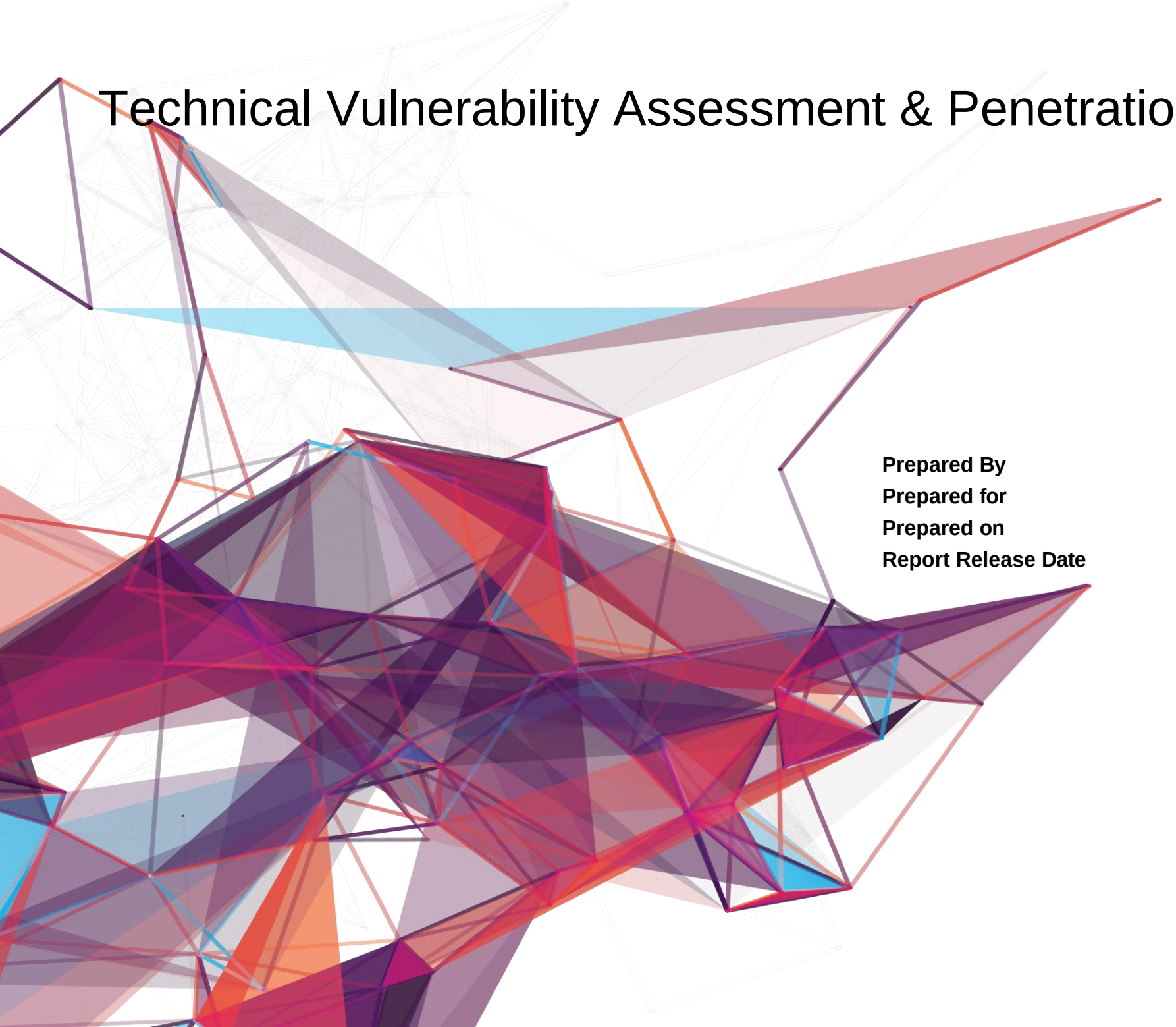
Technical Vulnerability Assessment & Penetration Testing



Prepared By	: we45
Prepared for	: YourEkai
Prepared on	: 18 Nov 2025
Report Release Date	: 28 Nov 2025

we45

Report Prepared For YourEkai

Disclaimer

This document contains information, which is the proprietary property of we45. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of we45. Nothing in this document constitutes a guarantee, warranty, or license, express or implied liability but not limited to merchantability; nor an infringement of intellectual property or other rights of any third party or of we45 indemnity or of others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of we45. we45 retains the right to make changes to this document at any time, without notice. we45 makes no warranty for the use of this document.

Copyright

Trademarks

Other product and corporate names may be trademarks of other companies and are used only as an explanation and to the owner's benefit, without any intent to infringe.

Document Authorization

Version	Prepared By	Reviewer	Date
1.0	Jayesh Sharma	Sujai Karthik	28 Nov 2025

Contents

Application Security Testing

Primer

Web Applications are the key drivers of the Internet Revolution. The Internet has evolved from a collection of static web pages to a complex network of applications that perform intricate and detailed business processes in a simple manner. providing the power of interoperability and incredible connectivity for individuals and enterprises all over the world. E-Commerce Applications, SaaS applications and several others have seen great growth in recent years and have been the driving force for the worldwide adoption of the web for business and personal use. However, there is a flip side to this story as well. As Web Applications have evolved, attackers have also begun to take cognizance of the fact that a great deal of sensitive information is exchanged and have consequently caused several web applications resulting in a compromise of billions of dollars in financial losses and irrecoverable reputation to organizations all over the world.

Web Application Security has become the order of the day because hackers (both internal and external to an organization) are exploiting vulnerabilities to gain access to sensitive and critical information contained within the web application. Organizations interested in the protection of their Critical Information Assets and their client's critical information assets have realized that security is one of the key requirements for the protection of information and have taken preventive and corrective measures to safeguard this. Web applications need to be protected from vulnerabilities like Cross-Site Scripting, SQL Injection, Session Fixation and Cross-Site Request Forgery, among several other attacks, which can have devastating effects on the organization. It is also widely known that 75% of Web Application Vulnerabilities are caused by flawed coding practices followed by developers.

Methodology for Web Application Security Assessment

Methodology

The following section describes in detail, the methodology followed by the Security Team to perform the Web Application Security Assessment. The analysis performed during the assessment is detailed and thorough during the entire process.

Application Profiling

One of the key steps in the security assessment of a Web Application is to understand the Application and its deployed environment. During this phase, the functional and business logic of the application along with the varied User Roles and the Profiling of each of them to gain a better perspective on Role-Based Access Control (RBAC) in the system is assessed.

Testing Techniques

There are several vulnerabilities that tend to manifest themselves due to non-secure coding practices, deployment or vulnerabilities present in underlying infrastructure elements like databases, web servers, application servers, proxies, etc. In certain cases, information is disclosed through the Internet which can be reached only using crafted Search Engine Queries and Information. The focus of this phase of testing is to identify vulnerabilities by testing the application from an external attacker's perspective. The Security Team use best practice techniques of OWASP, SANS, NIST, GHDB and Internal Benchmarks and Standards to identify vulnerabilities in the Web Application. They are detailed below :

1) Automated exploitation and accurate vulnerability validation

2) Comprehensive coverage of all OWASP application vulnerabilities such as Cross-site scripting, SQL injections, HTTP response splitting, Parameter tampering, Hidden field manipulation, Backdoors/debug options, Stealth commanding, Session fixation, Automatic intelligent form filling, Forceful browsing, Application buffer overflow, Cookie poisoning, Third-party misconfiguration, HTTP attacks, XML/SOAP tests, Content spoofing, LDAP injection, XPath injection and many more.

3) Support for modern websites that use JavaScript, Angular JS, Stateless Architecture, Macromedia Flash, AJAX, Java Applets and ActiveX, to name a few.

4) Business logic, validation and verification. This test parameter helps to validate the application and test it even from a Design as well as Functional standpoint.

5) Combination of automated testing with expert techniques and custom exploitation. Prioritized threat profiling with effective remediation is some of the key areas of our Test Coverage.

Executive Summary

Summary

We were engaged to perform the Vulnerability Assessment and Penetration Testing (VAPT) Assignment for YourEkai. The following were the objectives of this assessment: Identifying if an attacker can compromise defences given the security controls in place. We were required to test against these security controls in order to confirm their strong holding against any vulnerability.

Determining the impact of a security breach on the scope's :Data Integrity , Data Confidentiality , Data Availability. The Assessment has been performed in accordance with an established and repeatable methodology laid out in standards like the NIST SP 800-115 and the Penetration Testing Execution Standard (PTES).

We performed Vulnerability Assessments and Penetration Testing against the YourEkai Main web application and slack application. During our assessment, we found 4 Critical, 3 High vulnerability and 1 medium vulnerabilities.

During our revalidation, we observed that the reported vulnerabilities were fixed.

Executive Scope

Scope

The assessment was performed on a specific list of target systems. The below table lists the scope of the assessment.

Web Application:

- enterprise-api.yourekai.com
- enterprise-client.yourekai.com
- Ekai Slack Application

Vulnerability Statistics

Critical	High	Medium	Low	Info
4	3	1	0	0

Total Vulnerabilities : 8

All Vulnerabilities

Name	Severity	Status
Critical IDOR allows for leaking another tenant user's meeting data such as meeting URL, title and Summary	Critical	Fixed
Critical IDOR that accepts any fileID attachments irrespective of calling user allows for leaking complete meeting context and allows query/chat within the context	Critical	Fixed
Ability to leak long lived refresh token of any user using any valid access token	Critical	Fixed
Ability to use leaked refresh token to obtain valid google Oauth access token of any user and get google token scope access	Critical	Fixed
IDOR to change all settings of any user from a different tenant given the user ID is known	High	Fixed
Critical exposure of google refresh tokens and access token in the *updateEntity* endpoint	High	Fixed

Critical exposure of configuration tokens like slack and FCM of users	High	Fixed
Can view all user activities using any valid access token	Medium	Fixed