CYTOMATE

Technical Proposal for Vulnerability Assessment and Penetration Testing Services for Doha Bank

Table of Contents

[Point of Contact 3](#_bookmark0)

[Executive Summary 3](#_bookmark1)

[About Cytomate: Expertise, Innovation, and Achievements 3](#_bookmark2)

[About the Company 3](#_bookmark3)

[Why Us? 3](#_bookmark4)

[FIFA’22 World cup Contributions 4](#_bookmark5)

[Success Stories 5](#_bookmark6)

[Partners and Investors 5](#_bookmark7)

[Project Scope, Approach and Methodology 6](#_bookmark8)

[Scope 6](#_bookmark9)

[Methodology 10](#_bookmark10)

[External Vulnerability Assessment and Penetration Testing (Black Box & White Box) 10](#_bookmark11)

[API Security Pen testing 13](#_bookmark12)

[External Web Application Penetration Testing 14](#_bookmark13)

[Mobile Application Penetration Testing 15](#_bookmark14)

[Internal Vulnerability Assessment (Black Box-Grey Box) 16](#_bookmark15)

[Wireless Penetration Testing 19](#_bookmark16)

[Source Code Review 19](#_bookmark17)

[ATM Penetration Testing: 20](#_bookmark18)

[Re-Validation Scan (Post assessment & verification test) 20](#_bookmark19)

[Cytomate Proprietary tools: 21](#_bookmark20)

[Project Management 24](#_bookmark21)

[Deliverables 24](#_bookmark22)

[Reports 24](#_bookmark23)

[Executive Summary Reports 25](#_bookmark24)

[Follow-up Report 25](#_bookmark25)

[Communication Plan 25](#_bookmark26)

[Stakeholders: 25](#_bookmark27)

[Project Plan 26](#_bookmark28)

[Tentative Timeline 26](#_bookmark29)

[Terms and Conditions: 27](#_bookmark30)

[Client References & Contacts 28](#_bookmark31)

[Technical Report Template 29](#_bookmark32)

# Point of Contact

All communications relating to this Proposal shall be directed to the person designated to represent Cytomate. All notices shall be addressed to:

CYTOMATE SOLUTIONS AND SERVICES

#### Hamad Saleh Hadeed

#### Title: Chief Executive Officer Email: [hamad@cytomate.net](mailto:hamad@cytomate.net) Phone: +(974) 5000 3711

# Executive Summary

This document is for DOHA BANK, seeking Vulnerability Assessment & Penetration Testing services from a professional company to improve the security posture of IT infrastructure and networks. Cytomate’s approach to vulnerability assessment and penetration testing includes a thorough analysis of the DOHA BANK’s infrastructure and application systems (both grey box and white box), using both automated and manual testing methods. Our testing will include internal and external networks, software applications, Threat Modelling, Security Architecture review, Attack Surface Management, API security assessment, ATM penetration testing, thick client application security assessment, DMZ design review, database security assessment, firewall configuration review, and mobile and web-based applications security testing. Our team will also work closely with DOHA BANK’s IT department to ensure minimal disruption to daily operations. In addition to the testing services, Cytomate will provide a comprehensive report of our findings and mitigations for DOHA BANKs to improve its overall security posture. Our expertise and experience will enable us to assess DOHA BANK’s security posture comprehensively and effectively.

# About Cytomate: Expertise, Innovation, and Achievements

## About the Company

[Cytomate](https://cytomate.net/) is an innovative Qatari cybersecurity company based in Doha, Qatar with the power of Automation & Autonomicity (Artificial Intelligence). **Cytomate is evaluated, recommended, and invested in by Qatar Development Bank** (QDB)**, Qatar Foundation** (QF), **and Qatar Research and Development Institute** (QRDI). Cytomate is the only Qatari company to have the three proprietary products which are Breach and Attack Simulation (Breach+) solution, External Attack Surface Management (Racid), and Deception (Sarab) solution all empowered with Artificial Intelligence. Cytomate is **accredited** by **Qatar National Cyber Security Agency** (NCSA) for **penetration testing services.** Cytomate Breach+ is also **Common Criteria certified** by CC and NCSA which is accepted globally. Cytomate also holds **ISO-27001 certification**.

## Why Us?

Cytomate believes that there should be a continuous mechanism to test the applications and security controls that protect against the latest threats. Not limited to the available threats, our team’s seasoned security professionals spend significant time researching and developing advanced exploits. The wide range of dynamic exploits emulates sophisticated attacks used by cybercriminals in an automated and continuous way. Cytomate executes a series of attacks spanning the full MITRE ATT&CK matrix to evaluate your organization’s defenses. It creates unique exploits to evade security controls. To give organizations defense status given advanced attackers.

It provides organizations with prioritized actionable remediation insight for attacks that successfully bypassed security defenses. Cytomate has its Cytomate Lab where our researchers (Red Teamers, SOC Analysts, Deception Experts, and Reverse Engineers) are working on different projects.

##### Previous VAPT Experience

Cytomate provided VAPT services to **Sidra Medicine** in 2024. The project scope included a comprehensive assessment covering Vulnerability Assessment, Applications Testing, Web Applications Testing, Internal Network Testing, Wireless and VOIP Testing, and a Security Configuration Review. Cytomate delivered these services with a high level of professionalism and expertise, meeting the expectations set by Sidra Medicine. The project successfully uncovered critical vulnerabilities, enhancing the security posture of Sidra Medicine. Additionally, Cytomate provided both executive and detailed reports outlining the findings, as well as presentation, which facilitated the mitigation of identified vulnerabilities and misconfigurations. The services contributed to ensuring regulatory compliance and reducing risk exposure, further strengthening Sidra Medicine's overall cybersecurity defenses. Cytomate recently got **QAPCO** project for 2 years for VAPT of internal and external surface of the organization.

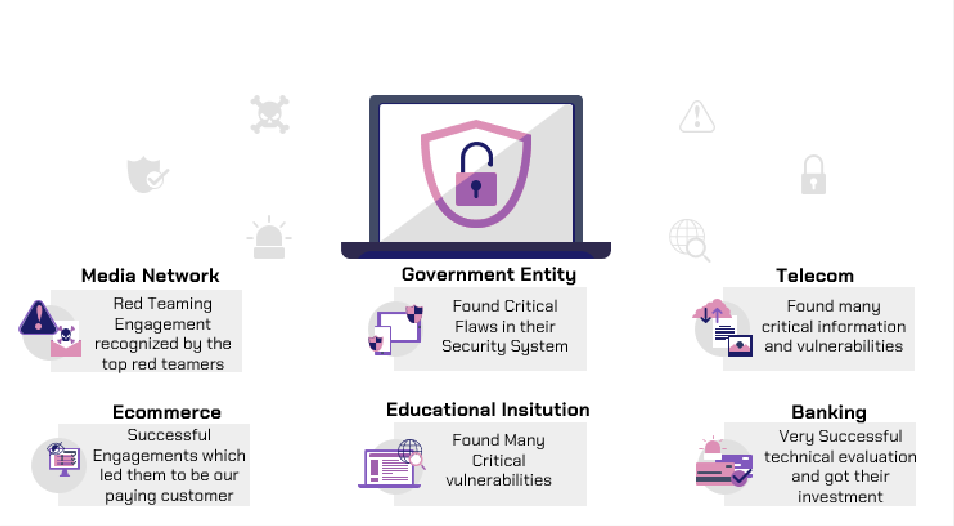
Although Cytomate has been in the market for only 3 years, it provided comprehensive VAPT and Red Teaming Services to notable organizations in Qatar. During the FIFA World Cup 2022, Cytomate conducted security assessments on critical organizations from different industries, such as government, telecommunications, healthcare and banking.

## FIFA’22 World cup Contributions

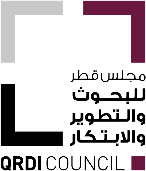
Cytomate was officially engaged by Amiri Diwan for covering the cyber security activities during the FIFA world cup 2022, following figures give very high-level details of such activities.



## Home | Sidra MedicineSuccess Stories



## Partners and Investors



# Project Scope, Approach and Methodology

Doha Bank is seeking a vendor to conduct Vulnerability Assessment and Penetration Testing (VAPT) of internal and external network infrastructure, Applications, and systems as part of the regular process of verifying the implemented cyber security controls and identifying any weaknesses and further enhancing the overall security of the Doha Bank.

The objective of this VAPT assessment is to:

* Gain an understanding of potential vulnerabilities of internal and external network infrastructure and systems.
* Evaluate the overall security posture of Doha Bank’s internal and external network

infrastructure and systems.

## Scope

The **VAPT assessment** includes the following activities performed **for 3 years**:

|  |  |  |
| --- | --- | --- |
| **Assessment Stage** | **Activity** | **Scope & Brief Methodology** |
| **Stage 1 (Remote/ onsite)** | External Vulnerability Assessment & Penetration Testing  (Black Box, Graybox) | Cytomate external penetration testing service meticulously tests and evaluates the security of your organization's digital assets, leveraging the PTES (Penetration Testing Execution Standard) and OWASP (Open Web Application Security Project) frameworks. These services can be provided in 2 types which are BlackBox, Whitebox. Our detailed assessments cover the following areas to Doha Bank external assets:   * **Continuous assessment** of public assets using Cytomate proprietary tool Racid (EASM) which will discover and monitor digital assets (Subdomains, IPs, SSL certificates, DNS records) of Doha bank, additionally continuous discovery of Threat exposure and brand monitoring which includes detects sensitive information disclosure on Dark and Surface web. * **Web Application**: Automated and Manual security assessment of all external web applications (Internet Banking, Corporate Banking, Websites) and all subdomains, to identify vulnerabilities such as SQL injection, cross-site scripting, and other exploitable weaknesses based on OWASP Top 10 and SANS top 25. * **API / Web Services**: Cytomate will assess authentication, authorization, input validation, and encryption for exposed API endpoints. Cytomate will perform automated and manual testing to |

|  |  |  |
| --- | --- | --- |
|  |  | identify and exploit vulnerabilities and check business logic, using OWASP API security top 10.  - **Mobile Applications**: Cytomate will evaluate all Mobile applications using SAST, DAST and manual application security assessment approach to identify bugs and improve the security posture of applications.  **Step 1 (Automated):** Cytomate will perform Automated assessment using **Racid** (Cytomate external attack surface management proprietary  solution), Burp, and Nessus to identify vulnerabilities. |
| **Step 2 (Manual):** Cytomate will perform penetration assessment based on the findings and results of Racid and other solutions to validate the findings and results and provide the **risks** of vulnerabilities and their **mitigations.** |
| **Stage 2 (Remote/ onsite)** | Internal Assessment – Network  (Black Box, Graybox) | Cytomate internal network assessment evaluates the security posture of below mentioned scope leveraging the PTES (Penetration Testing Execution Standard) and OWASP (Open Web Application Security Project) frameworks. Our detailed assessments cover the following scope:   * **Vulnerability assessment & configuration audits of network devices**: tested using commercial tools like nipper to identify vulnerabilities, misconfigurations and audit mapped on different frameworks like CIS. * **Wireless security**: In Network testing, Cytomate will evaluate the integrity and resilience of network components, including routers, switches, OS fingerprinting, network sniffing, spoofing, default credentials and wireless access points, WPA cracking and security. It includes vulnerability assessments, penetration testing, and traffic analysis to identify weaknesses and potential points of compromise. * **Network & Host Based Intrusion Prevention Systems** * **Firewall, Routers and Switches Assessment** * **Network and security devices config reviews** * **Review desktops and laptop for unauthorized software and data.**   **M**ost of the cases in this assessment will be |

|  |  |  |
| --- | --- | --- |
|  |  | performed with the help of automated tools. |
| **Stage 3 (Remote/ onsite)** | Internal Assessment - Application | Cytomate internal application assessment evaluates the security posture of below mentioned scope leveraging the PTES (Penetration Testing Execution Standard) and OWASP (Open Web Application Security Project) frameworks. Our detailed assessments cover the following scope:   * **Web Application**: Automated and Manual security assessment of all external web applications (Internet Banking, Corporate Banking, Websites) and all subdomains, to identify vulnerabilities such as SQL injection, cross-site scripting, and other exploitable weaknesses based on OWASP Top 10 and SANS top 25. * **API / Web Services**: Cytomate will assess authentication, authorization, input validation, and encryption for exposed API endpoints. Cytomate will perform automated and manual testing to identify and exploit vulnerabilities and check business logic, using OWASP API security top 10. * **Internal Application Services** |
|  |  | **Step 1 (Automated):** Cytomate will perform Automated assessment using Racid (Cytomate external attack surface management proprietary solution), Burp, MobSF, and Nessus to identify vulnerabilities.  **Step 2 (Manual):** Cytomate will perform manual penetration assessment based on the findings and results of Racid and other solutions to validate the findings and results and provide the **risks** of  vulnerabilities and their **mitigations.** |
|  | Internal | Cytomate internal vulnerability assessment and penetration on Operating Systems, Servers and Databases evaluates the security posture of below mentioned scope leveraging the PTES (Penetration Testing Execution Standard) and CIS framework. Our detailed assessments cover the following scope:   * Operating system vulnerability assessment using automated tools * Operating system security config review * Security hardening as per best practice * Database security configuration review * Penetration testing on internal network including |
| **Stage 4 (Remote/ onsite)** | Vulnerability Assessment and Penetration  testing – OS & |
|  | DB |

|  |  |  |
| --- | --- | --- |
|  |  | Active Directory: This assessment includes the testing of active directory and internal network devices, desktops, servers etc. and may include the installation of tools on deployed server to perform penetration testing.  Assessment will be performed both in manual and automated way, where tools utilized will be Nessus, Nipper, and Cytomate Breach+. |
| **Stage 5 (Remote/ onsite)** | ATM Security Assessment | In ATM security assessment Cytomate team will assess below mentioned scope:  - Thick client penetration testing: Our testers’ will analyze configured files, check for application and database communications in clear text protocol, sensitive information hardcoded in code, and checking whether encryption is applied for sensitive data on the wire or not. Client-side attacks will be performed to assess and identify any vulnerability and security gap.  Manual testing will be performed with the help of these tools, CFF explorer, Detect It Easy, dnSpy, Wireshark, tcpdump, Burpsuite, Process Hacker,  Ghidra, Immunity debugger, etc |
| **Stage 6 (Remote/ onsite)** | Application Code Review | **Automated:** Cytomate will use SonarQube for inspection of code to perform automatic reviews with static analysis of code to detect bugs.  **Manual:** Manual Source Code Analysis will be done to identify bugs, vulnerabilities, inefficiencies, or deviations from coding standards. |
| **Stage 7 (Remote/ onsite)** | Secure Network Architecture Review | Cytomate provides two approaches to validate the configuration of security controls. One approach includes simulating advanced attack paths and exploiting them in safe manner to validate the endpoint and network level security controls and also provide threat intelligence and signature to block threats. The second approach is to check the access  control, password policies, firmware version and vulnerabilities etc. |
| **Stage 8 (Remote/ onsite)** | Reporting | Detailed and Executive reports will be provided for each stage mentioned above which includes all  vulnerability details along with evidence and mapped to asset. |
| **Stage 8 (On-site & Remotely)** | Post remediation re- assessment | Cytomate will re-evaluate the fixes for vulnerabilities that will be deployed by Doha Bank’s security team to confirm all vulnerabilities are patched and no new vulnerabilities are |

|  |  |  |
| --- | --- | --- |
|  |  | present in the system |

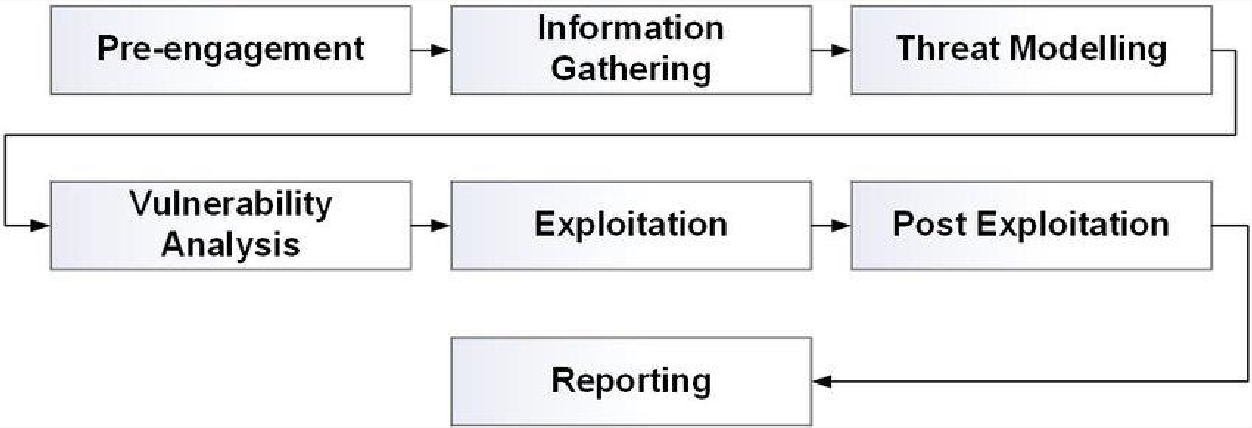
## Methodology

Cytomate adapts its penetration testing methodology based on client’s risk exposure and scope mentioned based on penetration testing execution standard (PTES) methodology and the other methodologies which provide guidelines are:

* Open-Source Security Testing Methodology Manual (“OSSTMM”) v3
* OWASP Testing Guides for Web, Mobile and API
* Scenario Based Testing
* PTES (Penetration Testing Execution Standard)
* NIST SP 800-42
* NIST 800-115

Penetration testing execution standard (PTES) covers everything related to a penetration test. From the initial communication, information gathering it also covers threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization, through vulnerability research, exploitation, and post exploitation.

The Cytomate Penetration Testing Methodology consists of seven phases:



PTES defines a baseline for the minimum that is required for a basic penetration testing, as well as several advanced scenarios that provide more comprehensive activities required for organizations with higher security needs.

### External Vulnerability Assessment and Penetration Testing (Black Box & White Box)

**Pre-engagement**

* **Step 1. Establish Rules of Engagement**: Before any testing can begin, the Doha Bank and the Cytomate should agree on the scope mentioned, the objectives, testing schedule, methods to be used, and what constitutes an acceptable level of risk during the assessment.
* **Step 2. Establish Contact Channels**: This step involves setting up secure and reliable communication channels between the Cytomate team and Doha Bank’s representatives. This ensures quick and effective communication in case of any security incidents during

the assessment.

**Black Box Testing**

##### Information Gathering

* + Step 1 Identify the Target: This is the first step in any black box testing, which involves identifying the target web application.
  + Step 2 Observe Publicly Available Information: Cytomate will look for any information available publicly, such as the technologies used, software versions, email addresses, etc.
  + Step 3 Crawl the Application: Cytomate will use automated tools and manually crawl the website to understand the application structure and functionalities.

##### Vulnerability Identification

* + Step 4 Conduct Automated Scanning: Cytomate will use automated tools to conduct a surface-level vulnerability assessment of the web application. This will help in identifying common issues quickly.
  + Step 5 Manual Testing: Cytomate will go through the OWASP Top 10 vulnerabilities and manually test for these vulnerabilities.
  + Step 6 Encryption Testing: Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Test for data at rest encryption in databases and storage systems, if applicable.
  + Step 7 Authorization and Access Control: Cytomate will test user roles and permissions to ensure users can only access appropriate resources. Verify that users cannot access unauthorized functionalities or data.
  + Step 8 Input Validation and Injection: Cytomate will test input fields for SQL injection, XSS (Cross-Site Scripting), and other injection attacks. Ensure proper input validation and output encoding to prevent injection vulnerabilities.

##### Exploitation

* + Step 9 Exploit Identified Vulnerabilities: Once the vulnerabilities have been identified, Cytomate will exploit them to understand their severity and potential impact.

##### Technical Details

##### Injection

Description: Testing for injection vulnerabilities by inserting malicious input into queries or commands.

Techniques: SQL Injection, NoSQL Injection, Command Injection.

##### Broken Authentication and Session Management

Description: Evaluating the strength of authentication mechanisms and session controls.

Techniques: Brute force attacks, session fixation, session hijacking.

##### Insecure Direct Object References

Description: Identifying direct access to internal objects via manipulated URLs or forms.

Techniques: Modifying URL parameters, form inputs to access unauthorized data.

##### Cross-Site Scripting (XSS)

Description: Injecting malicious scripts into web pages that other users will view. Techniques: Reflected XSS, Stored XSS, DOM-based XSS.

##### Insufficient Transport Layer Protection

Description: Assessing the encryption of data in transit.

Techniques: Inspecting HTTPS implementations, checking for outdated encryption protocols.

##### Failure to Restrict URL Access

Description: Testing for unauthorized access to restricted pages.

Techniques: Manual URL manipulation, automated scanning for access control gaps.

##### Sensitive Data Exposure

Description: Identifying exposure of sensitive data through weak encryption or misconfigurations.

Techniques: Examining data storage practices, inspecting transmitted data for encryption.

##### Cross-Site Request Forgery (CSRF)

Description: Testing for CSRF vulnerabilities by crafting requests that perform actions on behalf of authenticated users.

Techniques: Creating and submitting malicious forms or requests.

##### Un-validated Redirects and Forwards

Description: Identifying unvalidated redirects or forwards that could be exploited for phishing or malicious redirection.

* + Techniques: Modifying redirect parameters, analyzing HTTP headers for unsafe redirects.

**Grey Box Testing**

##### Information Gathering

* + Step 10: Utilize Provided Information: In grey box testing, DOHA BANK will provide some information about the application. Cytomate will use this information to better understand the target.

##### Vulnerability Identification

* + Step 11: Authenticated Scanning: Unlike black box testing, grey box testing often involves testing while authenticating the application. This can uncover vulnerabilities that might not be visible to unauthenticated users, such as session hijacking.
  + Step 12: Multi-Factor Authentication (MFA) Testing: Test MFA enforcement for applicable user roles and actions. Verify that MFA can't be bypassed or easily disabled.
  + Step 13: Conditional Access Testing: Cytomate will test different access scenarios based on the conditional access policies defined. For example, Cytomate will test accessing resources from different devices, locations, or times of day. Cytomate will verify that conditional access policies are correctly applied and that users are blocked or granted access as expected.
  + Step 14: Encryption Testing: Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Cytomate will test for data at rest encryption in databases and storage systems, if applicable.

##### Exploitation

* + Step 14 Exploit Identified Vulnerabilities: Cytomate will try to exploit the vulnerabilities identified during the authenticated scanning phase.

##### Technical Details

##### Injection

Description: Input validation testing for injection attacks in input fields. Techniques: SQL Injection, NoSQL Injection, Command Injection.

##### Broken Authentication and Session Management

Description: Evaluating the strength of authentication mechanisms and session controls.

Techniques: Brute force attacks, session fixation, session hijacking.

##### Insecure Direct Object References

Description: Identifying direct access to internal objects via manipulated URLs or forms.

Techniques: Modifying URL parameters, form inputs to access unauthorized data.

##### Cross-Site Scripting (XSS)

Description: Injecting malicious scripts into web pages that other users will view. Techniques: Reflected XSS, Stored XSS, DOM-based XSS.

##### Insufficient Transport Layer Protection

Description: Assessing the encryption of data in transit.

Techniques: Inspecting HTTPS implementations, checking for outdated encryption protocols.

##### Failure to Restrict URL Access

Description: Testing for unauthorized access to restricted pages.

Techniques: Manual URL manipulation, automated scanning for access control gaps.

##### Sensitive Data Exposure

Description: Identifying exposure of sensitive data through weak encryption or misconfigurations.

Techniques: Examining data storage practices, inspecting transmitted data for encryption.

##### Cross-Site Request Forgery (CSRF)

Description: Testing for CSRF vulnerabilities by crafting requests that perform actions on behalf of authenticated users.

Techniques: Creating and submitting malicious forms or requests.

##### Un-validated Redirects and Forwards

Description: Identifying unvalidated redirects or forwards that could be exploited for phishing or malicious redirection.

Techniques: Modifying redirect parameters, analyzing HTTP headers for unsafe redirects.

**Post-Testing**

* **Step 15 Report Preparation:** Cytomate will prepare a detailed report documenting the vulnerabilities identified, their potential impact, and recommended mitigations.
* **Step 16 Presentation to the Stakeholders:** Cytomate will present the report to the stakeholders to help them understand the security posture of the application and what steps need to be taken to address the identified vulnerabilities.
* **Step 17 Re-Validation:** Cytomate team will decide the timestamp with DOHA

BANK to re-validate the all-exploited issues and vulnerabilities after applying the mitigations.

### API Security Pen testing

##### API Discovery

* + **Step 1 Identify Existing APIs:** The first step is to identify all existing APIs across the infrastructure, both SOAP and REST APIs will be included.

##### Authentication & Authorization

* + **Step 2 Inspect Authentication Mechanisms:** Cytomate will check if the APIs implement strong authentication. For REST APIs, standard methods include OAuth or JWT. For SOAP APIs, WS-Security standard will be used.
  + **Step 3 Review Authorization Checks:** Cytomate will ensure that APIs have appropriate authorization checks in place, and the principle of least privilege is applied.

##### Input Validation

* + **Step 4 Input Validation:** Cytomate will verify that the APIs perform sufficient input validation to prevent attacks such as SQL injection, XML external entity (XXE) attacks (for SOAP APIs), or JSON injection (for REST APIs).

##### Key Management

* + **Step 5 Secure Storage:** Cytomate will verify that keys are stored securely, ideally in a dedicated key vault or secure configuration store.
  + **Step 6 Avoid Hardcoding**: Cytomate will ensure keys are not hardcoded directly into the source code or configuration files.

##### Encryption

* + **Step 7 Check Encryption:** Cytomate will ensure that data is encrypted in transit using protocols like HTTPS.

##### Error Handling

* + **Step 8 Review Error Handling:** Errors will be handled properly and should not disclose sensitive information.

##### Rate Limiting

* + **Step 9 Rate Limiting:** Cytomate will check if the APIs implement rate limiting to protect against DDoS attacks and brute-force attacks.

##### Logging & Monitoring

* + **Step 10 Logging and Monitoring:** Cytomate will ensure that all API calls are logged, and an effective monitoring system is in place to detect any suspicious activity.

##### Automated Security Scanning

* + **Step 11 Scan for Vulnerabilities:** Cytomate will use automated tools to scan APIs for common vulnerabilities.

##### Manual Testing

* + **Step 12 Manual Testing:** Cytomate will conduct manual testing to identify vulnerabilities that automated tools might miss.

##### Report

* + **Step 13 Compile and Present Report:** Finally, Cytomate will compile a detailed report documenting the identified vulnerabilities, their potential impact, and recommended mitigations. This report will be shared with relevant stakeholders for review and action.
  + **Step 14 Re-Validation:** Cytomate team will decide the timestamp with DOHA BANK to re-validate the all-exploited issues and vulnerabilities after applying the mitigations.

### External Web Application Penetration Testing

* + **Identify the Target:** This is the first step in any black box testing, which involves identifying the target web application. Information related to user roles and credentials will be provided by DOHA BANK.
  + **Observe Publicly Available Information:** Cytomate will look for any information available publicly, such as the technologies used, software versions, email addresses, etc.
  + **Crawl the Application:** Cytomate will use automated tools and manually crawl the website to understand the application structure and functionalities.
  + **Conduct Automated Scanning:** Cytomate will use automated tools to conduct a surface-level vulnerability assessment of the web application. This will help in identifying common issues quickly.
  + **Manual Testing:** Cytomate will go through the OWASP Top 10 vulnerabilities and manually test for these vulnerabilities.
  + **Encryption Testing:** Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Test for data at rest encryption in databases and storage systems, if applicable.
  + **Authorization and Access Control:** Cytomate will test user roles and permissions to ensure users can only access appropriate resources. Verify that users cannot access unauthorized functionalities or data.
  + **Input Validation and Injection:** Cytomate will test input fields for SQL injection, XSS (Cross-Site Scripting), and other injection attacks. Ensure proper input validation and output encoding to prevent injection vulnerabilities.
  + **Authenticated Scanning:** Cytomate will perform authenticated scans to uncover vulnerabilities in session management. This can uncover vulnerabilities that might not be visible to unauthenticated users, such as session hijacking.
  + **Multi-Factor Authentication (MFA) Testing:** Test MFA enforcement for applicable user roles and actions. Verify that MFA cannot be bypassed or easily disabled.
  + **Conditional Access Testing:** Cytomate will test different access scenarios based on the conditional access policies defined. For example, Cytomate will test accessing resources from different devices, locations, or times of day. Cytomate will verify that conditional access policies are correctly applied and that users are blocked or granted access as expected.
  + **Exploit Identified Vulnerabilities:** Cytomate will try to exploit the vulnerabilities identified during the authenticated scanning phase.
  + **Report Preparation:** Cytomate will prepare a detailed report documenting the vulnerabilities identified, their potential impact, and recommended mitigations.
  + **Presentation to the Stakeholders:** Cytomate will present the report to the stakeholders to help them understand the security posture of the application and what steps need to be taken to address the identified vulnerabilities.
  + **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

### Mobile Application Penetration Testing

* + **Scope**: Cytomate will gather scope from DOHA BANK for IOS and Android application testing. The scope will include which components of the application will be tested and information will be provided by DOHA BANK for testing. User accounts will be provided by DOHA BANK for testing. DOHA BANK will provide apk and ipa for Android and IOS testing
  + **Static Analysis:** Cytomate will start application testing with static analysis of applications. Static analysis will include checking for sensitive information in configuration files, such as API keys or passwords. Cytomate will also look for weak encryptions, local file storage and other weak ciphers. During static analysis reverse engineering will be done to read code of application to test obfuscation. During the

static analysis, the app’s resistance to tampering, such as modifying or repackaging the app without detection will be tested. Cytomate will also test the security of IPC mechanisms like intents, broadcast receivers, and content providers. Cytomate will also use their own tool Racid for static analysis of the application and discovery of any rogue application.

* + **Dynamic Analysis:** Cytomate will perform dynamic analysis of applications after static analysis. Cytomate will test the app during runtime to identify issues like insecure data storage, improper session handling, and weak encryption. Cytomate will perform input validation testing to detect vulnerabilities such as SQL injection, XSS, and buffer overflows. Cytomate will also verify the effectiveness of authentication and authorization mechanisms, ensuring they are robust against attacks like brute-force or session hijacking Verify the effectiveness of authentication and authorization mechanisms, ensuring they are robust against attacks like brute-force or session hijacking.
  + **Compile and Present Report:** After the test, Cytomate team compiles a detailed report outlining the methodology used, the vulnerabilities identified and exploited, the data that was accessed, and recommendations for improving security. This report is then presented to DOHA BANK.
  + **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

### Internal Vulnerability Assessment (Black Box-Grey Box)

##### Preparation and Planning

* + **Objective Definition:** Clearly define the scope and objectives of the assessment, including which systems, networks, and applications are in scope.
  + **Asset Inventory:** Compile a detailed inventory of all Windows and Linux servers within the scope.
  + **Permission and Access:** Obtain necessary permissions and access credentials to conduct the assessment without disrupting operations.

##### Environment Setup

* + **Tools Selection:** Choose appropriate vulnerability assessment tools compatible with both Windows and Linux environments (e.g., Nessus, OpenVAS, Qualys).
  + **Network Configuration:** Ensure network configuration allows the tools to communicate with the target servers. This may involve configuring firewall rules and network segmentation.

##### Information Gathering

* + **Network Mapping:** Use network discovery tools to map the network topology and identify active devices and open ports.
  + **Service Identification:** Identify running services on each server using tools like Nmap.
  + **OS and Software Enumeration:** Gather information about the operating systems, installed software, and their versions on each server.

##### Vulnerability Scanning

* + **Credentialed vs. Non-Credentialed Scans:** Decide on the use of credentialed (authenticated) or non-credentialed (unauthenticated) scans. Credentialed scans provide more comprehensive results.
  + **Configure Scans:** Configure the scanning tools with appropriate plugins and settings for both Windows and Linux systems.
  + **Execute Scans:** Run vulnerability scans during off-peak hours to minimize the impact on system performance.
  + **Scan Scheduling:** Schedule regular scans to maintain an up-to-date assessment of vulnerabilities.

##### Vulnerability Analysis

* + **Results Collection:** Collect and aggregate scan results from all tools used.
  + **False Positive Identification:** Validate findings to identify and eliminate false positives.
  + **Vulnerability Prioritization:** Prioritize vulnerabilities based on their severity, potential impact, and exploitability. Use Common Vulnerability Scoring System (CVSS) for standardization.
  + **Dependency Analysis:** Consider dependencies and the potential impact on interconnected systems.

##### Reporting

* + **Detailed Report Generation:** Generate a detailed report outlining identified vulnerabilities, their severity, potential impacts, and remediation recommendations.
  + Executive Summary: Create an executive summary for non-technical stakeholders highlighting key findings and overall security posture.

##### Remediation Guidance

* + **Patch Management:** Recommend patching and updating operating systems, software, and applications to mitigate identified vulnerabilities.
  + **Configuration Changes:** Suggest configuration changes to enhance security, such as disabling unnecessary services, closing open ports, and adjusting firewall rules.
  + **Access Control:** Provide recommendations on improving access control mechanisms, including the principle of least privilege and multi-factor authentication.

##### Internal Application Testing (BlackBox-GreyBox) GreyBox Testing:

* + Cytomate may request DOHA BANK to provide architecture diagrams or credentials.
  + The goal is to evaluate the authentication and authorization mechanisms more deeply.
  + This approach allows for a comprehensive analysis by understanding the internal workings of the application while maintaining an external testing perspective.

##### BlackBox Testing:

* + Conducted without any prior knowledge of the internal workings of the application.
  + Simulates an external attack to identify vulnerabilities that an attacker might exploit without insider knowledge.

##### Testing Methodology Common Vulnerabilities:

##### Broken Authentication:

* + Evaluate the mechanisms in place for user authentication.
  + Ensure that multi-factor authentication (MFA) is implemented where necessary.
  + Test for vulnerabilities in password reset functionalities and session handling.

##### Improper Session Management:

* + Assess the methods used for session creation, management, and termination.
  + Ensure session tokens are securely generated and exchanged.
  + Check for session expiration and invalidation mechanisms.

##### Data Transmission Security:

* + Verify that all data transmitted between clients and servers is encrypted using TLS/SSL protocols.
  + Ensure proper implementation of certificate pinning and validate the strength of the encryption algorithms used.

##### Single Sign-On (SSO) and Role-Based Access Controls (RBAC):

* + Review the implementation of SSO to ensure that it is properly integrated and secure.
  + Assess the configuration and enforcement of RBAC to ensure users have appropriate permissions based on their roles.
  + Verify that least privilege principles are applied and that roles are clearly defined and managed.

##### Network Scans

##### Open Ports and Services:

* + Conduct network scans to identify all open ports and services running on the servers.
  + Evaluate the security configurations of these services to identify potential vulnerabilities.
  + Ensure that unnecessary services are disabled or properly secured.
  + Vulnerability Identification:
  + Utilize automated tools and manual techniques to identify vulnerabilities associated with the identified services.
  + Prioritize findings based on their potential impact and ease of exploitation.

##### OWASP Top 10 Vulnerability Assessment

Cytomate will specifically focus on identifying and mitigating vulnerabilities listed in the OWASP Top 10, including but not limited to:

##### Injection:

* + Test for SQL, NoSQL, OS, and LDAP injection vulnerabilities.
  + Ensure proper use of parameterized queries and input validation.

##### Broken Authentication and Session Management:

* + As previously detailed, evaluate the robustness of authentication and session management mechanisms.

##### Insecure Direct Object References (IDOR):

* + Check for improper access controls that allow unauthorized access to sensitive data.

##### Cross-Site Scripting (XSS):

* + Identify and mitigate reflected, stored, and DOM-based XSS vulnerabilities.
  + Ensure proper input sanitization and output encoding.

##### Sensitive Data Exposure:

* + Verify that sensitive data is properly encrypted both at rest and in transit.
  + Assess the implementation of data protection mechanisms for personally identifiable information (PII) and other sensitive data.

##### Cross-Site Request Forgery (CSRF):

* + Test for CSRF vulnerabilities and ensure that proper anti-CSRF tokens are implemented and validated.

##### TLS Security:

* + Confirm the proper configuration and use of TLS to secure data transmission.
  + Evaluate the strength of the encryption protocols and ciphers in use.

##### Other Unknown Attack Vectors:

* + Continuously assess for emerging threats and unknown vulnerabilities using the latest threat intelligence and security research.

##### Reporting and Remediation

* + Cytomate will provide a detailed report outlining all identified vulnerabilities, their potential impact, and recommended remediation steps.
  + The report will prioritize vulnerabilities based on their severity and potential business impact.
  + Cytomate will work closely with DOHA BANK to ensure that remediation efforts are effectively implemented and validated through follow-up testing.

### Wireless Penetration Testing

* **Wireless Testing:** Cytomate will evaluate Wi-Fi security using tools like Aircrack-ng for WEP/WPA2/WPA3 cracking.
* **Wireless Attack Surface**: Cytomate will identify potential attack vectors, such as weak passwords, misconfigured APs, exposed management interfaces, and vulnerable client devices.
* **Rogue AP Detection**: Cytomate will try to find any unauthorized access points that are rogue and can try to steal information from clients.
* **Packet Sniffing:** Capture and analyze network traffic with Wireshark to identify sensitive data exposure.
* **ARP Spoofing:** Use tools like Ettercap and bettercap for ARP spoofing attacks to intercept network traffic.
* **Default Credential:** To check for default credential of network devices, Brute force attack to crack the password, DDoS attack to validate the network level security controls, and phishing attacks.
* **Reporting and Documentation:** Cytomate will compile comprehensive findings and impact assessment, detailing vulnerabilities, exploitation paths, and potential impact on patient data.
* **Remediation Recommendations:** Cytomate will provide actionable recommendations to remediate vulnerabilities and enhance security, including specific steps for securing internal networks and applications.
* **Collaboration and Debriefing:** Cytomate will collaborate with the organization's teams to discuss findings, impacts, and recommended remediation strategies.
* **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

### Source Code Review

##### Scope

The objective of this source code review is to identify and mitigate security vulnerabilities within the application codebase through Static Application Security Testing (SAST) and manual code analysis. The assessment will focus on exposing security flaws, such as coding errors, insecure practices, and potential vulnerabilities that could be exploited by attackers.

##### Methodology

* + Static Application Security Testing (SAST):
    - **Automated Scanning**: Utilize SAST tools to automatically scan the codebase for common security vulnerabilities, including SQL injection, cross-site scripting (XSS), buffer overflows, and insecure coding practices.
    - **Rule Set Customization**: Customize the scanning rules to align with the specific coding standards and security requirements of the application.
    - **Report Analysis**: Analyze the SAST reports to identify false positives, prioritize findings based on risk level, and categorize vulnerabilities by type.
  + Perform Code Analysis:
    - **Manual Code Review**: Conduct a manual review of critical code sections,

especially those handling sensitive data, authentication, authorization, and external inputs, to identify complex or context-specific vulnerabilities that automated tools may miss.

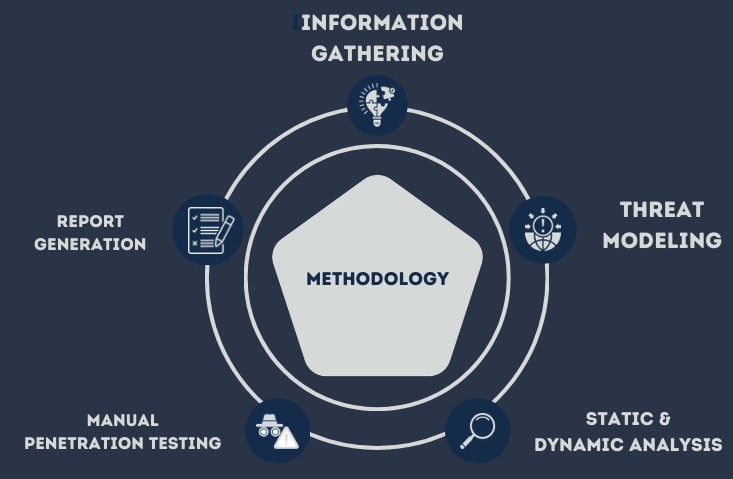
* + - **Coding Standards Compliance**: Verify that the code adheres to secure coding standards and best practices, such as OWASP Secure Coding Guidelines.
    - **Peer Review**: Implement peer review processes where developers examine each other’s code to catch potential issues and share knowledge about secure coding practices.

##### Expose Security Flaws in Code:

* + - **Vulnerability Identification**: Identify and document security flaws, such as logic errors, improper error handling, insecure use of cryptography, and hard-coded credentials.
    - **Threat Modeling**: Perform threat modeling to understand potential attack vectors and how identified vulnerabilities could be exploited in real-world scenarios.
    - **Remediation Guidance**: Provide actionable recommendations for fixing identified vulnerabilities, including code snippets, best practices, and reference materials to guide developers in secure coding.

### ATM Penetration Testing:

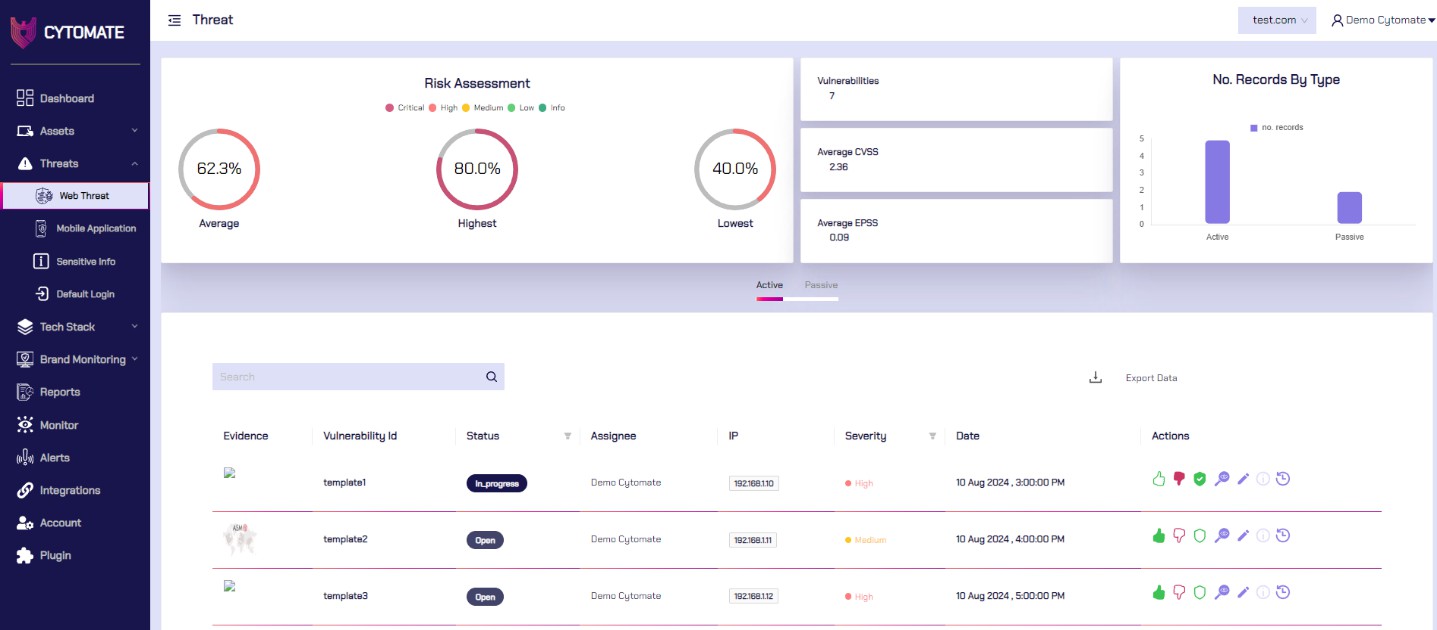
Thick client security assessment

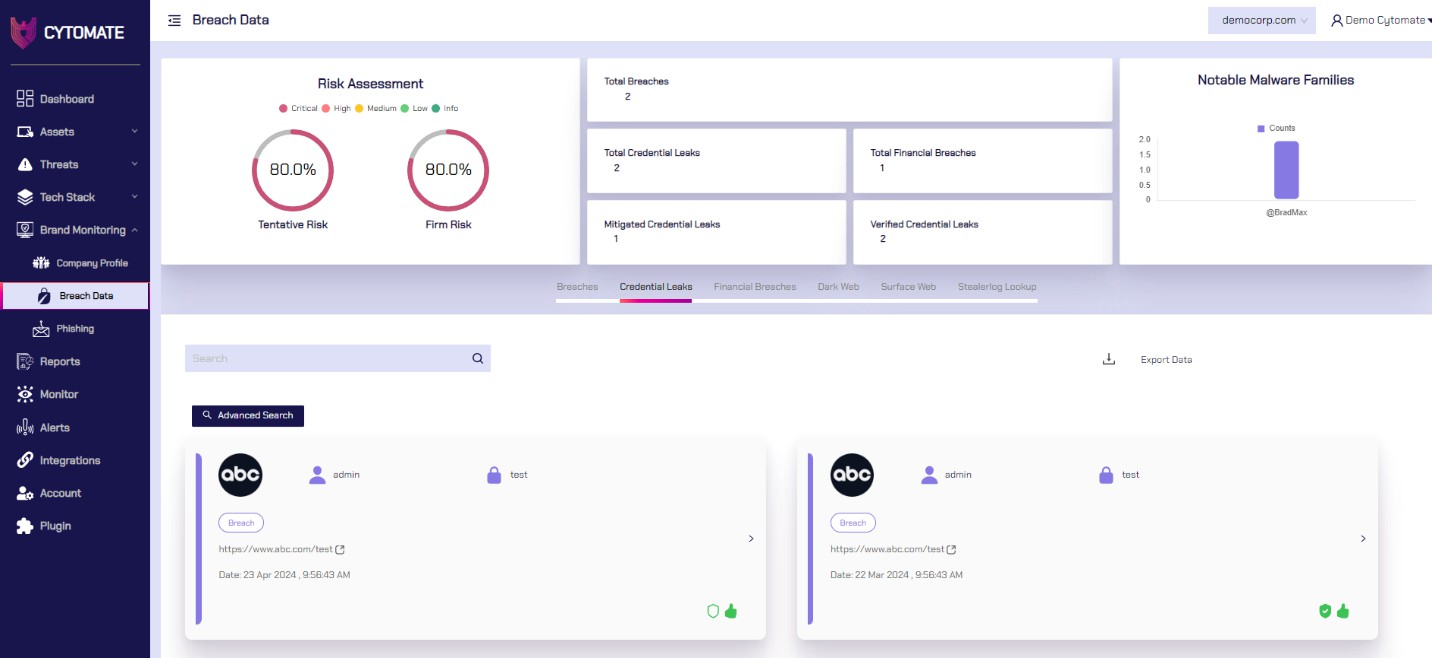


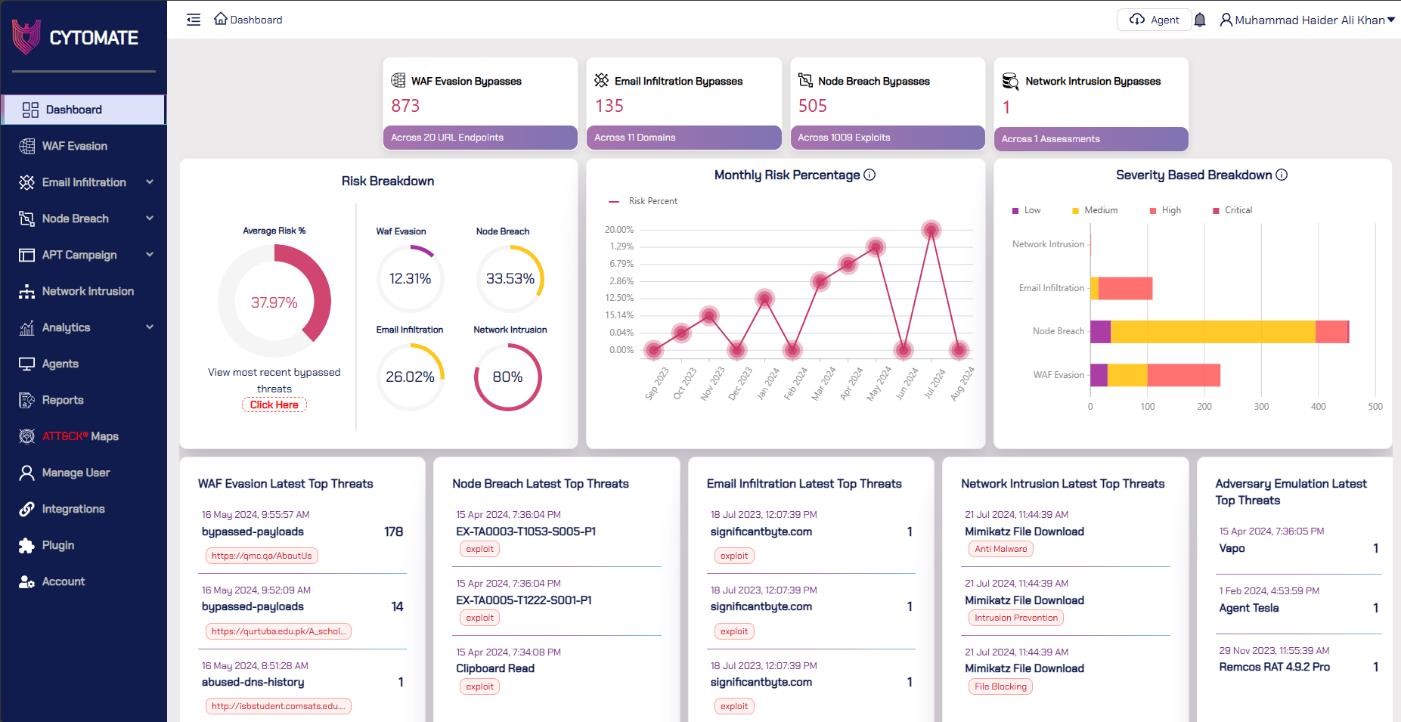
### Re-Validation Scan (Post assessment & verification test)

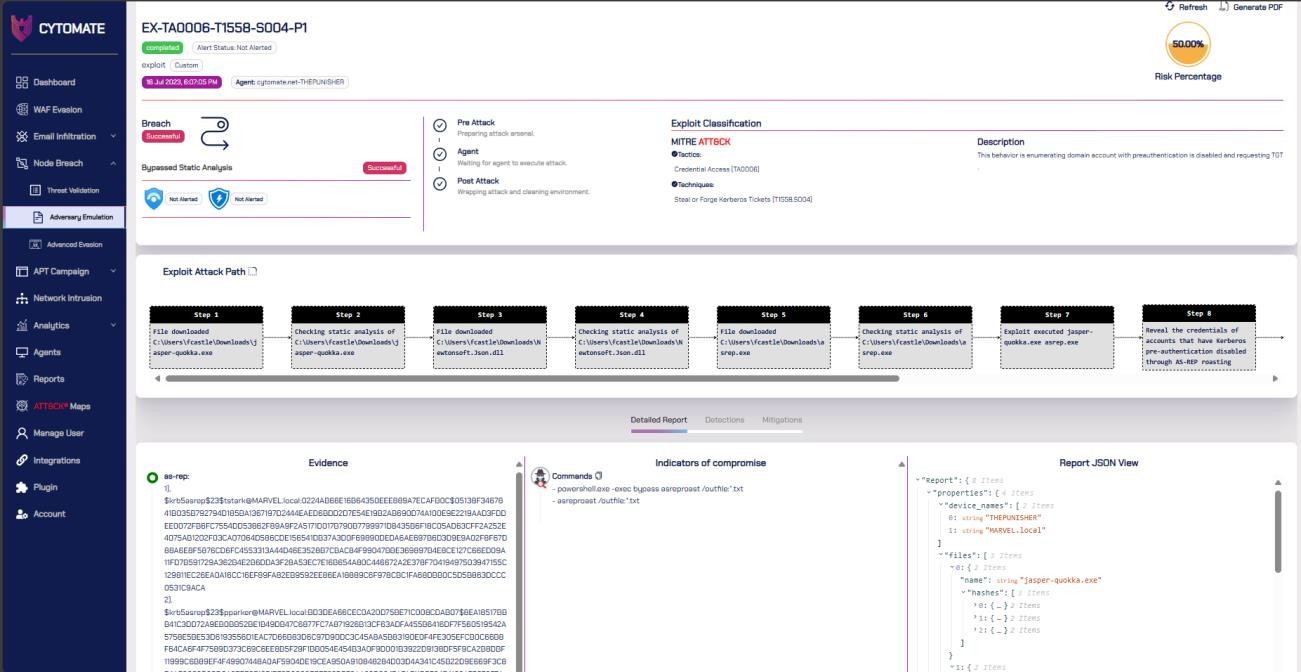
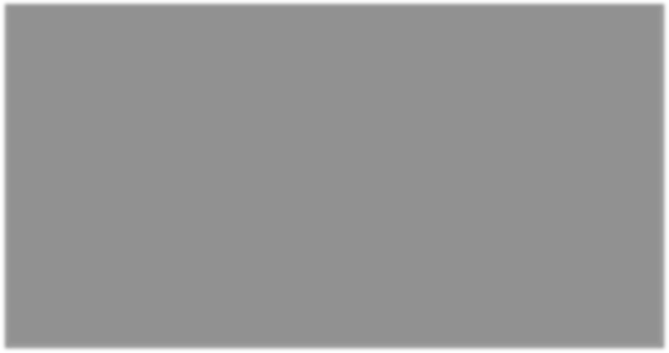
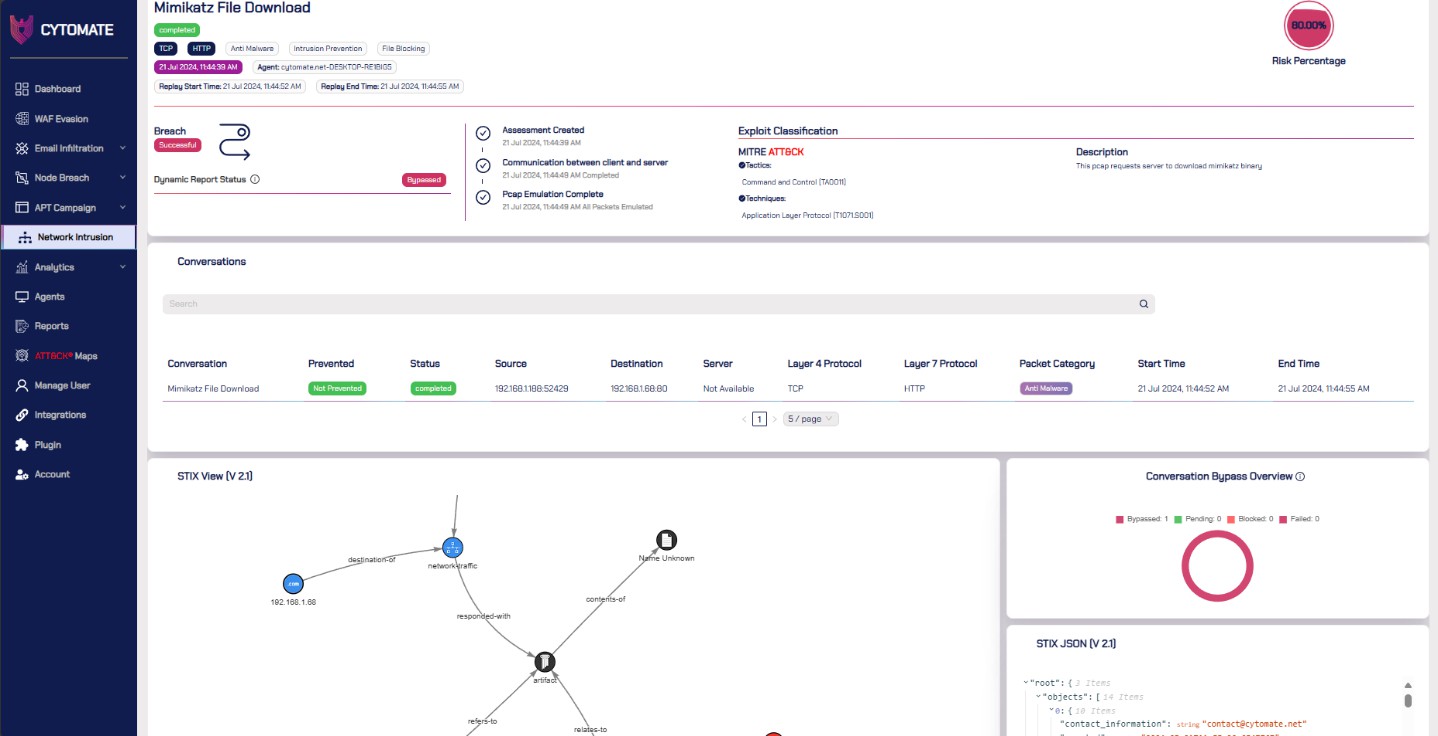
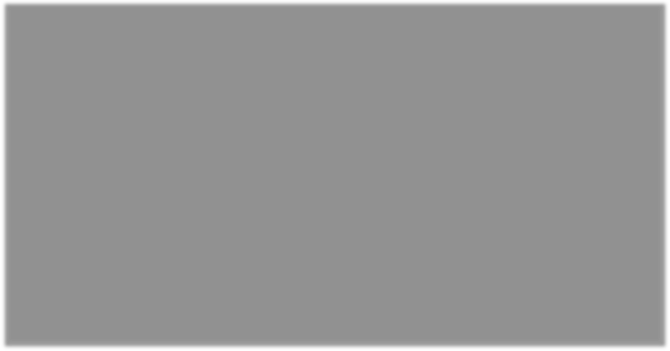
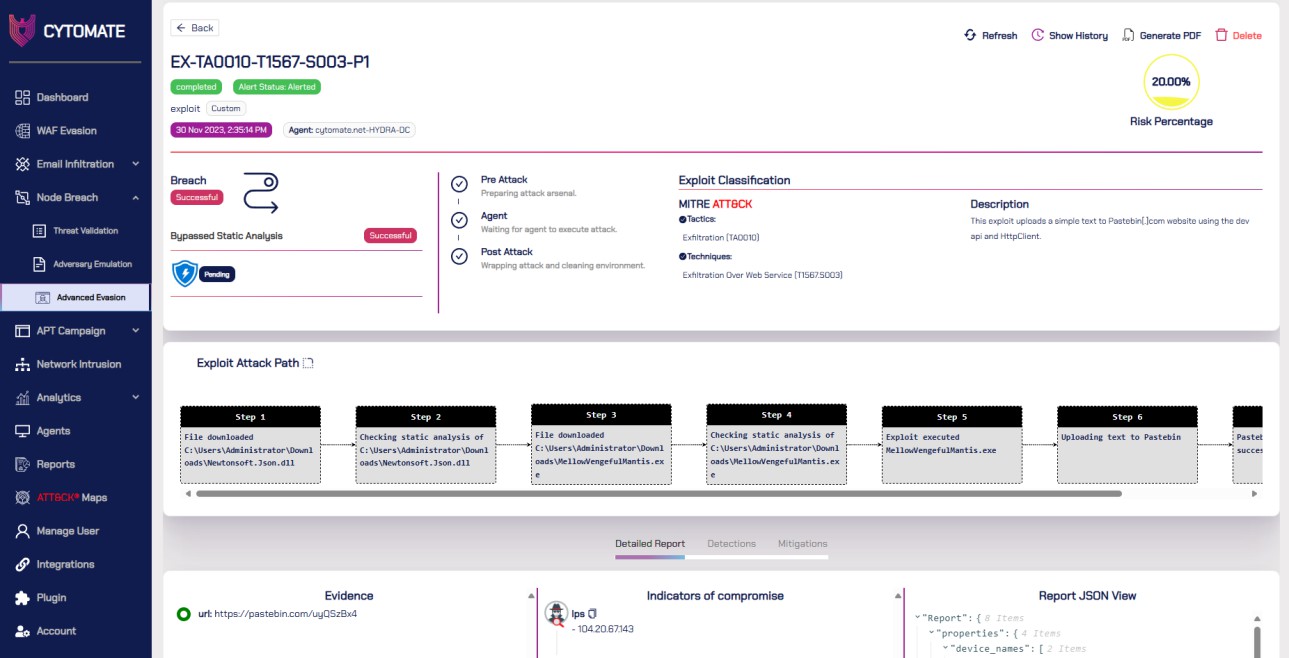
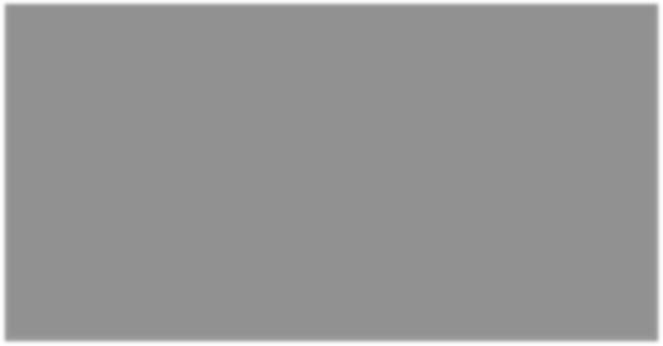
|  |  |
| --- | --- |
| A diagram of a test  Description automatically generated | This process involves a detailed examination and validation of previously identified vulnerabilities within a system or network. By conducting a confirmatory scan, security professionals can verify that these vulnerabilities have been adequately addressed and remediated. It also helps in identifying any new or overlooked vulnerabilities that might have emerged since the last assessment. |

### Cytomate Proprietary tools:

**Racid: Cytomate External Attack Surface Management**



**Breach+: Cytomate Breach and Simulation**



# Project Management

## Deliverables

Cytomate will provide the following deliverables.

* Results Presentation
* Initial Technical Report
* Final Technical Report
* Executive Summary Report
* Remediation Plan

## Reports

For each phase of the assessment, Cytomate will provide separate technical reports that will include the following sections:

* Detailed approach, tools, techniques, and methods used for the assessment, and a Risk Assessment Matrix adheres to international best practices and aligned to the assessment phases and in-scope assets.
* Identification of vulnerabilities/weaknesses, affected assets, observations, Risk Rating (High, Moderate, Low), level of exploitation, detailed Risks, and recommendations that align with standards, best practices, and regulations.
* Name of the vulnerability, Date of the discovery, Score based on CVE (Common Vulnerabilities and Exposures) databases.
* A detailed description of the vulnerability and affected systems
* Details of the process to fix/mitigate the vulnerability.
* POC (proof of concept) of the vulnerability for the system

### Executive Summary Reports

* An English executive summary report that will provide an overview of the assessment purpose, objectives, approach, and high-level summary.
* List of all identified issues under each activity with maturity levels.

### Follow-up Report:

We will provide a detailed report that lists the status of remediation for each revalidation.

## Communication Plan

Cytomate will conduct **weekly update meetings** with the **Doha Bank** team to discuss the ongoing progress of the project. These reports will include an overview of the overall project status, summaries of activities performed during the previous week, outlines of planned activities for the upcoming week, any required actions, and key findings. This regular communication ensures that the **DOHA BANK** team remains fully informed and can promptly address any emerging issues or requirements.

### Stakeholders:

**Stakeholder identification:**

The first step in stakeholder management is identifying the key stakeholders involved in or impacted by the VAPT project from both sides.

Above mentioned list is stakeholders involved from Cytomate.

|  |  |  |  |
| --- | --- | --- | --- |
| **Employee Name** | **Designation** | **Company** | **Contact** |
| Dr. Masoom Alam | Chief Technology Officer | Cytomate | [mmalam@cytomate.net](mailto:mmalam@cytomate.net) |
| Fraz Ahmad | Senior Cybersecurity Engineer | Cytomate | [fraz@cytomate.net](mailto:fraz@cytomate.net) |
| Muhammad Laiq | Pen tester | Cytomate | [laiq@cytomate.net](mailto:laiq@cytomate.net) |
| Zabi Ullah | Pen tester | Cytomate | [zabiullah@cytomate.net](mailto:zabiullah@cytomate.net) |

**Stakeholder meetings:**

* **Kick-off Meeting**: Introduce the project scope, timeline, and testing methodology to all stakeholders.
* **Mid-Project Review**: Discuss preliminary findings and assess if additional testing is needed.
* **Final Meeting**: Present the executive summary, detailed findings, and remediation plan.

## Project Plan

This table below provides an overview of the various assessment services offered in a VAPT project, detailing the frequency, scope (assets and quantities), and effort required in terms of man-days. It highlights the estimated effort required for each assessment per occurrence, as well as the total effort required annually in the project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technical Assessment Schedule and man days** | | | | |
| **Assessment** | **Scope** | **Assets and Quantity** | **Assessment Frequency** | **Man-days**  **proposed (per annum)** |
| Server, Operating Systems | Critical | 200 | Every quarter | 42 |
| Non-critical | 300 | Once a year. | 34 |
| Databases | Critical | 16 | Every quarter. | 10 |
| Non-Critical | 34 | Once a year. | 6 |
| Network & Security Devices | Critical | 60 | Every quarter. | 10 |
| Non-Critical | 140 | Once a year. | 10 |
| External website | Critical | 16 | Every quarter. | 20 |
| Application based Assessments (Web, Application & Middleware) | Critical | 30 | Every quarter. | 32 |
| Non- Critical | 40 | Once a year. | 16 |
| Mobile Applications (Huawei, Android & iOS) external | Critical | 6 | Every quarter. | 30 |
| Mobile Applications (Huawei, Android & iOS) internal | Critical | 6 | Once a year. | 40 |
| Source Code Review | Critical | 3 | Once a year. | 9 |
| ATM Security Assessment | Non-critical | 8 | Once a year. | 16 |
| Continuous Security Assessment | Critical | All Public Assets | Monthly | 0 (Cytomate Racid will be utilized) |
| Total Man days (per year) | | | | 275 |

## Tentative Timeline

The duration of a one-year VAPT test is 91.6 working days with 3 resources. Several activities will run in parallel, with multiple resources allocated to each task to ensure efficiency.

Critical assets will be tested each quarter and non-critical assets are divided into quarters but once a year.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TASKS** | **Quarter 1** | **Quarter 2** | **Quarter 3** | **Quarter 4** |
| **Server, Operating Systems** | 275 Assets  19 Man Days | 275 Assets  19 Man Days | 275 Assets  19 Man Days | 275 Assets  19 Man Days |
| **Databases** | 24 Assets  4 Man Days | 24 Assets  4 Man Days | 24 Assets  4 Man Days | 24 Assets  4 Man Days |
| **Network & Security Devices** | 95 Assets  5 Man Days | 95 Assets  5 Man Days | 95 Assets  5 Man Days | 95 Assets  5 Man Days |
| **External website** | 4 Assets  5 Man Days | 4 Assets  5 Man Days | 4 Assets  5 Man Days | 4 Assets  5 Man Days |
| **Application based Assessments (Web,**  **Application & Middleware)** | 40 Assets  12 Man Days | 40 Assets  12 Man Days | 40 Assets  12 Man Days | 40 Assets  12 Man Days |
| **Mobile Applications (Huawei, Android & iOS) External** | 6 Assets  8 Man Days | 6 Assets  7 Man Days | 6 Assets  7 Man Days | 6 Assets  7 Man Days |
| **Mobile Applications (Huawei, Android & iOS) internal** |  | 2 Assets  14 Man Days | 2 Assets  14 Man Days | 2 Assets  13 Man Days |
| **Source Code Review** |  | 2 Assets  6 Man Days | 1 Assets  3 Man Days |  |
| **ATM Security Assessment** | 4 Assets  8 Man Days |  |  | 4 Assets  8 Man Days |
| **Continuous**  **Security Assessment** | Monitored with proprietary solution (RACID EASM) 6 Assets | | | |
| **1 Resource Total Man Days** | 62 Man Days | 72 Man Days | 69 Man Days | 73 Man Days |
| **3 Resource Total Man Days** | 20.5 Man Days | 24 Man Days | 23 Man Days | 24 Man Days |

# Terms and Conditions:

* Offer Validity: We hereby confirm that this Technical Proposal is valid for 120 days starting from November 26th, 2024.
* Assessment Frequency: The frequency of assessments outlined in the table represents the

maximum number of assessments provided per year. Any additional assessments beyond the specified frequency will be subject to additional charges.

* Asset and Quantity Limits: The assets and quantities listed represent the maximum coverage for each service. Any requests to include additional assets beyond these limits will require a revised scope of work and may incur additional costs.
* Mobilization**:** Cytomate would require at least 7 to 10 calendar days for resources mobilization after project award.
* Variations: Cytomate would require an official variation order for any service not included in the original proposal. The exact scope and cost of such variations would be advised on actual.
* Accessibility: Cytomate would require physical and remote access to the client site and published services to deliver the VAPT services. Any delay due to accessibility and impacting the project delivery timeline should not penalize our project delivery and enough time to recover should be granted to Cytomate.

# Client References & Contacts

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Client Reference | Contact Person | Position | Phone |
| 1 | Dukhan Bank | Mahmoud Alsalakhi | CTO | 55821986 |
| 2 | SSB | Ahmed Al Naimi | Cybersecurity Director | 66653999 |
| 3 | QOC | Rasheed Al Nahlawi | Info Security consultant | 33609241 |
| 4 | Sidra Medicine | Tariq Abu Saqri | Senior Architect – Enterprise Architecture Solutions | 55252010 |
| 5 | HBKU | Mohammed Alhinndi | CIO | 66347331 |
| 6 | QDB | Mr. Dipu | System Engineer | 66999018 |

# Technical Report Template

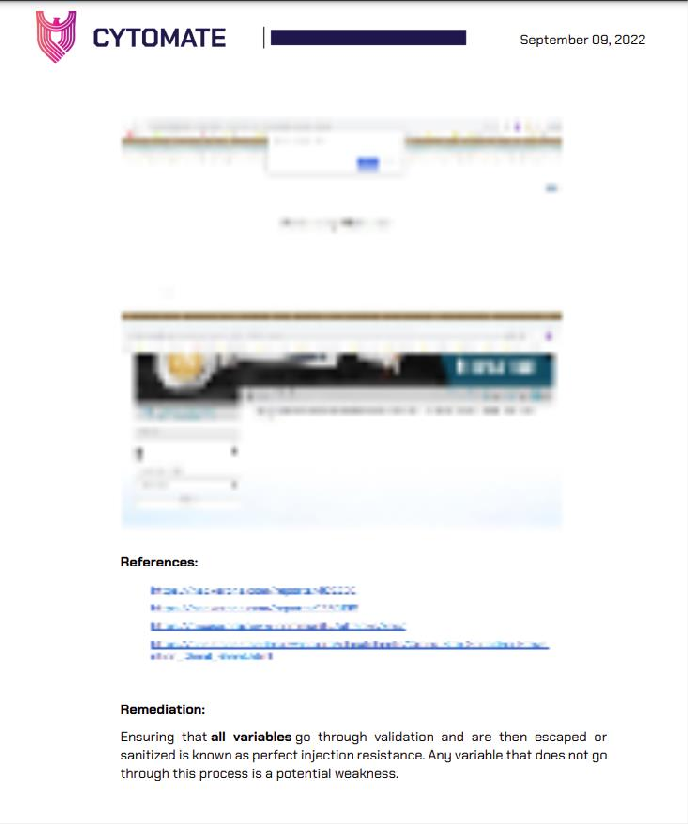
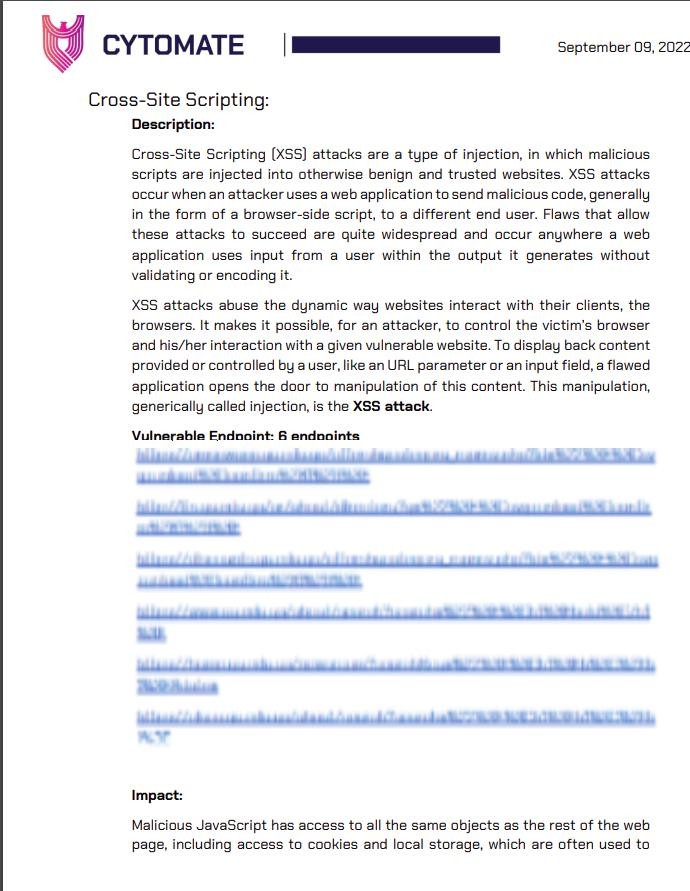


Figure 4: Cytomate report template for Web and API testing



Dr. Masoom Alam (Chief Technology Officer)