**Title of the project –** Adversarial attack and Defences

**Overview-**

Machine Learning (ML) has spread its wings in almost all domains from medical to industrial equipment maintenance [1]. Adversarial examples can be interpreted as optical illusions to ML models in layman terms. These examples are carefully perturbed as inputs to the ML models which subsequently generate erroneous outputs. While such perturbations may seem benign to human perception, it can elicit wrong predictions from the model with full confidence. For example, perpetrators could target self-driving vehicles by causing perturbations using paint or stickers that will cause vehicle to decipher the sign incorrectly. Adversarial examples depict that many modern ML algorithms can be deluded in incredibly simple ways. Such failures indicate that even simple ML models can have their behaviour manipulated. Traditional mechanisms for building robust ML models generally do not provide a pragmatic defence against adversarial examples. There are two effective methods that have provided a somewhat effective defence: adversarial training and defensive distillation. This article explores a much more superior defence algorithm against such adversarial examples, thereby eliminating the possibility of white-box attacks.

According to the recent studies, the vulnerability of state of the art Neural Networks to adversarial input samples has increased drastically. Neural network is an intermediate path or technique by which a computer learns to perform tasks using Machine learning algorithms. Machine Learning and Artificial Intelligence model has become fundamental aspect of life, such as self-driving cars [1], smart home devices, so any vulnerability is a significant concern. The smallest input deviations can fool these extremely literal systems and deceive their users as well as administrator into precarious situations. This article proposes a defense algorithm which utilizes the combination of an auto-encoder [3] and block-switching architecture. Auto-coder is intended to remove any perturbations found in input images whereas block switching method is used to make it more robust against White-box attack. Attack is planned using FGSM [9] model, and the subsequent counter-attack by the proposed architecture will take place thereby demonstrating the feasibility and security delivered by the algorithm

**List of Teammates-**

|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Name | Collage | Contact |
| 1 | Debjit | Bhopal | 6296138465 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**List of Vulnerability Table-**

**Main Website**

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE-No |
| 1 | 166906 - Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability | CVE-2022-42252 |
| 2 | 138591 - Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities | CVE-2020-13934  CVE-2020-13935 |
| 3 | 144050 - Apache Tomcat 9.x < 9.0.40 Information Disclosure | CVE-2021-24122 |
| 4 | 151502 - Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability | CVE-2021-30640 |
| 5 | 141446 - Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up | CVE-2020-13943 |
| 6 | 152182 - Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability | CVE-2021-33037 |
| 7 | 173251 - Apache Tomcat 9.0.0.M1 < 9.0.72 | CVE-2023-28708 |
| 8 | 180194 - Apache Tomcat 9.0.0.M1 < 9.0.80 | CVE-2023-41080 |
| 9 | 159464 - Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations | CVE-2021-43980 |
| 10 | 162498 - Apache Tomcat 9.0.30 < 9.0.65 vulnerability | CVE-2022-34305 |

**Vulnerabilities**

**Smuggling Vulnerability**

CWE: CWE-444

OWASP Category: Insecure Design

Description: The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.68\_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request

Business Impact: Insecure design process can make the practice website susceptible to a range of weaknesses. This documentation section addresses the potential impacts and suggests mitigation strategies to improve the security of this

**9.0.37 Multiple Vulnerabilities**CWE: 20-Improper Input Validation

OWASP Category: A1:Injections

Description: The version of Tomcat installed on the remote host is prior to 9.0.37. It is, therefore, affected by multiple

vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_9.0.37\_security-9 advisory. Note that Nessus

has not tested for this issue but has instead relied only on the application's self-reported version number.

Business Impact: Storing dangerous data, such as malicious scripts, in a database can have severe security implications. If executed, these scripts can potentially compromise user data and the overall integrity of the practice website.

**Information Disclosure**

CWE: CWE-200

OWASP Category: A1:2017 – Sensitive Data Exposure

Description: The version of Tomcat installed on the remote host is prior to 9.0.40. It is, therefore, affected by multiple

vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_9.0.40\_security-9 advisory.

- When serving resources from a network location using the NTFS file system, Apache Tomcat versions

10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP

source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE

API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API

(FindFirstFileW) in some circumstances. (CVE-2021-24122)

Business Impact: These vulnerabilities can allow attackers to execute arbitrary code, conduct denial-of-service attacks, or obtain sensitive information 12. The exploitation of these vulnerabilities can lead to the compromise of sensitive data, loss of revenue, and damage to the reputation of the organization

**151502 - Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5vulnerability**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

**141446 - Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up**

CWE: CWE-416

OWASP Category: A8:2017 – Insecure Deserilization

Description: The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This can lead to users seeing responses for unexpected resources.

Business Impact: it can lead to unauthorized access, data breaches, and identity theft.

Vulnerability Path

**152182 - Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability**

CWE: CWE-152182

OWASP Category: A8:2017 – Insecure Deserilization

Description: The version of Tomcat installed on the remote host is prior to 9.0.48. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.48\_security-9 advisory. - Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding. (CVE-2021-33037

Business Impact: It can lead to unauthorized actions being taken on behalf of the user, potentially compromising their account or dat

**173251 - Apache Tomcat 9.0.0.M1 < 9.0.72**

CWE: CWE-523

OWASP Category: A3:2017 – Sensitive Data Exposure

Description: The version of Tomcat installed on the remote host is prior to 9.0.72. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.72\_security-9 advisory. - When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the XForwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. (CVE-2023-28708).

Business Impact: This vulnerability may result in the user agent transmitting the session cookie over an insecure channel1. This could potentially lead to the disclosure of sensitive information2, which might include user credentials or other confidential dat.

**180194 - Apache Tomcat 9.0.0.M1 < 9.0.80**

CWE: CWE-601

OWASP Category: A10:2017 – Insufficient logging and monitoring

Description: The version of Tomcat installed on the remote host is prior to 9.0.80. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.80\_security-9 advisory. - URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. The vulnerability is limited to the ROOT (default) web application. (CVE-2023-41080)

Business Impact: This vulnerability may result in the user agent transmitting the session cookie over an insecure channel1. This could potentially lead to the disclosure of sensitive information2, which might include user credentials or other confidential dat.

**159464 - Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations**

CWE: CWE-502

OWASP Category: A8:2017 – Insecure Deserilization

Description: The version of Apache Tomcat installed on the remote host is 9.x prior to 9.0.62. - The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client. (CVE-2021-43980

Business Impact: This vulnerability is related to the Spring4Shell vulnerability23.

When successfully exploited, Spring4Shell allows a remote unauthenticated attacker to obtain control of the target and to compromise the entire underlying system4.

This could lead to unauthorized access to sensitive data, disruption of system functionality, and potential financial loss due to remediation efforts4.**62498 - Apache Tomcat 9.0.30 < 9.0.65 vulnerability**

CWE: CWE-79

OWASP Category: A7:2017 – Cross Site Scripting

Description: The version of Tomcat installed on the remote host is prior to 9.0.65. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.65\_security-9 advisory. - In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability. (CVE-2022-34305

Business Impact: An attacker may be able to exploit this vulnerability to compromise the confidentiality and integrity of data on the affected system5.

This could lead to data breaches, which can result in regulatory fines, loss of customer trust, and potential financial loss5.

**PracticeWebsite**

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE-No |
| 1 | 104743 - TLS Version 1.0 Protocol Detection | CWE-327 |
| 2 | 157288 - TLS Version 1.1 Protocol Deprecated | CWE-327 |
| 3 | 45590 - Common Platform Enumeration (CPE) | CWE-287 |
| 4 | 84502 - HSTS Missing From HTTPS Server | CWE-78 |
| 5 | 10107 - HTTP Server Type and Version | CWE-203 |
| 6 | 24260 - HyperText Transfer Protocol (HTTP) Information | CWE-22 |
| 7 | 95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) | CWE-838 |

**TLS Version 1.0 Protocol Detection (104743)**

CWE: CWE-326: Inadequate Encryption Strength1.

OWASP: Not available.

Description: This vulnerability is related to the detection of the TLS version 1.0 protocol. TLS 1.0 is outdated and has several known vulnerabilities1.

Business Impact: Using this outdated protocol could expose sensitive information during data transmission and potentially allow unauthorized access1.

**TLS Version 1.1 Protocol Deprecated (157288)**

CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm2.

OWASP: Not available

Description: This vulnerability is related to the use of the deprecated TLS version 1.1 protocol. TLS 1.1 lacks support for current and recommended cipher suites2.

Business Impact: Using this deprecated protocol could lead to potential security risks such as data breaches2.

.

**Common Platform Enumeration (CPE) (45590)**

CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor3.

OWASP: Not available.

Description: This vulnerability is related to the enumeration of CPE names that matched on the remote system3.

Business Impact: This could potentially expose sensitive system information to attackers3.

**HSTS Missing From HTTPS Server (84502)**

CWE: CWE-523: Unprotected Transport of Credentials4.

OWASP: A6:2017-Security Misconfiguration4.

Description: This vulnerability is related to the lack of HTTP Strict Transport Security (HSTS) on the HTTPS server4.

Business Impact: The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections4.

**HTTP Server Type and Version (10107)**

CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor5.

OWASP: A6:2017-Security Misconfiguration5

Description: This vulnerability is related to the exposure of the type and version of the remote web server5.

Business Impact: Exposing this information could potentially help attackers in finding vulnerabilities easier5.

.

**HyperText Transfer Protocol (HTTP) Information (24260)**

CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor6.

OWASP: A6:2017-Security Misconfiguration6.

Description: This vulnerability is related to the extraction of some information about the remote HTTP configuration6.

Business Impact: This could potentially expose sensitive system information to attackers6.

**SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) (95631)**

CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm7.

OWASP: A6:2017-Security Misconfiguration7

Description: This vulnerability is related to the use of a weak hashing algorithm in the SSL certificate7.

Business Impact: Using a weak hashing algorithm could potentially allow attackers to spoof SSL servers7.