



VicTrack

Perimeter & Application Security
Assessment

Project Number 2012-02

November 2012

Distribution list

Distribution	
Cynthia Lahiff	Acting Chief Executive Officer, VicTrack
Leo Felicissimo	Acting General Manager, Business Services, VicTrack
Arianne Rose	Company Secretary, VicTrack
Kristen Georgakopoulos	Manager, Information Technology, VickTrack
Alastair Banks	Partner, Deloitte
David Boyd	Partner, Deloitte
Ruth Farrugia	Director, Deloitte
Adrian Blount	Director, Deloitte

Contents

1	Executive summary	4
2	Vulnerability impact matrix	10
3	Application security criteria iconography	27
4	External network security assessment	29
5	SSL VPN security assessment	31
6	Mobile device management (AirWatch)	32
7	Bilmax web application security assessment	33
	Appendix A – Web application testing methodology	47
	Appendix B – Penetration testing inherent limitations	49
	Appendix C – Application profile	50
	Appendix D – Detailed Support for Findings	52
	Appendix E – Internal Audit Rating Guidance	67
	Appendix F – MDM Recommendations	69

Inherent Limitations

The Services provided are advisory in nature and do not constitute an assurance engagement in accordance with Australian Standards on Review or Assurance Engagements or any form of audit under Australian Auditing Standards, and consequently no opinions or conclusions intended to convey assurance under these standards are expressed.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made.

Our work is performed on a sample basis; we cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud.

Any projection of the evaluation of the control procedures to future periods is subject to the risk that the systems may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Recommendations and suggestions for improvement should be assessed by management for their full commercial impact before they are implemented.

We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by VicTrack personnel. We have not attempted to verify these sources independently unless otherwise noted within the report.

Limitation of Use

This report is intended solely for the information and internal use of VicTrack in accordance with our contract dated 19 June 2009 and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report. We do not accept or assume responsibility to anyone other than VicTrack for our work, for this report, or for any reliance which may be placed on this report by any party other than VicTrack.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Confidential - this document and the information contained in it are confidential and should not be used or disclosed in any way without our prior consent.

© 2012 Deloitte Touche Tohmatsu. All rights reserved.

Deloitte: Vic Track – Perimeter and Application Security Assessment

This report is intended solely for the information and internal use of VicTrack, and should not be used or relied upon by any other person or entity.

1 Executive summary

1.1 Introduction

As a part of the Internal Audit Services provided to VicTrack, Deloitte Touche Tohmatsu (Deloitte) has performed a security testing assessment of VicTrack's externally facing perimeter network (including VPN architecture and configuration assessment), the Bilmax web application and high level assessment of VicTrack's mobile management solution deployment process.

1.2 Background Objective and scope

The objective of this engagement was to identify services and vulnerabilities in VicTrack's externally facing perimeter network and examine security controls in key systems and applications identified by VicTrack. The following areas were included in the scope of this assignment.

External vulnerability assessment

The objective of this phase was to identify any publicly reported network security vulnerabilities within VicTrack's externally accessible network. The following activities were undertaken as part of this phase:

- System discovery – discover externally accessible systems and associated services from the internet
- Vulnerability scanning – unauthenticated automated network vulnerability assessment of selected networks and hosts
- Manual verification – manual analysis of automated results of the selected hosts.

The vulnerability scanning was performed between 11-18 September 2012.

The scope of this task included the following:

VicTrack network

#	HOST/IP	Description
01	203.149.88.249	Unknown
02	203.149.88.254	Unknown
03	203.149.88.250	Unknown
04	203.149.88.31	ActiveSync autodiscovery address
05	203.149.88.32	Outlook Web App
06	203.149.88.35	VicTrack website
07	203.149.88.251	Unknown
08	203.149.88.11	Juniper SSL VPN
09	203.149.88.36	Rail Skills Centre – Victoria website
10	203.149.88.12	Juniper SSL VPN
11	203.149.88.41	SIA login website

Table 1: VicTrack network

SSL VPN Security Assessment

The objective of this phase was to examine the SSL VPN configuration and determine whether security controls were implemented. The testing was performed on 19 September 2012. The following objectives were considered as part of this phase:

- Design of deployment architecture and protection to VicTrack’s internal systems and networks
- Strong authentication scheme and granular user rights management
- Strong cryptographic algorithms are in use
- Access is restricted to necessary services only
- Logging and auditing is configured.

Mobile device management (AirWatch)

AirWatch is an application used to manage security of remote devices. The objective of this phase was to examine the overall architecture, design and process documentation of the AirWatch MDM solution as deployed at VicTrack, in order to identify areas for improvement and potential weaknesses. The solution is currently not in production.

Bilmax Web Application Security Assessment

Bilmax is a telephone records system that provides telephone record information, including billing and calling records. This can be provided on an individual, group or organisational basis. We consider the key risk with this application is that customers may be able to access other customers' billing data.

The objective of this phase was to identify commonly exploited web application vulnerabilities within the Bilmax web application.

The security assessment of the Bilmax application was performed over the period 19 September 2012 to 2 October 2012 inclusive.

The scope of this task included the following security controls assessed through the penetration testing:

- Authentication
- Authorisation
- Data Validation
- Session Management
- Data Security
- Exception Handling
- Communication Security.

1.3 Constraints and limitations

This report should be read in the context of the following constraints and limitations:

- The BilMax application was tested in the VicTrack test environment. No access to production version of the application was permitted by the VicTrack IT group
- Throughout the assessment the BilMax web application experienced downtime and general intermittent operations
- The BilMax application encountered errors and as such the following could not be tested (Refer to 2, "Vulnerability impact matrix"):
 - Data security.6 "Use non-sequential identifiers to prevent information disclosure"
 - Data validation.9 "No un-validated email communication with users".
- Logs were requested for the production version of BilMax for the 24 September however complete logs were not available
- The AirWatch MDM deployment specific to VicTrack is not well documented and specific architecture and design documents could not be supplied on request
- The inherent limitations of security testing are outlined in Annexure B – Penetration Testing Inherent Limitations.

As an overall observation, it was found that the issues discovered in the testing of Bilmax are based on a weak security design of the application. To address these issues, we believe that a redesign of the application is required.

1.4 Summary of findings

An overview of our key findings is provided below:

External network vulnerability assessment

The external network vulnerability assessment was performed remotely, as an anonymous user from the Deloitte controlled network. The external network vulnerability assessment of the selected hosts (target hosts) did not identify technical vulnerabilities or weaknesses that could be used by an attacker to directly exploit external VicTrack's network perimeter.

SSL VPN security assessment

The Juniper SSL VPN is a remote access system that can allow external users to run a variety of applications remotely, including remote desktop connectivity applications, web applications and remote access applications. Deloitte identified vulnerabilities in the SSL VPN relating to the following:

- Unpatched and out-dated software
- Lack of administrator interface segregation
- Lack of regular security log monitoring of SSL VPN services.

Mobile device management (AirWatch)

The AirWatch Mobile Security policy lacks security controls independent of users' actions (e.g. remote wipe on loss of phone, malicious software or operations detection, etc.)

Bilmax web application security assessment

The Bilmax web application security assessment identified multiple vulnerabilities relating to:

- Weak session management
- Out-dated and unpatched applications
- Problems with the administrator interface
- Data validation and user input parsing
- Sensitive information is logged to plain text log files.

Please refer to section 2 for a summary of findings and to sections 3 to 7 for further technical information.

The table below highlights the High and Medium rated findings identified during our engagement.

Finding description	Reference	Observation Rating
<p>BILMAX</p> <p>A SQL injection vulnerability has been identified which increases the risk of a breach of confidentiality of the data, integrity of the database and the underlying platform. The issue occurs as a result of the web browser sending SQL queries to the server in plain text.</p>	Section 7	High
<p>BILMAX</p> <p>Privilege escalation allowing a low-level user to access administrator functions via the internal interface is possible.</p> <p>The issue is rated as medium due to the fact that it is only accessible by internal users. If it would be exposed to the Internet, the issue would be rated as 'high'.</p>	Section 7	Medium
<p>SSL VPN</p> <p>The SSL VPN system software hasn't been updated in almost three years and has known vulnerabilities (e.g. CVE-2010-2289) that can be exploited.</p>	Section 5	Medium
<p>SSL VPN</p> <p>Access to the administrator interface is allowed via the Internet. This increases the risk of a remote attacker gaining access to administrative functions.</p>	Section 5	Medium
<p>BILMAX</p> <p>The application does not set security flags (<i>secure</i> and <i>httponly</i>) on authentication cookies, increasing the risk of information being transmitted insecurely and enabling an attacker to breach the confidentiality of the application.</p>	Section 7	Medium
<p>BILMAX</p> <p>The application is vulnerable to session hi-jacking attacks.</p> <p>For example, it is possible to re-use a cookie from different network location to gain unauthorised authenticated access to the legitimate user's application account.</p>	Section 7	Medium
<p>BILMAX</p> <p>Encrypted passwords are displayed to the user which increases the risk of interception of that data by a malicious party or of an unauthorised party viewing this in a cache.</p>	Section 7	Medium

Finding description	Reference	Observation Rating
<p>BILMAX</p> <p>The application is vulnerable to cross-site request forgery attacks.</p> <p>The application does not differentiate between some HTTP POST and GET request types. Additionally, cross-site request forgery protection tokens (also known as one time transaction tokens) have not been observed.</p>	Section 7	Medium
<p>BILMAX</p> <p>The web server (telmax21) allows renegotiation, which is a known vulnerability in the encryption services. This could lead to unauthorised use of the application.</p>	Section 7	Medium
<p>MDM</p> <p>There is a lack of detailed Mobile Device Management policy and solution architecture.</p>	Section 6	Medium
<p>BILMAX</p> <p>The application uses a custom session management facility. There is an increased risk that unauthorised users could gain access to the system through weak session management controls.</p>	Section 7	Medium
<p>BILMAX</p> <p>The application did not lock out an administrator account on the external interface.</p>	Section 7	Medium

This report has been prepared on an exception basis. Refer to section 2 for details of all observations noted. In addition to the above, 21 “Low” rated observations were also noted.

Overall engagement rating¹

Requiring improvement

Several key controls are not systematic or consistently applied in the area subject to examination. One or more high items have been reported together with a few medium items that represent an internal control risk to the process subject to examination and require improvement within an appropriate timeframe.

1.5 Acknowledgement

We would like to take this opportunity to thank the staff at VicTrack for their cooperation and assistance during the course of our engagement.

¹ Please refer to Appendix E for further information in relation to overall engagement rating definitions.

2 Vulnerability impact matrix

The following matrix presents security failures identified during each phase of this security assessment (external network security assessment, SSL VPN security assessment, AirWatch security assessment and Bilmax web application security assessment).

It also provides an indication of the potential risk associated with each vulnerability taking into consideration the potential impact and likelihood. However, the risk ratings have been prepared without consideration of any business process controls (i.e. as this is not in scope for this engagement).

The risk ratings outlined in the tables below are intended to assist the reader in understanding the factors related to the vulnerability, and are not intended to provide “assurance” as defined by standards issued by the Australian Auditing Standards Board.

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Data validation.10	No SQL injection vulnerabilities	An attacker could gain access to sensitive information and application accounts resulting in a breach of confidentiality.	BILMAX A SQL injection vulnerability has been identified which increases the risk of a breach of confidentiality of the data, integrity of the database and the underlying platform. The issue occurs as a result of the web browser sending SQL queries to the server in plain text. Refer to Appendix D	High	Review the design of the application to validate input data and then use parameterised SQL queries and parameterised stored procedures.	Review of the application design will be undertaken. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authorisation.3	Authorisation data is controlled 'server side'	Users can gain access to unauthorised functions.	<p>BILMAX</p> <p>Privilege escalation allowing a low-level user to access administrator functions via the internal interface is possible.</p> <p>The issue is rated as medium due to the fact that it is only accessible by internal users. If it would be exposed to the Internet, the issue would be rated as 'high'.</p> <p>Refer to Appendix D</p>	Medium	Ensure server-side authorisation is used rather than relying on parameters supplied from the client.	<p>The design will be reviewed and options will be evaluated.</p> <p>Action owner: Manager Information Technology</p> <p>Target date: February 2013</p>
SSL.1 / IC.4	Deployment architecture is appropriate and provides appropriate protection to VicTrack systems and networks	A remote attacker could make use of known vulnerabilities in public-facing systems to gain control of VicTrack systems.	<p>SSL VPN</p> <p>The SSL VPN system software hasn't been updated in almost three years and has known vulnerabilities (e.g. CVE-2010-2289) that can be exploited.</p> <p>Refer to Appendix D</p>	Medium	Update the SSL VPN to the latest recommended version.	<p>The version will be updated and process incorporated to review and update version releases.</p> <p>Action owner: Manager Information Technology</p> <p>Target date: November 2012</p>

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
SSL.4	Access is restricted to only necessary services	A remote attacker could make use of the more vulnerable Internet environment to exploit administrator access and gain control of VicTrack systems.	SSL VPN Access to the administrator interface is allowed via the Internet. Refer to Appendix D	Medium	Enforce IP-based access control.	Completed. External access to administrator interface has been removed. Action owner: Manager Information Technology Target date: November 2012
Session management.3	Session tokens use cookie security flags	An attacker could use authentication information to impersonate a valid user and obtain access to view, change or delete confidential information.	BILMAX The application does not set security flags (<i>secure</i> and <i>httponly</i>) on authentication cookies, increasing the risk of information being transmitted insecurely and enabling an attacker to breach the confidentiality of the application.	Medium	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Session management.6	Session hi-jacking prevention	An attacker could use authentication information to impersonate a valid user and obtain access to view, change or delete confidential information.	BILMAX The application is vulnerable to session hi-jacking attacks. For example, it is possible to re-use a cookie from different network location to gain unauthorised authenticated access to the legitimate user's application account.	Medium	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013
Data security.1	Sensitive data should never be displayed	Sensitive information (i.e. passwords) could potentially be disclosed to third parties who are unauthorised to view this information.	BILMAX Encrypted passwords are displayed to the user which increases the risk of interception of that data by a malicious party or of an unauthorised party viewing this in a cache.	Medium	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Session management.7	No cross site request forgery (CSRF) vulnerabilities	An attacker could use authentication information to impersonate a valid user and obtain access to view, change or delete confidential information.	BILMAX The application is vulnerable to cross-site request forgery attacks. The application does not differentiate between some HTTP POST and GET request types. Additionally, cross-site request forgery protection tokens (also known as one time transaction tokens) have not been observed.	Medium	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013
Communication security.2	SSL/TLS does not use weak ciphers or contain protocol weaknesses	Combined with another attack, confidential data could be intercepted and be exposed to unauthorised parties.	BILMAX The web server (telmax21) allows renegotiation, which is a known vulnerability in the encryption services. This could lead to unauthorised use of the application.	Medium	Ensure that software is regularly updated with security patches.	Process will be implemented to review application and security patches and regularly update. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
MDM.1	MDM policy and solution architecture	Potential data loss and access to information the user is not authorised for.	MDM Lack of detailed Mobile Device Management policy and solution architecture	Medium	Develop a detailed Mobile Device Management policy and solution architecture.	Completed. The policy has been reviewed and recommendations have been incorporated Solution Architecture has been finalised and has been included in operational documentation. Action owner: Manager Information Security Target date: November 2012
Session management.1	An established, standardised and secure session management framework is used	An attacker could use authentication information to impersonate a valid user and obtain access to view, change or delete confidential information.	BILMAX The application uses a custom session management facility. There is an increased risk that unauthorised users could gain access to the system through weak session management controls.	Medium	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.8	Account lockout	An attacker could gain unauthorised access to user accounts via password guessing attack.	BILMAX The application did not lock out an administrator account on the external interface.	Medium	Enforce account lockout facility to prevent brute force password guessing attacks.	Customer logons have account lock out implemented using active directory. Local accounts need to be investigated. Action owner: Manager Information Technology Target date: February 2013
SSL.5	Appropriate logging and auditing is configured	A lack of appropriate oversight could lead to security incidents going unidentified.	No confirmation received as to whether regular technical audits or reviews of the SSL VPN are conducted. Potential vulnerabilities in the configuration or logs may go undetected if these are not conducted.	Low	Confirm whether logs and settings of the system are reviewed on a regular basis and implement this if necessary.	A system logging application will be implemented this financial year. Action owner: Manager Information Technology Target date: June 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Data validation.5	No DoS (Denial of Service) vulnerabilities	Unanticipated use of the application could lead to Bilmax administrators being unable to perform administrative functions until a database administrator performs a manual repair of the system.	BILMAX An exploit of a vulnerability in which a cookie is altered may lead to legitimate administrative users being denied access to the administrator interface. Refer to Appendix D	Low	Ensure that the application accepts and validates any and all input without adverse behaviour.	The design will be reviewed and investigation into validating input and prevention of denial of service vulnerabilities. Action owner: Manager Information Technology Target date: February 2013
Session management.2	Session tokens are destroyed server-side	An attacker could use authentication information to impersonate a valid user and obtain access to view, change or delete confidential information.	BILMAX The application does not securely destroy an authenticated session, enabling an unauthorised party to replay a previous request and gain access to confidential information.	Low	Revisit the design of the application to implement a standard and up-to-date session management system for the application that implements secure session management including cross site request forgery protection.	The design will be reviewed and investigation into implementing secure session management. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Data security.9	No sensitive information should be passed in URLs	People with access to the logs may have access to sensitive information such as encrypted passwords which they are not authorised for.	BILMAX The application stores names and encrypted passwords in logs which will allow those with access to logs to impersonate a valid user.	Low	Ensure that logs do not contain any sensitive information.	The design will be reviewed and investigation into preventing access to logs containing sensitive information will be undertaken. Action owner: Manager Information Technology Target date: February 2013
Exception handling.2	Logging of exception and failures	Without confirmation that actions are logged, unauthorised usage may go undetected or would be unable to be traced if it did occur.	BILMAX The logs for the correct date were not provided within the testing period and for the ones provided within the testing period, they did not have an appropriate level of exception logging.	Low	Ensure that authentication and exception logs are appropriately collected and securely stored from unauthorised access, modification or destruction.	The design will be reviewed and investigations into implementing exception logs and secure storage will be undertaken. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.13	User authentication logging	Without confirmation that actions are logged, unauthorised usage may go undetected or would be unable to be traced if it did occur.	BILMAX Complete logs for the correct date were not provided within the testing period.	Low	Ensure that authentication and exception logs are appropriately collected and securely stored from unauthorised access, modification or destruction.	The design will be reviewed and investigations into implementing exception logs and secure storage will be undertaken. Action owner: Manager Information Technology Target date: February 2013
Data security.5	Industry standard cryptographic algorithms are used	Combined with another attack, confidential data could be intercepted and be exposed to unauthorised parties.	BILMAX The web server (telmax21) allows renegotiation, which is a known vulnerability.	Low	Ensure that software is regularly updated with security patches and is configured appropriately to ensure the vulnerability is resolved.	Process will be implemented to review application and security patches and regularly updated. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Exception handling.1	Generic error messages	A remote attacker could make use of known vulnerabilities in public-facing systems to gain control of or disrupt VicTrack systems.	BILMAX Error messages, such as 404 Not Found, disclose version numbers, which allows infrastructure enumeration. The impact of this is that attackers will be able to identify known vulnerabilities in infrastructure and potentially gain access to confidential information or gain control of VicTrack systems.	Low	Prevent the web server from disclosing version information in HTTP responses.	The design will be reviewed and investigations into preventing version information in error messages will be undertaken. Action owner: Manager Information Technology Target date: February 2013
SSL.3 / IC.2 / IC.3	Strong cryptographic algorithms are in use	Insecure access to the SSL VPN could allow remote attackers control of or disrupt VicTrack systems.	SSL VPN Access via SSLv2 is allowed to the SSL VPN which is an out-dated version of the SSL protocol.	Low	Update the SSL VPN to the latest recommended version.	Sociability testing will be undertaken to investigate the impact to update the SSL version. Action owner: Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.1	Enforce Authentication	Unauthenticated users can gain access to documents that they are not authorised for, potentially breaching confidential data.	BILMAX The application allows unauthenticated users to access application pages. See section 0 for more information.	Low	Ensure that all resources are protected and that only authenticated users can access them.	The design will be reviewed and access control will be investigated. Action owner: Manager Information Technology Target date: February 2013
Authentication.3	Last login date/time displayed	Users would not detect unauthorised access to their application accounts.	BILMAX The application does not display last login date and time upon successful login. This could prevent the user from detecting an unauthorised account access.	Low	Display last logon date and time to the user.	The design will be reviewed and investigation into the ability to display last log on date and time to the user will be undertaken. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.4	No 'remember me' functionality	An attacker could gain access to VicTrack application accounts and therefore sensitive information.	BILMAX The application does not explicitly disable the web browser's native auto-complete functionality. This could allow an attacker with access to the user's workstation to gain access to their account.	Low	Explicitly disable autocomplete in the login form.	The design will be reviewed and investigation into the ability to disable autocomplete in the login form will be undertaken. Action owner: Manager Information Technology Target date: February 2013
Authentication.5	Detecting multiple concurrent logins	Users would not detect unauthorised access to their application accounts.	BILMAX The application does not detect and prevent multiple concurrent logins. This may prevent users from detecting unauthorised account access.	Low	Implement concurrent logon detection and logging facilities.	The design will be reviewed and investigations into implementing logon detection will be undertaken. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.6	Admin Interface: security roles and enforcement	An non-administrative user could gain administrative access to the application and access restricted functions.	BILMAX The administrative and operational interfaces are not segregated.	Low	Segregate administrative and operational interfaces, via different applications or IP based restrictions.	Investigation will be undertaken for separating and implementing operational interfaces. Action owner: Manager Information Technology Target date: February 2013
Authentication.10	Password change facility	An attacker could gain access to application accounts via password guessing attack, breaching confidentiality or disrupting the operation of the system.	BILMAX The application password change function has been disabled so users will be unable to set a password of their choice via the application.	Low	Implement self-management – password change facility for all users.	The design will be reviewed and investigations into implementing self-management password changes will be undertaken Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Authentication.1 1	Authentication history	Users would not detect unauthorised access to their application accounts.	BILMAX The application does not implement an authentication history facility. This will prevent users from reviewing their authentication history, in order to detect unauthorised account access or brute force password guessing attempts.	Low	Implement account authentication history viewing facility for all users.	The design will be reviewed and investigation into implementing account authentication history for users will be undertaken. Action owner: Manager Information Technology Target date: February 2013
Authorisation.4	Protected content is referenced using non-predictable identifiers	An attacker could predict the location of a resource and then attempt an attack on that resource, increasing the risk of that content being exposed to unauthorised access.	BILMAX The application uses predictable resource identifiers to reference site content. e.g. "May_2012/data/wbttop.csv". Predictable resource identifiers could allow an attacker to potentially access restricted or unpublished content, if future authorisation vulnerabilities were to be identified.	Low	Ensure that resources are accessed by the application using non-predictable identifiers.	The design will be reviewed and investigations will be undertaken for implementing non-predictable identifiers. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Data validation.1	Data is validated for size, data type, range, canonicalization and syntax	A malicious user could use the email function to send information to unauthorised locations.	BILMAX Input of invalid data in the email address field can lead to failures of data integrity and non-repudiation.	Low	Implement secure data validation facility to validate and encode all input data.	The design will be reviewed and investigations will be undertaken for secure validation of input data. Action owner: Manager Information Technology Target date: February 2013
Session management.5	Inactive session expiry	An unauthorised user could make use of an idle session to breach the confidentiality of the application.	BILMAX Idle session expiry timeout is not enforced – session remained active after 30 minutes of inactivity.	Low	Implement session idle timeout in the application.	The design will be reviewed and investigations into session timeout will be undertaken. Action owner: Manager Information Technology Target date: February 2013

Criteria ID	Criteria	Risk	Vulnerability	Technical Risk Rating	Recommendation	Management Response
Data security.2	Sensitive data should not be cached or stored client side	An attacker could obtain sensitive information by getting access to the client computer that a legitimate user is using.	BILMAX The application does not prevent the web browser from caching user information client-side.	Low	Ensure that no sensitive data is cached or stored client side.	The design will be reviewed investigation into ensuring no sensitive data is cached or stored client side. Action owner: Manager Information Technology Target date: February 2013
Data security.4	Production Data in Testing environments	Private or sensitive information could be exposed to those who have no authorisation to view it.	BILMAX Production data is being used in the testing environment which could allow unauthorised testing personnel access to the personal information of users. In discussion with IT was stated that it was standard VicTrack practice to use production data in the test environment and this was the case across a wide range of systems. It was also stated that test systems were protected to the same extent as the production systems. It is not normal practice within organisations to have production data in the test system because of the likelihood of wider access to the test systems.	Low	Establish whether it is normal practice and assess the risks associated with this practice. Establish if the test systems are secured to the same extent as the productions systems. There may be some production data which may be considered inappropriate to be in the test systems. If the decision is made to continue with this practice, a form of data masking may be required.	Test environments will be reviewed to ensure security is in line with productions systems. Access control is in line with production systems and this will be regularly reviewed. No additional access to test systems will be provided unless authorised by Manager Information Technology. Action owner: Manager Information Technology Target date: December 2012

3 Application security criteria iconography

Deloitte has used the icons presented in the following table throughout the document to provide readers with a quick assessment of the reviewed security controls.

The ratings outlined in the tables below are intended to assist the reader in understanding the impact of the detailed findings in relation to each criterion, and are not intended to provide “assurance” as defined by standards issued by the Australian Auditing Standards Board.

Table 3-1 - Compliance Ratings










	Tests performed indicated that the security control met the criterion.
	Tests performed indicated that the implementation of the security control did not fully meet the criterion.
	The security control was not implemented.
	The security control was not applicable to this application or was outside the scope of the application.









Table 3-2 - Severity Ratings

	<p>No associated risk.</p>
	<p>The application's gap with the criterion represents a Low level of risk.</p> <p>The risk may be addressed via existing countermeasures and normal operating procedures.</p>
	<p>The application's gap with the criterion represents a Medium level of risk.</p> <p>May have some value in mitigation.</p> <p>To be addressed as finance and resources become available.</p> <p>May be deemed an acceptable risk if mitigation is costly.</p>
	<p>The application's gap with the criterion represents a High level of risk.</p> <p>Requires attention as soon as Extreme risks have been addressed.</p> <p>Mitigation measures should be adopted where possible in order to reduce the risk.</p>
	<p>The application's gap with the criterion represents an Extreme level of risk.</p> <p>Immediate attention and risk mitigation measures are required as soon as possible to address the risk.</p>

4 External network security assessment

4.1 Intelligence gathering

4.1.1 Assessment



Ref #	Criteria	Assessment of Findings		
		Finding	Severity	Justification
IG.1	Intelligence gathering- DNS zone transfer DNS zone transfers are only allowed to authorised clients.			DNS zone transfer was unsuccessful.
IG.2	Intelligence gathering- traceroute Information Traceroute does not reveal unnecessary information.			The traceroute utility did not identify any intermediate network devices that could be tested during this assessment.
IG.3	Intelligence gathering- internet searching Google searching does not provide any significant or sensitive information.			No sensitive information was identified.
IG.4	Intelligence gathering- document metadata Documents available online do not reveal significant or sensitive information through metadata.			No sensitive information was identified.

4.2 Network reconnaissance

Deloitte conducted port scans over the common TCP and UDP ports of all internet accessible hosts nominated by VicTrack.

In addition, a version scan was undertaken to identify the network services accessible on each of the open ports.

4.2.1 Assessment









Ref #	Criteria	Assessment of Findings		
		Finding	Severity	Justification
PS.1	<p>Open ports - authorised services</p> <p>Only services authorised to provide Internet-sourced access have open ports.</p>			Scanned hosts did not disclose any open ports running vulnerable, sensitive or high-risk services.

4.3 Vulnerability research and verification

Deloitte performed a vulnerability assessment between 11 Sep 2012 and 18 Sep 2012 (inclusive), in order to identify common weaknesses and vulnerabilities that may be present in the publicly accessible VicTrack network infrastructure.

Please note that denial of service testing was not within the scope of this assessment.

4.3.1 Assessment











Ref #	Criteria	Assessment of Findings		
		Finding	Severity	Justification
IC.1	<p>Insecure configuration - service banners</p> <p>Service banners and/or headers displaying version and systems information have been removed.</p>			None identified
IC.2	<p>Insecure configuration - outdated SSL/TLS version</p> <p>Older versions of SSL/TLS are not enabled.</p>			<p>Access via SSLv2 is allowed to the SSL VPN</p> <p>See section 5: SSL VPN security assessment</p>
IC.3	<p>Insecure configuration - weak SSL/TLS cipher suite</p> <p>SSL/TLS cipher suite does not support weak ciphers.</p>			<p>Access via SSLv2 is allowed to the SSL VPN</p> <p>Refer to Appendix D</p> <p>See section 5: SSL VPN security assessment</p>
IC.4	<p>Insecure configuration – patching</p> <p>Running services are patched appropriately and not exploitable by publicly available vulnerabilities.</p>			<p>The SSL VPN system software has not been updated in almost three years and contains security updates that should be applied (e.g. CVE-2010-2289).</p> <p>Refer to Appendix D</p> <p>See section 5: SSL VPN security assessment</p>

5 SSL VPN security assessment

5.1 Configuration walkthrough

Deloitte examined configuration via a walkthrough with VicTrack staff to determine that appropriate security controls were in place.

5.1.1 Assessment

Ref #	Criteria	Assessment of Findings		
		Finding	Severity	Justification
SSL.1	Architecture Deployment architecture provides protection to VicTrack systems and networks			The SSL VPN system software has not been updated in almost three years and contains security updates that should be applied (e.g. CVE-2010-2289). Refer to Appendix D
SSL.2	Authentication Authentication scheme is in use and allows granular user rights management			RSA tokens used for access to the system.
SSL.3	Cryptography Cryptographic algorithms are in use			Access via SSLv2 is allowed to the SSL VPN
SSL.4	Access control Access is restricted to only necessary services			Access to the administrator interface is allowed via the Internet.
SSL.5	Review Logging and auditing is configured			No regular technical audits or reviews of the SSL VPN are conducted. Potential vulnerabilities in the configuration or logs may go undetected if these are not conducted.

6 Mobile device management (AirWatch)

6.1 Mobile device deployment security policy assessment

We were asked to perform a high level security policy assessment of the VicTrack's Mobile Device Management Security Policy for the nominated platform, AirWatch.

We understand that the deployment of the MDM solution is currently in the pilot phase and is currently being assessed for production.

We have assessed currently available policy documentation (Victorian Rail Track – Mobile Device Security Policy, IS-PO 014, version: 0.8) and suggested a number of updates.

For detailed information please see Appendix F – MDM Recommendations.

7 Bilmax web application security assessment

7.1 Introduction

The security controls of the VicTrack Bilmax application were assessed using the criteria indicated together with a justification for the rating provided. Additional details are presented with evidence of non-compliance in the form of screen captures, source code and/or log file extracts, where appropriate.

The following security controls were assessed through the penetration testing:

- Authentication
- Authorisation
- Data Validation
- Session Management
- Data Security
- Exception Handling
- Communication Security.

















7.2 Authentication











7.2.1 Description

Authentication controls provide a mechanism for users/devices to supply a unique identification and associated credential that represents their digital identity. Authentication is the process of verifying the claimed identity based upon the supplied credential – i.e. it checks that “you are who you claim to be”.

7.2.2 Application security criteria assessment

The following table details the application security criteria for authentication mechanisms within the application:

Authentication Criteria	Assessment of Findings		
	Finding	Severity	Justification
1. Enforce Authentication The application requires a remote identity to authenticate before allowing access to the internal processes and restricted data.			The application allows unauthenticated users to access application pages.
2. Unique login IDs Login IDs are unique, not sequential, generic or easily guessable by a remote user.			The application uses a combination of users' first and last name to generate a username for the application which is acceptable.
3. Last login date/time displayed The application shows the last login date/time to the user upon successful login.			The application does not display last login date and time upon successful login. This could prevent the user from detecting an unauthorised account access.
4. No 'remember me' functionality The application does not allow any 'remember me' functionality, such as explicit implementation or allowing browsers to remember login fields.			The application does not explicitly disable the web browser's native auto-complete functionality. This could allow an attacker with access to the user's workstation to gain access to their account.
5. Detecting multiple concurrent logins. The application detects multiple concurrent logins.			The application does not detect and prevent multiple concurrent logins. This may prevent users from detecting unauthorised account access.
6. Admin Interface: security roles and enforcement Administration interfaces to the application should be segregated from the core functionality supporting standard user access.			The administrative and operational interfaces are not segregated.
7. Account enumeration: authentication failure message When the application authentication fails a generic error message is returned that does not detail the exact reason for authentication failure (i.e. Login ID or password incorrect).			The login does not allow enumeration of user accounts.
8. Account lockout The application should lock an account after a specific period of failed attempts or block access from a particular IP address.			The application did not lock out an administrator account on the external interface.

Authentication Criteria	Assessment of Findings		
	Finding	Severity	Justification
9. Re-enablement of locked accounts Locked accounts should be unlocked after a short period of time (i.e. 10 minutes) to ensure a Denial of Service does not occur.			The application did not lock out an administrator account on the external interface. Refer to Authentication.8
10. Password change facility The application provides a facility for users to change their passwords.			The application password change function has been disabled so users will be unable to set a password of their choice via the application.
11. Authentication history The application allows the user to view their account authentication history.			The application does not implement an authentication history facility. This will prevent users from reviewing their authentication history, in order to detect unauthorised account access or brute force password guessing attempts.
12. User logout function The application should allow the user to effectively logout and terminate the session with the application.			The application allows the user to logout and prevent ongoing access to user data.
13. User authentication logging All authentication attempts to the application should be recorded in a security log.			The logs for the correct date were not provided within the testing period.

7.3 Authorisation











7.3.1 Description



Authorisation controls interact with the assigned authentication tokens for a user or entity. Authorisation is the process of enforcing access rules that define what resources can be accessed and operations/functions performed by a specific user or entity.

Authorisation is typically configured through either role, privilege or permission based schemes and is designed so that only the authorised users or entities with a particular credential are able to perform operations in the application.

7.3.2 Application security criteria assessment

The following table details the common application security criteria for authorisation mechanisms within the application:

Authorisation Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>1. User access is restricted to only those functions to which they are authorised.</p> <p>User access is configured in-line with company's data access requirements.</p>			No unauthorised user access to functions found.
<p>2. User access is restricted to only data or resources to which they are authorised.</p> <p>User access is configured in-line with company's data access requirements.</p>			Administrators have access to user telephone records which are generally confidential and there is no demonstrated business need for this to occur. Refer to Data Security.3
<p>3. Authorisation data is controlled 'server side'.</p> <p>The application does not expose client controllable authorisation data.</p>			Privilege escalation allowing a low-level user to access administrator functions is possible. Refer to Appendix D
<p>4. Protected content is referenced using non-predictable identifiers.</p> <p>The application does not expose identifiers for content or data using predictable resource names.</p>			The application uses predictable resource identifiers to reference site content. e.g. "May_2012/data/wbttop.csv". Predictable resource identifiers could allow an attacker to potentially access restricted or unpublished content, if future authorisation vulnerabilities were to be identified.
<p>5. No Insecure Direct Object Reference vulnerabilities</p> <p>The application checks that a user is authorised to perform a function on an object before allowing access.</p>			No Insecure Direct Object Reference vulnerabilities have been identified.

Authorisation Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>6. Direct access to URLs are restricted based on a user's role</p> <p>User access is restricted to URLs to which they are authorised.</p>			<p>No unauthorised authenticated user access to URLs has been identified.</p>

7.4 Data validation

7.4.1 Description











Most applications are designed to send, receive and/or process data submitted by users, databases or other application sources. Applications can restrict and verify the data that is accepted by the application based upon its content type, size and input location.

Data validation weaknesses are one of the major causes of application vulnerabilities. Most attacks exploit interfaces that have minimal or non-existent data validation routines applied to them. With minimal data validation controls in an application an attacker can make easy work of identifying and using weaknesses in the application to gain unauthorised access to resources.





Applications therefore need to handle all data input as tainted and, until validated; it should not be trusted or processed.

7.4.2 Application security criteria assessment

The following table details the application security criteria for data validation mechanisms within the application:

Data Validation Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>1. Data is validated for size, data type, range, canonicalization and syntax.</p> <p>Data that is received by the application that does not meet the validation requirements is rejected and the application stops processing the request - reject bad data, accept known good data.</p>			Input of invalid data in the email address field can lead to failures of data integrity and non-repudiation (e.g. information being sent to an invalid recipient).
<p>2. Data validation occurs on the server-side as a minimum.</p> <p>Data validation controls should be implemented server side and not rely client side scripting</p>			Refer to Data Validation.10.
<p>3. All input sources are validated.</p> <p>All input sources from the client are validated including URI, form fields, cookies, HTTP headers and session objects.</p>			The application validates input sources.
<p>4. Output data is encoded.</p> <p>The application displays data in an encoded format.</p>			The application displayed data in an encoded format.
<p>5. No DoS (Denial of Service) vulnerabilities.</p> <p>The application does not handle excess data or queries resulting in degraded performance.</p>			<p>An exploit of a vulnerability in which a cookie is altered may lead to legitimate administrative users being denied access to the administrator interface.</p> <p>Refer to Appendix D</p>

Data Validation Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>6. No XSS: storage-based Cross-Site Scripting (XSS) vulnerabilities</p> <p>The application protects against storage-based Cross-Site Scripting attacks by detecting and blocking malicious characters from all input/output handled by the application.</p>			No storage-based cross-site scripting vulnerabilities have been identified.
<p>7. No XSS: execution only storage-based cross-site scripting (XSS) vulnerabilities</p> <p>The application protects against execution only style Cross-Site Scripting attacks by detecting and blocking malicious characters from all input/output handled by the application.</p>			No execution only cross-site scripting vulnerabilities have been identified.
<p>8. No un-validated URL redirection.</p> <p>The application should check the format of the URL before redirecting.</p>			No un-validated URL redirection vulnerabilities have been identified.
<p>9. No un-validated email communication with users.</p> <p>The application validates format of data received from a user to protect against SMTP header injection, address forgery and phishing email content.</p>			Unable to test due to errors in the application.
<p>10. No SQL injection vulnerabilities</p> <p>The application protects against SQL injection attacks by ensuring all data is strong typed and not handled as strings when communicating with the database layer. For example, this can be achieved through SQL parameterised procedures.</p>			<p>A SQL injection vulnerability has been identified which increases the risk of a breach of confidentiality of the data or integrity of the database.</p> <p>Refer to Appendix D</p>
<p>11. No malicious HTML and Unicode injection vulnerabilities</p> <p>The application should protect against HTML Injection/Unicode Exploits by encoding all HTML data prior to being processed by the application.</p>			No malicious content injection vulnerabilities have been identified.
<p>12. No LDAP injection vulnerabilities</p> <p>The application validates data used in queries before making LDAP requests.</p>			No LDAP injection vulnerabilities have been identified.

Data Validation Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>13. No XPATH injection vulnerabilities</p> <p>The application validates that all XML type requests are serialised and encoded correctly to avoid possible XPATH or XML style injections.</p>			No XPATH injection vulnerabilities have been identified.
<p>14. No command injection vulnerabilities</p> <p>The application implements data validation and security controls to identify potential command injection attacks when handling and invoking OS based commands and files.</p>			No command injection vulnerabilities have been identified.













7.5 Session management



7.5.1 Description

Session management relates to the mechanisms that hold the application state data between a client and server communication. This data is retained whilst a session is established between the two devices. Typically the session values are maintained on the server with the client storing a specific unique identifier to identify itself to the server during communication. These are known as session tokens.

7.5.2 Application security criteria assessment

The following table details the application security criteria for session management mechanisms within the application:

Session Management Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>1. An established, standardised and secure session management framework is used.</p> <p>An established, standardised and secure session management framework is used.</p>			The application uses a custom session management facility. There is an increased risk that unauthorised users could gain access to the system through weak session management controls.
<p>2. Session tokens are destroyed server-side.</p> <p>The application should Secure destruction of authenticated sessions.</p>			The application does not securely destroy an authenticated session, enabling an unauthorised party to replay a previous request and gain access to confidential information.
<p>3. Session tokens use cookie security flags</p> <p>The application sets security flags on authentication Cookies, such as "HTTPOnly" and Secure.</p>			The application does not set security flags (<i>secure</i> and <i>httponly</i>) on authentication cookies, increasing the risk of information being transmitted insecurely and enabling an attacker to breach the confidentiality of the application.
<p>4. Session tokens only passed as cookies.</p> <p>Session tokens are only passed as cookies.</p>			The application only uses cookies for authentication, protecting against URL-based attacks.
<p>5. Inactive session expiry</p> <p>Session tokens should expire after a certain period of user inactivity that is appropriate to the type of application and user role.</p>			Idle session expiry timeout is not enforced – session remained active after 30 minutes of inactivity.
<p>6. Session hi-jacking prevention.</p> <p>Session tokens are validated against client information (e.g. IP address/web browser type/etc).</p>			<p>The application is vulnerable to session hi-jacking attacks.</p> <p>For example, it is possible to obtain a cookie to gain unauthorised authenticated access to the legitimate user's application account.</p>

Session Management Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>7. No cross site request forgery (CSRF) vulnerabilities</p> <p>The application should not authorise requests based only on credentials that are automatically submitted by the browser.</p>			<p>The application is vulnerable to cross-site request forgery vulnerabilities.</p> <p>The application does not differentiate between some HTTP POST and GET request types. Additionally, cross-site request forgery protection tokens (also known as one time transaction tokens) have not been observed.</p>













7.6 Data security







7.6.1 Description

Applications typically store large amounts of information about their users, transactions and history. Some or all of this information is sensitive and needs to be protected with the relevant security controls.

7.6.2 Application security criteria assessment

The following table details the common application security criteria for data security mechanisms within the application:

Data Security Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>1. Sensitive data should never be displayed.</p> <p>Sensitive data are never displayed to the user or administrator either in clear text or encrypted format.</p>			Encrypted passwords are displayed to the user which increases the risk of interception of that data by a malicious party or of an unauthorised party viewing this in a cache.
<p>2. Sensitive data should not be cached or stored client side</p> <p>The application should not allow sensitive data to be cached or stored client side.</p>			The application does not prevent the web browser from caching user information client-side.
<p>3. Sensitive data should only be available to authorised users.</p> <p>Personal data or other sensitive information should only be viewed by authorised users (i.e. system administrators should not have access to this information). This includes passwords, tax file numbers, storage and transmission.</p>			Administrators have access to user telephone records which are generally confidential and there is no demonstrated business need for this to occur.
<p>4. Production Data in Testing environments</p> <p>Sensitive production data must be handled in line with its classification.</p>			Production data is being used in the testing environment which means that confidential data could be exposed to unsafe environments such as untested code, unauthorised users, etc.
<p>5. Industry standard cryptographic algorithms are used.</p> <p>Cryptography used by the application should be implemented using Industry standard algorithms and standards. (For example, AES and TripleDES)</p>			The web server (telmax21) allows renegotiation, which is a known vulnerability. Combined with another attack, confidential data could be intercepted and be exposed to unauthorised parties.
<p>6. Use non-sequential identifiers to prevent information disclosure.</p> <p>The application should use non-sequential identifiers (i.e.. UUID, GUID, etc)</p>			Unable to test due to errors in the application

Data Security Criteria	Assessment of Findings		
	Finding	Severity	Justification
7. Storage of non-essential privacy related data. Non-essential privacy related data must not be stored.			The application does not store non-essential privacy related information.
8. Secure transmission of privacy related data. Privacy related data must be transmitted securely.			The application transmits all information using a secure channel (HTTPS).
9. No sensitive information should be passed in URLs. The application should not pass sensitive information in URLs which will get logged.			The application stores names and encrypted passwords in logs which will allow those with access to logs to impersonate a valid user.

7.7 Exception handling





7.7.1 Description

Exceptions are typically caused by either malicious or unexpected data input, or programming error. These can cause an application to stop processing information and return an exception in response to a request.

Exception handling must ensure that errors do not expose valuable information about the data flow through the application and how the application is structured.

7.7.2 Application security criteria assessment

The following table details the application security criteria for exception handling mechanisms within the application:

Exception Handling Criteria	Assessment of Findings		
	Finding	Severity	Justification
1. Generic error messages. When a failure or exception occurs, the application presents generic messages which do not disclose system failures or internal workings.			Error messages, such as 404 Not Found, disclose version numbers, which allows infrastructure enumeration. The impact of this is that attackers will be able to identify known vulnerabilities in infrastructure and potentially gain access to confidential information or gain control of VicTrack systems.
2. Logging of exception and failures. The application logs exceptions and failures.			The logs for the correct date were not provided within the testing period and for the ones provided within the testing period, they did not have an appropriate level of exception logging.

7.8 Communication security





7.8.1 Description

Applications need to communicate both internally with application components as well as with external clients and systems. Communication Security provides ways to ensure that the communication between these systems and applications is kept secure.

Typically, infrastructure based security methods such as SSL/TLS can be used to secure communication of web applications. Other forms of encryption or communication security can also be adopted.

7.8.2 Application security criteria assessment

The following table details the application security criteria for communication security mechanisms within the application:

Communications Security Criteria	Assessment of Findings		
	Finding	Severity	Justification
<p>1. Communications with client is secured.</p> <p>Communication between the client and server should be secured through the use of encryption technologies such as SSL or TLS:</p> <ul style="list-style-type: none"> - User login credentials - Sensitive application data. 			<p>All communications between the client and the server are secured.</p>
<p>2. SSL/TLS does not use weak ciphers or contain protocol weaknesses.</p> <p>The application should not allow the use of weak ciphers when encrypting traffic between the browser and the application.</p>			<p>The web server (telmax21) allows renegotiation, which is a known vulnerability.</p> <p>Combined with another attack, confidential data could be intercepted and be exposed to unauthorised parties.</p>

Appendix A – Web application testing methodology

Introduction

Web application penetration testing provides organisations with a method of identifying common application security vulnerabilities within their applications.

Penetration testing is performed at the later stages of the development lifecycle and is designed to provide a baseline for organisations against industry standards such as OWASP (Open Web Application Security Project).

Testing methodology

Testing emulated an attacker with access to the web application from the perspective of both “anonymous” (unauthenticated access) and users with valid accounts, representing authenticated attackers.

A walk-through of the application with development staff was conducted prior to testing. This enabled the Deloitte testers to gain an understanding of the functionality available to different user roles, identify areas of the application out of scope of the assessment, and to determine specific attack scenarios.

Testing was conducted using predominantly manual techniques with some tools used to assist in understanding how the application had been implemented and to automate some of the more tedious tasks, such as data validation checks, as appropriate. Log files from web application proxies were kept and further analysed to extend coverage.

Applications were tested against a set of key application security controls and associated criteria which are consistent with the OWASP guidance.

Testing criteria

The following security controls were assessed through penetration testing:

- External network intelligence gathering
- External network reconnaissance
- Vulnerability research and verification
- Authentication
- Authorisation
- Data Validation
- Session Management
- Data Security
- Exception Handling
- Communication Security.

Deloitte: VicTrack - Perimeter and Application Security Assessment

Each section covered a single security control and is structured as follows:

- Brief description of the security control
- Application security criteria assessment – the application’s compliance with the defined set of criteria, together with a justification for the rating provided
- Additional details – further information on the recommended key areas that require immediate attention are presented with evidence of non-compliance in the form of screen captures, URLs and input data, where required.

It should be noted that all types of ratings provided in sections 7.2 to 7.8 are intended to assist the reader in understanding the impact of the detailed findings in relation to each criterion, and are not intended to provide “assurance” as defined by standards issued by the Australian Auditing Standards Board.

Appendix B – Penetration testing inherent limitations

While penetration testing is an important tool used to help assess the relative security of the system or systems tested, it has a number of limitations that must be understood to ensure the correct interpretation of the results.

Due to practical considerations and cost issues, penetration tests are nearly always conducted over a limited duration. This means that not every possible test can be performed in the given time. Where possible, Deloitte will identify any additional tests which could be of value which were not performed due to time restrictions, because a potential attacker may not have time constraints.

Penetration testing is often performed in isolation, with very little background information on the nature of the system or systems that are being tested (also referred to as “blind” testing). In this case, the tester or testers will attempt a number of different attacks aimed at obtaining information about the systems and any associated vulnerabilities.

It must be noted that this type of information is often cryptic and incomplete in nature which forces the testers to draw upon their skills and experience to make appropriate interpretations of the segmentary information. Results must therefore be considered as a skilled interpretation and not absolute fact of the information collected. They should not be solely relied upon for accuracy.

Destructive tests are not conducted by Deloitte during a penetration test. However, Deloitte engineers will identify any systems considered to be vulnerable to such an attack and the nature of the vulnerability, because a potential attacker may choose to use these types of attacks.

As with all security tests, the information obtained and the results provided are only valid at the time of testing (results represent a snapshot in time). New vulnerabilities are continually being discovered. It is therefore critical that patches are kept current and security audits or penetration tests are performed regularly.

Whilst every effort is made to ensure information contained in the penetration test report is accurate and correct, due to the nature of a penetration test, Deloitte does not warrant the information contained in the report.

Appendix C – Application profile

Identification Information	
Application Name	Bilmax21
Version Number	As of testing on 21/9/2012
Developer	Trans-Mit

Application Characteristics	
Overview (purpose, users etc)	The VicTrack Bilmax system is used to provide telephone record information, including billing and calling records. This can be provided on an individual, group or organisational basis.
Technologies in which application was developed	Unknown
Underlying software (web /application / database servers etc)	Apache web server
Data/application sensitivity (e.g. internet banking; share trading; handles personal data; handles credit card data; handles payment transactions; sensitive documents etc)	The application contains sensitive information, specifically telephone calling records.
Special characteristics or requirements	None
Administration interface available over the internet?	No

Testing Information	
Production Status (In production, UAT, etc)	Testing
Testing environment (remote/on-site)	Web application - on-site
Testing window (period over which the application was tested and any time constraints)	19 September 2012 through 2 October 2012

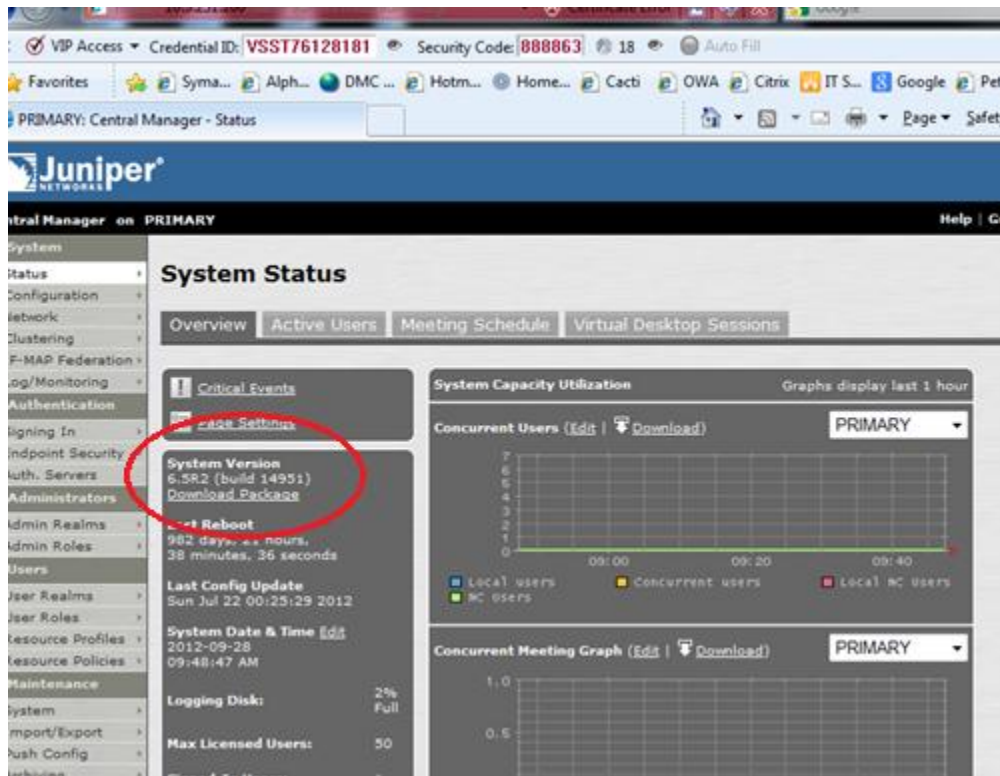
User Accounts Used For Testing	
Account Type	Account Login
Corporate access	sbelokamen
Corporate access	janastasios
Administrator	robyn.douglas@victrack.com.au
Account manager	caroline.dowell@victrack.com.au
Account manager	kristen.georgakopoulos@victrack.com.au
User	stephen.lilley@victrack.com.au

Appendix D – Detailed Support for Findings

SSL VPN security assessment

Architecture

The system version of SSL VPN is 6.5R2 and the server shows that the device hasn't been rebooted in 982 days, which would normally occur if an update was applied. The latest version is not as recommended by vendor (<http://www.juniper.net/support/products/sa/>)



Access control

Any external person may access the administrator interface.

The screenshot shows the Juniper Central Manager web interface in Internet Explorer. The browser address bar shows the URL `https://10.3.251.200/data-admin/auth/signin/policy.cgi`. The page title is "PRIMARY: Central Manager - Signing In". The interface includes a navigation menu on the left with categories like System, Authentication, Administrators, and Users. The main content area is titled "Signing In" and contains two tabs: "Sign-in Policies" and "Sign-in Pages". Under "Sign-in Policies", there are two unchecked checkboxes: "Restrict access to administrators only" and "Display multiple user sessions warning notification". Below these are buttons for "New URL...", "Delete...", "Enable", "Disable", and "Save Changes". The "Sign-in Pages" tab is active, displaying a table of administrator URLs. The table has four columns: "Administrator URLs", "Sign-In Page", "Authentication Realm(s)", and "Enabled". The entry `*/admin/` is circled in red. Below the administrator URLs table is a table for "User URLs" with the same columns. At the bottom, there is a "Meeting URLs" table.

Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */admin/	Active Directory	AD Admin Users	✓
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	✓

User URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */	Active Directory	Active Directory	✓
<input type="checkbox"/> */ext/	Non-ActiveDirectory	Non Active Directory	✓
<input type="checkbox"/> */tnms/	Active Directory	TNMS	✓
<input type="checkbox"/> */dot/	Active Directory	DOT	✓
<input type="checkbox"/> */siemens/	Active Directory	siemens	✓
<input type="checkbox"/> */iphone/	Active Directory	Active Directory	✓
<input type="checkbox"/> */transmit/	Active Directory	Active Directory	✓
<input type="checkbox"/> */Cloud/	Active Directory	Cloud	✓
<input type="checkbox"/> */BMS/	Active Directory	BMS	✓

Meeting URLs	Sign-In Page	Authentication Realm(s)	Enabled
--------------	--------------	-------------------------	---------

Cryptography

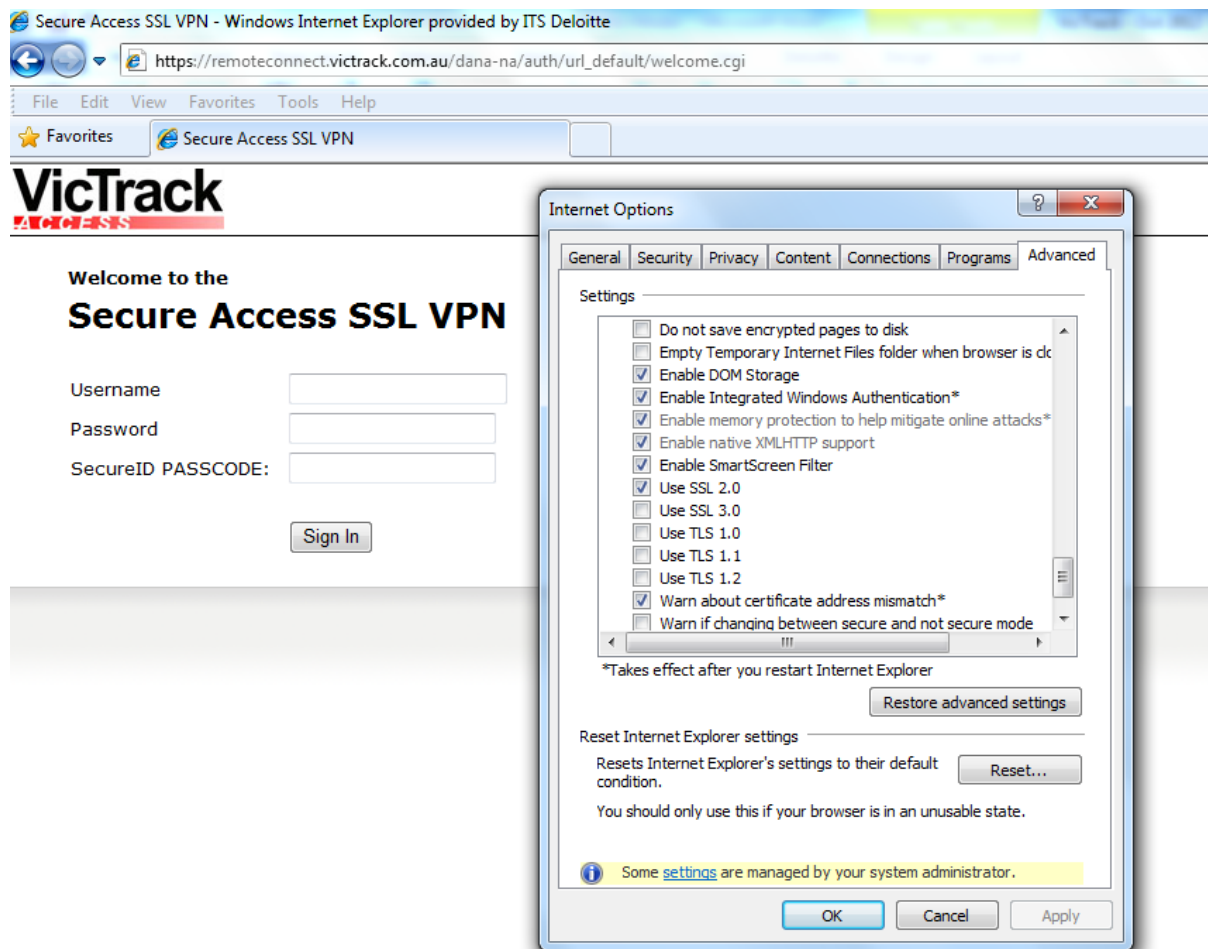


Figure 1: SSL2 access allowed to the SSL VPN

Authentication

Enforce authentication

The application allows unauthenticated users to access application pages.

The following (below) pages can be accessed and executed by an anonymous user:

URL: • <https://telmax21.victrackad.victrack.com.au/t21/topdat/common/nav/wbthelpdoc.pdf>

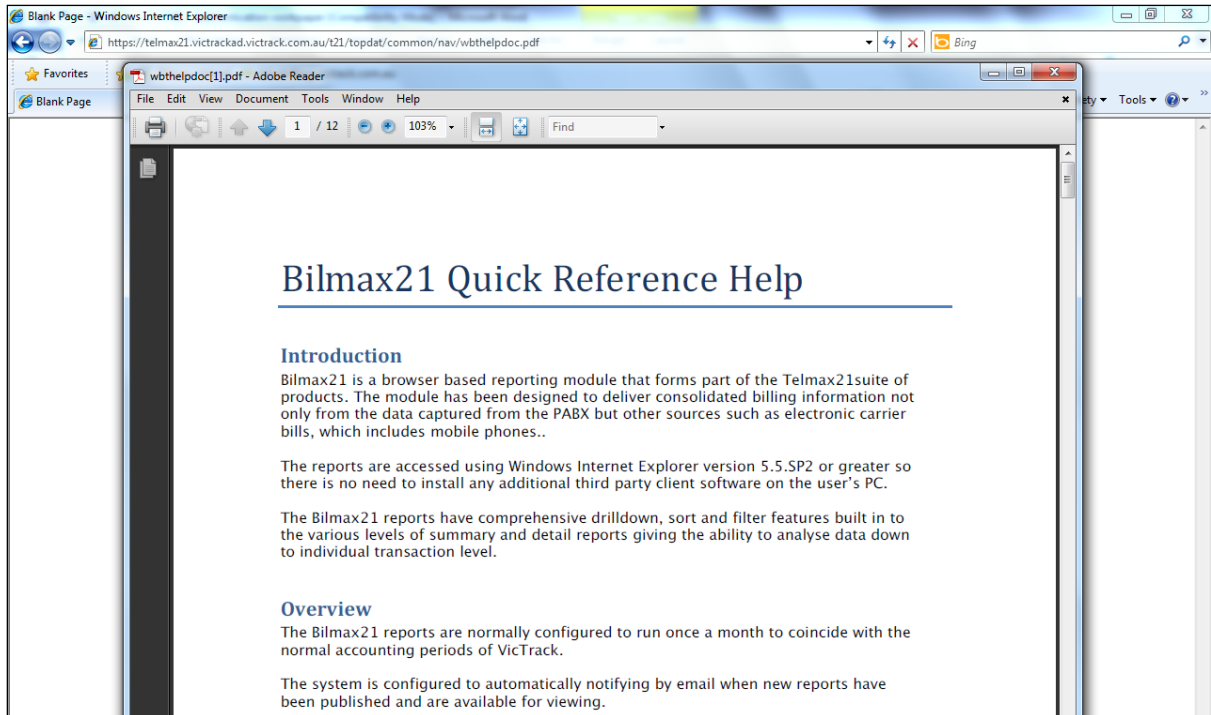


Figure 2: Access to help document

URL: • <https://telmax21.victrackad.victrack.com.au/t21/topdat/common/nav/wbtmainhome.html>

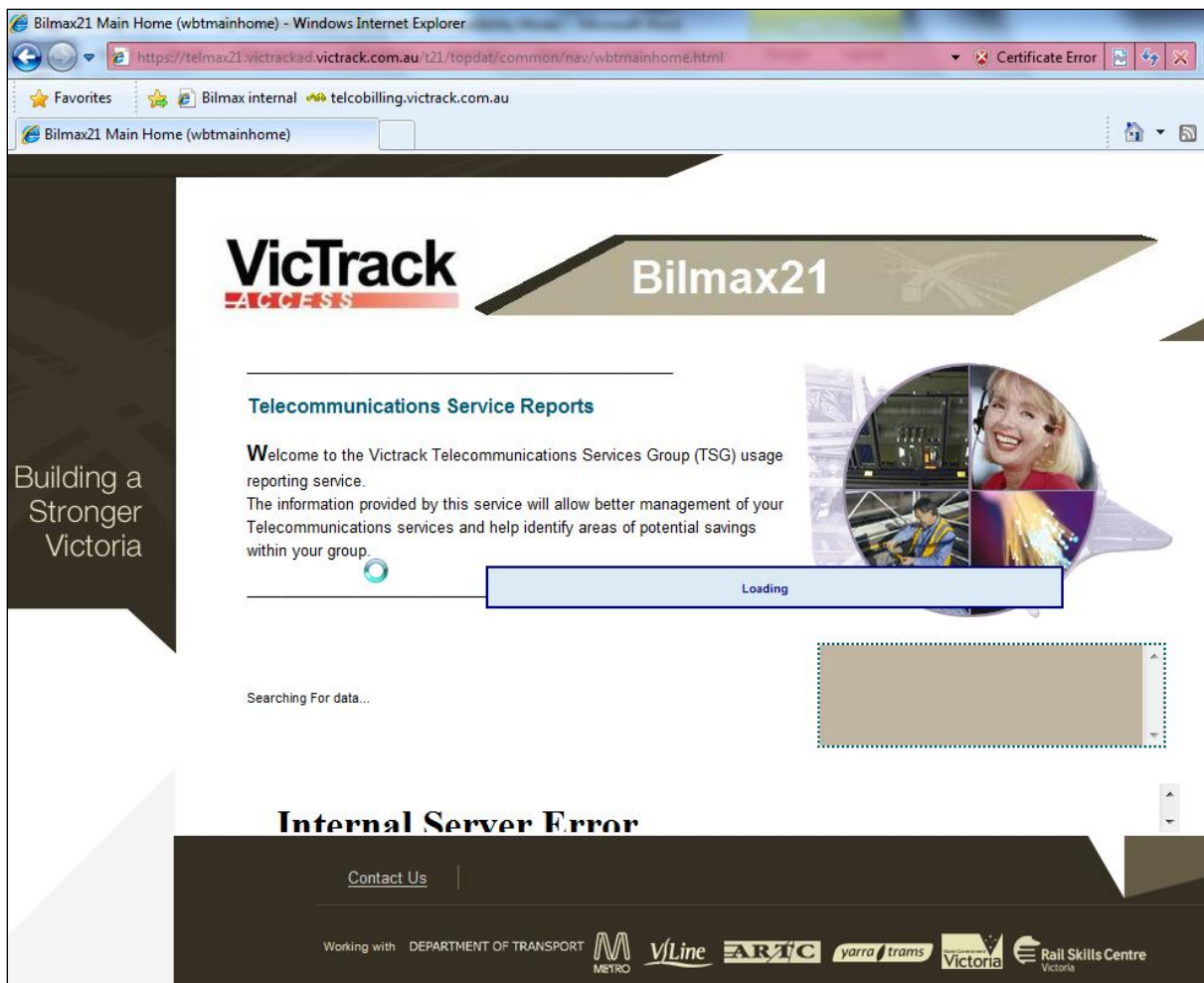


Figure 3: Access to home page

Deloitte: VicTrack - Perimeter and Application Security Assessment

Data validation

No DoS (Denial of Service) vulnerabilities

When modifying the value of the remuseradmin cookie it was observed that later, a legitimate administrative user was not able to access the administrator interface via the button. Enquired with Stephen Lilley (IT Service Delivery Manager) on 27/9/12 who advised that the developer has stated that this behaviour may be related to the exploit of this access.

```
}
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "Finding user access info for user stephen.lilley@victrack.com.au";
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "";
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
    set_wbt_web_usr ("stephen.lilley@victrack.com.au", "0x061fc70f18822130");
    set_wbt_appmode("PERSONAL");
    setCookie("entered_username", "stephen.lilley@victrack.com.au");
    setCookie("WB_recorder", "");
    setCookie("WB_loginoff", "0");
    setCookie("WB_extgrid", "");
    setCookie("WB_ACCCODE", "");
    //alert("login: document.cookie=[" + document.cookie + "]);
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
self.location.replace('wbt_telmax21.cgi')
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "Done.";
//--></SCRIPT>
</body>
</html>
```

Figure 4: Unmodified parameter

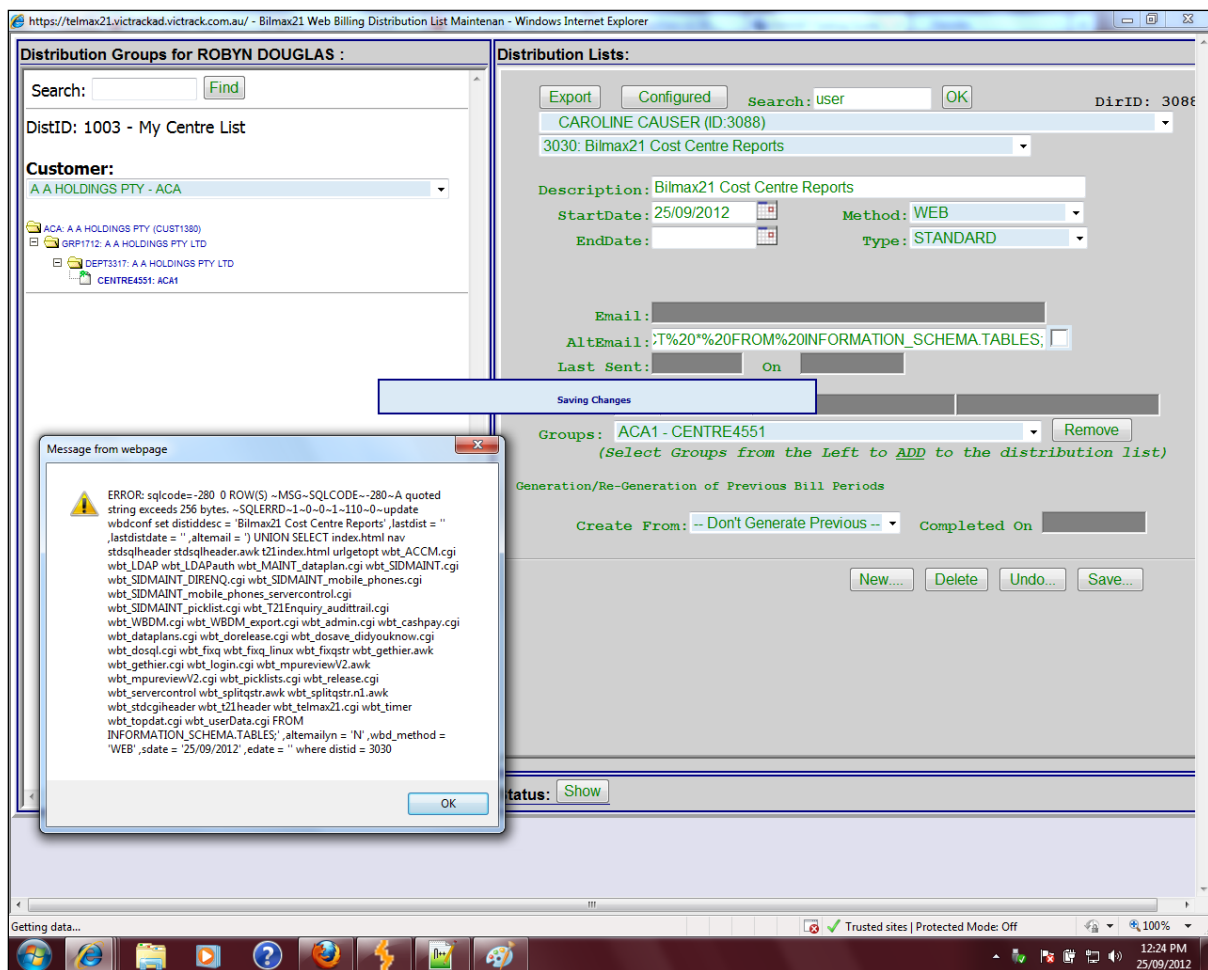


Figure 6: SQL injection result

```

=====
12:17:08 PM https://telmax21.vicrackad.vicrack.com.au:443 [10.3.0.122]
=====

POST
/t21/topdat/common/wbt_dosql.cgi?UNLID=68&DOSQLCMD="update%20wbdconf%20set%20distid%20esc%20=%20'Bilmax21%20Cost%20Centre%20Reports'%20,lastdist%20=%20''%20,lastdistdate%20=%20''%20,altemail%20=%20')%20UNION%20SELECT%20*%20FROM%20INFORMATION_SCHE%20MA.TABLES;%20,altmailyn%20=%20'N'%20,wbd_method%20=%20'WEB'%20,sdate%20=%20'25/09/2012'%20,edate%20=%20''%20where%20distid%20=%203030" HTTP/1.1

Accept: */*
Accept-Language: en-au
Referer: https://telmax21.vicrackad.vicrack.com.au/t21/topdat/common/nav/wbtWBDM.html
If-Modified-Since: Sat, 1 Jan 2000 00:00:00 GMT
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)
Host: telmax21.vicrackad.vicrack.com.au
Content-Length: 0

```

Connection: Keep-Alive
Cache-Control: no-cache
Cookie: remuser=robyn.douglas@victrack.com.au; remuserpwdes=0x061fc70f18822130;
WB_userid=robyn.douglas@victrack.com.au; remuserappmode=ADMIN;
entered_username=robyn.douglas@victrack.com.au; WB_monthtag=Jul_2012; WB_distid=1001;
WB_distiddesc=Bilmax21%20Cost%20Centre%20Reports;
WB_distidmtags=Aug_2012%7CJul_2012%7CJun_2012%7CMay_2012%7CApr_2012%7CMar_2012%7CFeb_2012%7CJan_2012%7CDec_2011%7CNov_2011%7COct_2011%7CSep_2011%7CAug_2011%7CJul_2011%7CJun_2011%7CMay_2011%7CApr_2011%7CMar_2011%7CFeb_2011%7CJan_2011%7CDec_2010%7CNov_2010%7COct_2010%7CSep_2010%7CAug_2010%7CJul_2010%7CJun_2010%7CMay_2010%7CApr_2010%7CMar_2010%7CFeb_2010%7CJan_2010%7CDec_2009%7CNov_2009%7COct_2009%7CSep_2009; WB_wbd_type=ADMIN;
WBLOGINADMINEMAIL=rod@transmit.com.au%3B%20helpdesk@victrack.com.au%3B%20robyn.douglas@victrack.com.au%3B%20steve.moodie@victrack.com.au%3B%20michael.bridges2@victrack.com.au; WBLOGINADMINEMAILSUBJECT=Bilmax21%20Query;
WBLOGINADMINEMAILBODY=Please%20include%20your%20name%2C%20phone%20number%2C%0Aand%20a%20short%20description%20of%20your%20query.%0A; WB_recordno=4668;
WB_loginoff=0; WB_extgrid=; WB_ACCCODE=; WB_ADMINDISABLED=0; WB_dodirectory=off;
WB_whichuserid=robyn.douglas@victrack.com.au; WB_wbd_method=WEB; WB_VERSION=2;
WB_RUNDAY=2

=====
HTTP/1.0 200 OK

Date: Tue, 25 Sep 2012 02:20:13 GMT

Server: Apache/2.2.6 (Unix) DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8

Connection: close

Content-Type: text/unl

Status:|SQLCODE~-280~A quoted string exceeds 256 bytes. ~SQLERRD~1~0~0~1~110~0~update
wbdconf set distiddesc = 'Bilmax21 Cost Centre Reports' ,lastdist = " ,lastdistdate = " ,altermail = '
UNION SELECT index.html nav stdsqlheader stdsqlheader.awk t21index.html urlgetopt
wbt_ACCM.cgi wbt_LDAP wbt_LDAPauth wbt_MAINT_dataplan.cgi wbt_SIDMAINT.cgi
wbt_SIDMAINT_DIRENQ.cgi wbt_SIDMAINT_mobile_phones.cgi
wbt_SIDMAINT_mobile_phones_servercontrol.cgi wbt_SIDMAINT_picklist.cgi
wbt_T21Enquiry_audittrail.cgi wbt_WBDM.cgi wbt_WBDM_export.cgi wbt_admin.cgi wbt_cashpay.cgi
wbt_dataplans.cgi wbt_dorelease.cgi wbt_dosave_didyouknow.cgi wbt_dosql.cgi wbt_fixq
wbt_fixq_linux wbt_fixqstr wbt_gethier.awk wbt_gethier.cgi wbt_login.cgi wbt_mpureviewV2.awk
wbt_mpureviewV2.cgi wbt_picklists.cgi wbt_release.cgi wbt_servercontrol wbt_splitqstr.awk
wbt_splitqstr.n1.awk wbt_stdcgiheader wbt_t21header wbt_telmax21.cgi wbt_timer wbt_topdat.cgi
wbt_userData.cgi FROM INFORMATION_SCHEMA.TABLES;' ,altermailyn = 'N' ,wbd_method = 'WEB'
,sdate = '25/09/2012' ,edate = " where distid = 3030|0

=====
Listing 1: Log of vulnerability exploit

Authorisation

Privilege escalation

Modifying the value of the Cookie parameter “remuserappmode” from “PERSONAL” to “ADMIN” allows access for a non-administrative user to a hidden high-privilege interface.

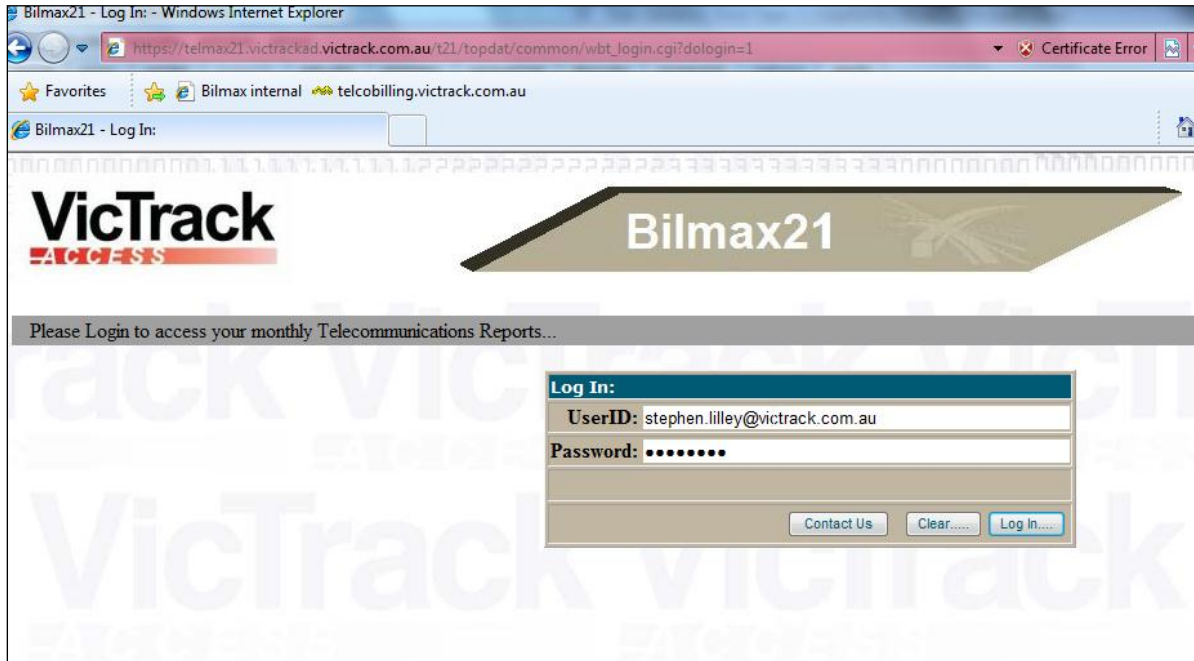


Figure 7: Vulnerability occurs at login

```
}
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "Finding user access info for user stephen.lilley@victrack.com.au";
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "";
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'>
    set_wbt_web_user("stephen.lilley@victrack.com.au", "0x061fc70f18822130");
    set_wbt_appmode("PERSONAL");
    setCookie("entire_username", "stephen.lilley@victrack.com.au");
    setCookie("WB_recorder", "");
    setCookie("WB_loginoff", "0");
    setCookie("WB_extgrid", "");
    setCookie("WB_ACCCODE", "");
    //alert("login: document.cookie=[" + document.cookie + "]);
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
self.location.replace('wbt_telmax21.cgi')
//--></SCRIPT>
<SCRIPT LANGUAGE='Javascript'><!--
window.status = "Done.";
//--></SCRIPT>
</body>
</html>
```

Figure 8: Unmodified parameter

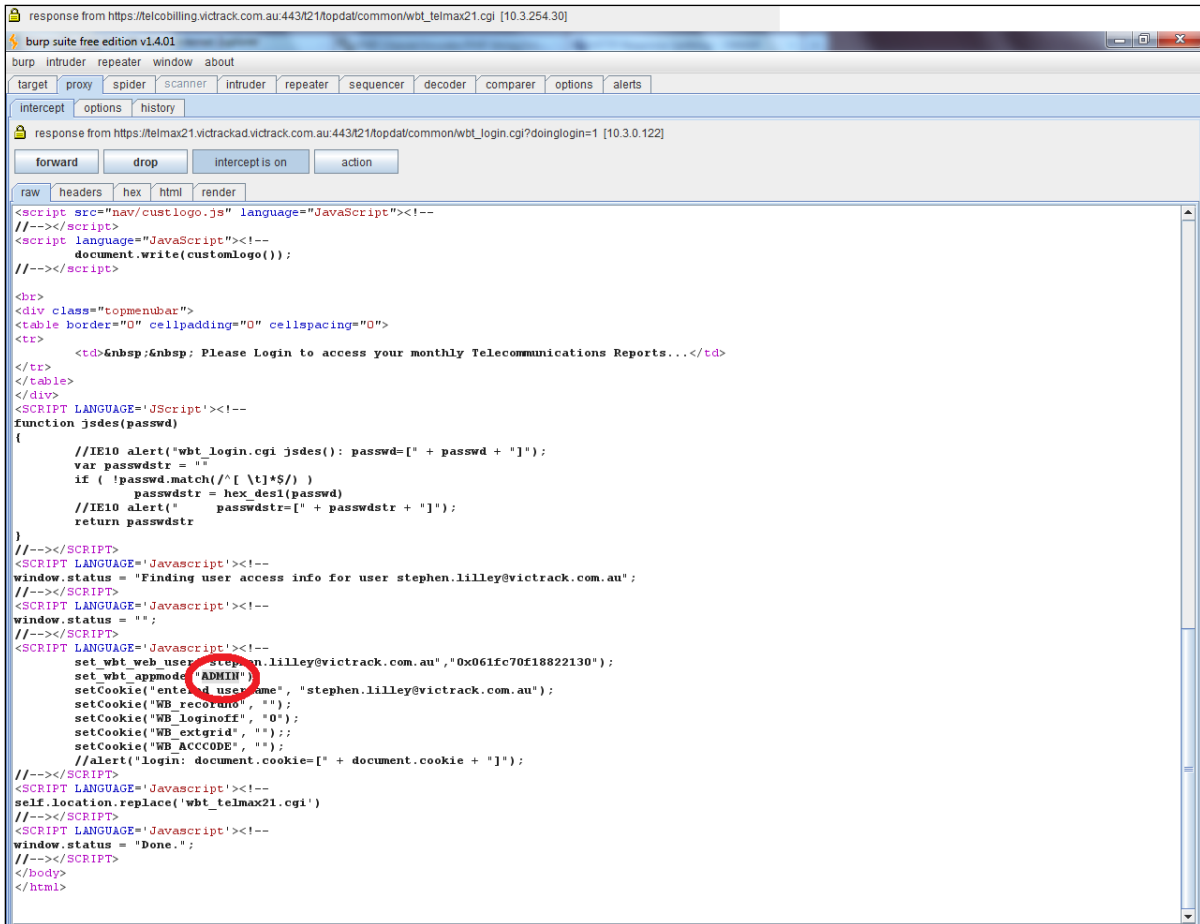


Figure 9: Modified parameter

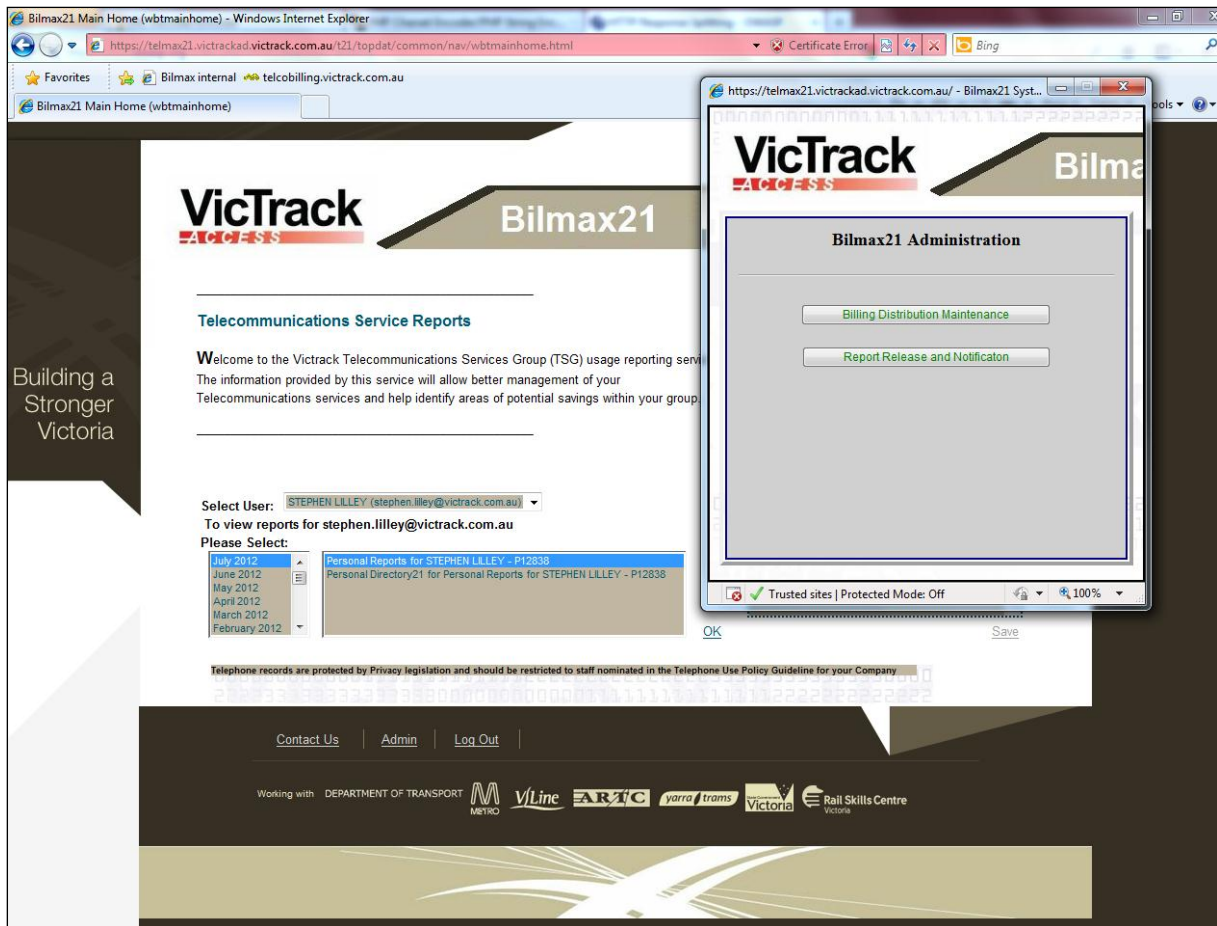


Figure 10: Escalated privileges obtained

Modifying the cookie value WB_ADMINDISABLED from 1 to 0 when connecting via the external interface will enable the Admin link for any user. This brings up a screen showing that the admin interface is disabled which is not normally available when connecting externally.

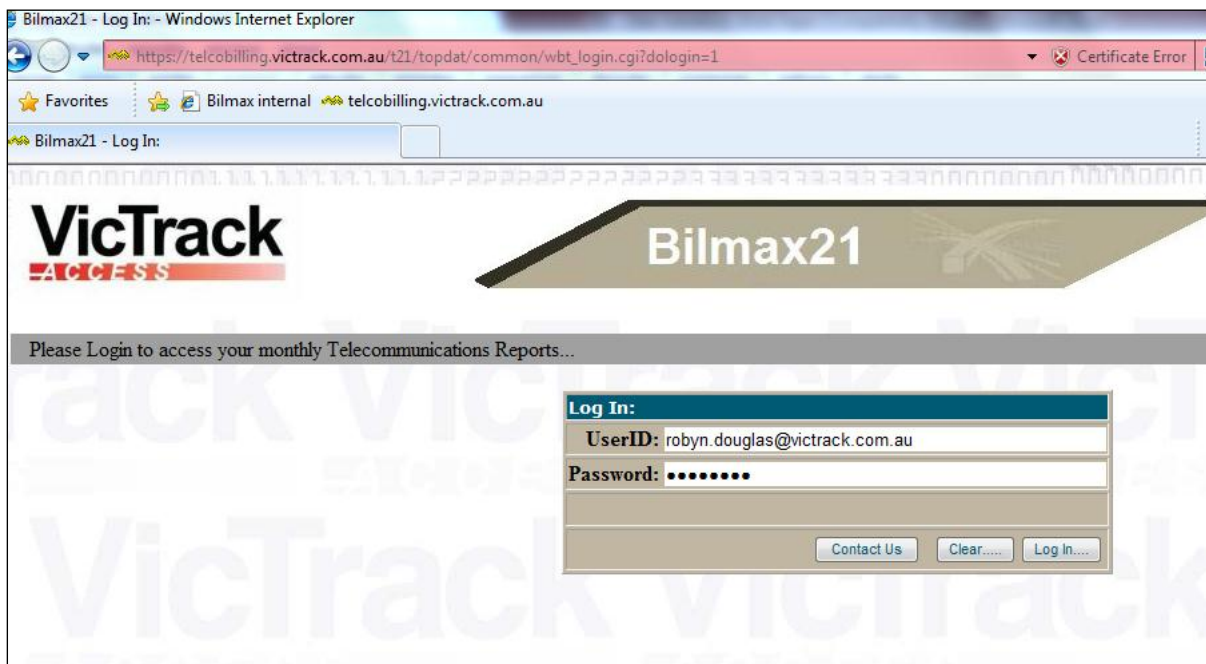


Figure 11: Vulnerability occurs at login

```

response from https://telcbilling.victrack.com.au:443/t21/topdat/common/wbt_telmax21.cgi [10.3.254.30]
forward drop intercept is on action
raw headers hex html render
<SCRIPT SRC='nav/t21lib.sct' LANGUAGE='JScript.Encode'><!--
//--></SCRIPT>
<SCRIPT SRC='nav/wbt.sct' LANGUAGE='JScript.Encode'><!--
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript' FOR='window' EVENT='onunload'><!--
//alert("wbt_stdcgiheader: window onunload")
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "Finding user access info for user robyn.douglas@victrack.com.au";
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "";
//--></SCRIPT>
<SCRIPT LANGUAGE="JavaScript"><!--
//alert("wbt_telmax21.cgi header alert")
//--></SCRIPT>
</head>
<body bgcolor='white'>
<STYLE>
.topmenubar { background: #A0A0A0; }
.topmenubar { padding-top: 2px; }
.topmenubar { padding-bottom: 2px; }
.topmenubar { padding-left: 2px; }
.topmenubar { padding-right: 2px; }
.topmenubar A { font-size: 8pt; font-family=Helvetica; }
.topmenubar A { color: white; font-weight: bold; text-decoration: none }
.topmenubar A:Hover { color: white; background: red }
</STYLE>
<script src="nav/custlogo.js" language="JavaScript"><!--
//--></script>
<script language="JavaScript"><!--
document.write(customLogo());
//--></script>
<br>
<SCRIPT LANGUAGE='JavaScript'><!--
//alert("Go wbt main home")
setCookie("WB_ADMINDISABLED", "1")
location.replace("nav/wbtmainhome.html")
//--></SCRIPT>
Telmax21 Billing
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "Done.";
//--></SCRIPT>
</body>
</html>

```

Figure 12: Original unmodified cookie


```

response from https://telcobilling.victrack.com.au:443/t21/topdat/common/wbt_telmax21.cgi [10.3.254.30]
response from https://telcobilling.victrack.com.au:443/t21/topdat/common/wbt_telmax21.cgi [10.3.254.30]
forward drop intercept is on action
raw headers hex html render
<SCRIPT SRC='nav/t21lib.sct' LANGUAGE='JScript.Encode'><!--
//--></SCRIPT>
<SCRIPT SRC='nav/wbt.sct' LANGUAGE='JScript.Encode'><!--
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript' FOR='window' EVENT='onunload'><!--
//alert("wbt_stdcgiheader: window onunload")
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "Finding user access info for user robyn.douglas@victrack.com.au";
//--></SCRIPT>
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "";
//--></SCRIPT>
<SCRIPT LANGUAGE="JavaScript"><!--
//alert("wbt_telmax21.cgi header alert")
//--></SCRIPT>
</head>
<body bgcolor='white'>
<STYLE>
.topmenubar { background: #A0A0A0; }
.topmenubar { padding-top: 2px; }
.topmenubar { padding-bottom: 2px; }
.topmenubar { padding-left: 2px; }
.topmenubar { padding-right: 2px; }
.topmenubar A { font-size: 8pt; font-family=Helvetica; }
.topmenubar A { color: white; font-weight: bold; text-decoration: none }
.topmenubar A:Hover { color: white; background: red }
</STYLE>
<script src="nav/custlogo.js" language="JavaScript"><!--
//--></script>
<script language="JavaScript"><!--
document.write(customlogo());
//--></script>
<br>
<SCRIPT LANGUAGE='JavaScript'><!--
//alert("Go wbt main home")
setCookie("WB_ADMINDISABLED" "0")
location.replace("nav/wbtmain_ome.html")
//--></SCRIPT>
Telmax21 Billing
<SCRIPT LANGUAGE='JavaScript'><!--
window.status = "Done.";
//--></SCRIPT>
</body>

```

Figure 13: Changed value

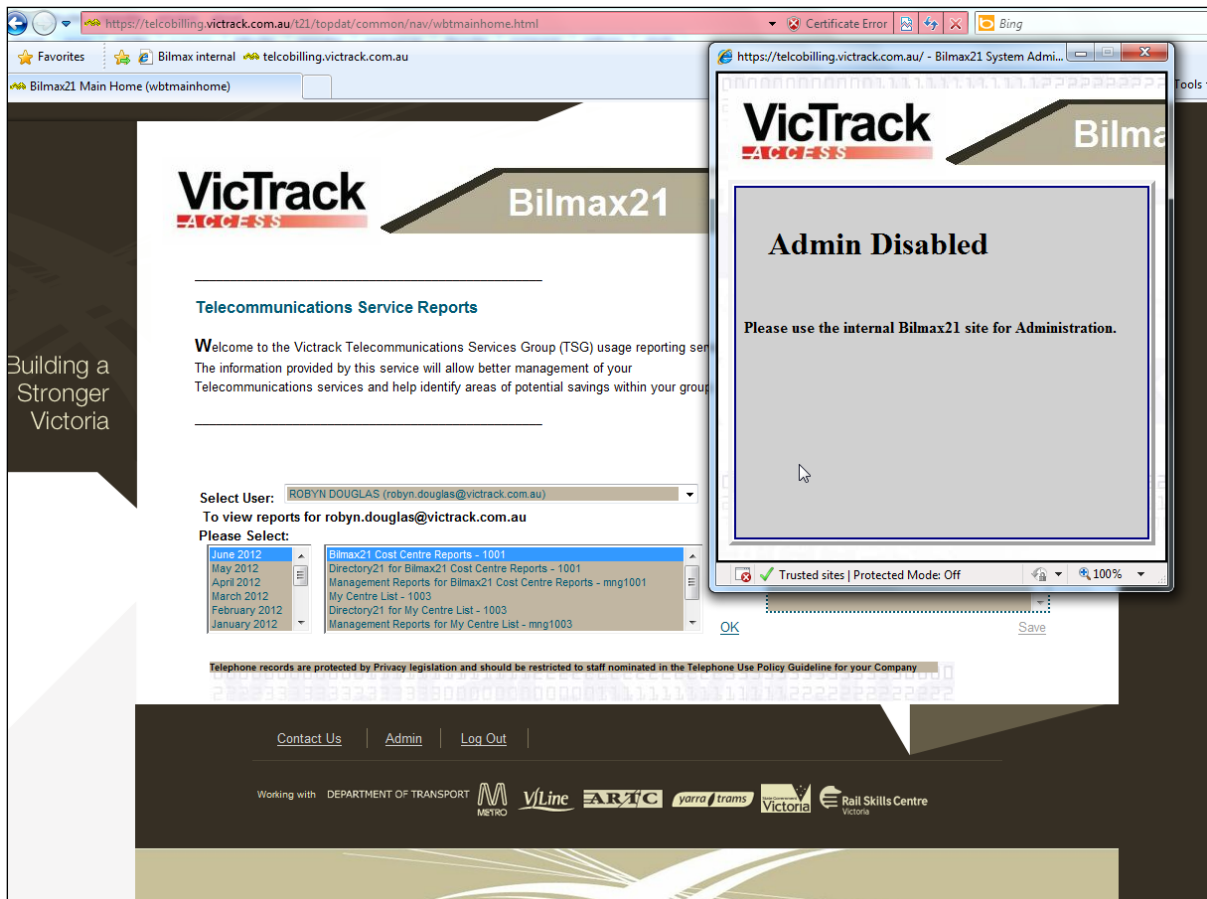


Figure 14: Button enabled and access to screen normally hidden

Cookies sending password

Instead of using a token value to maintain a session, the application stores all users' encrypted passwords as cookies on the client machine. This encrypted password is accepted as the legitimate method of authentication to the application.

26	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbtPB.sct	304	206	sct			10.30.122
25	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbtservercontrol.sct	304	206	sct			10.30.122
24	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbtgetunl.sct	304	206	sct			10.30.122
23	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbtmainhome.html	304	206	HTML	html		10.30.122
22	https://telmax21.victracka.com.au	GET	/t21/topdat/common/wbt_telmax21.cgi	200	2321	HTML	cgi	Bilmax21:	10.30.122
21	https://telmax21.victracka.com.au	POST	/t21/topdat/common/wbt_login.cgi?doinglogin=1	200	3814	HTML	cgi	Bilmax21 - Logi...	10.30.122
20	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/des1.js	304	206	script	js		10.30.122
19	https://telmax21.victracka.com.au	GET	/t21/topdat/common/wbt_login.cgi?dologin=1	200	5893	HTML	cgi	Bilmax21 - Logi...	10.30.122
18	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbt.sct	304	206	sct			10.30.122
17	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/wbt2lib.sct	304	207	sct			10.30.122
16	https://telmax21.victracka.com.au	GET	/t21/topdat/common/wbt_telmax21.cgi	200	1371	HTML	cgi	Bilmax21:	10.30.122
12	https://telmax21.victracka.com.au	GET	/t21/topdat/common/nav/custtogo.js	304	205	script	js		10.30.122
11	https://telmax21.victracka.com.au	GET	/t21/topdat/index.html	304	205	HTML	html		10.30.122
10	https://telmax21.victracka.com.au	GET	/	200	402	HTML		Welcome to the	10.30.122


```

request response
raw params headers hex
GET /t21/topdat/common/nav/wbtmainhome.html HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-AU
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)
Accept-Encoding: gzip, deflate
If-Modified-Since: Sun, 26 Aug 2012 11:21:23 GMT; length=9725
Host: telmax21.victrackad.victrack.com.au
Connection: Keep-Alive
Cookie: WB_monthtag=; WB_distid=; WB_distiddesc=; WB_distidmtags=; WB_wbd_type=; WBLOGINADMINEMAIL=rod@transmit.com.au43B420he1pdesk@victrack.com.au43B420robyn.douglas@victrack.com.au43B420michadges@victrack.com.au; WBLOGINADMINEMAILSUBJECT=Bilmax21; WBLOGINADMINEMAILBODY=Please%20include%20your%20name%20and%20phone%20number%20and%20a%20short%20description%20of%20your%20query.%20; remuser=robyn.douglas@victrack.com.au; remuseruid=0x061fc70f18822130; WB_userid=robyn.douglas@victrack.com.au; remuserappmode=ADMIN; entered_username=robyn.douglas@victrack.com.au; WB_recordno=4668; WB_loginoff=0; WB_extgrid=; WB_ACCCODE=; WB_ADMINDISABLED=0
  
```

Figure 15: Screenshot highlighting the obfuscated password being sent as a cookie

POST /t21/topdat/common/wbt_topdat.cgi?tdf=%22Feb_2012/data/wbttop.csv%22 HTTP/1.1

Deloitte: VicTrack - Perimeter and Application Security Assessment

```
Accept: */*
Accept-Language: en-au
Referer: https://telmax21.victrackad.victrack.com.au/t21/topdat/common/nav/wbtmainhome.html
If-Modified-Since: Sat, 1 Jan 2000 00:00:00 GMT
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)
Host: telmax21.victrackad.victrack.com.au
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:
WBLOGINADMINEMAIL=rod@transmit.com.au%3B%20helpdesk@victrack.com.au%3B%20robyn.douglas@victrack.com.au%3B%20steve.moodie@victrack.com.au%3B%20michael.bridges2@victrack.com.au; WBLOGINADMINEMAILSUBJECT=Bilmax21%20Query;
WBLOGINADMINEMAILBODY=Please%20include%20your%20name%2C%20phone%20number%2C%0Aand%20a%20short%20description%20of%20your%20query.%0A;
remuser=stephen.lilley@victrack.com.au; remuserpwdes=0x061fc70f18822130;
WB_userid=stephen.lilley@victrack.com.au; remuserappmode=PERSONAL;
entered_username=stephen.lilley@victrack.com.au; WB_recordno=; WB_loginoff=0; WB_extgrid=;
WB_ACCCODE=; WB_ADMINDISABLED=0
```

Listing 2: Session details being passed by cookie

Appendix E – Internal Audit Rating Guidance

Internal Control Ratings

The Internal Control Ratings have been set to allow allocation of resources to the areas of greatest concern.

Rating	Definition
High	Significant control weaknesses identified
Medium	Several control weaknesses of concern identified
Low	Small number of minor control weaknesses / opportunities for improvement identified

Engagement Ratings Definitions

An overall rating scale for each engagement has been set to allow allocation of resources to the areas of greatest concern. Outlined below are the ratings and their definitions. It should be noted that these ratings do not represent a “conclusion” as defined by Australian Standard on Assurance Engagements.

Rating	Definition
Effective	Key controls are systematic or applied consistently across the area subject to examination. Issues identified are isolated or relate to future plans. Areas where controls require improvement are relatively minor or low risk to the process subject to examination.
Satisfactory	Key controls are consistently applied in most cases across the area subject to examination. Only isolated high or medium issues have been identified. For those areas where controls were not effective, the key controls are supported by satisfactory mitigating activities. Other control issues are relatively minor or low risk to the process subject to examination.
Requiring improvement	Several key controls are not systematic or consistently applied in the area subject to examination. One or more high items have been reported or a number of medium items that represent an internal control risk to the process subject to examination and require improvement within an appropriate timeframe.
Unsatisfactory	Key controls are not systematic or consistently applied in the area subject to examination. High or medium issues reported are either numerous or have a high level of severity. The absence of effective key controls represents a major internal control risk to the process subject to review and requires immediate attention.

Appendix F – MDM Recommendations

MDM Recommendations

Based on: Victorian Rail Track – Mobile Device Security Policy, IS-PO 014; version: 0.8.

1. Shift device management and security away from users to technology based controls:
 - a. Device ‘rooting’ or ‘jailbreak’ detection and action (for example: isolate and deny access to offending device).
 - *Please note: ‘jailbreak’ and ‘rooting’ (unlocking) of the device does not necessarily imply that this has been performed by the device owner. Unlocking the device could be performed silently and without user’s knowledge or visual feedback. For example, if the device is compromised or infected by malware. To address this scenario – the device should be isolated and administrators alerted.*
 - b. VicTrack should periodically perform device assessment to monitor installed applications that may be malicious or not allowed in accordance with acceptable usage policy.
2. Standard vendor supplied operating systems (firmware) upgrades (e.g. Android OTA updates and new iOS releases) should not force the MDM solution to become unstable or unsupported. A standard SLA with the MDM supplier should be established to avoid the MDM solution lagging in support of newly updated mobility devices.
3. While the MDM solution has GPS tracking capabilities, users should be given an option and configuration guide how-to to disable this feature on their devices should they chose to do so. Please note: geo-tracking should not be enabled if the devices belong to individual i.e. for BYOD environment and/or if it is against the security and privacy regulations.
4. VicTrack should enforce mobility device security policy and consequential actions on the device. For example, the device should be forced to use four digit PIN based authentication (e.g. PIN instead of pattern on Android passed devices) and perform remote wipe of the device if the device detects multiple incorrect PIN entry attempts (e.g. no less than 7 entry attempts and no more than 10). This is a remote data security protection measure and should not be controlled by the end user/device owner if the mobility device has access to VicTrack data and/or network.
 - This can be achieved by configuring the MDM to push profile policies to all the devices. The following settings should be checked at the minimum:
 - Require password on device
 - Password complexity
 - Idle screen time-out
 - Password age
 - Password history.

5. The MDM solution should not differentiate between levels of security enforcement across devices – between VicTrack fleet devices and BYO device (i.e. the impact of a potential data compromise does not vary between private and fleet devices, neither should the security measures).
6. VicTrack should consider an anti-virus solution to be installed as part of its MDM deployment and device provisioning.
7. VicTrack should consider use of certificates to establish trust and identity of the device. Certificate-based authentication provides another form of authentication, in addition to the user credentials, to prove the identity of the device and user who is trying to access. Only devices with a valid client certificate and a trusted root certificate should be allowed to synchronize and communicate with corporate network, applications and/or data.
8. VicTrack should consider investigating and usage of Data Leakage Prevention (DLP) facilities of the MDM solution.
9. VicTrack should consider investigating and usage of mobility device disk encryption and 'security container' facilities of the MDM solution.
10. VicTrack should consider adding restrictions on usage of connectivity services such as NFC, Infrared, Bluetooth and public WiFi hotspots for MDM connected devices (e.g. accessing an insecure hotspot may result in compromise of mobile device or data interception attacks)