**Practical Activity of Unit 7 (daedalus-systems.tech-sourcery.co.uk)**

* What Operating System does the web site utilise?
* What web server software is it running?
* Is it running a CMS (WordPress, Drupal, etc?)
* What protection does it have (CDN, Proxy, Firewall?)
* Where is it hosted?
* Does it have any open ports?
* Does the site have any known vulnerabilities?
* What versions of software is it using? Are these patched so that they are up to date?

**Q1 What Operating System does the website utilise?**

To determine the operating system that the website uses we can use a number of techniques the first we will use is to grab the banner from the webserver using the curl tool

**curl -s -I daedalus-systems.tech-sourcery.co.uk | grep Server**

This returns the following

**HTTP/1.1 200 OK**

**Date: Thu, 27 Jan 2022 13:14:14 GMT**

**Server: Apache**

**X-Powered-By: PHP/7.3.33**

**Set-Cookie: OCSESSID=2aa0eb77950ebcbd4d21d5b84f; path=/**

**Set-Cookie: language=en-gb; expires=Sat, 26-Feb-2022 13:14:14 GMT; Max-Age=2592000; path=/; domain=daedalus-systems.tech-sourcery.co.uk**

**Set-Cookie: currency=USD; expires=Sat, 26-Feb-2022 13:14:14 GMT; Max-Age=2592000; path=/; domain=daedalus-systems.tech-sourcery.co.uk**

**Strict-Transport-Security: max-age=63072000; includeSubDomains**

**X-Frame-Options: SAMEORIGIN**

**X-Content-Type-Options: nosniff**

**Upgrade: h2,h2c**

**Connection: Upgrade**

**Content-Type: text/html; charset=utf-8**

From this we can see the see the server is running Apache and PHP while versions of these are available for windows it is more likely this is running a flavour of the Linux Operating System.

If we then then use the NMAP tool with the -O OS fingerprinting option we get the following output that would indicate that we were correct in our theory that the server was running Linux as its OS.

**Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 5.1 (93%), Linux 3.2 - 4.9 (93%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 4.10 (92%), Linux 4.2 (92%), Linux 4.4 (92%), Asus RT-AC66U WAP (92%), Linux 3.11 - 3.12 (92%)**

So In Answer to Question one the Most likely OS the server is running is **LINUX**

**Q2 What web server software is it running?**

From our initial curl and NMAP probe we know that the server is running a version of Apache but we don’t know the version as this information has been stripped from the HTML header

**curl --HEAD daedalus-systems.tech-sourcery.co.uk**

**HTTP/1.1 200 OK**

**Date: Thu, 27 Jan 2022 13:35:08 GMT**

**Server: Apache**

**X-Powered-By: PHP/7.3.33**

**Set-Cookie: OCSESSID=3e562b84ced9042abfaf777ec9; path=/**

**Set-Cookie: language=en-gb; expires=Sat, 26-Feb-2022 13:35:08 GMT; Max-Age=2592000; path=/; domain=daedalus-systems.tech-sourcery.co.uk**

**Set-Cookie: currency=USD; expires=Sat, 26-Feb-2022 13:35:08 GMT; Max-Age=2592000; path=/; domain=daedalus-systems.tech-sourcery.co.uk**

**Strict-Transport-Security: max-age=63072000; includeSubDomains**

**X-Frame-Options: SAMEORIGIN**

**X-Content-Type-Options: nosniff**

**Upgrade: h2,h2c**

**Connection: Upgrade**

**Content-Type: text/html; charset=utf-8**

Our Next step is to run a NMAP probe with version detection enabled

**Nmap -sV -T4 -F daedalus-systems.tech-sourcery.co.uk**

This returns Apache httpd (W3 Total Cache/0.9.4.6.4) which indicates Apache with the W3 Total Cache Plugin (<https://github.com/szepeviktor/w3-total-cache-fixed/releases>) but from this we are unable to tell the exact version of apache the site is running but in answer to the question the webserver software the server is running is **Apache**

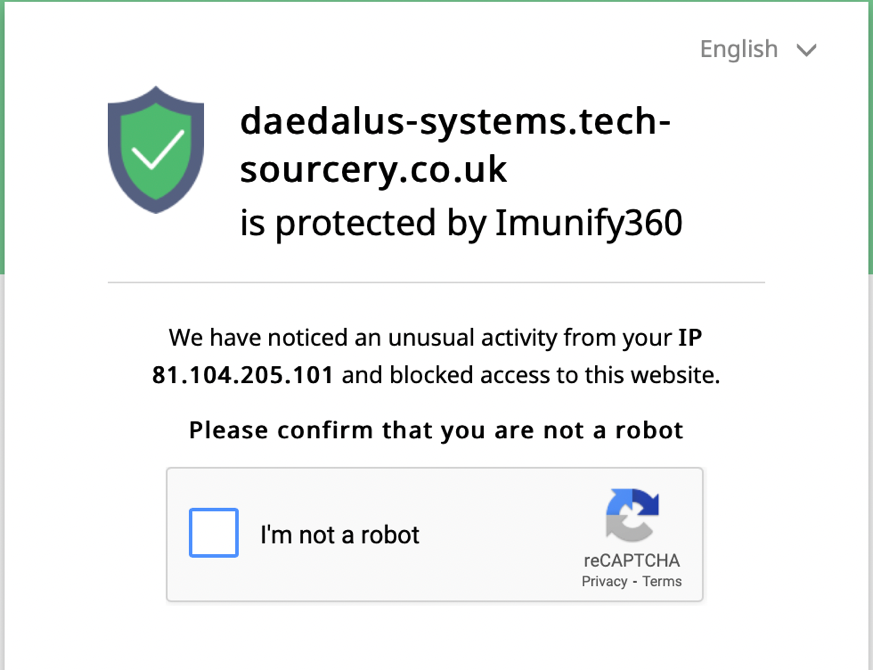
**Q3 Is it running a CMS (WordPress, Drupal, etc)?**

Based on the version string of Apache httpd (W3 Total Cache/0.9.4.6.4) this would indicate that the site is running a version of WordPress due to the W3 Total Cache software being a WordPress plugin. While our site does not appear to use WordPress the platform also appears to be shared and other sites on the platform do use WordPress as can be seen by the footer on the default page.



**Q4 What protection does it have (CDN, Proxy, Firewall?)**

The service is protected by the Imunfy360 <https://www.imunify360.com/> web application firewall this can be seen by the message that can be presented to a user to prove they are not an automated process



We can see from the whois record that there is no CDN information listed against the registration

**Domain name:**

**daedalus-systems.co.uk**

**Data validation:**

**Nominet was able to match the registrant's name and address against a 3rd party data source on 01-Aug-2020**

**Registrar:**

**eNom LLC [Tag = ENOM]**

**URL: http://www.enom.com**

**Relevant dates:**

**Registered on: 01-Aug-2020**

**Expiry date: 01-Aug-2022**

**Last updated: 01-Aug-2021**

**Registration status:**

**Registered until expiry date.**

**Name servers:**

**ns1.a2hosting.com**

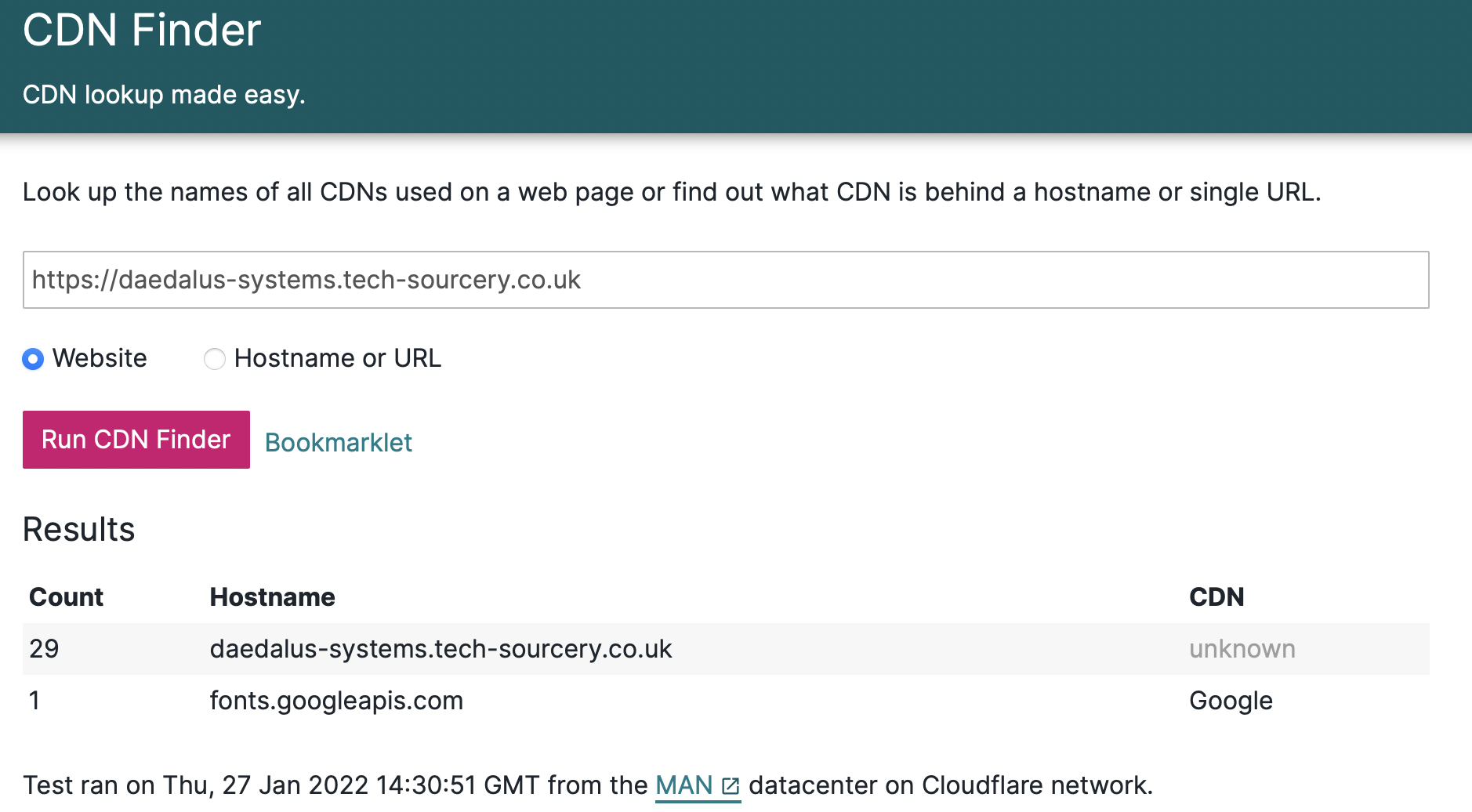
**ns2.a2hosting.com**

**ns3.a2hosting.com**

**ns4.a2hosting.com**

**WHOIS lookup made at 14:27:34 27-Jan-2022**

This is also backed up by the use of online CDN finder tools which also indicate that the site is not part of a CDN network.



So in Answer to the Question the protection in place is a **Web Application Firewall**

**Q5 Where is it hosted?**

To Determine this there are a number of techniques that can be used but the one used here is using the lookup of IP address to geographic location for this a python script was written that takes a dictionary of IP addresses obtained from our traceroute and using the dataset provided by freegeoip returns information about the IP address based on the whois record that allows us to determine the location of the site.

**import json**

**import urllib.request**

**import socket**

**IP\_Address = ["62.115.120.238", "209.124.94.237"]**

**Resolver = "https://freegeoip.app/json/"**

**try:**

**for hop, ip in enumerate(IP\_Address):**

**with urllib.request.urlopen(Resolver + ip) as url:**

**data = json.loads(url.read().decode())**

**print("Hop Number:" + str(hop))**

**print("IP Address:" + data["ip"]**

**print("Country Code:" + data["country\_code"])**

**print("Country Name:" + data["country\_name"])**

**print("Time Zone:" + data["time\_zone"])**

**print("Latitude:" + str(data["latitude"]))**

**print("Longitude:" + str(data["longitude"]) + "\n")**

**except urllib.request.URLError:**

**print("Error Getting Data")**

**except KeyError:**

**print("Error Getting JSON Key")**

This then returns the following data from the JSON webservice

|  |  |
| --- | --- |
| **Hop Number** | **0** |
| **IP Address** | **192.168.0.1** |
| **Country Code** |  |
| **Country Name** |  |
| **Time Zone** |  |
| **Latitude** | **0** |
| **Longitude** | **0** |

|  |  |
| --- | --- |
| **Hop Number** | **1** |
| **IP Address** | **80.0.142.213** |
| **Country Code** | **GB** |
| **Country Name** | **United Kingdom** |
| **Time Zone** | **Europe/London** |
| **Latitude** | **52.5852** |
| **Longitude** | **-0.236** |

|  |  |
| --- | --- |
| **Hop Number** | **2** |
| **IP Address** | **62.254.42.174** |
| **Country Code** | **GB** |
| **Country Name** | **United Kingdom** |
| **Time Zone** | **Europe/London** |
| **Latitude** | **51.4964** |
| **Longitude** | **-0.1224** |

|  |  |
| --- | --- |
| **Hop Number** | **3** |
| **IP Address** | **213.46.174.118** |
| **Country Code** | **NL** |
| **Country Name** | **Netherlands** |
| **Time Zone** | **Europe/Amsterdam** |
| **Latitude** | **52.3824** |
| **Longitude** | **4.8995** |

|  |  |
| --- | --- |
| **Hop Number** | **4** |
| **IP Address** | **62.115.120.238** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **5** |
| **IP Address** | **62.115.122.188** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **6** |
| **IP Address** | **213.155.136.99** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **7** |
| **IP Address** | **62.115.134.26** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **8** |
| **IP Address** | **62.115.120.227** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **9** |
| **IP Address** | **62.115.120.229** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **10** |
| **IP Address** | **62.115.145.217** |
| **Country Code** | **SE** |
| **Country Name** | **Sweden** |
| **Time Zone** | **Europe/Stockholm** |
| **Latitude** | **59.3247** |
| **Longitude** | **18.056** |

|  |  |
| --- | --- |
| **Hop Number** | **11** |
| **IP Address** | **209.124.94.237** |
| **Country Code** | **US** |
| **Country Name** | **United States** |
| **Time Zone** | **America/Chicago** |
| **Latitude** | **37.751** |
| **Longitude** | **-97.822** |

|  |  |
| --- | --- |
| **Hop Number** | **12** |
| **IP Address** | **68.66.247.187** |
| **Country Code** | **US** |
| **Country Name** | **United States** |
| **Time Zone** | **America/Chicago** |
| **Latitude** | **37.751** |
| **Longitude** | **-97.822** |

From this data our estimated traffic path is

|  |  |
| --- | --- |
| **No** | **Country** |
| 1 | United Kingdom |
| 2 | Netherlands |
| 3 | Sweden |
| 4 | United States |

The end point can be further verified by doing a whois on the last IP address in our traceroute chain



***Figure 5***

This command returns the following data

|  |  |
| --- | --- |
| **OrgName:** | **A2 Hosting, Inc.** |
| **OrgId:** | **A2HOS** |
| **Address:** | **P.O. Box 2998** |
| **City:** | **Ann Arbor** |
| **StateProv:** | **MI** |
| **PostalCode:** | **48106** |
| **Country:** | **US** |
| **RegDate:** | **2004-03-16** |
| **Updated:** | **2021-10-13** |
| **Comment:** | **http://www.a2hosting.com** |
| **Ref:** | [**https://rdap.arin.net/registry/entity/A2HOS**](https://rdap.arin.net/registry/entity/A2HOS) |

This however is not the whole story as we now know the site is hosted with a2hosting while this provider is US based hence the US information in the Geocoded and whois record. Their core network is US based but from lookup up public information about this provider <https://www.a2hosting.com/about/data-center> (Anon) we can see that they have a number of datacentres located in the following areas.

|  |  |  |
| --- | --- | --- |
| **Country** | **City** | **IP Range** |
| USA | Michigan | 75.98.175.109 |
| USA | Arizona | 68.66.224.6 |
| Netherlands | Amsterdam | 68.66.248.31 |
| Asia | Singapore | 03.227.176.4 |

From our traceroute result we can see our last hop is **68.66.247.187** which would seem to indicate that our site is actually physically hosted in the a2hosting Amsterdam datacentre. So, in answer to the question our site is located in **Amsterdam** which would also tie in with GDPR regulations as hosting a site outside of Europe for a European organisation can be complex in regard to data protection and compliancy legislation.



***Figure 6 (Likely Location of Amsterdam Datacentre based on Public Lat / Lon Values)***

Therefore, the answer to where the site is Located is **Amsterdam**

**Q7 Does it have any open ports?**

To Answer this, we will again use the NMAP tool by running a basic scan against the host we will run the scan Twice to pick up both Open TCP ports and Open UDP Ports the scans returned the following results.

**TCP Ports Open**

|  |  |  |
| --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** |
| **21/TCP** | **OPEN** | **FTP** |
| **25/TCP** | **OPEN** | **SMTP** |
| **53/TCP** | **OPEN** | **DOMAIN** |
| **80/TCP** | **OPEN** | **HTTP** |
| **110/TCP** | **OPEN** | **POP3** |
| **143/TCP** | **OPEN** | **IMAP** |
| **443/TCP** | **OPEN** | **HTTPS** |
| **465/TCP** | **OPEN** | **SMTPS** |
| **587/TCP** | **OPEN** | **SUBMISSION** |
| **993/TCP** | **OPEN** | **IMAPS** |
| **995/TCP** | **OPEN** | **POP3S** |
| **2525/TCP** | **OPEN** | **-** |
| **3396/TCP** | **OPEN** | **MYSQL** |
| **5432/TCP** | **OPEN** | **POSTGRES** |

**UDP Ports Open**

|  |  |  |
| --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** |
| **19/UDP** | **OPEN** | **CHARGEN** |
| **53/UDP** | **OPEN** | **DOMAIN** |
| **162/UDP** | **OPEN** | **SNMPTRAP** |
| **1900/UDP** | **OPEN** | **UPNP** |

**Q8 Does the site have any known vulnerabilities**

While it is always possible to have Zero Day exploits from what we know about the sites while there are CVEs for some of the software components so based on what we can see yes the site does have known vulnerabilities but the ability to exploit these is limited due to most needing local or authenticated access to the host. If however an attacker could gain a shell on the host they could use these to escalate access.

**Q9 What versions of software is it using? Are these patched so that they are up to date?**

|  |  |  |  |
| --- | --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** | **Version** |
| **21/TCP** | **OPEN** | **FTP** | **PureFTP-D** |
| **25/TCP** | **OPEN** | **SMTP** |  |
| **53/TCP** | **OPEN** | **DOMAIN** | **ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)** |
| **80/TCP** | **OPEN** | **HTTP** | **Apache httpd (W3 Total Cache/0.9.4.6.4)** |
| **110/TCP** | **OPEN** | **POP3** | **Dovecot pop3d** |
| **143/TCP** | **OPEN** | **IMAP** | **Dovecot imapd** |
| **443/TCP** | **OPEN** | **HTTPS** | **Apache httpd (W3 Total Cache/0.9.4.6.4)** |
| **465/TCP** | **OPEN** | **SMTPS** | **Exim smtpd 4.94.2** |
| **587/TCP** | **OPEN** | **SUBMISSION** | **Exim smtpd 4.94.2** |
| **993/TCP** | **OPEN** | **IMAPS** | **Dovecot imapd** |
| **995/TCP** | **OPEN** | **POP3S** | **Dovecot pop3d** |
| **2525/TCP** | **OPEN** | **-** | **Exim smtpd 4.94.2** |
| **3396/TCP** | **OPEN** | **MYSQL** | **MySQL 5.5.5-10.3.23-MariaDB-cll-lve** |
| **5432/TCP** | **OPEN** | **POSTGRES** | **PostgreSQL DB 9.6.0** |

To Determine if the versions of the software is up to date we first need to know the current version to do this we again reach for NMAP as this has the ability to identify software versions.

|  |  |  |
| --- | --- | --- |
| **Software** | **Our Version** | **Current Version** |
| **ISC BIND** | **9.11.4-P2** | **9.18.0** |
| **Apache httpd (W3 Total Cache)** | **0.9.4.6.4** | **0.9.6.1** |
| **Exim smtpd** | **4.94.2** | **4.95** |
| **MySQL** | **5.5.5-10.3.23** | **8.0.28 / 18 January 2022** |
| **PostgreSQL DB** | **9.6.0** | **14.1** |

From these we can see that BIND and Apache (W3 Cache) are up to date or we can assume they were when the systems were put together the two databases however are running quite old versions of the software MYSQL 5.5.5 having been released December 2010 and PostGreSQL being released September 2016.