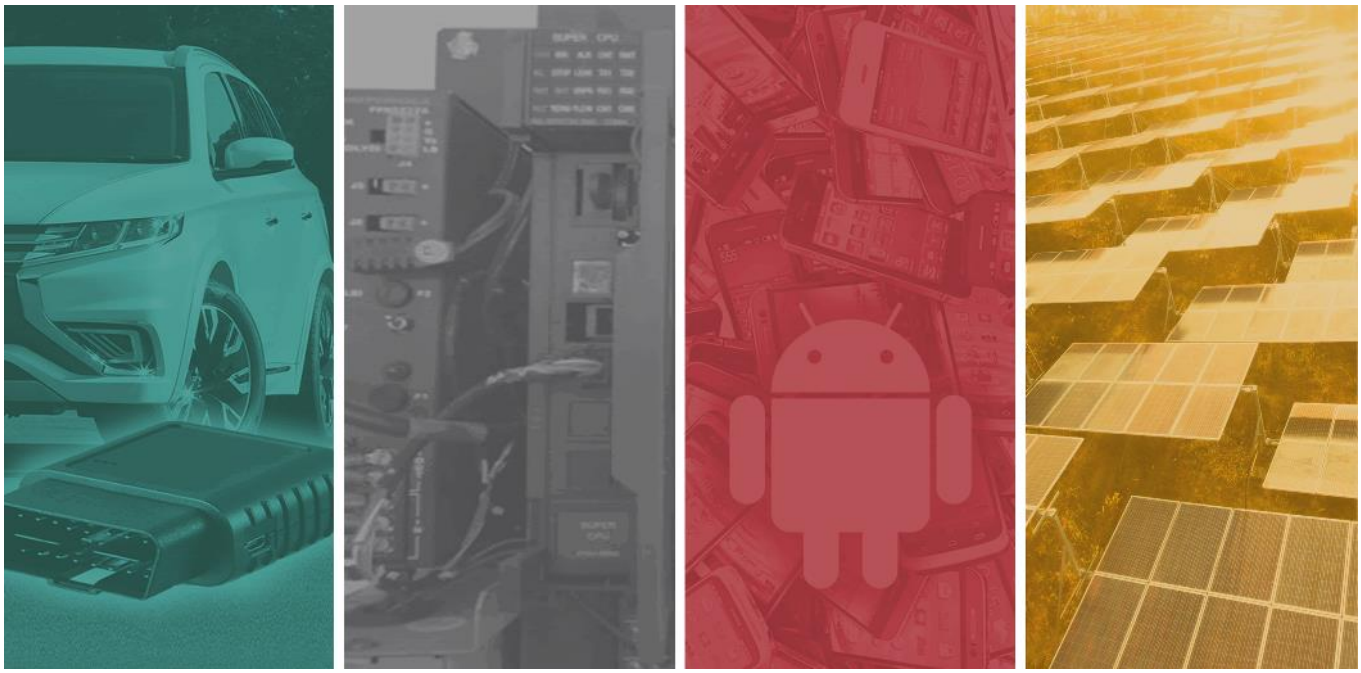
PEN TEST PARTNERS

Bebop Web Application Test

for

Wintermute Trading



PTP Job ID: 12326
Version 1.0
30th May 2022

Technical Consultant: Senad Zukic
Account Manager: Mark Harrison

CVSS CREST

TIGERSCHEME
Providing excellence in penetration testing

1. Business Risk Summary

Test	Risk
Bebop Web Application	

Introduction

Wintermute Trading (Wintermute) engaged Pen Test Partners (PTP) to perform an API test against the Bebop application. This was to identify misconfigurations and security weaknesses that affect the security posture of the in-scope environment and assess any potential risks that could cause a breach of the application security or damage the brand.

Areas of Good Practice

The host server was found to only have HTTPS service opened and no other services were enabled, also, the TLS configuration was found to be correctly configured. No issues were identified with the APIs, however, other issues were found with the overall application and host which require remediation.

Key Findings

The application test identified one “medium” and three “low” rated issues; these issues were all caused due to poor configuration of the web application. The host was found to be running an out-of-date version of the NGINX web server.

A number of HTTP security headers were found to be missing, including HTTP Strict Transport Security (HSTS). Another issue disclosed the underlying version of the web server technology; this could allow an attacker to better target the application should a vulnerability for that version be released.

Conclusion

Overall, the application was found to need some improvements. The issues identified mostly concern the configuration of the web applications, this ranges from out-of-date webserver software to missing HTTP headers. It is recommended that these findings be remediated toimprove the overall security of the web applications.

2. Technical Summary

The table below lists all security issues that were identified on systems within the scope of this test.

2.1. Bebop Web Application Test

Issue ID	Vulnerability	Affected	CVSS
WEB-M1	Nginx Web Server Out of Date	bebop.finance TCP/443 bebop.xyz TCP/443	**6.9**
WEB-L2	HTTP Security Headers Not Implemented or Not Securely Configured		**3.5**
WEB-L3	Information Disclosure in HTTP Headers		**3.5**
WEB-L4	Cacheable HTTPS Response Being Cached		**3.1**
WEB-I5	Source Code Disclosure		**Info**

3. Table of Contents

4. Document and Test Control

4.1. Version History

Version	Date	Author	Comment	Distribution
0.1	17/05/2022	Senad Zukic	Author	
0.2	19/05/2022	Kate Owen	Grammar QA	
0.3	25/05/2022	Lewis Kimber	Technical QA	
1.0	**30/05/2022**	**Senad Zukic**	**Release**	**Eric McEvoy**

4.2. Engagement Scope

Wintermute Trading (Wintermute) engaged Pen Test Partners (PTP) to perform a web application test of their Bebop platform. This phase of testing took place between 5th May and 12th May 2022 and was authorised by Eric McEvoy of Wintermute Trading.

This report details the following elements of work:

- Web Application
    - https://bebop.finance (mid-way through the test a new domain was purchased and used https://bebop.xyz)

The following consultant was involved in this engagement:

- Senad Zukic - Security Consultant

No Denial-of-Service (DoS) attacks were performed.

4.3. System Rollback

Not applicable due to the use of Web3 technologies which do not use traditional accounts.

5. Application

5.1. Introduction

The following applications were selected for the web application testing phase:

- https://bebop.finance (mid-way through the test a new domain was purchased and used https://bebop.xyz)

The following screenshot shows the main landing pages of these applications:

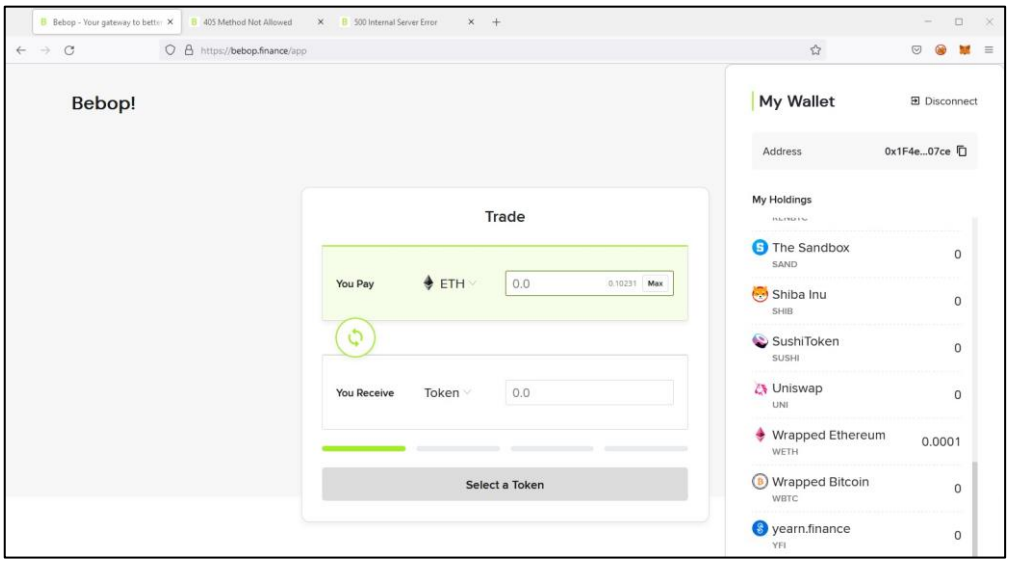


Figure 1: Initial view of the Bebop application

A full SYN port scan was carried out against the host, only one port was found to be open, this shows good security practice.

```
$ sudo nmap -sSCV -p - -Pn bebop.xyz
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 14:07 BST
Nmap scan report for bebop.xyz (18.168.19.25)
Host is up (0.026s latency).
rDNS record for 18.168.19.25: ec2-18-168-19-25.eu-west-2.compute.amazonaws.com
Not shown: 65534 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/*
|_http-title: Bebop - Your gateway to better trades in DeFi
| ssl-cert: Subject: commonName=bebop.xyz
| Subject Alternative Name: DNS:bebop.xyz, DNS:www.bebop.xyz
| Not valid before: 2022-05-10T14:12:34
|_Not valid after:  2022-08-08T14:12:33
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 2: Full SYN port scan

A review of the TLS configuration was completed during the test and no issues were identified.

```
Start 2022-05-12 14:36:40        -->> 18.168.19.25:443 (bebop.xyz) <<--

 rDNS (18.168.19.25):    ec2-18-168-19-25.eu-west-2.compute.amazonaws.com.
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   http/1.1 (advertised)
 ALPN/HTTP2 http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            not offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

Figure 3: TLS configuration review

As part of the test, the consultant assessed the overall application. It was found that the application was still being developed. However, the majority of the functionality was carried out by third-party API's, using various Web3 technologies.

A part of the applications source code was accessible due to the use of client-side technologies:

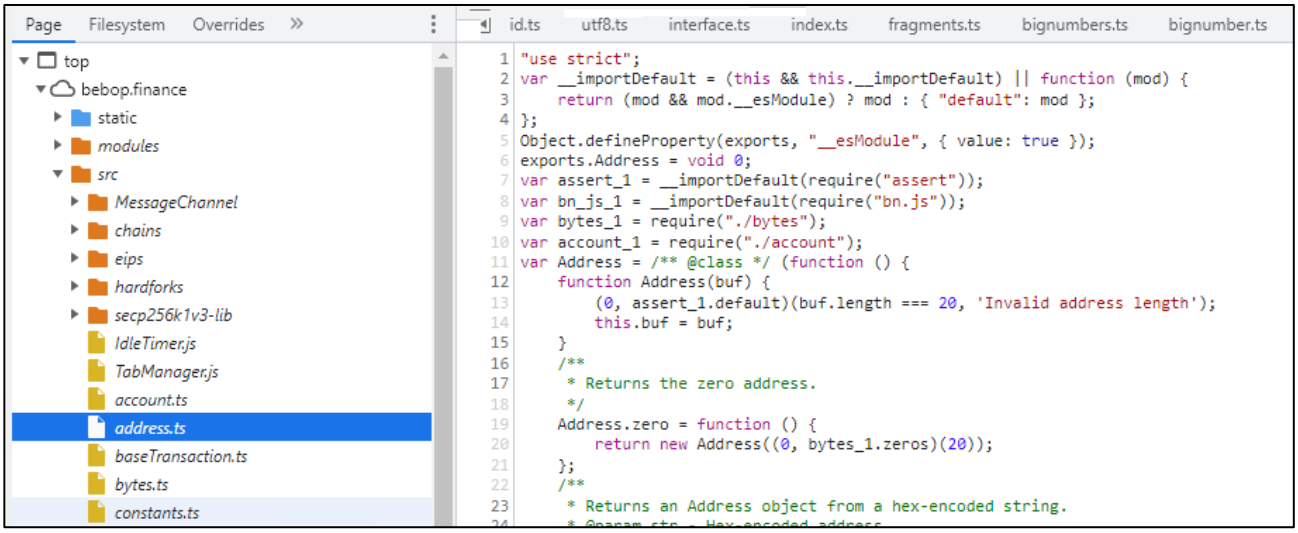


Figure 4: Client-side source disclosure

There was no sensitive information disclosed that could severely impact the operation of the application. However, because the client-side code could be modified, it was possible to bypass the “allow” feature which only allowed specific wallet addresses.

The following file `/static/js/main.b41046cc.chunk.js` contained all the allowed wallet addresses, the highlighted address is the consultant’s own address that was put on the allow list by the client.

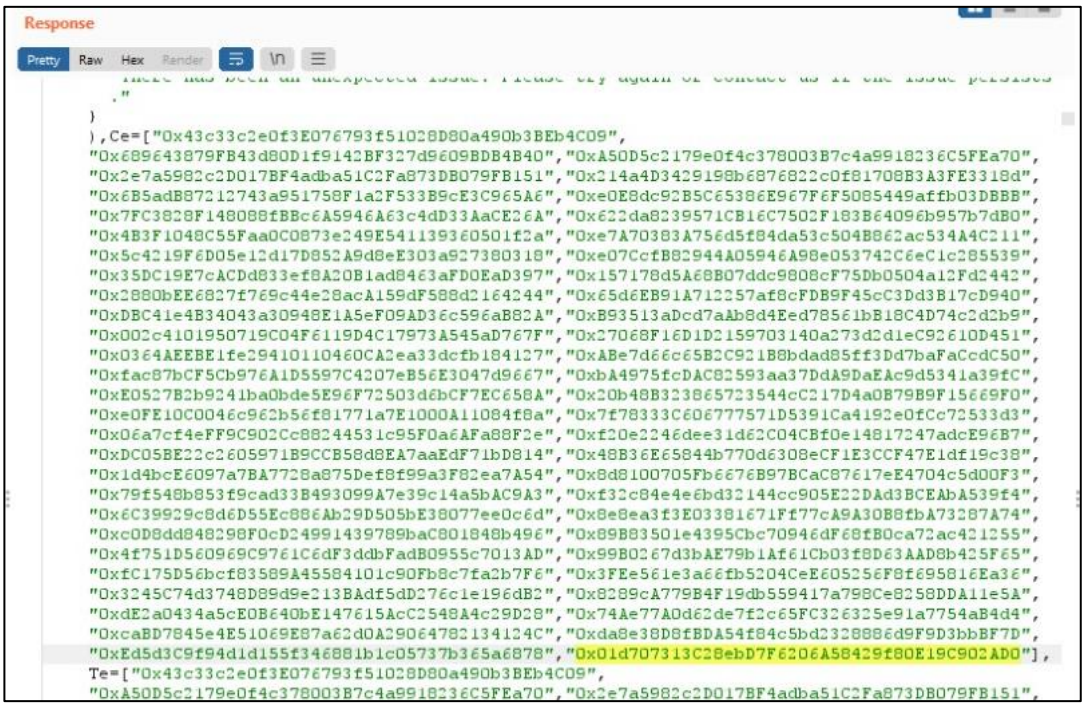


Figure 5: List of allowed wallet addresses

These addresses can also be found in the `/static/js/config.js` in the source code files:

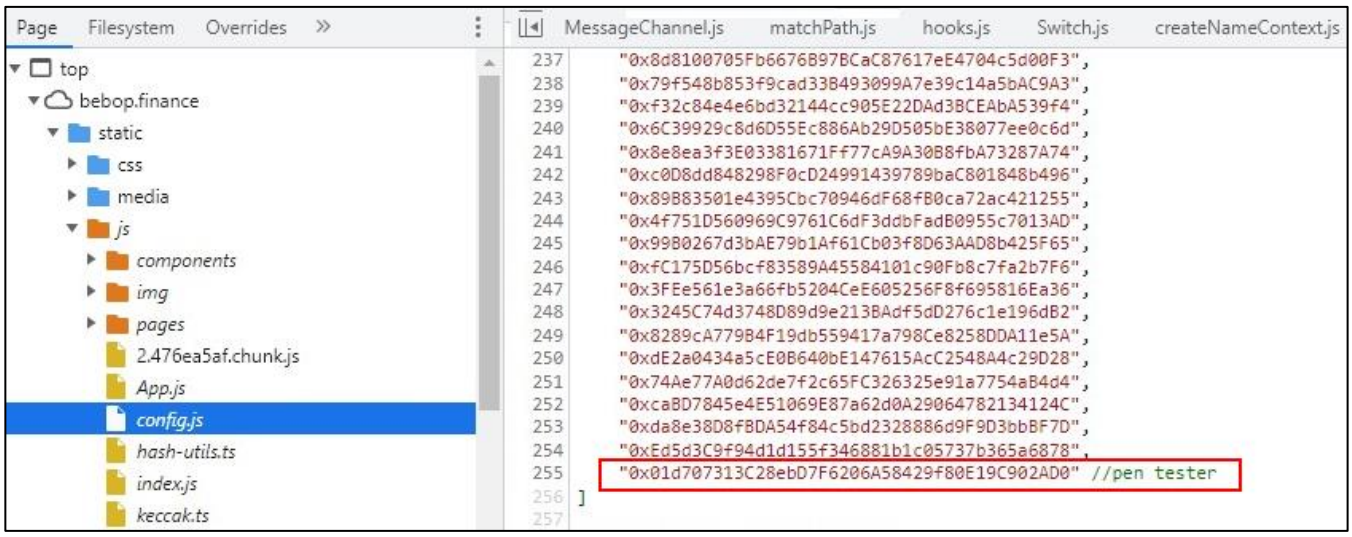


Figure 6: Source code view of the "config.js" file

It was possible to manipulate the `/static/js/main.b41046cc.chunk.js` file on the client-side to add another address that could then be used to access the application:

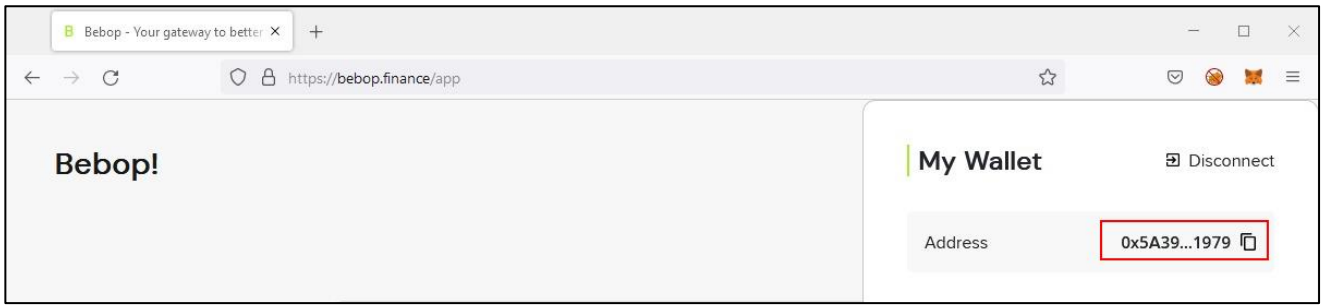


Figure 7: Accessing the application using another wallet address

It should be noted that this allow list is used to limit who can participate in the Beta program and, as such, should not be an issue in the live environment.

However, if this feature was to be used in live environment, then a server-side API call should be made to validate the address before access is granted.

6. Findings

6.1. WEB-M1: NGINX Web Server Out of Date

The affected NGINX web servers were fingerprinted to an outdated version, making them susceptible to known vulnerabilities.

It is recommended that all affected instances be patched to the latest stable versions.

Medium Risk
CVSS 6.9

Description

A NGINX web server was found which, according to the server header, is an outdated version which is susceptible to known vulnerabilities, mainly a remote code execution vulnerability. A security issue in NGINX resolver was identified, which might allow an unauthenticated remote attacker to cause a 1-byte memory overwrite, by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

It was not possible to exploit this issue during the testing window and the consultant has instead relied on the application's self-reported version number.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 11 May 2022 09:55:22 GMT
Content-Type: application/json
Content-Length: 3316
Connection: close
Access-Control-Allow-Origin: *

{"usd_prices":{"1INCH":"1.020090467800000011","AAVE":"106.013190731199998140","ACH"
:"0.018500740700000001","AGLD":"0.679388130600000029","ALCX":"43.345723955200000432
","ALPHA":"0.217801495700000014","AMP":"0.012480497700000001","ANGLE":"0.1179795759
00000008",
```

Figure 8: HTTP response showing server version

Recommendations

The mentioned software should be upgraded to its latest stable version. In order to mitigate the documented vulnerabilities, the version should be equal or later than 1.21.0.

Affected	bebop.finance TCP/443 bebop.xyz TCP/443
References & CVSSv3 Metrics	CVE-2021-23017: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23017 Root Cause: Patching Base Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H (8.2) Temporal Metrics: E:U/RL:O/RC:R (6.9) Environmental Metrics: CR:M/IR:M/AR:M (6.9)

6.2. WEB-L2: HTTP Security Headers Not Implemented or Not Securely Configured

There are a number of security headers that have been added to the HTTP specification, or are not formalised but widely supported, that can provide defence-in-depth protection against certain vulnerabilities.

Although their absence does not create an active security risk, use of these headers can help prevent future attacks against the API.

Low Risk
CVSS 3.5

Description

There are several security headers that have been added to the HTTP specification, either formally or informally, that tell the user agent to perform more checks and restrictions when rendering the content of the site. Some of these headers were found to be missing, or incorrectly set.

The table below highlights any weaknesses in the security headers present on a 'per-host' basis. Where headers are marked with an "×", this means that the header has not been set.

Where an "×" has been set, this indicates that the value falls short of current industry best practice recommendations.

Table 1: Security headers

Host	Strict-Transport-Security	X-Frame-Options	X-Content-Type-Options	Content-Security-Policy	Referrer-Policy	Feature-Policy
bebop.finance TCP/443 bebop.xyz TCP/443	×	×	×	×	×	×

Although this does not create an active security risk, use of these headers can help prevent future attacks against the host.

The extra headers can be found detailed below:

- **Strict-Transport-Security:** This asks the browser to only ever return to the site using HTTPS and thus can prevent certain man-in-the-middle attacks. It is not suitable for sites that do serve some of their content over HTTP.

- **X-Frame-Options**: Tells the user agent how to handle the site if it is rendered inside of a frame and thus prevent clickjacking attacks. Although clickjacking can be mitigated with frame busting JavaScript, using the header is the most supported and effective solution.

- **X-Content-Type-Options:** This instructs the user agent to use the MIME type of any content rather than attempt to intelligently work it out from the content. This can protect against client attacks from uploaded content.

- **Content-Security-Policy:** This provides a policy to tell the user agent how to manage supplied content (e.g., in-line JavaScript).

- **Referrer-Policy:** This allows a site to control how much information the browser includes with navigations away from a document.

- **Feature-Policy:** This allows a site to control which features and APIs can be used in the browser.

Recommendations

The recommendations below are for secure configurations of the mentioned security headers. Their use can influence the application's functionality and, therefore, should be reviewed in line with its requirements and other security measures.

"`Strict-Transport-Security: max-age=31536000; includeSubDomains`" enforces Strict Transport security on the application. All subsequent requests are forced by the browser onto HTTPS for all subdomains at least within the timeout period (in this example the timeout is 1 year). An optional setting for this header is the keyword 'preload' which causes the application's URL to be loaded into databases for pre-validation of HSTS, provided its HTTPS and HSTS configuration is correct. This follows good security practices, but it is difficult to revert and causes non-HTTPS content on the application to be nearly impossible to serve.

"`X-Content-Type-Options: nosniff`" asks supported browsers not to second guess the content type of files, but just to rely on what the web server specifies.

`Content-Security-Policy: script-src 'self'` is a basic CSP header that prevents loading resources from third-party domains. It should be noted that Content Security Policy (CSP) requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way a browser renders pages (e.g., in-line JavaScript disabled by default and must be explicitly allowed in policy). Please consult the references.

`Referrer-Policy: no-referrer` is a basic Referrer-Policy header that instructs the browser never to send the referrer header with requests that are made from your site. This may be too restrictive, however, and 'no-referrer' could instead be replaced with an alternative option such as 'same-origin'. Which value used depends on the requirements of the application. Please consult the references.

`Feature-Policy: <directive> <allowlist>` shows the syntax for a 'feature-policy' header. This header will vary greatly from site-to-site depending on the functionality that is required. Please consult the references.

In general, use of the extra HTTP headers is better supported and more effective than JavaScript hacks to perform the same functions. Setting security headers could be carried out on the web server configuration, on the application's code or even injected in reverse proxies fronting the application.

Browser compatibility with each header is variable, so functional validation is required. Please see references for more information.

Affected	bebop.finance TCP/443 bebop.xyz TCP/443
References & CVSSv3 Metrics	OWASP: Secure Headers Project: https://www.owasp.org/index.php/OWASP_Secure_Headers_Project Analyse your HTTP response headers: https://securityheaders.io Content Security Policy (CSP) Quick Reference Guide: https://content-security-policy.com/ Root Cause: Configuration Base Metrics: AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N (4.0) Temporal Metrics: E:U/RL:O/RC:C (3.5) Environmental Metrics: CR:M/IR:M/AR:M (3.5)

6.3. WEB-L3: Information Disclosure in HTTP Headers

The server sent information about the environment in the headers sent with each response from the server. This could reveal information about the server and reveal potential vectors for attack.

Review default banners sent to minimise information leakage.

Low Risk
CVSS 3.5

Description

The web server was found to send unnecessary HTTP headers with every request which may give away information about the server and environment in which the server runs. This included the NGINX version number.

This information would allow an attacker to perform a more targeted attack on the site.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 11 May 2022 09:55:22 GMT
Content-Type: application/json
Content-Length: 3316
Connection: close
Access-Control-Allow-Origin: *

{"usd_prices":{"1INCH":"1.020090467800000011","AAVE":"106.013190731199998140","ACH"
:"0.018500740700000001","AGLD":"0.679388130600000029","ALCX":"43.345723955200000432
","ALPHA":"0.217801495700000014","AMP":"0.012480497700000001","ANGLE":"0.1179795759
00000008",
```

Recommendations

Review the configuration of the web server to ensure that no extra HTTP headers are sent. Particular attention should be paid to headers that return exact version information.

Affected	bebop.finance TCP/443 bebop.xyz TCP/443
References & CVSSv3 Metrics	Root Cause: Configuration Base Metrics: AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N (4.0) Temporal Metrics: E:U/RL:O/RC:C (3.5) Environmental Metrics: CR:M/IR:M/AR:M (3.5)

6.4. WEB-L4: Cacheable HTTPS Response Being Cached

Unless otherwise directed, browsers may store a local cached copy of content received from web servers. This may give an attacker access if the victim's machine is compromised.

The application should return caching directives instructing browsers not to store local copies of any sensitive data.

Low Risk
CVSS 3.1

Description

Web browsers may cache HTTP content locally, unless otherwise directed, even if it is accessed via HTTPS. If sensitive information is received from the web application, then it may be stored in the local cache, which may be retrieved by other users with access to the same computer at the same or a future time.

All or part of the tested application was served in HTTP inside an encrypted tunnel (HTTP over SSL or HTTPS). However, the application failed to take all possible steps to prevent the caching of HTTPS pages within the local machine browser cache. If an attacker could gain access to the client computer, they may then be able to read the information contained in the cache.

The purpose of using HTTPS is to provide a secure medium in which potentially sensitive data could be transferred. Browser caches are usually not encrypted, so if one such user agent is compromised the information becomes instantly available. Potentially, session identifiers (particularly if leaked in GET parameters), login credentials, personal information and other resources may be cached by the browser.

Static content such as images, CSS code or JavaScript can usually be safely cacheable, even if transferred over HTTPS because its content is not generally of sensitive nature.

These were some of the files that were found to be cached:

- /server/getPrice
- /server/getUSDTokenPrices

Recommendations

The application should be modified to include non-caching directives in the HTML code of pages or with any type of sensitive data. This prevents browsers from storing local copies of such pages. Most web development platforms allow control of the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content.

At the protocol level, the web server can be configured to inject non-caching HTTP headers into the relevant paths or scripts within the web root. Caching may be locally disabled for HTML resources via an extra pair of META tags in the HEAD section.

Cache control of all other resources (JavaScript, XML, JSON, others) must be implemented via HTTP response headers:

```
Pragma: no-cache
Cache-control: no-store
```

Affected	bebop.finance TCP/443 bebop.xyz TCP/443
References & CVSSv3 Metrics	RFC 2616, Section 13: Caching in HTTP: http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html Caching Tutorial for Web Authors and Webmasters: http://www.mnot.net/cache_docs/ Root Cause: Configuration Base Metrics: AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N (3.5) Temporal Metrics: E:U/RL:O/RC:C (3.1) Environmental Metrics: CR:M/IR:M/AR:M (3.1)

6.5. WEB-I5: Source Code Disclosure

The application discloses a large part of its source code written in JavaScript and TrueScript including the libraries and dependencies used by NodeJS.

It is recommended that all sensitive information be stored and processed on the server-side.

Informational Only

Description

It was possible to view the applications source code. Although in this instance no sensitive information could be found, an attacker could use this information to figure out the applications functions also find any hidden functionality or routes.

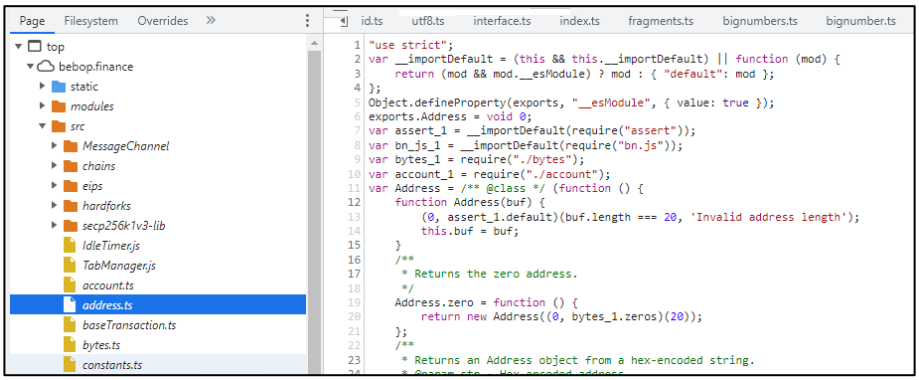


Figure 9: Client-side source disclosure

```
<Switch>
  <Route path="/" exact component={Home} />
  <Route path="/app" exact component={TradeInterface} />
  <Route path="/testmany" exact component={ManyToOne} />
  <Route path="/testapp" exact component={DupeTradeInterface} />
  <Route path="/faqs" exact component={Faqs} />
  <Route path="/devapp" exact component={TradeInterfaceDev} />
  <Route path="/singlescreen" exact component={SingleScreenApp} />
  <Route path="/manyui" exact component={ManyToOneUI} />
  <Route path="" exact component={NotFound} />
```

Figure 10: List of routes

Recommendations

Ensure that all source code is disclosed as intended and that no sensitive information is stored in these files.

Affected	bebop.finance TCP/443 bebop.xyz TCP/443
References & CVSSv3 Metrics	Root Cause: Configuration

7. Appendix - Risk Rating

Risk Rating

This report scores vulnerabilities using CVSS v3, the latest industry standard. It combines this with the simplicity of colour coding. This enables access to this report by all levels of management.

Issue Alerts

"Issue Alerts" allow the reader to quickly and easily identify issues and their associated severities. In each section, the reader can read a detailed description of the issue, how it was identified, and the associated mitigation that has been recommended.

Issues are rated either critical, high, medium or low risk depending on their CVSS v3 score. Informational recommendations may also be made that do not relate to a specific vulnerability or associated risk. Each risk group is assigned its own colour as shown below:

Informational	Low Risk	Medium Risk	High Risk	Critical Risk

CVSS v3 Explanation

CVSS (currently version 3) is the Common Vulnerability Scoring System. This is a vendor independent way of scoring vulnerabilities in a more granular way than just being assigned as a critical, high, medium, or low risk.

This system takes a variety of factors (known as metrics) into account such as the level of complexity required to reach the affected system, whether or not exploit code exists, the impact successful exploitation of the issue would have on the business and the type of area of concern (availability, confidentiality and integrity).

By applying these factors to each unique vulnerability, a score from 0 to 10 is calculated and assigned.
Pen Test Partners assigns critical, high, medium or low to each vulnerability based on the following criteria:

Critical:	Any issue with a CVSS score of 9.0 or higher
High:	Any issue with a CVSS score of 7.0 or higher but lower than 9.0
Medium:	Any issue with a CVSS score of 4.0 or higher but lower than 7.0
Low:	Any issue with a CVSS score lower than 4.0

This assures that each vulnerability has been tailored to the client, as each vulnerability affects each client in different ways.

For example, an SQL injection issue affecting a public facing website would be an extremely high risk. That same issue on an internal host with adequate firewall configurations could be classed as a medium risk. A high-risk issue on a low impact server may carry a lower CVSS score than a medium risk issue on a critical server.

For more information on CVSS please refer to the First.org website link: http://www.first.org/cvss/.