Texas Higher Education Coordinating Board
Statement of Work (SOW)

WEB APPLICATION PENETRATION TESTING SERVICES
SOW NO. 781-1-25208

Questions and Answers
September 1, 2021

1. What is the budget for this project?

Response: This is a competitive solicitation, and we are unable to provide a budget.

2. What date do we want the response back?

Response: Please see the calendar of events in section 8.01 the Statement of Work (SOW).

3. When are you going to send the responses back to us?

Response: See the response to question 2.

4. Is a Web Application Smoke Test or Web Application Security Assessment required? Description below.

Black-box Web Application Smoke Test of each application's runtime environment. The Web Application Smoke Test provides an automated, software-based runtime analysis of application layer vulnerabilities. The results of the analysis will then be manually reviewed to eliminate false positives, resolve any errors encountered during the analysis, and identify common and potentially high-risk vulnerabilities.

Grey-box Web Application Security Assessment (Web Application, Web Services) to perform vulnerability analysis with an emphasis on manual testing to assess the application run-time environment. The testing effort will focus on identifying security vulnerabilities in the application that present the highest risk, such as the most sensitive components that are exposed to the largest user base.

Response: THECB is looking for a vendor who is capable of conducting a targeted web application penetration testing assessment of the target web application and supporting services from both an unauthorized/unauthenticated and authorized/authenticated users' perspective following a well-developed and proven methodology. Vendor should include the details of the methodology in its proposal. If a Web Application Smoke Test or a Web Application Security Assessment is part of the methodology, please include the related information.

5. Will THECB provide an application discovery document for each application?

Response: THECB will not provide a formal document for each application.

6. How will the sequence of testing be scheduled?

Response: THECB will work with the selected vendor to coordinate testing and other related activities.

7. Will multiple web apps be tested concurrently or sequentially?

Response: In most cases, multiple applications will be tested sequentially.

8. Will there be limitations on testing times and/or days of the week?

Response: In most cases, testing will be done during normal business hours.

9. In what environment will web apps be tested (production, UAT, QA, etc.)?

Response: Testing will take place in the UAT environment.

10. Will any web apps not be accessible from the internet (internal network access required)?

Response: If a web application is not accessible from the Internet, THECB will grant the vendor's staff network access prior to the assessment and after the vendor's staff has completed the required Systems Access & Data Use Agreement and Cybersecurity training as noted in section 7.03 of the SOW.

11. How many user roles per application require testing (unauthenticated user, basic authenticated user, admin, etc)?

Response: It depends on the roles and permissions built in each application.

12. Other than the standard technical report included for each web app, will additional reporting be required (executive summary, customer summary)?

Response: The technical report is the main report that THECB will use to review and assess the results from each penetration test. The acceptance criteria for the Final Report can be found in section 8.01 of the SOW.

13. Will credentials be provided for authenticated-level testing? If yes, how many sets of user credentials and/or roles will be provided for testing?

Response: Yes. The number of sets of user credentials and/or roles depends on the roles and permissions built in each application.

14. Approximately how many dynamic pages, forms, and/or screens are part of each application? A dynamic page is a page that accepts and returns user input.

Response: The number of dynamic pages varies from application to application but on average the range is between ten and fifteen.

15. Have load tests been performed against systems in the environment. If yes, have any stability issues been identified?

Response: THECB will ensure the vendor's staff has a stable environment to work with during each assessment.

16. Are there known memory leaks within any of the application components? If yes, is it possible to get a reboot of the system before beginning application scans?

Response: Before each scan, THECB staff will work with the vendor's staff to ensure there is no memory leak within any of the application components.

17. Are there any web services or APIs that will be included in testing? No Yes If yes, please confirm if they are SOAP or REST.

Response: Some applications will use REST APIs.

18. Would you be able to provide a demo of the application for our application security specialists to better understand the scope of work?

Response: Our subject matter experts will be available to help the vendor's staff gather information needed to scope a penetration test. Typically, the information includes the number and types of web applications to be tested, number of static and dynamic pages, etc.

19. Will the source code to the application be provided to expedite the testing time? No Yes

Response: No.