TEXAS HIGHER EDUCATION COORDINATING BOARD

Statement of Work (SOW)
WEB Penetration Testing

SOW No. 781-4-29775

Questions and Answers
October 16, 2023

1. 3.02 Deliverables: Does the system integrate with third-party services or APIs? If so, can you indicate an average API size? (i.e. how many endpoints / operations; how many interfaces)

   Response: In general, our applications use 1-3 interfaces, no more than 5.

2. General: Can you provide a brief description of the complexity of the web applications (presence of Payment functionality, integration etc.)

   RESPONSE: The agency uses Texas.gov payment services engine. We don't capture credit card information. The majority of the applications have low- to medium-complexity.

3. General: Are there any mobile application available for testing?

   RESPONSE: The agency doesn't have mobile applications, although some of the applications that we host are mobile friendly.

4. General: Is the underlying infrastructure also in scope? (e.g backend servers, Cloud infrastructure etc.)

   RESPONSE: The focus of the pen test is on the application. The selected vendor is not expected to perform assessment or pen test on backend servers or underlying infrastructure.

5. General: Are technical user manuals available?

RESPONSE: Technical user manuals are not available. Prior to each engagement, the agency security team will meet with the selected vendor and provide general information about the system/application and help answer any questions.

6. General: Are network and data flow architecture documents available?

   RESPONSE: We have application-specific documentation and information that we can share with the selected vendor prior to each engagement.

7. General: Will this be a black/white box testing (access to source code)?

   RESPONSE: It's a black box testing. The selected vendor will not be given access to the source code.

8. General: Will testing be conducted in a production-like environment, a staging environment, or a separate testing environment? Please clarify

   RESPONSE: Testing will be conducted in a staging environment.

9. General: Are there any areas of the testing scope that should be explicitly omitted? Please clarify.

   RESPONSE: It will be decided on a case-by-case basis. The scope of the engagement will be determined based on the target application/system.

10. General: "What would be the security testing timeframe? Are there any restrictions on performing testing during business hours (i.e., to avoid production impact)?"

    RESPONSE: A staging environment will be used for these tests. Tests can be performed during business hours.

11. General: Are there specific areas or data that are particularly critical and should be the focus of testing?

    RESPONSE: It will be decided on a case-by-case basis. The scope of the engagement will be determined based on the target application/system.

12. General: Are there any compliance or regulatory requirements that the penetration test should address (e.g., PCI DSS, HIPAA)?

    RESPONSE: It will be decided on a case-by-case basis. The agency doesn't host HIPAA or credit card information. We do host FERPA and other PII information.

13. General: Have you performed any recent security assessments or vulnerability scans on your systems?

    RESPONSE: The agency conducts network pen tests on a regular basis.

14. General: Are there any known vulnerabilities or concerns that you would like us to pay special attention to?

    RESPONSE: This information is confidential.

15. General: Are there any legal or contractual constraints that we should be aware of (e.g., signed agreements, non-disclosure agreements)?

    RESPONSE: The awarded vendor must have active cooperative contract with DIR in place prior to the issuance of a purchase order by THECB. The security team will ask the vendor staff to sign a copy of the Data Use Agreement during the onboarding process. While we do not anticipate the need for the awarded vendor to have access to any student-level data, a data sharing agreement would also have to be executed between the awarded vendor and THECB before the awarded vendor would be granted access to any student-level data or to any THECB networks that host student-level data.

16. General: Are there any security mechanisms in place that might detect or obstruct the testing?

    RESPONSE: The agency security team will make sure that the selected vendor can perform the test successfully.