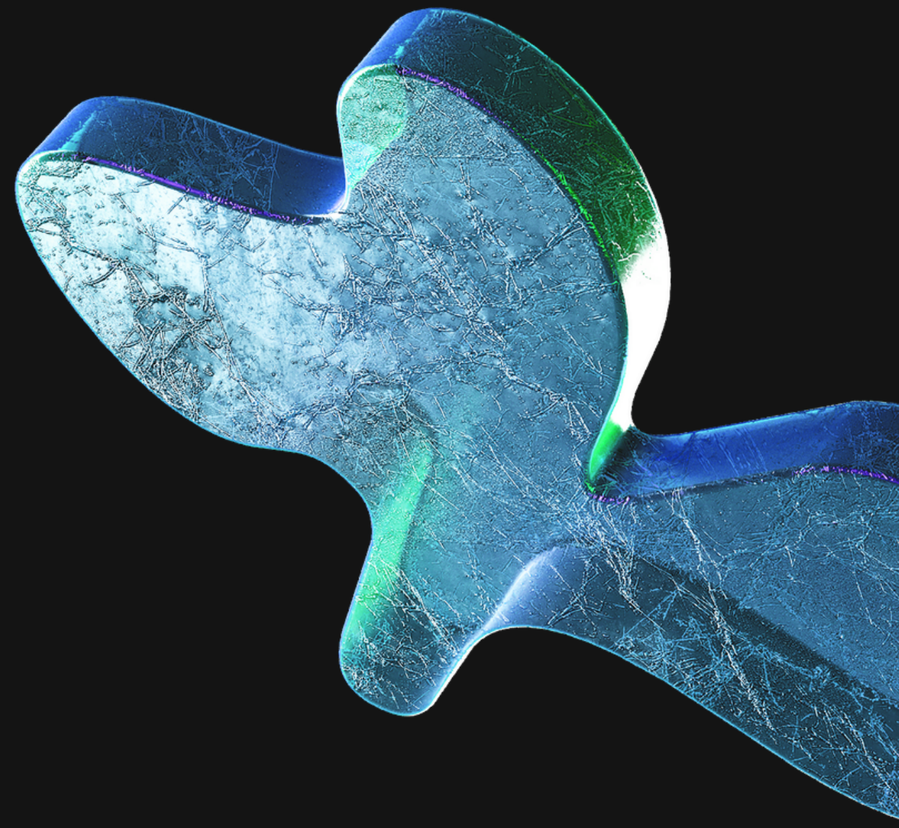
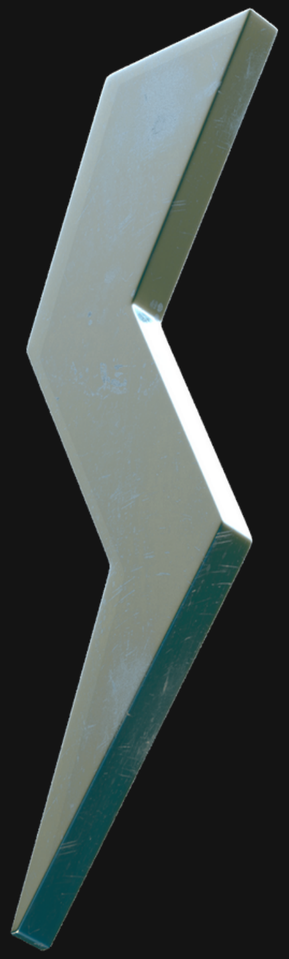
Internship Studio

# TASK 2 REPORT



Spoorthi Udupa

# What to do?



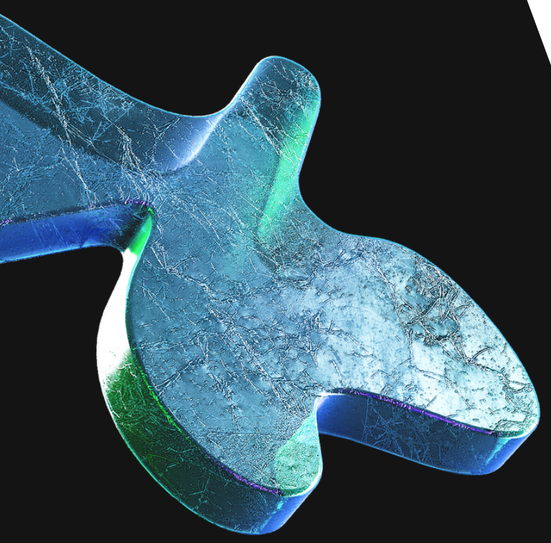
Step 1: Add Website you want to s to the dialogue box.

Step 2: Define the customization option to scan as per your need

Step 3: It will start scanning it automatically

Step 4: Choose any one of the Critical Vulnerabilities.

# Report for the vulnerablilities found



- One of the critical vulnerabilities that was found in the given website was that it had an Out-of-Date version of tomcat that has been used. http://zero.webappsecurity.com/ has been using 7.0.70 version of tomcat when the latest version is of 10.0.5. This mainly gives out 44 other vulnerabilities along with this main.

- The only remedy that would rectify this vulnerability is to upgrade the version of tomcat to stabilise the website.

The main known vulnerabilities in this is about Apache Tomcat Deserialization of untrusted data vulnerability. This allows the attacker to be able to upload a file with arbitrary content. The attacker also has full control over the filename, and knows the location where it is uploaded. It allows any anonymous attacker with internet access to submit a malicious request to a Tomcat Server that has PersistentManager enabled using FileStore.

One more vulnerability is of exposure of sensitive information to an authorized actor in apache tomcat. This could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A’s request.