|  |  |
| --- | --- |
| Name: | Mazhar Hussain C K |
| Lab User ID: | 23SEK3324\_U06 |
| Date: | 10-01-2024 |
| Application Name: | DataDog-Java |

**Follow the below guidelines:**





System Architecture:

(Understand the system and document the physical and logical architecture of the system, use the shapes and icons to capture the system architecture)

EC2 Instances

Docker Engine

Website Tester Container

Access via internet using ip and port

Define system’s normal behavior:

(Define the steady state of the system is defined, thereby defining some measurable outputs which can indicate the system’s normal behavior)

Upon initializing the web server, it becomes active and starts monitoring designated ports, such as the IP address:

8000. When a user accesses the website hosted on this server through a web browser, they encounter a website

structured into three main sections: the header division, domain search division, and the ping results section.

Should the user input the correct domain name within the domain search division, the website initiates a ping

operation directed at that specific domain name. The ping results division then displays all the data retrieved from pinging that particular website.

Hypothesis:

(During an experiment, we need a hypothesis for comparing to a stable control group, and the same applies here too. If there is a reasonable expectation for a particular action according to which we will change the steady state of a system, then the first thing to do is to fix the system so that we accommodate for the action that will potentially have that effect on the system. For eg: "If one of our database servers fails, our service will automatically switch to a backup server, and users will not experience any downtime or data loss.")



**Known**

We are aware that this is a intentionally vulnerable app

That have been used for study purposes

Things we are aware of but don’t understand.

942236

**Unknown**

**Unknown**

**Known**

Things we are neither aware of nor understand.

Things we understand but are not aware of.

Experiment:

(Document your Preparation, Implementation, Observation and Analysis )

After installation of docker on the machine,we just have to run one command for the Installation of the web application

**docker run --rm -p 8000:8000 ghcr.io/datadog/vulnerable-java-application**

After that the application is available over port number 8000 on the machine ip

A screenshot of a computer

Description automatically generated

We have used snyk and zap baseline scan for vulnerability scanning

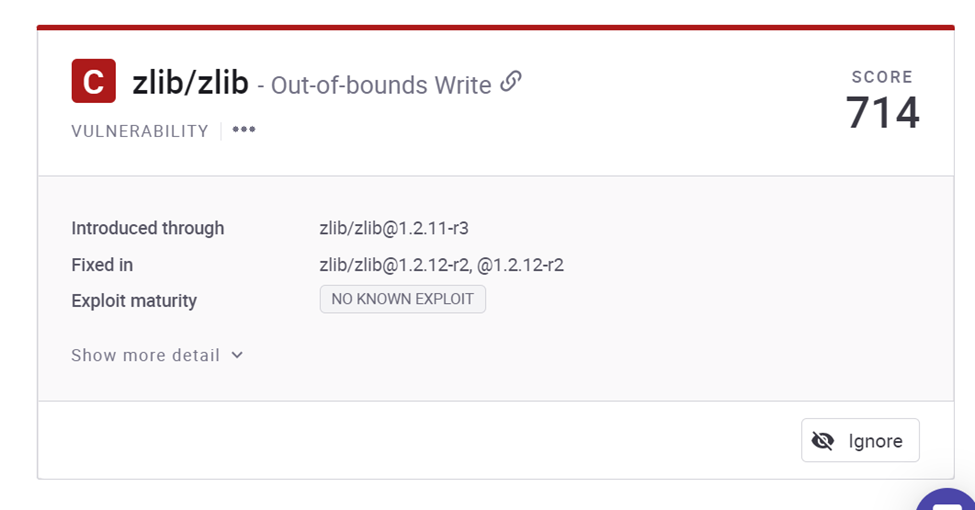
Snyk is used for repository scanning while Zap baseline scanning is used for scanning the live web application

**Scanning using snyk**

**A close-up of a computer screen

Description automatically generated**

As you can see there many vulnerabilities and some are specified below



The zlib library has an out-of-bounds write vulnerability that could be exploited during data processing, allowing unauthorized access to memory and potential data manipulation. To stay secure, users should update the zlib library with the latest patches provided by its maintainers. This update helps strengthen security for applications using the library for compression and decompression tasks.

A screenshot of a computer

Description automatically generated

For the OpenSSL libcrypto1.1 library, there's a Buffer Overflow vulnerability that could permit attackers to overwrite nearby memory areas, leading to potential unauthorized code execution or system crashes. To safeguard against this risk, users should promptly update their OpenSSL installation to the latest version provided by the maintainers. This update resolves vulnerabilities and ensures the secure operation of applications relying on cryptographic functions within libcrypto1.1. Regularly staying updated with these security patches helps maintain a robust and secure software environment.

A screenshot of a computer error

Description automatically generated

Off-by-one Error: This error occurs when a product wrongly calculates or utilizes a maximum or minimum value that's either 1 more or 1 less than the correct value. To address this issue, it's crucial to ensure correct sizing when working with character arrays or manipulating characters in methods. In C, functions like strcpy(), strncpy(), strcat(), strncat(), printf(), sprintf(), scanf(), and sscanf() are susceptible to this weakness. Ensure that the size parameter considers the null terminator needed at the end of the array to prevent such errors.

A screenshot of a computer

Description automatically generated

Loop with Unreachable Exit Condition: In the method processMessagesFromServer, an attempt is made to establish a connection to a server and read/process messages. This is achieved using a do/while loop that persistently tries to establish the connection if attempts fail. However, ensure that the loop has a reachable exit condition to avoid an infinite loop scenario where the process becomes stuck indefinitely. This could be achieved by incorporating a timeout mechanism or implementing a maximum attempt limit within the loop to gracefully exit after a reasonable number of unsuccessful attempts.

**Scanning using ZAP Baseline scan**

Zap baseline scan is done using docker

docker run -t ghcr.io/zaproxy/zaproxy:stable zap-baseline.py -t https://www.example.com

in place of example.com,we have to place our website address

A screen shot of a computer

Description automatically generated