Making the Internet work better

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

2020-02-05

IETF Executive Director
exec-director@ietf.org

Overview

The IETF Administration LLC is soliciting bids for a Security Review and Remediation of the RFC Production Center Web Accessible Code.

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

05 February 2020	RFP Issued
19 February 2020	Questions and Inquiries deadline
26 February 2020	Answers to questions issued and RPF updated if required
4 March 2020	**Bids due**
18 March 2020	Preferred bidder selected and negotiations begin
1 April 2020	Contract execution and work begins

RFP Process

The process for the RFP is as follows:

1. The RFP is publicly issued, posted to our website at www.ietf.org and announced to the IETF Announce mailing list.
2. Potential bidders have until 19 February 2020 to submit any questions by email to ietf-rfps@ietf.org. Questions will be treated as anonymous but not private, as explained below.
3. A written response to all questions is provided on or before 26 February 2020, both direct to those parties that sent questions and posted on our website. The response will include the questions asked and the answers, but will not identify the company

asking the question. If required, then the RFP may be updated to correct or clarify any issues identified.

4. Bids are due by **4 March 2020** by email to ietf-rfps@ietf.org. The bid should include the following information:
    a. Executive summary
    b. Project approach including any assumptions.
    c. Project plan and schedule including when the work will begin and end, and any other milestones, as well as any dependencies that may delay delivery.
    d. Fee and payment schedule. Fixed priced bids are preferred but if that is not possible then a maximum fee must be specified.
    e. Warranty including a proposal for fee reduction/refund due to late- or non-delivery
5. The IETF Administration LLC and designated contractors and volunteers will select a preferred bid and notify the bidder by 18 March 2020. The selection process may include questions by email and/or conference call.
6. The IETF Administration LLC then enters into contract negotiation with the preferred bidder, based on its standard contract and using the relevant sections of the Statement of Work below. If contract negotiation fails then a different preferred bidder may be chosen.
7. Contract negotiation is anticipated to complete by 1 April 2020 and result in the award of the contract. All RFP contract awards are posted on our website and announced to the IETF Announce mailing list. The terms of the contract are later posted publicly on our website, with the fee information redacted. In addition any Conflict of Interest declarations required of the preferred bidder are also posted publicly on our website. This transparency is non-negotiable.
8. Work generally begins immediately after award of the contract, unless specified otherwise in the Statement of Work.

Jay Daley

IETF Executive Director

IETF Administration LLC

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.

This code has, to date, only been reviewed by the RFC Production Center programmers and staff. This will be the first formal security review.

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
2. A list of all identified security vulnerabilities including the following details for each:
    a. Attack vector / Invocation mechanism
    b. Proof of concept and/or reference to standard vulnerability documentation
    c. Potential impact
    d. Proposed remediations
3. Changes to the codebase implementing agreed upon remediations.
4. A clean repository ready to be made available openly to the public.

Note:

- 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.

Details

Code

The code to be reviewed is mainly PHP 5.5. Work has begun to move the codebase to PHP 7 but this is still in the early stages. No PHP frameworks are used though much of the code interacts with WordPress 5.0.3.

Some of the code is Javascript using JQuery 1.8.1 and targeting modern, popular, actively supported mobile and desktop browsers in their default configuration. Support should include at least Chrome, Firefox, Safari, and Edge. IE support is not required.

The database is MySQL.

No frameworks or libraries are used other than those listed above.

Nothing in the code requires compilation/building.

A full list of files, source language and word count is given below.

Repository

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

Path	Included	Commentary
rfcscripts	**yes**	Code associated with the public website running under WordPress.
rfcscripts/images	no	No executable code
rfcscripts/reports	**yes**	Various counts, reports and sanity checks. Some of the reports are generated through cron, resulting in updated html files.
rfcscripts/scripts	**yes**	Javascript to support code associated with the public website running under WordPress
rfcscripts/search	**yes**	Centralized search
rfcscripts/search/js	**yes**	Javascript to support centralized search
rfcscripts/search/css	**yes**	CSS to support centralized search

rfc-ed	no	Empty except for sub-directories
rfc-ed/bin	**possible**	Not expected to be reviewed by this project unless they are invoked by the web services code.
rfc-ed/web	no	Empty except for sub-directories
rfc-ed/web/rfc	no	Empty except for sub-directories
rfc-ed/web/rfc/cgi-bin	no	Not used
rfc-ed/web/rfc/htdocs	no	Legacy - their functionality has been moved to other parts of the codebase.
rfc-ed/web/staff	**yes**	Mixed PHP and JS files.
rsestats	no	Django application providing statistics reports, which does not need review by this project.

A full listing of files as of October 2019 is given below. Since this listing was generated, some work to move to PHP 7 has begun but without any significant change in the size of the codebase:

```
/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

/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

/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

/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
```

As noted above, the following files are not expected to be analysed but will need to be if called from code that is, and so these are listed for completeness:

```
/rfc-ed/bin $ wc *

     56     218    1418 ABNFextract
     41     162    1144 AUTH48post
     44     139     841 INDEXrec
```

```
  54     175    1218 Qscrape.pl
 112     428    2996 abnf.ParserIO.pm
 433    1296    9062 abnfcheck2
 215     724    6500 addSymLink.pl
  37     141    1069 add_new
  62     260    2331 after_INDEX_updated.sh
  27     121    1060 archive-mysql-backups.sh
 198     627    5863 area_directors.pl
 115     459    3851 auth48_list.py
  42     170    1040 autoarch
 355    1286    7622 autoroff
 304    1058    9327 build_clusters.pl
  50     188    1775 check-in-notes.py
  96     366    3069 checkNrefs.pl
  18      98     496 checkabnf
  18      99     470 checkbcp14
  17      93     435 checkxml
  80     346    2563 ckText
  96     444    2646 ckText1
  85     287    1929 cleanDir.pl
  72     339    2129 cleanup
  26     140    1016 cleanup-mysql-backup-archive.sh
 834    2956   30492 cluster_support_lib.php
 264    1221    9269 clusters_lib.pl
 386    1032    9153 consistencyCheck.pl
 248     758    6799 create-categories.pl
  16      68     563 create-index.xml.sh
 392    1525   10888 create-indexes.sh
 155     462    4555 create-pdfrfc-dir.pl
 168     460    4472 create-pdfrfc.pl
1090    3298   27391 create-rfcxx00.pl
 200     635    5606 create7and30dayZIPandTAR
 179     736    5302 createLatestZIPandTAR.pl
 298     838    7353 createSTAR.pl
 196     564    5310 createZIPandTAR
  49     175    1504 db.php
  65     247    2347 dbi.php
 270     979    5854 dotblank
  14      43     274 draftstat
  38     153     854 dupewords
  16      38     480 errata_json.sh
  56     183    2023 errata_json_creator.php
  43     131    1214 extract_abstract
 175     550    5325 extract_abstract.php
  37     123    1194 extract_pagecount
  99     280    3113 extract_pagecount.php
  43     131    1200 extract_title
 163     527    4980 extract_title.php
  46     293    1814 fix.pl
 510    2137   16736 format_queue.pl
 519    2194   17615 format_queue2.pl
  16      53     680 format_queues.sh
 589    2159   18976 generate_INDEX_from_db.pl
  34     114    1679 get-citations.sh
```

```
 40     113     942 get-comments.py
 67     205    1802 get-comments2.py
 50     159    1822 get_index_doc.php
100     355    2968 htmlwdiff
 22      78     678 in-notes_notify.sh
 35     139    1252 index_json.sh
248     839   10100 index_json_creator.php
 49     122     870 indsubs
151     455    3582 init-stars.pl
 87     296    2804 make-backups.pl
 10      37     220 make-rfc
331    1361   10884 make-rfcxx99
  8      31     215 make.bin.map.sh
247    1278    8644 make_bcp_ref.pl
194    1050    6603 make_ref.pl
246    1277    8657 make_std_ref.pl
 15      87     760 makeall
 14      43     384 makehtml
132     629    3849 maketoc
157     795    4819 maketocAH
132     633    3876 maketocL2
132     633    3875 maketocL3
152     770    4691 maketocb3
152     770    4686 maketocbv
213     997    5980 matchref
226    1023    6181 matchref2
162     862    5793 missref.pl
 64     310    2662 mk_rfc_errata_list.pl
 66     224    1492 mkv3diff
 21     120     965 move-backups-weekly.sh
195     498    5498 new-id-search-db.pl
211     478    5180 new-search-db
 18      96     448 newdupe
 18      99     463 newspell
175     693    4310 pagerfcs2date.pl
 40     124    1242 parse-bcpref.py
 30      98     912 parse-rfcref.py
 40     124    1242 parse-stdref.py
 36     118    1106 pdfrfcZIPandTAR.sh
 42     190    1286 postv2
 27     111     698 printable
 61     170    1662 printable.pl
 68     215    1944 printable0.pl
 48     156    1526 printable2.pl
 46     122    1320 printable3.pl
 22      50     712 printable5.sh
1714    5680   62563 queue-stat.pl
240     765    8979 queue_data.php
171     721    5198 recreateZIPandTAR.pl
112     311    2953 rfc-index-latest-entry.pl
 96     292    2983 rfc-index-reverse-split.php
 72     234    2377 rfc-index-split.php
724    2428   26495 rfc2doi.py
168     740    6628 rfc2txt.py
```

```
  229     435    7330 rfc_element_html_templates.xsl
  107     449    4706 rfc_index2html.xsl
  108     452    4711 rfc_index2html_rev.xsl
 1140    4791   35783 rfcdiff
  204     748    8554 rfcindex.py
   72     219    1889 rfcstrip
 1421    3042   30869 rfcxx00.last.pl
 1125    3104   25079 rfcxx00.lasttxt.pl
   37      93     784 rfcxx00.run.pl
   38     165    1686 scripts_to_run_after_INDEX_update.sh
   73     380    2444 simple-bcp-fix.pl
   22      76     672 single_json_generator
  298    1049    9350 state_check.pl
  208     560    6603 state_history_lib.php
   22      85     835 state_null_notify.sh
    6      18     107 tab8
   28      94     699 test4rfcinfo
 8719   30571  253836 tkdiff
  107     465    3297 tvf_rfc_lib.pl
  460    1637   15041 twelveRecentRFCs.pl
   97     254    2422 urltest.pl
   46     155    1112 v3add_new
   86     405    2660 v3cleanup
   92     337    2324 v3copy2number
   78     285    2329 v3post
  169     645    5969 v3postlast
  124     397    3661 whatsnew.pl
  374    1042   10219 working_group.pl
   32     192    1154 working_group_cron.sh
  141     675    5714 working_group_update.pl
  826    3366   26859 xmlIndex.pl
   88     339    3288 xmlIndexDaily.sh
  364    1123   15650 xmlRFCref.php
  542    2043   16410 xxx-index-html.pl
35241  124622 1060712 total
```

ENDS