacted] test item: M8 - Error Message Information Leak
- Attack: Fingerprinting

FTO-01	Detailed error messages	Low Risk

- Weakness: Information Leakage

Business impact / attack scenario

An attacker could abuse this issue to identify limited information about applications internals. Such information could assist in identifying additional security issues, or enable the attacker to craft exploits which target the application's underlying platform.

Risk rating

The likelihood of this issue being identified and exploited is RARE, as error messages are easily triggered but provide limited utility to attackers. The consequence of exploitation is VERY LOW as this is very minor information disclosure issue, which does not permit unauthorised access to the platform or data.

As a result, this is considered a **LOW** risk item.

Recommendation

Modify error handling functionality to display a generic error messages only.

This may involve catching exceptions raised by the service.

The best practice approach to implementing error handling is as follows:

- Log error message contents in a database or internal server file
- Display a generic error message stating only that an error has occurred.
- Provide the user a reference to the entry in the database or log file for later troubleshooting and support.
- Implement a global/default error handler to catch all unhandled exceptions.

4.1.5 TCA-03 Authentication and authorisation

If authentication is not conducted robustly, an attacker may be able to access application functionality without identifying themselves to the system or may be able to supply a fraudulent identity when performing application actions. It may also be possible for an attacker to masquerade as a legitimate user – accessing private information or executing actions on behalf of the victim. The failure of authorisation and access controls may allow an attacker to view data or perform actions which they are not entitled to access.

No issue relating to authentication and authorisation were identified during the assessment. Testing was conducted from an anonymous perspective.

4.1.6 TCA-04 Session management

It is common for applications to track an individual's navigation through the use of stored session information, especially when authentication is involved. Session management is closely linked to authentication, as sessions are typically used to prevent the need for a user to provide authentication credentials for every request. This means an attacker who successfully hijacks a valid user session or otherwise subverts session functionality, can access the web application as if they were the session's rightful owner.

No issue relating to authentication and authorisation were identified during the assessment. Testing was conducted from an anonymous perspective.

No issues relating to session management were identified during the assessment. The publicly facing components of the site did not appear to associate personal or sensitive information in sessions.

4.1.7 TCA-05 Data validation

Appropriate data validation within an application allows it to detect and handle incorrect, malformed or unexpected inputs before passing such data to subsystems for processing or execution. Insufficient or inappropriate data validation within an application may allow an attacker to supply unauthorised or malicious commands or parameters to subsystems which may affect the results of processing or cause unauthorised actions to be performed. Data validation issues may occur directly or may arise indirectly through second-order injection attacks where previously stored values are used without validation.

FTO-02	SQL Injection	Closed

Providing specific data to an application in areas where data is used directly in an SQL query can cause the SQL server to execute data passed to it directly as code. This can often allow an attacker complete access to the SQL database used by the application.

Retest findings

During retesting [redacted] was unable to exploit this issue, indicating that it has been successful remedied.

Original Issue details

The application was found to suffer from SQL injection,

- Page: http://[redacted]/global/search/searchContent.aspx
  Method: POST
  Parameter: orderby
  PoC: PublicationID=2232&IssueToSearch=39402&pagesize=500&SearchTerm=Insurance&OrderBy=(select case when (ascii(user) = 100) then issueid else pagename end)
  Notes: The above PoC was used to demonstrate that the database user name begins with the letter 'd' (ASCII code 100). Modification of the number 100 to any other value results in an error message.

Classification

- [redacted] test item: M3 - SQL Injection
- Attack: SQL Injection
- Weakness: Insufficient Input Handling

Business Impact / attack scenario

An attacker could exploit this issue to access the back-end databases directly circumventing all access control mechanisms implemented by the application. This issue may allow an attacker to deface the website.

Risk rating

The likelihood of this issue being identified and exploited is UNLIKLEY as the injection appears to be blind and occurs within an 'order by' clause, which may hinder attacks. The consequence of

FTO-02	SQL Injection	Closed

exploitation is considered MEDIUM. Whilst the server does not store sensitive [redacted] data, the issue could only be abused to perform web site defacement.

As a result, this item is considered to pose a **MODERATE** risk to [redacted]

Note: The risk to Realview has not been considered and may be considerably greater than that posed to [redacted]

FTO-03	Cross-site scripting	Low Risk

Cross-site scripting vulnerabilities in an application potentially allow an attacker to execute malicious script on other users' systems and hence compromise their sessions, authentication credentials, or even conduct other malicious activity. This can occur if HTML or script can be written to an application data store and be retrieved by other users, or if an attacker can coerce a victim into clicking on a malicious link.

Retest findings

The following instance was confirmed as fixed:

- Page: http://[redacted]
  Parameter: xml
  Method: GET
  Type: Reflected
  PoC: http://[redacted]?xml='%2balert(document.cookies)%2b'&iid=39402&startpage=4
  Notes: Shown below

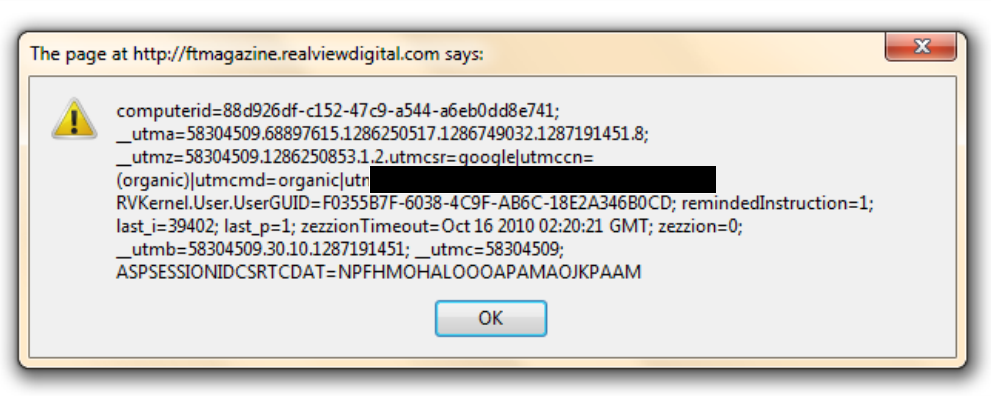
However the second instance of cross-site scripting had not been successfully addressed and the proof of concept has been updated below. Additionally [redacted] identified a further instance of cross-site scripting which was not detected during the initial assessment. The issue detail has been updated below.

Issue details

Two instances of cross-site scripting were identified within the application:

- Page : /global/print.asp
  Parameters: path, pages,p,i
  Type: Reflective
  Method: Get
  PoC:
  /global/print.asp?path=/djvu/[redacted]/Issue%202%27%3E%20%3Cscript%3Ealert%28document.cookie%29%3C/script%3E&pages=page0000005&type=single&pageset=width&p[redacted]&i=Issue%202&remote=false&remoteprefix=http://content.[redacted]&pagecount=44
- Page: http:/[redacted]/default.aspx
  PoC:
  http://[redacted]/default.aspx?iid=38980&startpage=./test/../../../web.config"style%3d"x:expression(document.write('Cross-site scripting'))"
  Parameter: startpage
  Notes: Only affects Internet Explorer with XSS filter disabled. Show below

FTO-03	Cross-site scripting	Low Risk



Classification

- [redacted] test item: M4 - Cross Site Scripting
- Attack: Cross-site scripting
- Weakness: Improper Output Handling

Business Impact / attack scenario

An attacker could exploit this issue by sending a legitimate user a maliciously crafted link, which when clicked, compromises the integrity of the victim's browsing session or causes the victim's browser to display a defaced version of the website.

Defaced pages could request advisor credentials and transmit them to the attacker, or display content which is defamatory, offensive of misleading.

Risk rating

The likelihood of this issue being identified and exploited is RARE as the victim must be coerced into viewing a malicious URL. The consequence of exploitation is LOW as the issue could result in brand damage to [redacted] and provides a vector for phishing attacks

As a result, this is considered a **LOW** risk item.

Recommendation

Apply output sanitisation to all untrusted data (preferably all data values) before rendering within application output. Specifically, encode HTML and JavaScript meta-characters including the following:

- & : Ampersand
- < : Left Angle Bracket
- : Right Angle Bracket
- / : Forward Slash
- ' : Single Quotation Mark
- " : Double Quotation Mark
- \ : Backslash
- ; : Semicolon

4.1.8 TCA-06 Use of cryptography

Failing to secure application data or communications may result in information disclosure or data compromise. Cryptography often provides a means of securing an application and its data however

it is notoriously complex to design, implement, and configure securely. Issues with cryptography often result in the compromise of data held within the system as protections are usually applied to important components.

No issues relating to the use of cryptography were identified during the assessment.

4.1.9 TCA-07 Business logic

An individual application contains workflows and implements business rules and policies specific to that application. Business logic can be susceptible to flaws which allow for actions outside these workflows and business rules to be performed. Such issues impact applications in ways specific to their individual context. Certain functionality, by its very nature, may also pose a risk and weak implementations may provide a vector for system or data compromise.

No issues relating to business logic were identified during the assessment.

4.1.10 TCA-08 Denial of service

Denial of service attacks seek to disrupt the business function being provided an application. There are many forms of denial of service attacks however all target ability of an application to achieve its intended goal are therefore analysed in terms of the applications context.

[redacted] did not identify any application functions which result in the consumption of excessive system resources. As a result, the application is not believed to be at a heightened risk of a denial of service attacks.

4.1.11 TCA-09 Auditing and logging

Logs are a fundamental component of the intrusion detection process and often form much of the audit trail. In many applications all non-repudiation is provided by logs. Testing of log mechanisms seeks to verify that the data stored can be tampered with, disguised, or otherwise manipulated. Furthermore, it seeks to ensure that logs store a complete and thorough record of events.

No issues were identified in the application's auditing and logging functionality. [redacted] was not provided with application logs during the assessment of this system.

Appendix A - Document management

Version	Date	Description
0.1	14-OCT-10	Internal review release
0.2	20-OCT-10	Client review release

Table 3 – Document history

Copyright notice:
This document contains information protected by copyright.
© [redacted]
The material in this document may not be commercialized without prior written permission from [redacted]

Appendix B - Technical appendix

Shared hosting details

Below is a list of the address which share the same hosting as the assessed application,

- http://mag.gpweek.com/
- http://www.realview.com.au/
- http://smhformguide.realviewtechnologies.com/
- http://hm.realviewusa.com/
- http://digitaledition.centralmag.com.au/
- http://digitaledition.wentworthcourier.com.au/
- http://voyeur.realviewtechnologies.com/
- http://archives.newyorker.com/?i=2009-05-25
- http://digitaledition.southerncourier.com.au/
- http://barossa.realviewtechnologies.com/
- http://digitaledition.manlydaily.com.au/
- http://obr.bankingreview.com.au/
- http://digitaledition.expressadvocate.com.au/
- http://digitaledition.southerntimes.com.au/
- http://scoop.realviewtechnologies.com/
- http://digital.boundmagazine.com/
- http://www.holidaysaway.net/
- http://dailytelegraphformguide.realviewtechnologies.com/
- http://heralddomain.realviewtechnologies.com/
- http://www.novaholisticjournal.com/
- http://straightfurrow.realviewtechnologies.com/?xml=Straight_Furrow
- http://www.asianwater.com.my/
- http://heraldsunformguide.realviewtechnologies.com/
- http://digitaledition.hornsbyadvocate.com.au/
- http://www.flexomag.com/
- http://digitaledition.blacktownadvocate.com.au/
- http://epaper.themalaysianreserve.com/
- http://theageformguide.realviewtechnologies.com/
- http://digitaledition-innercity.innerwestcourier.com.au/
- http://illawarradrive.realviewtechnologies.com/?xml=illawarra-drive.xml
- http://digitaledition.innerwestcourier.com.au/
- http://digitaledition.messengernews.com.au/
- http://qldbowler.realviewtechnologies.com/
- http://drivelife.realviewtechnologies.com/?xml=Drive_Life

Shared hosting details

- http://digitaledition.parramattaadvertiser.com.au/
- http://digitaledition.mosmandaily.com.au/
- http://digitaledition.northshoretimes.com.au/
- http://portnews.realviewtechnologies.com/
- http://drivefairfax.realviewtechnologies.com/?xml=The_Age_Drive&iid=38951
- http://digitaledition-wyong.expressadvocate.com.au/?xml=express_wyong.xml
- http://saltmagazine.realviewtechnologies.com/?xml=Salt_Magazine
- http://fusioncats.realviewtechnologies.com/
- http://digitaledition.fairfieldadvance.com.au/
- http://goodfoodguide.realviewtechnologies.com/?xml=Good_Food_Guide
- http://www.ajp.com.au/
- http://c-store.realviewtechnologies.com/
- http://digitaledition.mynorthside.com.au/
- http://www.agrimarketingdigital.com/
- http://drivefairfax.realviewtechnologies.com/?xml=The_Age_Drive&iid=37645
- http://illawarramercury.realviewtechnologies.com/
- http://digitaledition.guardianmessenger.com.au/
- http://digitaledition.theweekender.com.au/
- http://digitaledition.theexpress.com.au/
- http://digitaledition.penrithpress.com.au/
- http://digitaledition.hillsshiretimes.com.au/
- http://www.realviewusa.com/
- http://www.placemagazine.com.au/
- http://themercurycarsguide.realviewtechnologies.com/
- http://gartnerbrochure.realviewtechnologies.com/
- http://bowlsnsw.realviewtechnologies.com/
- http://islandofcontrasts.realviewtechnologies.com/
- http://digital.goodreadingmagazine.com.au/
- http://digitaledition.rousehilltimes.com.au/
- http://dijones.realviewtechnologies.com/?xml=dijones.xml
- http://digitaledition.easterncourier.com.au/?startpage=4&iid=26780
- http://www.nationalnewsagent.com.au/
- http://digitaledition.alivesydney.com.au/
- http://roadahead.racq.com.au/
- http://digitaledition.adelaidematters.com.au/
- http://digitaledition-innerwest.innerwestcourier.com.au/
- http://whatson.realviewtechnologies.com/
- http://snapshot.realviewtechnologies.com/
- http://www.eretailworld.com.au/

Shared hosting details

- http://communityaccessprogram.realviewtechnologies.com/
- http://property.manlydaily.com.au/?xml=Manly_Daily_Gloss_Real_Estate
- http://crtvic.realviewtechnologies.com/?xml=CRT_VIC
- http://apb.softpressmedia.com/
- http://albanyweekender.realviewtechnologies.com/
- http://bluemountainsgazette.realviewtechnologies.com/
- http://digital.theinternationalexpress.com/
- http://gstn.realviewtechnologies.com/?xml=On_The_Land
- http://propertypressdomain.realviewtechnologies.com/
- http://digitaledition.macarthurchronicle.com.au/
- http://hepmagazines.realviewtechnologies.com/
- http://digitaledition.wktmessenger.com.au/
- http://avon.realviewtechnologies.com/
- http://suncity.realviewtechnologies.com/
- http://redland.realviewtechnologies.com/
- http://agtrader.realviewtechnologies.com/?xml=AgTrader
- http://portstephens.realviewtechnologies.com/

Appendix C - Risk rating scheme

C.1 Likelihood

The likelihood rating of an issue encompasses both the likelihood of the issue being identified and attacked as well as the likelihood of an attack being successful. This is evaluated by taking into consideration the following aspects:

- Exploitability
  - Difficulty and technical knowledge or skill required to identify/exploit the issue
  - Time or resources required to mount a successful attack
  - Availability of exploit code and automated attack tools
- Reproducibility
  - Ease of reproducing a successful attack
  - Additional requirements for the attack to be successful, for example:
    - Victim user must be logged in
    - Some level of interaction by the victim user is required
- Discoverability
  - Number of instances of the vulnerability identified in the system
  - Level of authentication required to access affected components
  - Accessibility of the system
  - Degree of specific Insider knowledge required
- Frequency
  - How often the issue is likely to occur over a period of time
  - History of the issue in the industry
  - Existence of self-propagating malware targeting the issue

These factors will be employed to formulate a final likelihood rating for a given issue and a table of examples is provided below.

Likelihood rating	Example frequency	Example scenario
Rare	1 incident every 5+ years	Highly skilled and determined attacker with substantial resources
Unlikely	1 incident every 2 years	A skilled attacker with some degree of insider knowledge
Moderate	1 incident every year	An attacker with technical knowledge
Likely	1 incident every 6 months	Published and widely available exploit code exists
Almost Certain	1+ incidents every month	Worm propagating in the wild or widespread availability of an automated attack tool

Table 4: Likelihood Rating Scheme

Table 5: Likelihood Rating Scheme

C.2 Consequence

The consequence rating assesses the significance of exposure to a particular risk. This is evaluated by considering the impacts to the affected system and the underlying business. The factors under consideration are outlined in the following table provided by [redacted]

	ORSA Risk Ratings				
	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Damage Potential - **Financial** (source: ORSA)	Direct Loss or cost of up to 0.5 to 1.0% of Annual Budget / Revenue Target	Direct Loss or cost of between 1% to 5% of Annual Budget / Revenue Target. Reduction in business opportunities from key clients.	Direct Loss or cost of between 5% to 15% of Annual Budget / Revenue Target. Zero return on investment Potential loss of key business opportunities.	Direct Loss or cost of between 15% to 30% of Annual Budget / Revenue Target. Negative return on investment Loss of key business opportunities.	Direct Loss or cost of greater than 30% of Annual Budget / Revenue Target Sustained negative return on investment Significant loss of business opportunities.
Damage Potential - **Reputational** (source: ORSA)	Reputation intact, internal knowledge only. Minimal or no impact on customers.	Industry knowledge of incident, but no media attention. Client/Customer concerns.	Adverse local media coverage Concerns raised by shareholders. Customers demonstrate willingness to move business.	Adverse capital city media coverage. Significant decrease of shareholder support. Customers demonstrate willingness to move business.	Adverse global/national media coverage Parliamentary enquiry Major public concerns raised. Major loss of shareholder support. Loss of many key customers.
Damage Potential - **Regulatory** (source: ORSA)	Regulatory/Exchange requirements not met. No reprimand or special undertaking.	Verbal warning from Regulators/Exchange.	Regulatory/Exchange formal written warning.	Exchange/Regulator requires immediate press statement. Regulatory imposed fines.	Loss of banking licence Suspended from trading on Exchanges.
Damage Potential - **Internal** (source: ORSA)	Events that are absorbed into normal activity.	Low staff turnover An event, the impact of which can be absorbed, but management effort is required to minimise the impact Some staff morale	Poor reputation as employer. A key employee leaves. A significant event which can be managed under normal circumstances.	Some key executives leave the company. Bank is not perceived as an employer of choice. A critical event which can be managed with escalation and	Large number of key executives leave the company. An event that Management is not able to impact by increased management.

		problems.		significant management effort.	

Table 6: Consequence Rating Scheme

C.3 Risk

A risk measure or rating is determined by the likelihood and adjusted consequence ratings. Use the matrix below to determine each risk.

		Consequence				
		Very Low	Low	Medium	High	Very High
Likelihood	Almost Certain	HIGH	HIGH	EXTREME	EXTREME	EXTREME
	Likely	MODERATE	HIGH	HIGH	EXTREME	EXTREME
	Moderate	LOW	MODERATE	HIGH	EXTREME	EXTREME
	Unlikely	LOW	LOW	MODERATE	HIGH	EXTREME
	Rare	LOW	LOW	MODERATE	HIGH	HIGH

Figure 3: Risk rating scheme