**detailed project execution plan**

# Work Schedule and Planning for deliverables

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S. No. | Deliverable (D) | Days | | | | | | | | | | | |
| 7 | 12 | 14 | 15 | 15 | 8 | 45 | 8 | 3 |  |  | Total |
| 1 | Scoping |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Information Gathering |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Discovering and Scanning |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Vulnerability Assessment and False Positive Analysis |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Exploitation |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Reporting and Presentation |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Remediation Period |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | Reverification Testing |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | Release of Final Report |  |  |  |  |  |  |  |  |  |  |  |  |

# Detailed Work Plan

Based on information provided by the BRAC, we are prepared to start the Vulnerability assessment and penetration testing at a mutually agreeable date. Depending on the schedules of the BRAC, we expect the project to end in February 2023 with detailed time below.

We have broken down the work plan as per the deliverable’s objectives.

1. **Scoping**

**Main Activities**

* Preliminary Meeting
* Rules of engagement and Timescales
* Establish Lines of Communication
* Understanding the service, architecture, and assets details
* Methodology of assessment (Black Box, Gray Box, White Box)

**Duration:** 7 Days.

1. **Information Gathering**

**Main Activities**

* Prioritize scope and timescales (production and staging environment)
* Automated information gathering
* Passive Reconnaissance
* Active Reconnaissance
* Identify Protection Mechanisms

**Duration:**  12 Days

1. **Discovery and scanning**

**Main Activities**

* Enumeration: Finding Attack Vectors
* Web application scanning and content discovery
* Network Scanning
* Automated and custom discovery and scanning

**Duration:** 14 Days

1. **Vulnerability Assessment and False Positive Analysis**

**Main Activities**

* Automated & Manual Web Vulnerability Assessment
* Network Vulnerability Assessment
* Classify Vulnerability found through industry standard guideline
* Validation & Correlation using compliance framework
* Public Research (Vulnerability Databases, Vendor Advisories)
* Private Research (Testing Configurations, Fuzzing, potential avenues/vectors creations)

**Duration:** 15 Days

1. **Exploitation (Penetration Testing)**

**Main Activities**

* Exploiting found vulnerabilities
* Tailored Exploits
* Post Exploitation
* Privilege escalation
* Remove all executable, scripts and temporary files from a compromised system.
* Remove any user accounts created for connecting back to compromise systems.

**Duration:**  15 Days

1. **Reporting**

**Main Activities**

* Executive Report
* Technical Report
* Report Presentation

**Duration:** 8 Days

**Milestone:** Within 3 Days of Penetration Testing report

**Final Output:** Draft Report

1. **Remediate Period**

**Main Activities**

* Prioritizing Vulnerabilities
* Vulnerability remediation Plan
* Remediation Consultation

**Duration:** 10 Days

1. **Reverification Testing**

**Main Activities**

* Revalidation testing of the patched vulnerabilities
* Reporting of unpatched vulnerabilities

**Duration:** 8 Days

**Final Output:**

   Reverification Testing report

1. **Final Report**

**Main Activities:** Release of Final Report

**Duration:** 3 Days

# Reporting Format Details

Throughout the engagement, we will provide draft deliverables to the BRAC Program Manager for review and comment. This will provide opportunities to review the deliverables and obtain the BRAC’s feedback on their content and quality.

final report deliverable to consist of:

• Executive Summary Report

• Detailed Findings Report

**Executive Summary Report**

 The target audience for this report is the BRAC’s executive management. This report will comprise the assessment scope, objectives, and approach of each of the assessments. The report will also summarize the urgent and high-risk security vulnerabilities identified by the scanning tool in clear terms, as well as provide potential remediation strategies.

**Detailed Findings Technical Report**

The target audience for this report is the BRAC’s security management, operations teams, and application development teams. This report will outline the scope of the assessment activity, procedures used to perform the activity, and summary of identified vulnerabilities. This data will be structured to include a severity rating for Vulnerability Risk Classification based on industry standards. Items that are deemed a critical risk will be escalated to you at the time of discovery, and will also be reported in this document.

At the conclusion of the engagement, deliverable reports, supporting evidence, related documentation, raw output from tools and assessments, and other beneficial data will be presented to the Brac Program Manager on email for distribution to the appropriate Brac teams. In addition, two printed copies of the final report will also be delivered.

The advice, recommendations, work product, and deliverables provided as part of this engagement will be developed for BRAC management, and are not intended for use by any other party or for any other purpose, and may only be relied upon by BRAC management and will be so marked.