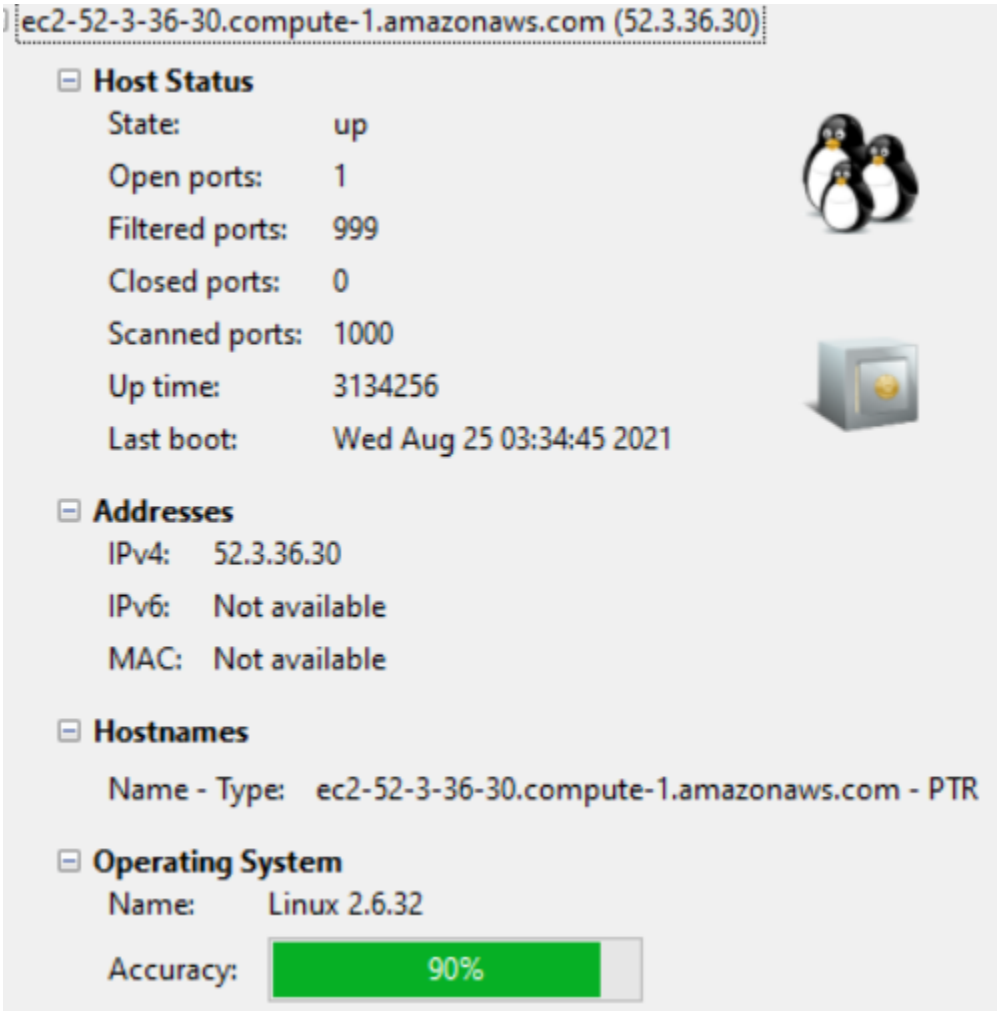
Scan results for http://52.3.36.30/
Prepared by Kikelomo Obayemi and Suresh Sigera (TEAM B)

What Operating System does the web site utilise?



What web server software is it running?

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Your Thoughts
```

Is it running a CMS (Wordpress, Drupal, etc?)

- No CMS were fingerprinted on this host

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

- This web application is hosted on a platform that is protected by a rule-based firewall

Where is it hosted? Does it have any open ports?

- Yes port 80

Does the site have any known vulnerabilities?

- Yes, according to the security scan performed by https://sitecheck.sucuri.net/results/52.3.36.30, the server has no firewall and it is prone to website hacks and DDoS attacks.
- The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).
- Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without the user's consent (ex: delete user, subscribe to newsletter, etc) (Mozilla, 2021). This is called a Clickjacking attack.

- The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

What versions of software is it using?

- Web Servers- Apache
- Web Frameworks - Twitter Bootstrap
- JavaScript Frameworks - jQuery 1.8.3

Are these patched so that they are up to date?

- Website runs on JQuery 1.8.3. It should be updated to stable version 3.6.0

Reference

Mozilla (2021) X-frame Options. Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options [Accessed 21 October 2021]