…making excellence a habit.™

Web Application Test Report

Dragon InfoSec
Temtum Wallet

BSI Reference:	CSIRUKPRJ-366-RPT-01
Version:	1.0

21st December 2018

Testing Team

Duncan Winfrey

BSI Cybersecurity and Information Resilience (UK) Limited
Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP
Telephone: +44 345 080 9000 Email: cyber@bsigroup.com

Document Control Information

1.1 Document Details

Property	Value
Client	Dragon InfoSec
Title	Dragon InfoSec Temtum Wallet Web Application Test Report
Author	Duncan Winfrey
Version	1.0
Date	21/12/2018
Document Reference	CSIRUKPRJ-366-RPT-01
Status	Final

1.2 Revision History

Version	Date	Author	Summary of Changes
0.1	17/12/2018	Duncan Winfrey	Initial Draft
0.2	21/12/2018	Euan Kerr	Internal QA
1.0	21/12/2018	Euan Kerr	Definitive Issue

1.3 Approvals

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

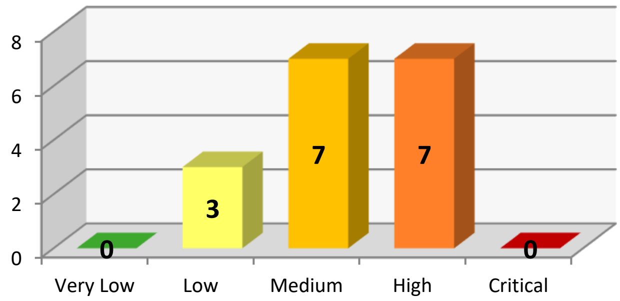
1.4 Distribution

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

Table of Contents

2 Executive Summary

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a web application test against the Temtum Android Wallet. Testing was undertaken between the 11th and 13th December 2018 remotely.



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 and medium areas of risk have been identified within the environment. These were all resolved during testing apart from one medium risk relating to username enumeration.

Android Application Testing

Three high risks were identified within the android application testing. Firstly, the application was permitted to run on rooted devices, increasing the level of access to the underlying operating system for the user, thus, putting the components of the application at increased risk of compromise. The issue was remediated during testing by adding google SafetyNet to validate the device status before running the application. The second and third high risk issues relate to the Password PIN that a user can setup to protect outgoing payments. The PIN was found to be too short, so it could be brute forced. It was also found that it could be bypassed by overwriting it with a new attacker-controlled PIN. Both issues were resolved during testing.

Three medium risks were identified. It was possible to enumerate usernames of the application using the user search function when sending tokens, allowing an attacker to easily collect a list of usernames to brute force. It is recommended that login usernames are not easily enumerated. The web server installed was found to be outdated, making it vulnerable to denial-of-service. The web server software was updated to the latest version during testing. It was also found that the wallet server had SSH exposed, increasing the risk of compromise by either a future software flaw or password brute force attack. To remediate the SSH service was locked down to a network whitelist.

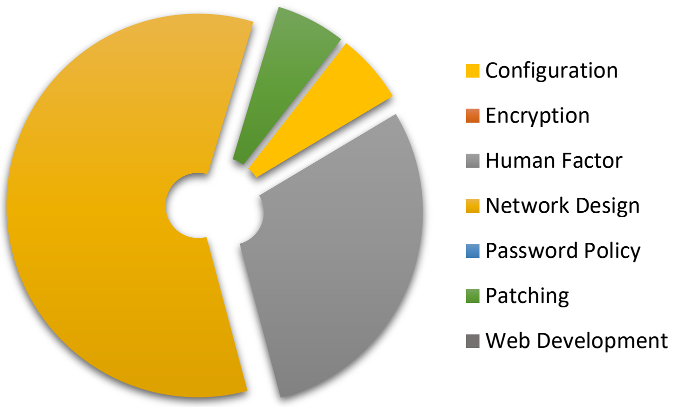
Six low risks were found, which were also resolved. These mainly related to best practices such as setting security headers and information disclosure. Further details of the issues can be found in the main body of the report.

SQLite Review

The SQLite database used by the Android Application was found not to be encrypted, therefore if the device was rooted the applications authentication tokens could be accessed. The issue was partially resolved as the tokens are now encrypted within the database with the encryption key being stored within the android KeyStore. It is recommended that the whole database is encrypted.

Server Build Review

Four medium risks were identified, all resolved within testing. The issues included overly permissive file permissions, access to the server permitted as the root user and no antivirus or firewall configured on the server.



This graph shows the distribution of risk within the environment. It is useful to get a sense of the proportion of higher risk issues that need immediate attention.

3 Introduction

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a web application test against the Temtum Android Wallet. Testing was undertaken between the 11th and 13th December 2018 remotely.

3.1 Background

Dragon InfoSec required the testing of their Android cryptocurrency wallet for Temtum. All testing was carried out using BSI Cybersecurity and Information Resilience standard application testing methodology. A full copy of this methodology can be provided on request.

3.2 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.

3.3 Scope

The scope of the engagement was as follows:

Android Application Test:

- Temtum Android Wallet v1.4.0 (https://wallet.temtum.com/api)

The following user accounts were used for testing:

- bsigroup
- dwinfrey88
- test1csirapp

Testing was focused on the implementation of the two-factor authentication feature.

Database configuration Review:

- Wallet SQLite Database - App.db

Server Build Review:

- CI-SERVER (Debian 7.11)

3.3.1 Limitations

The following limitations were identified:

- BSI does not perform exploitation of vulnerabilities that may impact upon service availability or stability due to the live nature of systems.
- Access to the CI-SERVER was not possible so testing was limited to scripts provided.

4 Results of Android Application Testing

This section provides the detailed findings of the security testing that was performed between the 11th and 13th December 2018.

4.1 No Root Detection

Finding No 1.	Systems Affected	`wallet.dragon`
	Finding	The application was found to run on a rooted android device.
	CVE Number	N/A
	Root Cause	**Web Development**
	Impact	**4** 🟩 🟨 🟧 🟧 🟥
	Likelihood	**4** 🟩 🟨 🟧 🟧 🟥
	Overall Risk Rating	**16 (High Risk)**
	Status	**RESOLVED**

4.1.1 Retest Status

Retesting confirmed the addition of SafetyNet that prevented the application running on rooted or modified devices.

4.1.2 Summary

The process of jailbreaking or rooting of a mobile device results in an increased level of access to the underlying operating system for the user, thus, putting the components of the application at increased risk of compromise. Additionally, jailbreaking or rooting often decreases the security posture of a device, meaning that the application and its data could be compromised by other malicious application or malicious users.

4.1.3 Technical Details

It was identified that the mobile application did not employ robust controls to prevent it from being successfully run on rooted devices.

4.1.4 Recommendation

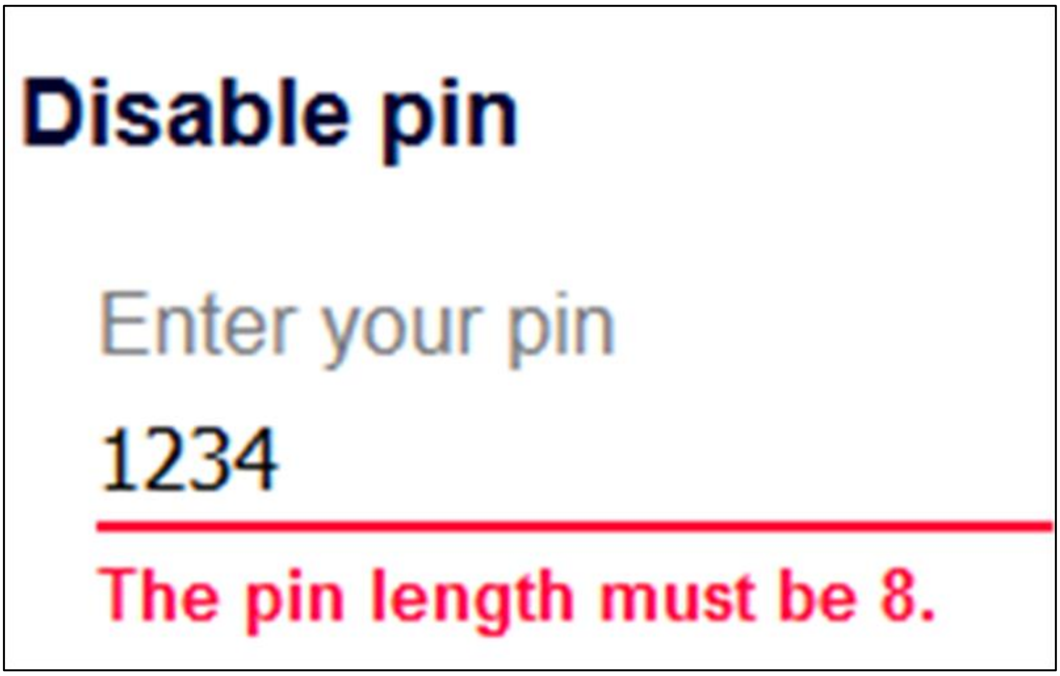
BSI recommends that the application performs root checking at run time.

4.2 Weak Payment Password PIN

Finding No 2.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	The Payment Password PIN was found to be short and vulnerable to brute force.
	CVE Number	N/A
	Root Cause	**Web Development**
	Impact	**4** 🟩🟨🟧🟧🟥
	Likelihood	**3** 🟩🟨🟧🟧🟥
	Overall Risk Rating	**12 (High Risk)**
	Status	**RESOLVED**

4.2.1 Retest Status

Retesting confirmed the PIN had been changed to 8 digits, as the screenshot below demonstrates:



Disable pin

Enter your pin

1234

The pin length must be 8.

Figure 1 - Longer Security PIN

4.2.2 Instances

/api/user/transaction/create

/api/user/settings/pin/change

/api/user/settings/pin/disable

4.2.3 Summary

Strong authentication credentials are a key component of a systems security. Generally, the greater the number of characters within a password the stronger the password will be. With a short minimum password length configured a user could set a short password, requiring less time for an attacker to brute-force the authentication password.

4.2.4 Technical Details

The Payment Password PIN was found to be 4 digits, this could be brute forced. Therefore, allowing the PIN to be recovered and fraudulent transactions made.

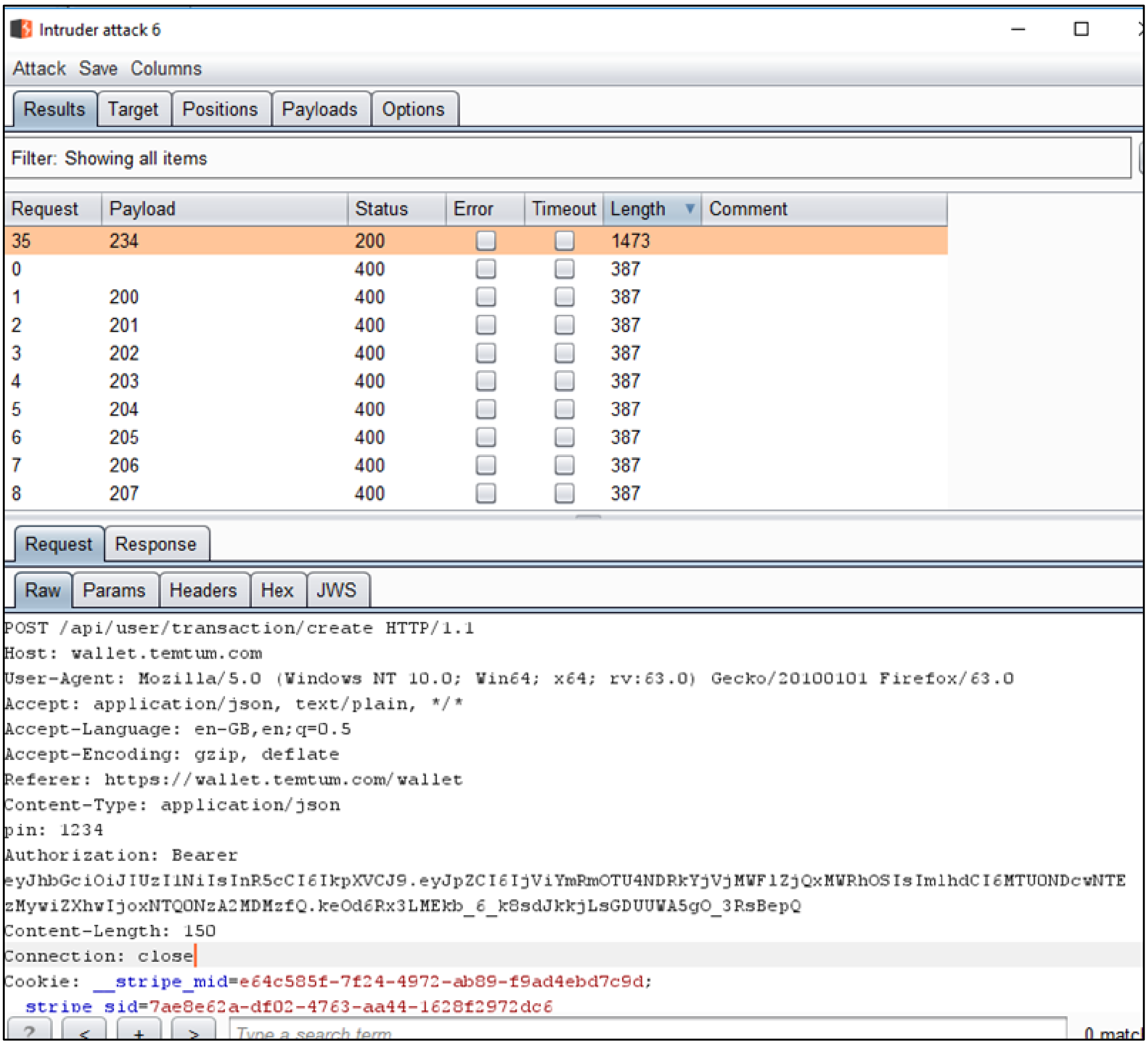
The screenshot section below demonstrates the recovery of the pin "1234".

The instances section above lists the vulnerable API methods.

4.2.5 Recommendation

BSI recommends that a longer Payment Password PIN should be used.

4.2.6 Screenshots



Intruder attack 6
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Response
Raw Params Headers Hex JWS
?
<
+
>
Type a search term
0 matc

Request	Payload	Status	Error	Timeout	Length	Comment
35	234	200	□	□	1473	
0		400	□	□	387	
1	200	400	□	□	387	
2	201	400	□	□	387	
3	202	400	□	□	387	
4	203	400	□	□	387	
5	204	400	□	□	387	
6	205	400	□	□	387	
7	206	400	□	□	387	
8	207	400	□	□	387	

```
POST /api/user/transaction/create HTTP/1.1
Host: wallet.temtum.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: application/json, text/plain, */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://wallet.temtum.com/wallet
Content-Type: application/json
pin: 1234
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjViYmRmOTU4NDRkYjVjMWF1ZjQxMWRhOSIsImlhdCI6MTUONDcwNTE
zMywiZXhwIjoxNTQONzA2MDMzfQ.keOd6Rx3LMEkb_6_k8sdJkkjLsGDUUWA5gO_3RsBepQ
Content-Length: 150
Connection: close
Cookie: __stripe_mid=e64c585f-7f24-4972-ab89-f9ad4ebd7c9d;
  stripe_sid=7ae8e62a-df02-4763-aa44-1628f2972dc6
```

Figure 2 - Brute Force of Payment Password

4.3 Payment Password PIN Force Reset

Finding No 3.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	It was possible to overwrite the Payment Password without knowing the current Payment PIN.
	CVE Number	N/A
	Root Cause	**Web Development**
	Impact	**4** 🟩🟨🟧🟧□
	Likelihood	**3** 🟩🟨🟧□□
	Overall Risk Rating	**12 (High Risk)**
	Status	**RESOLVED**

4.3.1 Retest Status

Retesting confirmed it was no longer possible to overwrite the existing PIN.

4.3.2 Summary

Strong authentication credentials are a key component of a systems security. It is therefore important that a user chooses a strong password and that it is changed on a regular basis. Generally, the greater the number of characters within a password the stronger the password will be. With a short minimum password length configured a user could set a short password, requiring less time for an attacker to brute-force the authentication password.

The minimum password length policy setting is used to force users to set passwords that are at least the specified number of characters in length.

4.3.3 Technical Details

It was found that the Payment Password PIN could be overwritten with a call to the set API as shown below:

```
Request:
POST /api/user/settings/pin/set HTTP/1.1
Host: wallet.temtum.com

{"pin":"5555"}
Server Response:
HTTP/1.1 200 OK


{"message":"Successfully setted PIN!"}
```

Therefore the attacker could use the new PIN to authorize a transaction or disable the PIN.

4.3.4 Recommendation

BSI recommends that a longer Payment Password PIN should be used.

4.4 User Account Enumeration

Finding No 4.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	The application was found to present error messages that facilitated the enumeration of valid user accounts.
	CVE Number	N/A
	Root Cause	**Web Development**
	Impact	**2** 🟩🟨⬜⬜⬜
	Likelihood	**5** 🟩🟨🟧🟧🟥
	Overall Risk Rating	**10 (Medium Risk)**
	Status	**ONGOING**

4.4.1 Instances

/api/signup/check/user

/api/user/find/address

4.4.2 Summary

It was possible to carry out user enumeration using the error messages returned by the login 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.

4.4.3 Technical Details

Testing of the application identified user enumeration was possible within two parts of the application.

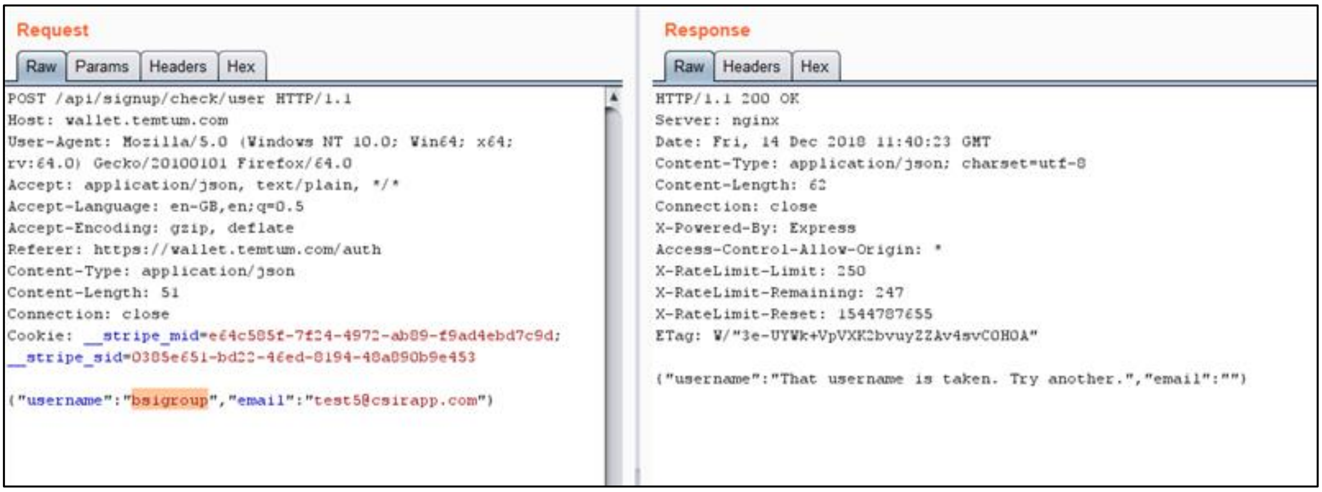
The first instance on the user sign up page, where the error message "That username is already taken" is returned indicating the usernames exists. The second instance is within the application itself when searching for users to send tokens to. The example requests below demonstrate the username "dwinfrey88" being disclosed.

```
Request:
POST /api/user/find/address HTTP/1.1
{"username":"dwin"}
Response:
{"users":[{"address":"042f2a4a0ca2fc5faf9713e427af6cc14f6604e5e72c469d2aa6e682c61
110c23200f9bdfba4523643f56407f45c520f51fe4559a5b1c5ba1e39e413a866b77a04","usernam
e":"dwinfrey88"}]}
```

4.4.4 Recommendation

BSI recommends that the application be configured to return generic error messages to ensure that they do not indicate whether a valid user account has been provided or not.

4.4.5 Screenshots



```
POST /api/signup/check/user HTTP/1.1
Host: wallet.temtum.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:64.0) Gecko/20100101 Firefox/64.0
Accept: application/json, text/plain, */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://wallet.temtum.com/auth
Content-Type: application/json
Content-Length: 51
Connection: close
Cookie: __stripe_mid=e64c585f-7f24-4972-ab89-f9ad4ebd7c9d;
__stripe_sid=0385e651-bd22-46ed-8194-48a890b9e453

{"username":"bsigroup","email":"test5@csirapp.com"}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 14 Dec 2018 11:40:23 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 62
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
X-RateLimit-Limit: 250
X-RateLimit-Remaining: 247
X-RateLimit-Reset: 1544787655
ETag: W/"3e-UYWk+VpVXK2bvuyZZAv4svCOHOA"

{"username":"That username is taken. Try another.","email":""}
```

Figure 3 - Username Enumeration On Sign Up Page

4.5 Multiple Vulnerabilities Within Nginx Web Server

Finding No 5.	Systems Affected	**TCP Port 80** `wallet.temtum.com (54.38.214.253)`	
	Finding	Multiple vulnerabilities were identified in the version of the Nginx Web Server software running on the system.	
	CVE Number	CVE-2018-16843, CVE-2018-16844, CVE-2018-16845	
	Root Cause	**Patching**	
	Impact	**3**	🟩🟨🟧🟧🟥
	Likelihood	**3**	🟩🟨🟧🟧🟥
	Overall Risk Rating	**9 (Medium Risk)**	
	Status	**RESOLVED**	

4.5.1 Retest Status

Retesting confirmed Nginx had been updated to 1.14.2.

4.5.2 Summary

Multiple vulnerabilities were identified in the version of the Nginx Web Server running on the system. Detailed information regarding these vulnerabilities has not yet been disclosed publicly.

4.5.3 Technical Details

An out of date version of Nginx Server was found to be installed, as determined through the HTTP banner.

```
Server: nginx/1.14.0
```

The following information is currently available regarding these vulnerabilities.

- An unspecified error exists related to the module 'ngx_http_v2_module' that allows excessive memory usage.

(CVE-2016-16843)

- An unspecified error exists related to the module 'ngx_http_v2_module' that allows excessive CPU usage.

(CVE-2016-16844)

- An unspecified error exists related to the module 'ngx_http_mp4_module' that allows worker process crashes or memory disclosure. (CVE-2016-16845)

Further details regarding these vulnerabilities can be found on the Nginx Web Server security vulnerabilities webpage:

http://nginx.org/en/security_advisories.html

4.5.4 Recommendation

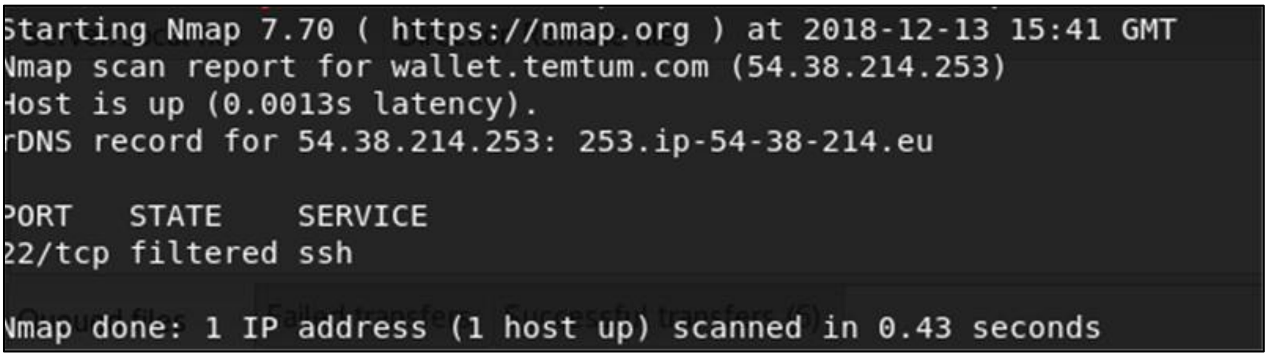
BSI recommends that the Nginx HTTP server be upgraded to the latest stable version.

4.6 Unnecessary Admin Service Exposed to the Internet

Finding No 6.	Systems Affected	**TCP Port 22** `wallet.temtum.com (54.38.214.253)`
	Finding	The SSH admin service was found to be unnecessarily exposed to the Internet.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**4** 🟩🟨🟧🟧🟥
	Likelihood	**2** 🟩🟨
	Overall Risk Rating	**8 (Medium Risk)**
	Status	**RESOLVED**

4.6.1 Retest Status

Retesting confirmed SSH was no longer internet accessible as the following screenshot demonstrates:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-13 15:41 GMT
Nmap scan report for wallet.temtum.com (54.38.214.253)
Host is up (0.0013s latency).
rDNS record for 54.38.214.253: 253.ip-54-38-214.eu

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Figure 4 - SSH Port Closed

4.6.2 Summary

It is best practice to ensure that minimal services are exposed to the Internet. This helps reduce the exposure the server may have to attack and to protect against future vulnerabilities. Although the running of unnecessary services is not always an immediate vulnerability, it may provide an attacker with additional avenues of potential attack against the server.

4.6.3 Technical Details

The server administration server SSH was found to be exposed to the Internet on the affected system, in addition to those that would normally be expected for a web application, such as HTTP and HTTPS services.

- Port 22 : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1 with SSH supported authentication of publickey and password

No currently known vulnerabilities were identified in any of the exposed service, however it is recommended that the exposed service be blocked by a firewall unless specifically required to ensure that the servers are not exposed to unnecessary risk of compromise.

4.6.4 Recommendation

BSI recommends that the identified service be reviewed and if they are not functionally required, then access from the Internet should be blocked by a firewall.

4.7 Weak Phone Number Verification PIN

Finding No 7.	Systems Affected	`https://wallet.temtum.com/api`	
	Finding	The verification PIN was found to be short and vulnerable to brute force.	
	CVE Number	N/A	
	Root Cause	**Web Development**	
	Impact	**2**	🟩🟨🟨🟧🟥
	Likelihood	**2**	🟩🟨🟨🟧🟥
	Overall Risk Rating	**4 (Low Risk)**	
	Status	**RESOLVED**	

4.7.1 Retest Status

Retesting confirmed the PIN has been increased to 8 digits.

4.7.2 Instances

/api/sms/verify

4.7.3 Summary

Strong authentication credentials are a key component of a systems security. Generally, the greater the number of characters within a password the stronger the password will be. With a short minimum password length configured a user could set a short password, requiring less time for an attacker to brute-force the authentication password.

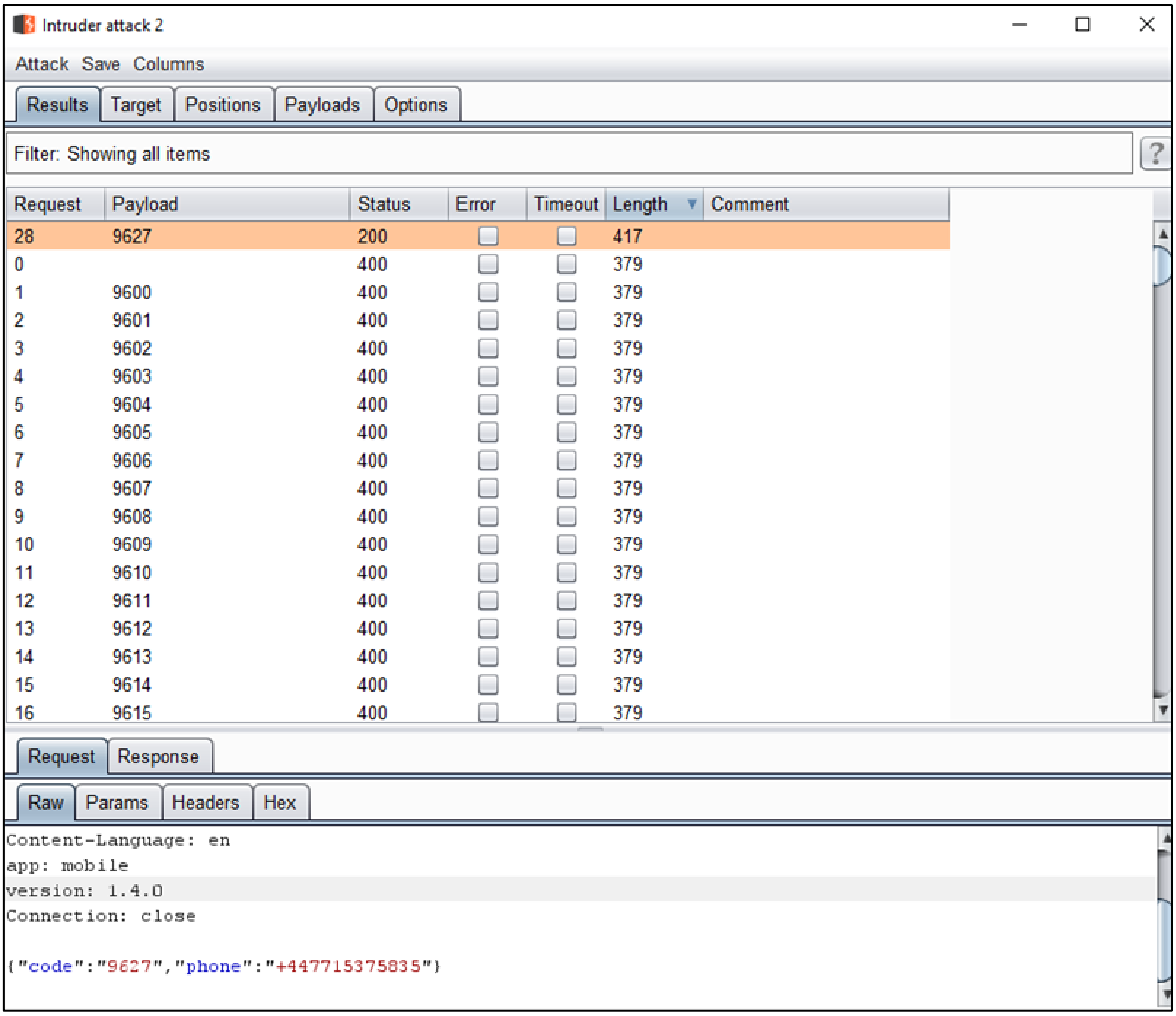
4.7.4 Technical Details

The PIN that is used to verify a user is linking a legitimate phone number to an account was too short, allowing it to be brute forced. The screenshot section below demonstrates the PIN being recovered.

4.7.5 Recommendation

BSI recommends that a longer Phone Number Verification PIN should be configured.

4.7.6 Screenshots



Request	Payload	Status	Error	Timeout	Length	Comment
28	9627	200	□	□	417	
0		400	□	□	379	
1	9600	400	□	□	379	
2	9601	400	□	□	379	
3	9602	400	□	□	379	
4	9603	400	□	□	379	
5	9604	400	□	□	379	
6	9605	400	□	□	379	
7	9606	400	□	□	379	
8	9607	400	□	□	379	
9	9608	400	□	□	379	
10	9609	400	□	□	379	
11	9610	400	□	□	379	
12	9611	400	□	□	379	
13	9612	400	□	□	379	
14	9613	400	□	□	379	
15	9614	400	□	□	379	
16	9615	400	□	□	379	

```
Content-Language: en
app: mobile
version: 1.4.0
Connection: close

{"code":"9627","phone":"+447715375835"}
```

Figure 5 - Phone Number Verification PIN Brute forced.

4.8 Self-Signed SSL/TLS Certificate

Finding No 8.	Systems Affected	**TCP Port 6001** `wallet.temtum.com (54.38.214.253)`
	Finding	Network testing identified a self-signed SSL/TLS certificate.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**2** 🟩🟨⬜⬜⬜
	Likelihood	**2** 🟩🟨⬜⬜⬜
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

4.8.1 Retest Status

Retesting confirmed the service on was disabled, therefore not exposing the self-signed certificate.

4.8.2 Summary

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link over an untrusted network, often between a web server and a browser.

If a client encounters an invalid SSL certificate, their web browser will often display an alert to the user informing them of the potential security implications. This can cause the users of the web application to lose confidence in the authenticity of the web site and may prevent them from proceeding further.

4.8.3 Technical Details

The following SSL/TLS certificate was identified as self-signed and not generated by a trusted Certificate Authority:

- C=GB/ST=England/L=London/O=Dragon Infosec Ltd/CN=dragoninfosec/E=enquiries@dragoninfosec.com

SSL server certificates are intended to be used by the client so that they know that the server's public key belongs to the intended server. The guarantee comes from the SSL certificate being signed by a trusted third-party Certificate Authority (CA), which is required to perform extensive verification of the requester identity before issuing the certificate. When a web client (the user and their web browser) "accepts" a certificate which has not been issued by one of the CAs that the client trusts, there is a risk is that the client could be communicating with a malicious server.

4.8.4 Recommendation

BSI recommends that new certificate be generated for the identified services using valid details from a trusted Certification Authority.

4.9 Information Disclosure Through HTTP Headers

Finding No 9.	Systems Affected	**TCP Port 80** `wallet.temtum.com (54.38.214.253)`
	Finding	Testing identified information disclosure within the HTTP response headers, which revealed technical configuration details.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**1** 🟩⬜⬜⬜⬜
	Likelihood	**4** 🟩🟨🟧🟧⬜
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

4.9.1 Retest Status

Retesting confirmed the removal of the version information from the server banner.

4.9.2 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.

4.9.3 Technical Details

The following HTTP response was returned disclosing that Nginx is supporting the web 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)

4.9.4 Recommendation

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

4.10 HTTP Strict Transport Security Not Enforced

Finding No 10.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	The application did not utilise a header to mandate all client connections over a secure connection.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**2** 🟩🟨🟨🟧🟥
	Likelihood	**2** 🟩🟨🟨🟧🟥
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

4.10.1 Retest Status

Retesting confirmed the addition of the security header as follows:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
```

4.10.2 Summary

The application did not utilise a header to mandate all client connections over a secure connection.

4.10.3 Technical Details

HTTP "Strict-Transport-Security" (HSTS) was not found in the HTTP headers sent by the application.

An attacker who is able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser does not attempt to use an encrypted connection.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. The 'sslstrip' tool can be used to automate this process.

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

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

https://developer.mozilla.org/en-US/docs/Web/Security/HTTP_strict_transport_security

4.10.4 Recommendation

BSI recommends that the application should instruct web browsers to only access the application using HTTPS.

To do this, enable HSTS by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

4.11 Missing Content Security Policy Header

Finding No 11.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	No Content Security Policy has been defined.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**2** 🟩🟨🟨🟧🟥
	Likelihood	**2** 🟩🟨🟨🟧🟥
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

4.11.1 Retest Status

Retesting confirmed the addition of the CSP header as follows:

```
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'
'unsafe-eval' https://ssl.google-analytics.com https://www.google.com
https://ssl.google-analytics.com https://www.google.com https://assets.zendesk.com
https://connect.facebook.net https://js.stripe.com/  https://www.gstatic.com
https://assets.zendesk.com https://connect.facebook.net; img-src 'self'
https://ssl.google-analytics.com https://s-static.ak.facebook.com
https://assets.zendesk.com; style-src 'self' 'unsafe-inline'
https://fonts.googleapis.com https://assets.zendesk.com; font-src 'self'
https://themes.googleusercontent.com; frame-src https://www.youtube.com/
https://js.stripe.com https://www.google.com https://assets.zendesk.com
https://www.facebook.com https://s-static.ak.facebook.com
https://tautt.zendesk.com; object-src 'none'
```

4.11.2 Summary

The HTTP Content-Security-Policy (CSP) response header allows web site administrators to control resources the user is allowed to load for a given page. It is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

4.11.3 Technical Details

The web application was found to be missing the "Content-Security-Policy" header.

Further details on the CSP header can be found at the following URLs:

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

https://content-security-policy.com/

https://csp-evaluator.withgoogle.com/

4.11.4 Recommendation

BSI recommends that a strict Content Security Policy is defined.

An example strict Content-Security-Policy is:

```
script-src 'strict-dynamic' 'nonce-rAnd0m123' 'unsafe-inline' https:;

object-src 'none';

base-uri 'none';

report-uri https://csp.example.com;
```

A strict content security policy can be achieved by adding nonce-source to every script tag to only allow specific trusted JavaScript to run. Each nonce should be unique to every web request, as if an attacker knows the nonce it can simply be embedded in the payload and used to bypass the protection.

To implement nonce-source, tag each script with a nonce as shown below:

```
<script nonce="2726c7f26c">

var inline = 1;

</script>
```

Then add the following CSP header to permit that block of inline JavaScript to be executed:

```
Content-Security-Policy: script-src 'nonce-2726c7f26c'
```

Further details on how to implement CSP a nonce can be found at the following URLs:

https://rehansaeed.com/content-security-policy-for-asp-net-mvc/

https://scotthelme.co.uk/csp-nonce-support-in-nginx/

4.12 Cross-Site Framing Vulnerability

Finding No 12.	Systems Affected	`https://wallet.temtum.com/api`
	Finding	It was possible to load the web application within an iFrame and access the application's functions as normal.
	CVE Number	N/A
	Root Cause	**Web Development**
	Impact	**2** 🟩🟨🟨🟧🟥
	Likelihood	**2** 🟩🟨🟨🟧🟥
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

4.12.1 Retest Status

Retesting confirmed the addition of the X-Frame-Options header as follows:

```
X-Frame-Options: SAMEORIGIN
```

4.12.2 Summary

Cross-Site Framing, also known as ClickJacking, is a vulnerability in the way the application renders itself within an iFrame. An attacker controlling a parent frame could capture keystrokes within a child frame. It is therefore imperative to the application's security that it cannot be rendered inside an iFrame.

4.12.3 Technical Details

Testing identified that it was possible to embed the application within an iFrame and use the application as normal via this frame.

An attacker could host a malicious page that loaded the application and allowed the details entered by a user to be captured by an attacker.

This type of attack would involve some element of social engineering.

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

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

4.12.4 Recommendation

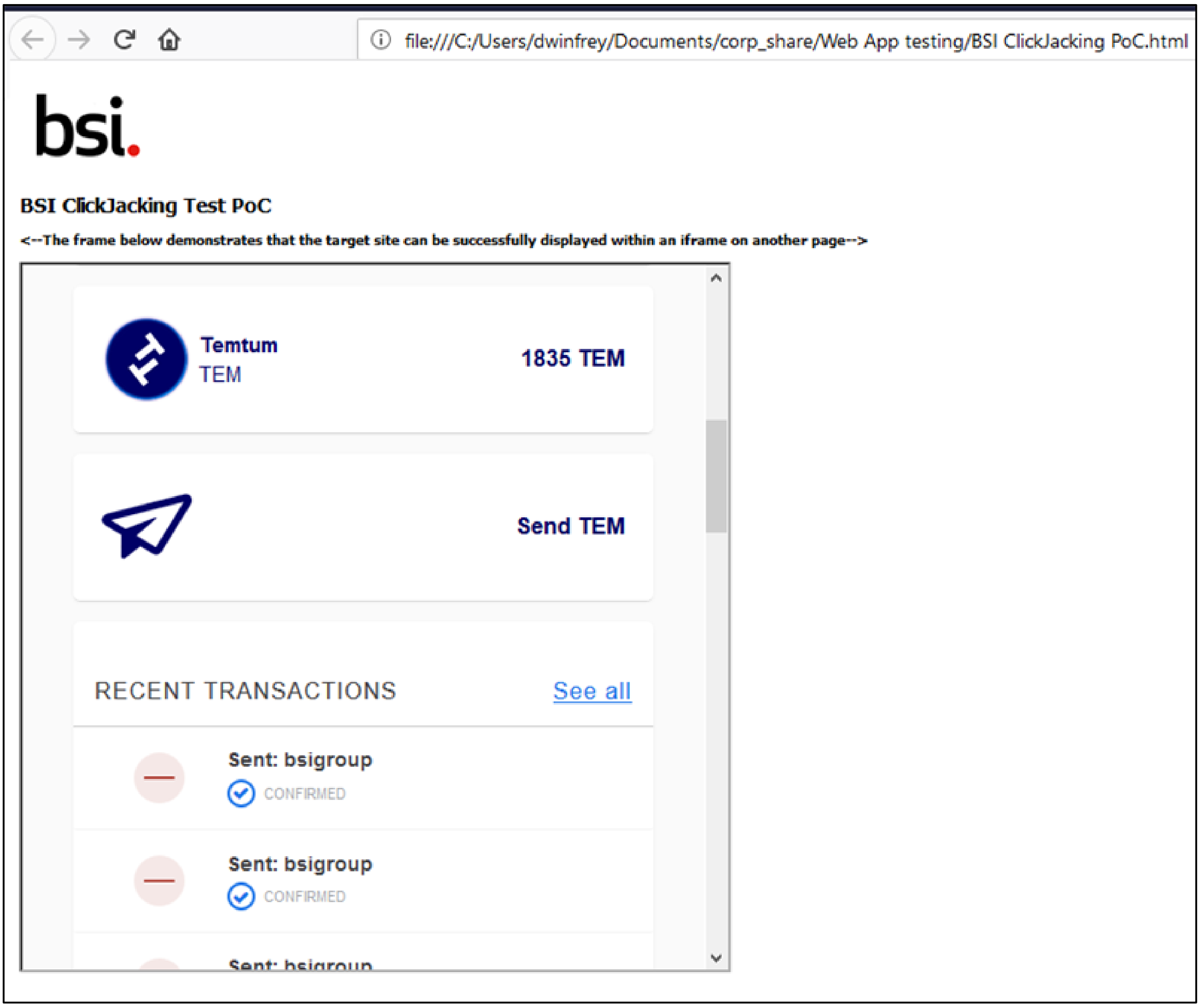
BSI recommends that “X-Frame-Options” header be employed by the applications to ensure that pages do not load inside an iFrame.

The "X-Frame-Options: DENY" header can be set to prevent browsers from loading applications within an iFrame.

Further information on “X-Frame-Options” can be found at the following web document:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

4.12.5 Screenshots



file:///C:/Users/dwinfrey/Documents/corp_share/Web App testing/BSI ClickJacking PoC.html

BSI ClickJacking Test PoC

<--The frame below demonstrates that the target site can be successfully displayed within an iframe on another page-->

Figure 6 - Temtum Wallet within an iFrame.

5 Results of SQLite Review

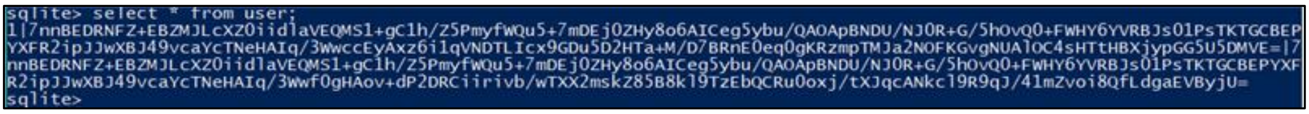
This section provides the detailed findings of the database review that was performed between the 11th and 13th December 2018.

5.1 No SQLite Database Encryption

Finding No 13.	Systems Affected	`App.db`
	Finding	It was identified that the SQLite database was not encrypted.
	CVE Number	N/A
	Root Cause	**Encryption**
	Impact	**5** 🟩🟨🟧🟧🟥
	Likelihood	**2** 🟩🟨
	Overall Risk Rating	**10 (Medium Risk)**
	Status	**PARTIALLY RESOLVED**

5.1.1 Retest Status

Retesting confirmed the token and refresh token that are used to authenticate with the API have been encrypted using Secured-Preference-Store that uses the android KeyStore (shown below).



```
sqlite> select * from user;
1|7nnBEDRNFZ+EBZMJLcXZ0iidlaVEQMS1+gC1h/Z5PmyfWQu5+7mDEj0ZHy8o6AICeg5ybu/QAOApBNDU/NJ0R+G/5hOvQ0+FWHY6YVRBJs01PsTKTGCBEP
YXFR2ipJJwXBJ49vcaYcTNeHAIq/3WwccEyAxz6i1qVNDTLIcx9GDu5D2HTa+M/D7BRnE0eq0gKRzmpTMJa2NOFKGvgNUA1OC4sHTtHBXjypGG5U5DMVE=|7
nnBEDRNFZ+EBZMJLcXZ0iidlaVEQMS1+gC1h/Z5PmyfWQu5+7mDEj0ZHy8o6AICeg5ybu/QAOApBNDU/NJ0R+G/5hOvQ0+FWHY6YVRBJs01PsTKTGCBEPYXF
R2ipJJwXBJ49vcaYcTNeHAIq/3Wwf0gHAov+dP2DRCiirivb/wTXX2mskZ85B8k19TzEbQCRu0oxj/tXJqcANkc19R9qJ/41mZvoi8QfLdgaEVByjU=
sqlite>
```

Figure 7 - JSON Web Token Encrypted

5.1.2 Summary

SQLite is a very basic database that stores data within a flat file. If this file is compromised all data within it can be read. If the android device is rooted the file can be read. Therefore, it is best practice to encrypt the SQLite database.

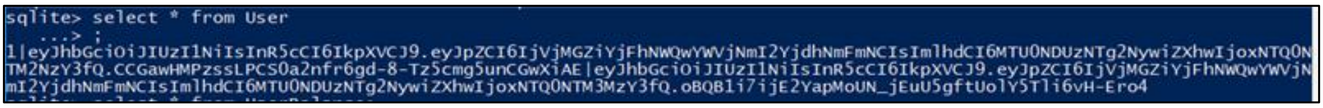
5.1.3 Technical Details

It was identified that the SQLite used by the android app (app.db) was not encrypted. The database contains the JSON Web Token that is used as authentication to the wallet API.

5.1.4 Recommendation

BSI recommends that data encryption technology is used to protect the data stored or sensitive session data is not stored within the database.

5.1.5 Screenshots



```
sqlite> select * from User
   ...> ;
1|eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjVjMGZiYjFhNWQwYWVjNmI2YjdhNmFmNCIsImlhdCI6MTU0NDUzNTg2NywiZXhwIjoxNTQ0N
TM2NzY3fQ.CCGawHMPzssLPCS0a2nfr6gd-8-Tz5cmg5unCGwXiAE|eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjVjMGZiYjFhNWQwYWVjN
mI2YjdhNmFmNCIsImlhdCI6MTU0NDUzNTg2NywiZXhwIjoxNTQ0NTM3MzY3fQ.oBQB1i7ijE2YapMoUN_jEuU5gftUolY5Tli6vH-Ero4
```

Figure 8 - JSON Web Token Stored within the SQLite Database

6 Results of Server Build Review

This section provides the detailed findings of the server build review that was performed between the 11th and 13th December 2018.

6.1 World Writeable Files Identified

Finding No 14.	Systems Affected	`192.168.0.28 (CI-SERVER)`
	Finding	Files were identified which permitted write access by any user on the UNIX operating system.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**3** 🟩🟨🟧⬜⬜
	Likelihood	**3** 🟩🟨🟧⬜⬜
	Overall Risk Rating	**9 (Medium Risk)**
	Status	**RESOLVED**

6.1.1 Retest Status

Retesting confirmed the files listed were no longer world writable.

6.1.2 Summary

Data in world-writable files can be modified and compromised by any user on the system. World-writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

6.1.3 Technical Details

The following files were identified as being world writeable:

- /var/lib/veeam/mountlock
- /var/lib/veeam/svclock
- /var/log/veeam/Backup/_backup/sessions_logs.8.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.10.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.6.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.11.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.1.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.9.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.5.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.2.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.4.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.7.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.3.tar.gz
- /var/log/veeam/Backup/_backup/sessions_logs.12.tar.gz
- /var/log/veeam/veeamsvc.log.gz
- /root/.npm/_cacache/index-v5/21/32/0f0c342557663e857aa54fa96025616fe9fc30afdf329802a461f5f0f026

- /root/.npm/_cacache/index-v5/ff/48/5e30648e089b4166b1a323ec42c2a63a71a338904b4b7469fe1edf540ccf
- /root/.npm/_cacache/index-v5/6a/21/7c903ed803323f2a936f08b149547e58ae8d80a8a6895e84597c8fdcadbd
- /root/.veeam/ui_start_counter
- /run/lvm/.cache
- /run/veeamservice.pid
- /srv/tmp/{ab152fdc-1d05-465e-90e1-69932c3e2404}/lvm.conf

The following command, executed as root, can be used to view all world writeable files on the server:

```
find / -type f \( -perm -0002 -a ! -perm -1000 \) -ls
```

6.1.4 Recommendation

BSI recommends that a review be carried out on the permissions assigned to the identified files and, where not specifically required, world writeable file permissions should be removed.

Normally, it is advisable to remove write access for the "other" category, which can be achieved using the following command.

```
chmod o-w <filename>
```

It is highly recommended that if the files are part of a software component, that any relevant vendor documentation is consulted prior to making any changes in order to prevent breaking any application dependencies on a given file.

6.2 SSH Server Permits Remote Root Login

Finding No 15.	Systems Affected	**TCP Port 22** 192.168.0.28 (CI-SERVER)
	Finding	The Secure Shell (SSH) service allows the root user to login remotely.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**4** 🟩🟨🟧🟧🟥
	Likelihood	**2** 🟩🟨🟨🟧🟥
	Overall Risk Rating	**8 (Medium Risk)**
	Status	**RESOLVED**

6.2.1 Retest Status

Retesting confirmed remote root login had been disabled. The sshd_config file is as follows:

```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

6.2.2 Summary

The SSH service allows the root user to login remotely. This does not follow best security practice and would allow an attacker to attempt to brute force the root password. If the password was guessed, the user would have full root privileges to the system.

6.2.3 Technical Details

A review of the server configuration identified that the SSH service was configured to allow the root user to login remotely, as shown in the following extract from /etc/ssh/sshd_config:

```
# Authentication:

LoginGraceTime 120

PermitRootLogin yes

StrictModes yes
```

6.2.4 Recommendation

BSI recommends that the SSH service should be configured so that the root user cannot login directly.

This can be accomplished by modifying the PermitRootLogin directive in the SSH server configuration file (/etc/ssh/sshd_config) as shown below:

```
PermitRootLogin no
```

Standard user accounts should be configured that have SUDO permissions to run privileged tasks if and when required.

6.3 No Antivirus Software Installed

Finding No 16.	Systems Affected	`192.168.0.28 (CI-SERVER)`
	Finding	No antivirus software was found to be installed.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**3** 🟩🟨🟧
	Likelihood	**2** 🟩🟨
	Overall Risk Rating	**6 (Medium Risk)**
	Status	**RESOLVED**

6.3.1 Retest Status

Retesting confirmed ClamAV 0.99.4 was installed.

6.3.2 Summary

Antivirus software is designed to provide protection for systems against the threat of viruses and other malicious software. Antivirus software protects against infections caused by many types of malware, including viruses, worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware.

6.3.3 Technical Details

No antivirus software was found to be installed on the system reviewed, and therefore it is not protected against the aforementioned threats and unnecessarily exposed to potential compromise by known threats that would otherwise be detected and blocked.

6.3.4 Recommendation

BSI recommends that antivirus software be installed. In addition, checks should be made to ensure that regular signature updates are performed to help mitigate against the latest malware threats.

6.4 No Local Firewall Configured

Finding No 17.	Systems Affected	`192.168.0.28 (CI-SERVER)`
	Finding	The local firewall was found to not be configured on the system.
	CVE Number	N/A
	Root Cause	**Configuration**
	Impact	**2** 🟩🟨🟨🟧🟥
	Likelihood	**2** 🟩🟨🟨🟧🟥
	Overall Risk Rating	**4 (Low Risk)**
	Status	**RESOLVED**

6.4.1 Retest Status

Retesting confirmed ufw was configured.

6.4.2 Summary

Installing a local firewall reduces the attack surface of the system and can also be used for simple egress filtering. A firewall implementation can significantly hinder an attacker from gaining remote access to a server or workstation.

6.4.3 Technical Details

A review identified that no local firewall was configured on the system, and therefore it was possible to connect to all services listening on the systems when connected to the internal network.

If a worm infected a single machine on the network, there is a risk that the same vulnerability would be present in other machines. A local firewall only permitting access to specific ports from specified machines would help to stop malware from spreading throughout the infrastructure.

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

https://technet.microsoft.com/en-gb/library/cc700820.aspx

6.4.4 Recommendation

BSI recommends that the local firewall be configured and enabled where appropriate.

Ports for remote administration should be only open to administrative workstations and servers.

7 Summary of Findings

7.1 Results of Android Application Testing

Finding No.	Impact	Likelihood		Overall Risk	Finding	Recommendation	Status
1	4	4		**High**	**No Root Detection** The application was found to run on a rooted android device.	BSI recommends that the application performs root checking at run time.	**RESOLVED**
2	4	3		**High**	**Weak Payment Password PIN** The Payment Password PIN was found to be short and vulnerable to brute force.	BSI recommends that a longer Payment Password PIN should be used.	**RESOLVED**
3	4	3		**High**	**Payment Password PIN Force Reset** It was possible to overwrite the Payment Password without knowing the current Payment PIN.	BSI recommends that a longer Payment Password PIN should be used.	**RESOLVED**
4	2	5		**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 configured to return generic error messages to ensure that they do not indicate whether a valid user account has been provided or not.	**ONGOING**
5	3	3		**Medium**	**Multiple Vulnerabilities Within Nginx Web Server** Multiple vulnerabilities were identified in the version of the Nginx Web Server software running on the system.	BSI recommends that the Nginx HTTP server be upgraded to the latest stable version.	**RESOLVED**
6	4	2		**Medium**	**Unnecessary Admin Service Exposed to the Internet** The SSH admin service was found to be unnecessarily exposed to the Internet.	BSI recommends that the identified services be reviewed and if they are not functionally required, then access from the Internet should be blocked by a firewall.	**RESOLVED**

Finding No.	Impact	Likelihood		Overall Risk	Finding	Recommendation	Status
7	2	2		**Low**	**Weak Phone Number Verification PIN** The verification PIN was found to be short and vulnerable to brute force.	BSI recommends that a longer Phone Number Verification PIN should be configured.	**RESOLVED**
8	2	2		**Low**	**Self-Signed SSL/TLS Certificate** Network testing identified a self-signed SSL/TLS certificate.	BSI recommends that new certificate be generated for the identified services using valid details from a trusted Certification Authority.	**RESOLVED**
9	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 headers are removed or obfuscated in order to prevent unnecessary information disclosure.	**RESOLVED**
10	2	2		**Low**	**HTTP Strict Transport Security Not Enforced** The application did not utilise a header to mandate all client connections over a secure connection.	BSI recommends that the application should instruct web browsers to only access the application using HTTPS.	**RESOLVED**
11	2	2		**Low**	**Missing Content Security Policy Header** No Content Security Policy has been defined.	BSI recommends that a strict Content Security Policy is defined.	**RESOLVED**
12	2	2		**Low**	**Cross-Site Framing Vulnerability** It was possible to load the web application within an iFrame and access the application's functions as normal.	BSI recommends that “X-Frame-Options” header be employed by the applications to ensure that pages do not load inside an iFrame.	**RESOLVED**

7.2 Results of SQLite Review

Finding No.	Impact	Likelihood		Overall Risk	Finding	Recommendation	Status
13	5	2		Medium	**No SQLite Database Encryption** It was identified that the SQLite database was not encrypted.	BSI recommends that data encryption technology is used to protect the data stored or sensitive session data is not stored within the database.	PARTIALLY RESOLVED

7.3 Results of Server Build Reviews

Finding No.	Impact	Likelihood		Overall Risk	Finding	Recommendation	Status
14	3	3		**Medium**	**World Writeable Files Identified** Files were identified which permitted write access by any user on the UNIX operating system.	BSI recommends that a review be carried out on the permissions assigned to the identified files and, where not specifically required, world writeable file permissions should be removed.	**RESOLVED**
15	4	2		**Medium**	**SSH Server Permits Remote Root Login** The Secure Shell (SSH) service allows the root user to login remotely.	BSI recommends that the SSH service should be configured so that the root user cannot login directly.	**RESOLVED**
16	3	2		**Medium**	**No Antivirus Software Installed** No antivirus software was found to be installed.	BSI recommends that antivirus software be installed. In addition, checks should be made to ensure that regular signature updates are performed to help mitigate against the latest malware threats.	**RESOLVED**
17	2	2		**Low**	**No Local Firewall Configured** The local firewall was found to not be configured on the system.	BSI recommends that the local firewall be configured and enabled where appropriate.	**RESOLVED**

Appendix A - Testing Team

This project was undertaken using the following consultants:

- Duncan Winfrey

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.

```
Overall risk = Seriousness x 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.

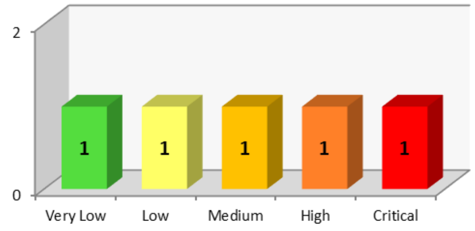
Likelihood					
5	Low	Medium	High	Critical	Critical
4	Low	Medium	High	High	Critical
3	Low	Medium	Medium	High	High
2	V. Low	Low	Medium	Medium	Medium
1	V. Low	V. Low	Low	Low	Low
	1	2	3	4	5

Seriousness (Impact)

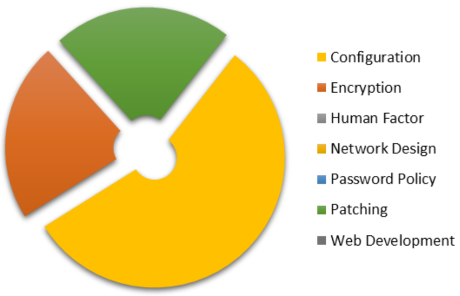
Overall Risk Rating
Critical (20-25)
High (12-16)
Medium (6-10)
Low (3-5)
Very Low (1-2)

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:

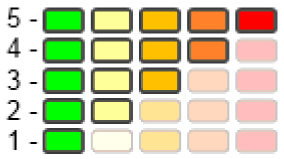
- Configuration
- Encryption
- Human Factor
- Network Design
- Password Policy
- Patching
- Web Development

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).  (visual representation)
	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.