



...making excellence a habit.™

Web Application Test Report

Dragon InfoSec
Teetum Wallet (Retest)

BSI Reference: CSIRUKPRJ-336-RPT-01

Version: 1.0

6th December 2018

Testing Team

Mark Woan



Document Control Information

1.1 Document Details

Property	Value
Client	Dragon InfoSec
Title	Teetum Wallet Web Application Retest Report
Author	Mark Woan
Version	1.0
Date	06/12/2018
Document Reference	CSIRUKPRJ-336-RPT-01
Status	Definitive

1.2 Revision History

Version	Date	Author	Summary of Changes
0.1	28/11/2018	Mark Woan	Initial Draft
0.2	04/12/2018	Daniel Elliott	Internal QA
1.0	06/12/2018	Daniel Elliott	Definitive Issue

1.3 Approvals

Name	Organisation	Role
Peter Viranyi	BSI Cybersecurity and Information Resilience	Head of Security Testing

1.4 Distribution

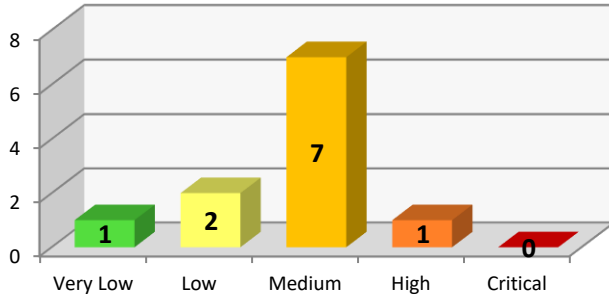
Name	Organisation	Role
Peter Viranyi	BSI Cybersecurity and Information Resilience	Head of Security Testing
Richard Dennis	Dragon InfoSec	CTO

Table of Contents

- DOCUMENT CONTROL INFORMATION..... 2**
 - 1.1 Document Details2
 - 1.2 Revision History2
 - 1.3 Approvals.....2
 - 1.4 Distribution2
- 2 EXECUTIVE SUMMARY 4**
- 3 INTRODUCTION 5**
 - 3.1 Approach5
 - 3.2 Scope5
- 4 RESULTS OF WEB APPLICATION TESTING 6**
 - 4.1 Application Available Over Unencrypted HTTP6
 - 4.2 Stored Cross-Site Scripting7
 - 4.3 No Lockout after Multiple Login Failures9
 - 4.4 Inadequate Application Session Timeouts10
 - 4.5 Unverified Password Change11
 - 4.6 Unverified Email Change12
 - 4.7 User Account Enumeration13
 - 4.8 Potential Private Key Information Leakage14
 - 4.9 Private Key Download Did Not Require Reauthentication16
 - 4.10 Private Key Email Did Not Use Archive Encryption17
 - 4.11 Unverified Smart Authentication Disable18
 - 4.12 Information Disclosure Through HTTP Headers.....19
 - 4.13 Insecure TLS Version Supported20
 - 4.14 Unauthorised Device History Deletion.....21
 - 4.15 Login IP Geo-Location Incorrect.....22
- 5 SUMMARY OF FINDINGS 23**
 - 5.1 Results of Web Application Testing23
- APPENDIX A - TESTING TEAM 26**
- APPENDIX B - FINDINGS DEFINITIONS 27**

2 Executive Summary

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a web application penetration test against the Teetum Wallet web application. Testing was undertaken remotely between the 26th and 27th November 2018.



This graph illustrates the level of risk that is exposed across the systems tested. It shows the number of vulnerabilities identified during this assessment along with their severity.

As can be seen from the graphs above, high areas of risk have been identified within the application.

The application was previously tested in September 2018 under the reference IA14347. The previous assessment identified a total of eight issues, classified as three high, three medium, one very low risk and one informational issue.

Finding	Issue	Risk	Status
1	Application Uses Clear Text HTTP Protocol	High	Fixed
2	Stored Cross-Site Scripting	High	Ongoing
3	No Account Lockout	High	Fixed
5	Unverified Password Change	Medium	Ongoing
6	Unverified Email Address Change	Medium	Fixed
7	User Account Enumeration	Medium	Ongoing
14	Unauthorised Device History Deletion	Very Low	Unknown
15	Login IP Geo-Location Incorrect	Informational	Fixed

In addition to the ongoing issues previously identified, BSI identified a further seven issues, classified as five medium and two low risk.

The newly identified medium risk issues primarily relate to a lack of user verification when performing account functions such as password modification, downloading of wallet information, disabling of authentication protection. The remaining medium risk issues include:

- A lack of encryption when emailing the user’s wallet details which if accessed by an attacker, would result in the attacker gaining control of the wallet
- A potential disclosure of the user’s private wallet information, which potentially could be used to gain access to the user’s wallet
- No session timeout within the application which increases the window of opportunity where an attacker with local access could use application as the targeted user

3 Introduction

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a web application penetration test against the Teetum Wallet web application. Testing was undertaken remotely between the 26th and 27th November 2018.

The application was previously tested in September 2018 under the reference IA14347.

3.1 Approach

All testing was carried out using BSI Cybersecurity and Information Resilience standard testing methodology. A full copy of this methodology can be provided on request.

3.2 Scope

The scope of the engagement was as follows:

- Perform a retest of the application;
- Test new functionality including the Bitcoin to Teetum conversion and 2FA.

3.2.1 Limitations



The following limitations were identified:

- BSI were unable to test the individual **2 Step Verification** settings (login, transactions, settings) as the server returned an **Invalid permissions** error for each request;
- BSI were unable to change the **Phone** number associated with the test account;
- BSI were unable to test the **Bitcoin to Teetum** conversion functionality as only the card payment functionality was working;
- BSI were unable to carry out any retesting against finding 14.

4 Results of Web Application Testing

This section provides the detailed findings of the web application testing that was performed between the 26th and 27th November 2018.

4.1 Application Available Over Unencrypted HTTP

Finding No 1.	Systems Affected	https://wallet.temtum.com/		
	Finding	The web application was available over the unencrypted HTTP protocol		
	CVE Number	N/A		
	Impact	5		
	Likelihood	3		
	Overall Risk Rating	15 (High Risk)		
	Status	RESOLVED		

4.1.1 Retest Status

The application was only available over the encrypted HTTP protocol. This finding is now resolved.

4.1.2 Summary

The clear text HTTP protocol provides no encryption of the communication between the web browser and the application, including any authentication details and data transferred.

4.1.3 Technical Details

Due to the lack of encryption provided by the HTTP service, an attacker who is able to monitor a session would be able to view all of the authentication credentials and data transmitted in the session. The attacker could then attempt to gain unauthorised access to the application using the authentication credentials extracted from the session and potentially gain access under the context of that user.

Further information relating to this issue can be found in the following OWASP document:

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

4.1.4 Recommendation

BSI recommends that the HTTP service be replaced with the cryptographically secure alternative HTTPS.

4.2 Stored Cross-Site Scripting

Finding No 2.	Systems Affected	https://wallet.tentum.com/		
	Finding	A stored Cross-Site Scripting (XSS) vulnerability was identified which could be exploited by an authenticated user.		
	CVE Number	CWE-79		
	Impact	4		
	Likelihood	3		
	Overall Risk Rating	12 (High Risk)		
	Status	ONGOING		

4.2.1 Retest Status

The application has been modified since the last test and the injected HTML did not appear to affect the user interface displayed to the user, however, the underlying HTML was still accepted by the application. This issue is not resolved.

4.2.2 Summary

Stored Cross-Site Scripting vulnerabilities occur when data entered by one user is stored within the application and then later displayed to other users without being sufficiently filtered or validated. A common scenario which may present this vulnerability would be a forum where users can submit their own posts.

This vulnerability would be exploited by an attacker by entering malicious code into a page which is then stored within the web application. A victim would then navigate to the page through normal use of the application and the malicious script would execute in the user’s browser within their security context.

An attacker who successfully exploits this issue could hijack application user accounts and run malicious code on the client machines.

4.2.3 Technical Details

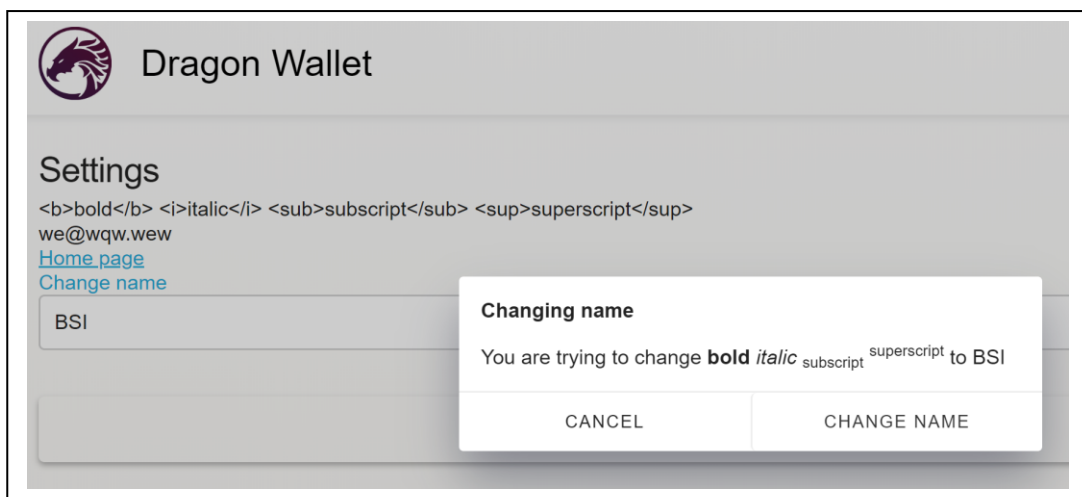
Stored Cross-Site Scripting vulnerabilities were identified in the **change name** functionality. The application attempted to validate the user input, however, the validation was only performed on the client-side.

An example of a HTTP POST request (edited for brevity) used to submit a name value with invalid characters is shown below:

```
POST /user/change/name HTTP/1.1
Host: 54.38.214.253:9001
Content-Length: 15
Accept: application/json, text/plain, */*
Origin: http://54.38.214.253
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjViODkzNGViNGE1ZDI3MDhiZmNhMmVjMCI6ImV4cCI6MTUzNzE5MTc2MSwiYWFWF0IjoxNTM3MTkwODYxQ.1nEisiHuL0SX_qIm-vodBP74WqaA_4RwsPGaH4XOp_E
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/json; charset=UTF-8
Referer: http://54.38.214.253/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB, en-US; q=0.9, en; q=0.8
Connection: close

{"name":"<b>bold</b> <i>italic</i> <sub>subscript</sub> <sup>superscript</sup>"}
```

The result of the injected HTML characters can be seen in the screenshot below:



The instance of XSS identified required that the user was authenticated to the application, reducing the likelihood of an unauthorised attacker exploiting this vulnerability. The issue could potentially be used to perform an attack against administrative users that have visibility of the user's name data.

Successful exploitation of the most critical of these vulnerabilities could allow an attacker to gain valid credentials to the application.

4.2.4 Recommendation

BSI recommends that all client supplied input is sufficiently filtered before being echoed back to the client's browser. Input validation should be carried out on all input fields to ensure that only input that matched an expected pattern is accepted. In addition, the application should implement output encoding to ensure that any potential unsafe data is properly encoded or escaped to prevent execution within the client's browser.

Further information relating to this issue can be found in the following OWASP documents:

[https://www.owasp.org/index.php/Cross-site Scripting \(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

[https://www.owasp.org/index.php/XSS \(Cross Site Scripting\) Prevention Cheat Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

4.3 No Lockout after Multiple Login Failures

Finding No 3.	Systems Affected	https://wallet.tentum.com/		
	Finding	The application did not enforce an account lockout policy		
	CVE Number	N/A		
	Impact	4		
	Likelihood	3		
	Overall Risk Rating	12 (High Risk)		
	Status	RESOLVED		

4.3.1 Retest Status

The application has been modified to limit access after a set number of fail login attempts. The application has also introduced Two Factor Authentication (2FA) for the login process. This finding is now resolved.

4.3.2 Summary

The application login page does not protect against brute force password guessing attacks

4.3.3 Technical Details

It was possible to attempt unlimited attempts to login to a given user account.

An attacker could use this vulnerability in order to carry out a password brute-force attack in order to obtain the correct password for known user accounts. If successful, this would allow the attacker to gain unauthorised access to the application and its data under the context of the compromised user account.

The password policy was enforced with the following parameters:

- Eight characters minimum length
- Mix of lower- and upper-case alphanumeric characters
- Mix of numeric and alphanumeric characters, and special characters

4.3.4 Recommendation

BSI recommends that an account lockout policy be enforced for incorrect login attempts in line with the organisation's password policy requirements.



An example of a secure lockout policy is:

- Lockout after 3-5 unsuccessful attempts.

The exact policy should be based on the sensitivity of the application.

BSI highly recommends that Two Factor or Multi-Factor authentication be implemented and enforced for all logins and transaction authorisations.

4.4 Inadequate Application Session Timeouts

Finding No 4.	Systems Affected	https://wallet.tentum.com/		
	Finding	The web application was found to have inadequate session timeouts configured		
	CVE Number	N/A		
	Impact	3		
	Likelihood	3		
	Overall Risk Rating	9 (Medium Risk)		
	Status	ONGOING		

4.4.1 Summary

The application sessions did not expire after a period of inactivity. Session timeouts help protect applications against session hijacking.

Session tokens that do not expire can allow an attacker unlimited time to guess or brute-force a valid authenticated session token. If a user's cookie is captured or brute-forced, then an attacker can use these session tokens to gain unauthorised access to that user's web accounts. This issue is particularly severe in shared environments, where multiple users have access to individual workstations.

4.4.2 Technical Details

Testing identified that a valid login session did not expire after a period of inactivity of over 5 hours.

Session timeout management and expiration must be enforced server-side. If the client is used to enforce the session timeout, for example using the session token or other client parameters to track time references (e.g. number of minutes since login time), an attacker could manipulate these to extend the session duration.

Further information relating to this issue can be found in the following OWASP document:

https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Automatic_Session_Expiration

4.4.3 Recommendation

BSI recommends that all login sessions be terminated and users logged out after a set period of inactivity.

For highly protected applications this should be set to from 5 minutes to no more than 20 minutes for low risk applications. The exact session timeout should be determined based on the risk profile of the application.

4.5 Unverified Password Change

Finding No 5.	Systems Affected	https://wallet.tentum.com/			
	Finding	User password could be updated without verifying the current user			
	CVE Number	N/A			
	Impact	4			
	Likelihood	2			
	Overall Risk Rating	8 (Medium Risk)			
	Status	ONGOING			

4.5.1 Retest Status

Retesting identified that this issue was still present within the application. This finding is not resolved.

4.5.2 Summary

The password change functionality permitted the modification of the user’s current password without verifying the authenticity of the user.

4.5.3 Technical Details

The application allows an account's password to be changed whilst authenticated without requiring the existing (old) password to be entered, i.e. without verifying the authenticity of the user.

Therefore, if the account is temporarily compromised e.g. via SQL Injection; XSS; CSRF; session hijacking; or similar, the attacker would be able to change the password on the account without requiring any knowledge of the existing password. As such they would lock out the legitimate user and effectively seize control of the account.

4.5.4 Recommendation

BSI recommends that the application be modified to require users to input the current password of the account prior to permitting the password change. The server should then use the password submitted to verify the authenticity of the user submitting the request and check that they are permitted to make such a change.

Best practice would be for the request to be given a threshold number of password change requests before temporarily locking the account in order to prevent attackers from brute-forcing the password on such a request.

4.6 Unverified Email Change

Finding No 6.	Systems Affected	https://wallet.tentum.com/		
	Finding	User email address could be updated without verifying the current user		
	CVE Number	N/A		
	Impact	4		
	Likelihood	2		
	Overall Risk Rating	8 (Medium Risk)		
	Status	RESOLVED		

4.6.1 Retest Status

The application has been modified to send a verification email to the users registered email account to validate the change. This finding is now resolved.

4.6.2 Summary

The email change functionality permitted the modification of the user’s current email address without verifying the user.

4.6.3 Technical Details

The application allows an account's email address to be changed whilst authenticated without requiring the user’s current password to be entered, i.e. without verifying the authenticity of the user.

Therefore, if the account is temporarily compromised e.g. via SQL Injection; XSS; CSRF; session hijacking; or similar, the attacker would be able to change the email address on the account without requiring any knowledge of the existing password. The email account could subsequently be used to seize control of the account.

4.6.4 Recommendation

BSI recommends that the application be modified to require users to input the current password of the account prior to permitting the email change. The server should then use the password submitted to verify the authenticity of the user submitting the request and check that they are permitted to make such a change.

BSI further recommends that the application be modified verify email account ownership and to send an email to the existing (old) email account to provide visibility of the change.

4.7 User Account Enumeration

Finding No 7.	Systems Affected	http://54.38.214.253		
	Finding	The application was found to present error messages that facilitated the enumeration of valid user accounts.		
	CVE Number	N/A		
	Impact	2		
	Likelihood	3		
	Overall Risk Rating	6 (Medium Risk)		
	Status	ONGOING		

4.7.1 Retest Status

Retesting identified that this issue was still present within the application. This finding is not resolved.

4.7.2 Summary

It was possible to carry out user enumeration using the error messages returned by the login, forgotten password and sign up pages.

4.7.3 Technical Details

It was possible to carry out user enumeration using the error messages returned by the login, forgotten password and sign up pages. Using the difference in error messages returned, it was possible to determine valid user accounts. An attacker could leverage this vulnerability in order to identify user accounts, which could then be targeted in future attacks, such as brute force password guessing, once their accounts have been identified.

Testing of the application identified user enumeration was possible on the following pages:

- Login
- Forgotten password
- Sign up

The following indicates the revealing error messages returned by the respective pages:

- Authentication failed. User not found
- No account with that email address exists
- Username already exists

4.7.4 Recommendation

BSI recommends that the application be modified to return generic error messages to ensure that they do not indicate whether a valid user account exists.

4.8 Potential Private Key Information Leakage

Finding No 8.	Systems Affected	https://wallet.tentum.com/
	Finding	The server returned information that was potentially related to the user's wallet private key.
	CVE Number	N/A
	Impact	4
	Likelihood	2
	Overall Risk Rating	8 (Medium Risk)
	Status	ONGOING

4.8.1 Summary

The server returned information that was potentially related to the user's wallet private key within an error message.

4.8.2 Technical Details

When creating a transaction with invalid data the server responded with a HTTP 400 Bad Request error. Within the HTTP response body returned, a value called **privateKey** was included. The **privateKey** value does not directly relate to the users' wallet private key as the two values are different, however, the value name indicates that it is related and therefore should not be directly exposed by the application.

An example (edited for brevity) HTTP request and response is shown below:

```
POST /api/user/transaction/create HTTP/1.1
Host: wallet.tentum.com
...
Content-Type: application/json

{"amount":1,"amount":-1,
"to":"04948ade641e8eb3499e8ed9fc13979c8408a1e5f644d80c59a5f470ac64de53adeb36bf29b5bc7746
988aa2ff8b82104f1317c37dd136bb983f67e4ae3581aa90","from":"049fa7f033976bd13f1e3e1ccbea1c
5ba3d337938b56e8792612290a2bfd9be5eefc48bac5d96629845a6d784198d62f8a99b49a75639b9ff9893d
a20e91d94b93"}

HTTP/1.1 400 Bad Request
...
Server: nginx/1.14.0 (Ubuntu)

{"message":"400 - {"message":"Invalid
amount.\"}", "method":"POST", "uri":"http://54.38.214.253:3001/transaction/create", "json":
{"from":"049fa7f033976bd13f1e3e1ccbea1c5ba3d337938b56e8792612290a2bfd9be5eefc48bac5d9662
9845a6d784198d62f8a99b49a75639b9ff9893da20e91d94b93", "to":"04948ade641e8eb3499e8ed9fc139
79c8408a1e5f644d80c59a5f470ac64de53adeb36bf29b5bc7746988aa2ff8b82104f1317c37dd136bb983f6
7e4ae3581aa90", "amount":-
1, "privateKey":"ac78f499168ab33e1778bdbc6b7574b550644867a0b432fc467ff597d5a723ff"}, "simp
le":true, "resolveWithFullResponse":false, "transform2xxOnly":false}
```

4.8.3 Recommendation

BSI recommends that the application be modified to respond with generic HTTP error messages that do not expose any information.

4.9 Private Key Download Did Not Require Reauthentication

Finding No 9.	Systems Affected	https://wallet.tentum.com/		
	Finding	The Private Key download functionality did not require re-authentication.		
	CVE Number	N/A		
	Impact	4		
	Likelihood	2		
	Overall Risk Rating	8 (Medium Risk)		
	Status	ONGOING		

4.9.1 Summary

The **Private Key** download functionality did not require user verification before permitting the download of the user’s wallet public/private keys.

4.9.2 Technical Details

The application allows the user’s wallet public/private keys to be downloaded without requiring the user’s current password to be entered, i.e. without verifying the authenticity of the user.

Therefore, if the account is temporarily compromised e.g. via SQL Injection; XSS; CSRF; session hijacking; or similar, the attacker would be able to gain access the key data that controls the wallet without requiring any knowledge of the existing password.

4.9.3 Recommendation

BSI recommends that the application be modified to verify the user before permitting the download of the wallet keys.

4.10 Private Key Email Did Not Use Archive Encryption

Finding No 10.	Systems Affected	https://wallet.tentum.com/		
	Finding	The Private Key email functionality did not encrypt the wallet keys before transmission via email		
	CVE Number	N/A		
	Impact	4		
	Likelihood	2		
	Overall Risk Rating	8 (Medium Risk)		
	Status	ONGOING		

4.10.1 Summary

The **Private Key** email functionality did not encrypt the wallet keys before transmission via email.

4.10.2 Technical Details







The **Private Key** email functionality sends an email to the user account registered with the application, the email has a zip archive attachment that contains the user’s wallet keys. The zip archive did not utilise any form of encryption.

The unencrypted archive would be susceptible to interception during transmission, along with storage within the user’s email client. An attacker able to gain access to the keys would have complete control of the wallet.

4.10.3 Recommendation

BSI recommends that the application be modified to encrypt the zip archive with AES256 and transmit the password via a secondary method such as SMS.

4.11 Unverified Smart Authentication Disable

Finding No 11.	Systems Affected	https://wallet.tentum.com/			
	Finding	The Smart Authentication functionality does not require user verification to disable the feature			
	CVE Number	N/A			
	Impact	2			
	Likelihood	3			
	Overall Risk Rating	6 (Medium Risk)			
	Status	ONGOING			

4.11.1 Summary

The **Smart Authentication** functionality does not require user verification to disable the feature.

4.11.2 Technical Details

The application allows the Smart Authentication functionality to be disabled without requiring the user’s current password to be entered, i.e. without verifying the authenticity of the user.

Therefore, if the account is temporarily compromised e.g. via SQL Injection; XSS; CSRF; session hijacking; or similar, the attacker would be able to reduce the security posture of the application without requiring any knowledge of the existing password.

4.11.3 Recommendation

BSI recommends that the application be modified to verify the user before the modification of **any** security feature.

4.12 Information Disclosure Through HTTP Headers

Finding No 12.	Systems Affected	https://wallet.tentum.com/		
	Finding	Testing identified information disclosure within the HTTP response headers, which revealed technical configuration details.		
	CVE Number	N/A		
	Impact	1		
	Likelihood	4		
	Overall Risk Rating	4 (Low Risk)		
	Status	ONGOING		

4.12.1 Summary

Information disclosure was identified within HTTP response headers revealing details of the supporting software. This information could assist an attacker in formulating an attack against the application and its supporting infrastructure.

4.12.2 Technical Details

The following HTTP response was returned by all pages disclosing the server software and version information that is used by the application:

```
Server: nginx/1.14.0 (Ubuntu)
```



Further information relating to this issue can be found in the following OWASP document:

[https://www.owasp.org/index.php/Fingerprint_Web_Server_\(OTG-INFO-002\)](https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002))

4.12.3 Recommendation

BSI recommends that HTTP response headers are removed or obfuscated in order to prevent unnecessary information disclosure.

4.13 Insecure TLS Version Supported

Finding No 13.	Systems Affected	https://wallet.tentum.com/		
	Finding	An insecure version of the TLS protocol which is affected by cryptographic flaws was identified.		
	CVE Number	N/A		
	Impact	4		
	Likelihood	1		
	Overall Risk Rating	4 (Low Risk)		
	Status	ONGOING		

4.13.1 Summary

An insecure version of the TLS protocol which is affected by cryptographic flaws was identified. An attacker may be able to exploit these flaws to conduct Man-in-the-Middle attacks or to decrypt communications between the affected service and connecting clients. The widespread POODLE and BEAST exploits are just a couple examples of how attackers have taken advantage of weaknesses in SSL and early TLS to compromise organizations.

4.13.2 Technical Details

Testing identified that TLSv1 was enabled on the nginx web server:

4.13.3 Recommendation

BSI recommends that only TLS versions 1.1 and 1.2 are enabled. The nginx configuration needs to have the following line set:

```
ssl_protocols TLSv1.1 TLSv1.2;
```

4.14 Unauthorised Device History Deletion

Finding No 14.	Systems Affected	https://wallet.tentum.com/		
	Finding	Authenticated users could delete the device history of other users		
	CVE Number	N/A		
	Impact	1		
	Likelihood	2		
	Overall Risk Rating	2 (Very Low Risk)		
	Status	ONGOING		

4.14.1 Summary

Authenticated users could delete the device history of other users.

4.14.2 Technical Details

BSI determined that it was possible to delete individual records of login device history associated with other users.

An example of a HTTP POST request for device history deletion is shown below. The JSON **id** parameter value was used to perform the attack, as highlighted below:

```
POST /user/device/delete HTTP/1.1
Host: 54.38.214.253:9001
Content-Length: 33
Accept: application/json, text/plain, */*
Origin: http://54.38.214.253
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Content-Type: application/json; charset=UTF-8
Referer: http://54.38.214.253/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{"id": "5ba49ad07c47ab6f08899cdf"}
```

An attacker would be required to know the device history **id** value belonging to another user. The **id** value is a 24-character token, and therefore the brute-forcing of such values would be unfeasible.

4.14.3 Recommendation

BSI recommends that the application be modified to ensure that appropriate authorisation checks are performed for all user actions.

4.15 Login IP Geo-Location Incorrect

Finding No 15.	Systems Affected	https://wallet.tentum.com/
	Finding	The login geo-location functionality did not correctly identify the location of the login IP addresses
	CVE Number	N/A
	Impact	0
	Likelihood	0
	Overall Risk Rating	Informational Risk
	Status	RESOLVED

4.15.1 Retest Status

The application has been modified to correctly identify the IP address location. This finding is now resolved.

4.15.2 Summary

The login geo-location functionality did not correctly identify the location of the login IP addresses.

4.15.3 Technical Details

All of the IP addresses displayed in the **Recent login history** section of the applications settings were identified as being in Minsk.

Recent login history			
Have a quick overview of five recent login sessions to your account			
Date	IP	Geolocation	Status
2018-09-21 08:16:32	::ffff:81.131.108.82	Minsk	Login success
2018-09-17 23:46:06	::ffff:158.38.156.228	Minsk	Login success
2018-09-17 23:40:02	::ffff:158.38.156.228	Minsk	Login success

Whilst there is no direct security risk associated with the issue, the geo-location data would be used by the users to ensure that no authorised access had occurred.

4.15.4 Recommendation

BSI recommends that the geo-location functionality be modified to correctly identify the location associated with the login IP addresses.

5 Summary of Findings

5.1 Results of Web Application Testing

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
1		3	High	Application Available Over Unencrypted HTTP The web application was available over unencrypted HTTP protocol.	BSI recommends that the HTTP service be replaced with the cryptographically secure alternative HTTPS protocol	RESOLVED
2	4	3	High	Stored Cross-Site Scripting A stored Cross-Site Scripting (XSS) vulnerability was identified which could be exploited by an authenticated user	BSI recommends that all client supplied input is sufficiently filtered before being echoed back to the client's browser. Input validation should be carried out on all input fields to ensure that only input that matched an expected pattern is accepted. In addition, the application should implement output encoding to ensure that any potential unsafe data is properly encoded or escaped to prevent execution within the client's browser	ONGOING
3	4	3	High	No Lockout after Multiple Login Failures The application did not enforce an account lockout policy	BSI recommends that an account lockout policy be enforced for incorrect login attempts in line with the organisation's password policy requirements. BSI highly recommends that Two Factor or Multi-Factor authentication be implemented and enforced for all logins and transaction authorisations	RESOLVED

COMMERCIAL IN CONFIDENCE

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
4	3	3	Medium	Inadequate Application Session Timeouts The application sessions did not expire after a period of inactivity. Session timeouts help protect applications against session hijacking.	BSI recommends that all login sessions be terminated, and users logged out after a set period of inactivity.	ONGOING
5	4	2	Medium	Unverified Password Change User password could be updated without verifying the current user	BSI recommends that the application be modified to require users to input the current password of the account prior to permitting the password change	ONGOING
6	4	2	Medium	Unverified Email Change User email address could be updated without verifying the current user	BSI further recommends that the application be modified to verify email account ownership	RESOLVED
7	4	2	Medium	Potential Private Key Information Leakage The server returned information that was potentially related to the user's wallet private key	BSI recommends that the application be modified to respond with generic HTTP error messages that do not expose any information.	ONGOING
8	4	2	Medium	Private Key Download Does Not Require Reauthentication The Private Key download functionality did not require user verification.	BSI recommends that the application be modified to verify the user before permitting the download of the wallet keys	ONGOING
9	4	2	Medium	Private Key Email Does Not Use Archive Encryption The Private Key email functionality did not encrypt the wallet keys before transmission via email	BSI recommends that the application be modified to encrypt the zip archive with AES256 and transmit the password via a secondary method such as SMS.	ONGOING
10	2	3	Medium	User Account Enumeration The application was found to present error messages that facilitated the enumeration of valid user accounts.	BSI recommends that the application be modified to return generic error messages to ensure that they do not indicate whether a valid user account exists.	ONGOING

COMMERCIAL IN CONFIDENCE

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
11	2	3	Medium	Unverified Smart Authentication Disable The Smart Authentication functionality does not require user verification to disable the feature	BSI recommends that the application be modified to verify the user before the modification of any security feature.	ONGOING
12	1	4	Low	Information Disclosure Through HTTP Headers Testing identified information disclosure within the HTTP response headers, which revealed technical configuration details.	BSI recommends that HTTP response headers are removed or obfuscated in order to prevent unnecessary information disclosure.	ONGOING
13			Low	Insecure TLS Version Supported An insecure version of the TLS protocol which is affected by cryptographic flaws was identified.	BSI recommends that only TLS versions 1.1 and 1.2 are enabled	ONGOING
14	1	2	Very Low	Unauthorised Device History Deletion Authenticated users could delete the device history of other users	BSI recommends that the application be modified to ensure that appropriate authorisation checks are performed for all user actions.	ONGOING
15	N/A	N/A	Info	Login IP Geo-Location Incorrect The login geo-location functionality did not correctly identify the location of the login IP addresses	BSI recommends that the geo-location functionality be modified to correctly identify the location associated with the login IP addresses.	RESOLVED

Appendix A - Testing Team

This project was undertaken using the following consultant:

- Mark Woan

Any queries regarding this testing and report should be directed to:

BSI Cybersecurity and Information Resilience Operations Team

Tel: +44 (0) 345 222 1711

Email: Operations.Cyber.UK@bsigroup.com

The primary point of contact at Dragon InfoSec was Richard Dennis (richard@dragoninfosec.com).

Appendix B - Findings Definitions

BSI Cybersecurity and Information Resilience have developed a method for evaluating vulnerabilities and presenting the results in a way which enables clients to easily assess the risks they pose to the organisation.

B.1. Risk Ratings

Each finding is categories by its "Seriousness" and "Likelihood". The overall risk rating is calculated as a multiple of the two values.

$$\text{Overall risk} = \text{Seriousness} \times \text{Likelihood}$$

Below are guidance on rating definitions; exact ratings may depend on particular environment.

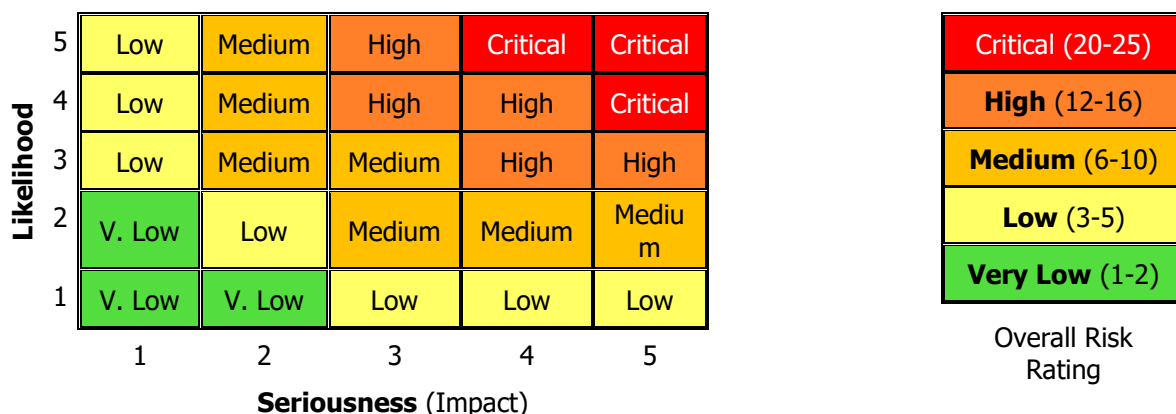
Seriousness (Impact)

- 5** - Remotely gaining administrative access;
- 4** - Remote privilege escalation or unauthorised read/write access;
- 3** - Local privilege escalation or unauthorised read-only access to data;
- 2** - Sensitive information disclosure. Minor security configuration weakness;
- 1** - Minor non-sensitive information disclosure.

Likelihood (exploitability)

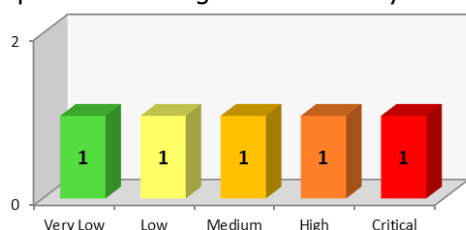
- 5** - Trivial to exploit by unskilled person;
- 4** - Require exploit code or tool which was in the public domain, or easy to exploit with some knowledge;
- 3** - Require some exploit code development or effort to exploit, or require specific knowledge/skill;
- 2** - Attacker may require specific access;
- 1** - Theoretical vulnerability where there is no known exploit code and/or would require a lot of resources to exploit.

Rating may also take in to account existing defences which may restrict the exploitability.



B.2. Executive Summary

The executive summary provides a number of graphical representations as to the most common root cause of the vulnerabilities identified. A summary of the number of different root cause categories are summarised in a graph in the management summary.



In addition, all findings are plotted onto a graph so that the severity of the vulnerabilities identified can easily be visualised. This enables the client to concentrate their efforts for resolution in specific areas



The pie chart depicts the most common root causes of the vulnerabilities identified.

B.2.1. Root Causes

The root causes for infrastructure tests include:

- ❖ Configuration
- ❖ Encryption
- ❖ Human Factor
- ❖ Network Design
- ❖ Password Policy
- ❖ Patching
- ❖ Web Development

The root causes for application tests include:

- ❖ Authentication
- ❖ Client Side Controls
- ❖ Configuration
- ❖ Default Content
- ❖ Design Error
- ❖ Encryption
- ❖ Input Validation
- ❖ Logic Error
- ❖ Password Policy
- ❖ Session Control

B.3. Findings Box

The table below provides a key to understand the findings description.

Finding No. X	Systems Affected	List of devices which are vulnerable. This will either take the form of IP addresses (DNS names) or URLs.
	Finding	An overview of the vulnerability identified.
	CVE number	Where possible, references will be made to a common reference identifier such as CVE or CWE. These references to external sources allow clients to find out additional details regarding the vulnerability and how to mitigate it.
	Root Cause	Each finding will be categorised as to the perceived root cause. Further details are discussed in the section below.
	Seriousness (Impact)	Impact if the vulnerability is successfully exploited. Rated from 5 (serious) to 1(not serious). <div style="display: flex; align-items: center; justify-content: center;"> <div style="margin-right: 10px;"> 5 - ■ ■ ■ ■ 4 - ■ ■ ■ ■ 3 - ■ ■ ■ ■ 2 - ■ ■ ■ ■ 1 - ■ ■ ■ ■ </div> <div style="margin-left: 10px;">(visual representation)</div> </div>
	Likelihood	How easy is the vulnerability to exploit? Ratings from 5 (easy) to 1 (difficult).
	Overall Risk rating	The overall risk rating takes into account the seriousness of the issue, the likelihood of the vulnerability being exploited, as well as other factors that could impact the overall risk.

Note: It should be noted that the definitions defined above for the seriousness and likelihood ratings are only guidelines.