# Incident Postmortem: Coordinated Attack on “/tomcatwar.jsp” Endpoint

## Summary

Between 3:16:34 AM to 3:21:00 AM UTC on March 20,2022, our system experienced an automated coordinated attack targeting the “/tomcatwar.jsp” endpoint. The attack utilized a python script to exploit a vulnerability in our sysyem, posing a significant security threat.

## Impact

The attack posed a severe risk, including unauthorized access, potential data breaches, system compromise, or service disruptions. Immediate actions were vital to mitigate the threat and safeguard our infrastructure and data.

## Detection

Our security operations team detected the attack through anomalous traffic patterns, identifying malicious activity directed at “tomcatwar.jsp” endpoint. The incident was promptly reported to the nbn team for swift actions.

## Root Cause

The incident stemmed from a system vulnerability enabling attackers to exploit “tomcatwar.jsp” endpoint using crafted HTTP POST requests. This flaw exposed our system to unauthorized access and potential compromise.

## Resolution

To counter the threat, a firewall rule was implemented promptly to block traffic attempts on the “tomcatwar.jsp” endpoint. This proactive measure prevented further exploitation of the vulnerability, bolstering of our system’s defence.

## Action Items

Conduct a thorough security assessment to identify patch existing vulnerabilities.

Deploy additional security measures, such as IDS and web application firewalls, to fortify defenses against similar attacks.

Enhance monitoring and alerting capabilities for rapid detection and response to security incidents.

Provide ongoing cybersecurity training to all personnel to reinforce awareness and vigilance.