IETF Security Review and Remediation of the RFC Production Center Web Accessible Code RFP

2019-09-27

IETF Executive Director
Exec-director@ietf.org
Overview

The IETF Administration LLC (IETF LLC) is soliciting proposals ("Proposals") for the Security Review and Remediation of the RFC Production Center Web Accessible Code RFP. The RFC Production Center (RPC) currently maintains a private CVS repository that houses the code for the RFC Editor website and the public web services provided there, as well as staff-only web services, command line tools, and utilities used by the RPC. There is an effort to move this repository to one that is open to the public to bring the resources of the Tools Team and volunteer developers to bear on evolving the codebase. An important first step in this move is inspecting the code for the web services to ensure the released code does not advertise any obvious security vulnerabilities, such as SQL insertion attacks against the underlying databases.

It is not known if there are any such vulnerabilities in the current codebase. However, it is known that the source contains at least one embedded password used for communicating with the datatracker. One possible output of this project is a report that the codebase is ready to move into the open with only simple modifications to address embedded passwords.

Timeline

27 Sep: RFP Issued
04 Oct: Questions and Inquiries deadline
07 Oct: Answers to questions issued, RFP Addenda and Update issued
14 Oct: Proposals due
21 Oct: Selection made, negotiations begin
01 Nov: Contract execution
08 Nov: Work begins

Specifications

This is the process for the Request for Bids:

1. The Statement of Work (SOW) is attached.
2. Any questions about the Work must be submitted by 04 October 2019. A response to all parties shall be provided by 07 October 2019. The response will include the questions asked and the answers, but will not identify the company asking the question.
3. Bids are due by 14 October 2019. The bid must provide a not-to-exceed price, the expected start date, the expected completion date, any assumptions, and a description of any dependencies that might cause delays in the schedule.
4. The IETF LLC will discuss the Bids and may ask questions by email and/or conference call.
5. Once the answers are received a decision will be made to select the bidder to perform the work and a Work Order will be prepared for execution. We anticipate an award on or before 21 October 2019.
6. This is the Bid format:
   a. Executive Summary
   b. Project Approach & Plan
   c. Schedule - When the work will begin and end, as well as dependencies and other milestones.
d. Test Plan  
e. Cost & Payment Schedule  
f. Warranty & Late Delivery Consequence  
g. Technical Support & Maintenance  
h. Miscellaneous  


Please reply with questions, if any, and a bid if you are interested in pursuing this opportunity to ietf-rfps@ietf.org.

Thanks in advance.

Portia Wenze-Danley
Statement of Work: Security Review and Remediation of the RFC Production Center Web Accessible Code

Overview
The RFC Production Center (RPC) currently maintains a private CVS repository that houses the code for the RFC Editor website and the public web services provided there, as well as staff-only web services, command line tools, and utilities used by the RPC. There is an effort to move this repository to one that is open to the public to bring the resources of the Tools Team and volunteer developers to bear on evolving the codebase. An important first step in this move is inspecting the code for the web services to ensure the released code does not advertise any obvious security vulnerabilities, such as SQL insertion attacks against the underlying databases.

It is not known if there are any such vulnerabilities in the current codebase. However, it is known that the source contains at least one embedded password used for communicating with the datatracker. One possible output of this project is a report that the codebase is ready to move into the open with only simple modifications to address embedded passwords.

Deliverables
1. A report assessing the security the web-facing code in the repository from two angles:
   a. Security provided to users of the service
   b. Resistance to an infrastructure breach
   Each security issue must include the following sections:
   a. Attack vector
   b. Proof of concept
   c. Impact to the target
   d. Proposed remediations
2. Changes to the codebase implementing agreed upon remediations.
3. A clean repository ready to be made available openly to the public.

Details
The CVS repository currently houses 3 projects, with this high-level directory structure:

- rfc-ed
  - bin
  - web
    - rfc
    - cgi-bin
    - htdocs
  - staff
- rfcscripts

○ images
○ reports
○ scripts
○ search
  ■ js
  ■ css
○ rsestats

The directories needing review are /rfcscripts and /rfc-ed/web/staff.

The files at /rfc-ed/web/rfc/cgi-bin are not used.

The files at /rfc-ed/web/rfc/htdocs are legacy; their functionality has been moved to other parts of the codebase.

The files under /rsestats are a django application providing statistics reports. This application does not need review by this project.

The files under /rfc-ed/bin are not expected to be reviewed by this project unless they are invoked by the web services code.

The files to review under /rfcscripts and /rfc-ed/web/staff are primarily php.

The files under /rfcscripts are associated with the public website are running under WordPress. The javascript files associated with /rfcscripts files are under /rfcscripts/scripts

```
/rfcscripts/ $ wc *.php

  200   627   6802 all_clusters.php
  49   132  1415 ams_util_lib.php
  197   595   6633 auth48_cluster.php
  179   564   5702 auth48_cluster_lib.php
  351  1097  9956 auth48_status.php
  122   290   3005 cluster_info.php
  673  2336 22199 cluster_lib.php
  893  3089 32134 cluster_support_lib.php
   99   255   4548 config.php
   59   210   2126 core_lib.php
  501  1716 19148 current_queue.php
   67   259   2093 db.php
 2333 8321 85569 edit_lib.php
  255   859   8460 editor_lib.php
  123   412   3813 errata.php
  231   872  8103 errata_authen_lib.php
   67   195  2091 errata_confirm.php
  131   398  5445 errata_dataentry.php
  116   294  3339 errata_dataentry_confirm.php
   94   262  2727 errata_dataentry_insert.php
  202   584  6445 errata_edit.php
   91   195  2326 errata_edit_complete.php
   88   242  2599 errata_edit_confirm.php
   68   158  1665 errata_edit_list.php
```
The RPC uses /rfcscripts/reports for various counts, reports and sanity checks. Some of the reports are generated through cron, resulting in updated html files.
The RPC uses /rfcscripts/search/ for the centralized search. The search related files are under /rfcscripts/search and search related javascript files are under /rfcscripts/search/js/. The search application uses css from /rfcscripts/search/css/.
The RPC staff directory holds mainly php scripts and a few support javascript files.

/rfc-ed/web/staff $ wc*.php

437 1348 15124 Auth48Email.php
57 186 1579 add_draft.php
87 249 2253 ams_util_lib.php
327 829 8810 area_assignment.php
211 607 6359 auth48_edit.php
1236 3299 36874 auth48_lib.php
59 254 2134 auth48_setup.php
894 3089 32137 cluster_support_lib.php
510 1767 19774 current_queue.php
252 651 8915 current_rfced_time.php
61 229 1991 db.php
121 361 4387 display_adjust.php
7 15 90 doi.php
141 476 3952 edit_draft.php
2421 8684 89858 edit_lib.php
290 972 9627 editor_lib.php
23 39 489 errata_controls.php
247 791 7745 exportINDEX.php
50 138 1391 exportQueue.php
89 278 3089 export_lib.php
61 180 1581 format_lib.php
82 213 2487 header.php
24 103 1160 index-offline.php
20 37 342 index.php
130 411 4543 index_controls.php
395 1131 15322 insert_draft.php
384 1101 14577 insert_draft_test.php
300 972 10874 json_msg_lib.php
297 942 10383 json_msg_lib_test.php
714 2548 24817 list_drafts.php
34 72 1364 log_controls.php
749 2265 22167 makeAnnouncement.php
20 36 345 misc_controls.php
1 3 20 phpinfo.php
105 248 2825 postIndexDttracker.php
103 299 3485 publishDraft.php
246 646 9107 rfc_ed_time.php
93 265 3320 rfc_ed_time_index.php
587 1737 18907 rfc_state_lib.php
33 59 640 rfc_state_message.php
The public repository will not contain unused files (such as those under /rfc-ed/web/rfc/cgi-bin/). The contractor will work with the Tools Team and the RPC to identify the full set of files that will not carry forward into the public repository.

Changes to the codebase to remediate any identified vulnerabilities will be done in the new repository being created by this project. The contractor will not modify the existing CVS repository.