Making the Internet work better

IETF Security Review and Remediation of the RFC Production Center Web Accessible Code Questions & Answers

2020-02-25

IETF Executive Director
Exec-director@ietf.org

Questions and Answers

1. *Are you open to a Canadian agency doing this work or do you have a preference for a location?*

   Answer: We have no preference for the location of the selected bidder. We note that the selection team has an international composition.

2. *Could you identify how many lines of code in total would need to be reviewed (even approximately)?*

   Answer: The RFP includes a listing of each applicable directory and the output of the unix 'wc' command. The first figure in the output of the 'wc' command is the number of lines in the file, the second is the number of words and the third is the number of characters. A total of these figures is provided for each directory and we recommend totalling these across all directories to identify the total lines of code.

3. *Is there an architecture drawing of the codebase along with its various interactions?*

   Answer: Unfortunately not.

4. *The move to v7; how would you like the winning proponent to deal with this; i.e. review both the old v5.5 and the new v7 or only the older version or only the newer versions for the ones moved across?*

   Answer: There is only one codebase to be reviewed. This code is in the process of being converted to v7 and we expect the conversion to be complete by the time the review starts. However, the winning bidder will need to be capable of reviewing both v5.5 and v7 code in case it has not all been converted.

5. *As part of this work is it to remediate the issues as well or only identify the issues?*

   Answer: We want recommendations for remediation, which we expect will vary, depending on the complexity of the remediation required, from specific code changes to general recommendations on the nature of a code rewrite that is required.

6. *With regards to pricing, would it be safe to say you are looking for a hourly rate as opposed to a fixed price considering the vagueness in scope, especially if its a yes to #5 above?*

   Answer: As stated in the RFP - "Fixed priced bids are preferred but if that is not possible then a maximum fee must be specified."

7. *What is your ideal timeline for the work to be completed within?*

   Answer: We prefer sooner rather than later and will consider the proposed start date and estimated timetable of each bid as part of our assessment of the bids.

8. *Does the IETF have an internal schedule for when the respective milestones are expected to be completed?*

   Answer: See our answer to question 7.

9. *Regarding Deliverable 1:*

a. *“Security provided to users of the service“: It’s not fully clear which "security should be provided *to users of the service*“. Could you please elaborate which security-measures you’d expect for which kind of user (public/staff)? Does this refer to whether data collected from users (including their credentials) is kept secure?*

   Answer: The report should point out places where users of the system are at risk of having their interaction's security compromised in any way. This includes, but is not limited to, risks to privacy and integrity both during individual transactions and over time. At a higher level, we want to make sure that there are no security vulnerabilities in the code that anyone reading/scanning the code, after it has been made public, is able to discover, even if those are only exploitable by certain types of user.

b. *“Resistance to an infrastructure breach“: Does this refer to the risk that the code may cause an infrastructure breach (e.g. by allowing execution of arbitrary shell commands through the web-facing code), or do you mean the risks posed by the code after an infrastructure breach (caused by something else) has happened (e.g. hard-coded credentials to other systems like the Datatracker)?*

   Answer: Both.

10. *Which points do you expect for the warranty beyond the mentioned ones? Is liability an issue here? (Apologies if this questions has an obvious answer for you, but as the legal systems of the US and Germany differ we’d need to know what we’d be signing up for ;-))*

    Answer: We understand that nobody can provide a 100% guarantee for this sort of work and so in general (in saying this here we are not making a contractual commitment) we only expect liability for negligence and so do not expect you to indemnify us in the general case that a security vulnerability in the code that you had not identified is later reported or exploited. However, it would be helpful if your warranty explains what action you will take in the event that a vulnerability is found and it is one that we could reasonably have expected you to identify.

11. *Is it in the interest of the IETF to “split“ the bid into two packages of deliverables 1+2 and 3+4 with a final definition of 3+4 after 1+2 are completed?*

    Answer: You may structure your bid in this way if you choose, but we will only be awarding a single contract and preference will be given to bids that provide a fixed price for all deliverables.

12. *Hi, what happened to the process last fall?*

    Answer: We did not receive any bids that met our needs.

ENDS