Making the Internet work better

Cybersecurity Testing Services Questions & Answers

2025-02-24

IETF Executive Director
exec-director@ietf.org

Questions and Answers

Datatracker Security Review:

1. *What methodology would be expected here, white-box with source code access and all needed info for full coverage or grey-box with access to URLs, test users and documentation?*

   ANSWER: We expect a methodology that is best suited to the specific requirements and environment we set out in the RFP. In our experience, that is a mixture of white-box, grey-box and black-box.

2. *What is the type of assessments is required? (Grey Box - Black Box)*

   ANSWER: See our answer to Q1 above.

3. *How many lines of code does the application in scope consist of and what are they written in? Any noteworthy frameworks that are being used?*

   ANSWER: We do not count LoC but we are aware that there are multiple readily-available tools that can count LoC in GitHub repositories and, as noted in the RFP, our code repositories are all public. The RFP details the languages and frameworks used.

4. *Code Review: How many lines of code for the Datatracker?*

   ANSWER: See our answer to Q3 above.

5. *Is the GitHub repository included as part of the DataTracker test?*

   ANSWER: Yes.

6. *How many API endpoints does the application expose? In the case of GraphQL, how many queries and mutations are present?*

   ANSWER: There are no GraphQL APIs exposed. You can see the APIs that are exposed by inspecting the source. They are concentrated in the /api application[1].

7. *How many user roles does the application expose, is there any admin user or super-admin, maybe even with their own UI or backend interface?*

[1] https://github.com/ietf-tools/datatracker/blob/72a23d4abbbdbc1d885a9cad715a81e972f59b45/ietf/api/urls.py

ANSWER: See the section “Authenticated access to Datatracker” in the RFP. Note that this is a Django application and uses the Django admin.

8. *Would the underlying infrastructure be in scope as well and, if so, would we test this grey-box (i.e. as external testers) or get console access and look at the internal set-up as well?*

   ANSWER: The RFP is for two projects, one of which is an infrastructure security review.

Infrastructure Security Review:

9. *Could you provide an approximate count and breakdown of the infrastructure components in scope (e.g., servers, virtual machines, containers, databases)?*

   ANSWER: The RFP includes two diagrams with this level of detail.

10. *Configuration Review: How many network devices will be included in the upcoming cloud infrastructure?*

    ANSWER: See our answer to Q9 above.

11. *Could you clarify whether the infrastructure follows a segmented network design, or if all services are fully containerized?*

    ANSWER: The diagrams in the RFP answer most of this question. The components running in Kubernetes are necessarily fully containerized. The components running directly on droplets are not. The principles of a segmented network design are in use.

12. *Do you have the IAM?*

    ANSWER: This question is too unclear to answer.

13. *Will a dedicated staging/testing environment be provided for both Datatracker and the cloud infrastructure tests, or will certain tests need to be performed in production?*

    ANSWER: As the RFP states, Datatracker testing, as much as possible, must be on a local instance and any that needs to be done on the production environment must be agreed in advance. As the diagrams note, we have a completely separate staging cloud infrastructure mirroring the production cloud infrastructure. To the extent possible, testing should be run against local and staging instances. Where testing the cloud infrastructure requires testing against production, we will accommodate with advance agreement.

14. *To what extent will security testers have access to Cloudflare configurations and logs to assess attack patterns, security events and WAF effectiveness?*

    ANSWER: We aim to provide full visibility of configurations and logs to testers, noting that this may be a mixture of login access for the testers and the provision of log extracts and/or copies of configurations.

15. *Will testers be provided with credentials to analyze Kurbernetes RBAC policies and cluster configurations, or will this be limited to external testing only?*

    ANSWER: We aim to provide full visibility of configurations and logs to testers, noting that this may be a mixture of login access for the testers and the provision of log extracts and/or copies of configurations.

16. *Are there any specific security frameworks (e.g., ISO 27001, NIST, CIS Benchmarks) that IETF follows and that should be considered during testing?*

    ANSWER: No.

17. *Is the expectation for a full cloud config review, including review of the IaC files and (read-only) authenticated review of the Azure and DigitalOcean environments along with external network penetration testing?*

    ANSWER: Yes. See also the answer to question 13.

18. *Do the second round of second project will be the same scope for Penetration Testing?*

    ANSWER: This question is too unclear to answer. The scope of penetration testing for each part of the project is detailed in the RFP.

Other technical:

19. *Regarding the operational IT Systems Penetration Testing:*
    a. *How many systems in scope?*
    b. *Can you give us a brief about each system?*
    c. *What the size of each system in form of functions, user roles?*
    d. *Do this include any mobile applications? If yes, how many and what is the type of it?*

    ANSWER: This question appears to misunderstand the scope of this RFP.

20. *Regarding other systems Penetration Testing:*
    a. *How many systems in scope?*
    b. *Can you give us a brief about each system?*
    c. *What the size of each system in form of functions, user roles?*

d. *Do this include any mobile application? If yes, how many and what is the type of it?*

ANSWER: This question appears to misunderstand the scope of this RFP.

General:

21. *Do you consider RFP bids from overseas companies, in this case [REDACTED]?*

    ANSWER: Yes.

22. *What is the expected lead time for upcoming projects? Specifically, how quickly will the preferred bidder need to transition from notification to project execution?*

    ANSWER: As set out in the RFP, we aim to complete contracting by mid-April 2025 and, in our experience, contractors normally prefer to start soon after. However, we are open to a later start but we will take into consideration our meeting dates[2] and our general policy on a change freeze (and pentest freeze) starting two weeks before the meeting.

23. *Should we prepare a single proposal encompassing both projects, or are separate proposals required for each?*

    ANSWER: See bullet 4 of "RFP Process" in the RFP.

24. *Do you want us to agree on a fixed Manday rate to be consumed during the project? For example, 500 Mandays for the whole project and the payment to be pay as you go any extra Manday to be with the same rate during the project duration?*

    ANSWER: If the proposal is based on a daily rate, then yes.

25. *Can we provide the activities remotely? If no, please list all physical locations and the scope if each location.*

    ANSWER: Remotely only.

ENDS

[2] https://www.ietf.org/meeting/upcoming/