IETF

Making the Internet work better

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

7. Instructions for IETF Software Development Contractors will apply. See https://trac.tools.ietf.org/tools/ietfdb/wiki/ContractorInstructions?version=26

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
   104    318   3545 errata_edit_mail_select.php
   103    265   3017 errata_edit_select.php
   201    490   5585 errata_headers.php
   169    533   6261 errata_insert.php
  2861   8744  98544 errata_lib.php
    61    168   1533 errata_list.php
   310   1110  11899 errata_mail_lib.php
   169    490   5352 errata_reject.php
   378   1150  13995 errata_report.php
   260    829   8519 errata_search.php
   739   1956  23844 errata_search_lib.php
    77    213   2209 errata_thanks.php
   212    594   7264 errata_update.php
    89    271   3022 export_lib.php
   912   2851  34453 format_html_header.php
    10     52    674 handler_config.php
    98    293   3492 handler_lib.php
    80    143   1686 header.php
   304    923  10185 qsumm.php
   585   1734  18848 rfc_state_lib.php
   382    979  11697 rfc_subseries_lib.php
   112    433   4856 rfchandler.php
  1578   4420  49778 rfcmeta.php
   209    561   6619 state_history_lib.php
   244    676   6743 status_changes.php
    26     89    844 support_functions.php
   133    336   3963 verifier_name.php
    67    147   1683 verify_complete.php
   107    356   4089 verify_db_update.php
   246    773   8588 verify_errata.php
    47    112   1381 verify_errata_confirm.php
   214    564   7014 verify_errata_select.php
    91    287   3284 verify_hold_report.php
   185    459   5558 verify_login.php
    60    147   1660 verify_logout.php
   115    297   3392 verify_reject.php
 18727  57725 633419 total
```

```
/rfcscripts/scripts $ wc*.js

  369  1353 11496 errata_report_edits.js
   86   341  2572 rfcxml.js
  104   387  2978 rfcxml_rev.js
   31   109   921 validate_rejection.js
  272  1024  8796 validate_rfcsearch.js
   31   129  1072 verify_login_form.js
   60   238  2020 verify_name_email.js
  953  3581 29855 total
```

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.

```
/rfcscripts/reports $ wc*.php

    33     96    897 ams_util_lib.php
   893   3089  32134 cluster_support_lib.php
    64    259   2090 db.php
  2334   8321  85570 edit_lib.php
   256    859   8461 editor_lib.php
    86    258   2968 export_lib.php
    21     39    912 reports_config.php
   586   1734  18849 rfc_state_lib.php
   577   1854  26975 state_change_summary.php
   209    561   6619 state_history_lib.php
   166    547   5712 subpub_pub.php
    81    195   2296 subpub_stats.php
   211   1123  14533 subpub_stats1.php
   137    449   4553 subpub_sub.php
   643   1835  23836 summary_stats.php
  6297  21219 236405 total
```

```
/rfcscripts/reports $  wc *.sh

  34  140 1148 email_monthly_sum.sh
  19   86  561 monthly_sum.sh
  23  102  672 summary_stats.sh
  76  328 2381 total
```

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/.

```
/rfcscripts/search $ wc *.php

    71    252   2058 db.php
   136    351   4504 rfc_headers.php
  2369   6920  86180 rfc_lib_new.php
    29     24    479 rfc_search.php
   647   2094  26525 rfc_search_detail.php
     6      8    230 search_config.php
     5      8    162 search_constant.php
    37     72    923 standards.php
  1062   3017  42113 standards_detail.php
   155    381   4439 standards_headers.php
  4517  13127 167613 total
```

```
/rfcscripts/search/js $ wc *js

9301 39443 260018 jquery.js
482 1687 19167 validate_rfcsearch.js
9783 41130 279185 total
```

```
rfcscripts/search/css $ wc *css
  30    69   534 rfcsearch_mobile.css
  358   683  5543 rfcsearch_new.css
  392  1217  9505 rfcsearch_wp.css
  780  1969 15582 total
```

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
   124    340   4135 rfcatom.php
    88    277   3211 rfcrss.php
   365   1031  11616 sendEMail.php
   546   1524  18009 state_history_lib.php
   369   1254  15038 track_by_editor.php
 13390  41956 456853 total

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

  18   56  441 area_assignment.js
  72  314 2159 auth48.js
  69  197 2077 index_controls.js
  15   36  310 validate.js
 174  603 4987 total
```

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.