OpenSSF Best Practices WG Notes - 2021

Thanks to the WG for a GREAT 2021! This document is closed for updates. See 2022 Meeting notes for current group activities.

~~~~~Template - copy below for each call ~~~~~

< TEMPLATE DATE>

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Jon Zeolla (Seiso)
- Altaz Valani (Security Compass)
- Xavier Rene-Corail (GitHub)
- Vinod Anandan (Citi)
- Art Manion (CERT/CC)
- Kim Lewandowski (Google)
- Dave Russo (Red Hat)
- Björn Kimminich (OWASP)
- Matt Rutkowski (IBM)
- Ryan Ware (Intel)
- Beth White (Codethink)
- Glenn ten Cate(SKF)
- Azeem Shaikh (Google)
- Manuel Ifland (SAFECode/Siemens Energy)
- Ben Stoltz
- Daniel Silverstone (Codethink)
- Michael Scovetta (Microsoft / SAFECode)
- Marta Rybczynska (OSTC)
- Jacob Wilson (Synopsys)
- Patricia Tarro (Dell)
- Arnaud J Le Hors (IBM)

Meeting Notes:

-

New friends:

-
~~~~~

Project Updates
(please enter and speak to anything interesting)

CII Best Practices Badge (David A. Wheeler)

-

edX Course (David A. Wheeler)

- No new news.

SKF(Glenn)

-

Inventory

-

Scorecard

-
-

Future WG collaboration:

- Great MFA Giveaway - https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit#heading=h.1sasnsizzrv0
- “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

~~~~~~~~~~~~~~~~~~~~~~~~

2022 WG Notes moved to this doc

20211207

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Xavier Rene-Corail (GitHub)
~~~~~~~~~~~~~~~~~~~~~~~~

- Glenn ten Cate(SKF
- Marta Rybczynska (OSTC)
- Arnaud J Le Hors (IBM)
- Georg Kunz (Ericsson)
- John Naulty (Coinbase)
- Laurent Simon (Google)

Meeting Notes:

-

New friends:

- Yotam Perkal (Rezilion)

Project Updates
(please enter and speak to anything interesting)

Great MFA Distribution Project

- This is VERY time-sensitive, so request that we complete this agenda item FIRST & then others as needed.
- Purpose of Great MFA Distribution Project is to send *FREE* hardware MFA tokens (generously provided by Google & GitHub, 500 each) to critical OSS projects. This helps counter some attacks, e.g., attackers using stolen passwords of legitimate developers to distribute subverted source code and/or packages
- More info at https://github.com/ossf/great-mfa-project (some details at https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit#heading=h.1sasnsizzrv0)
- Which projects to distribute to? OpenSSF critical projects WG has developed a list of ~100 critical OSS projects here: https://docs.google.com/spreadsheets/d/1ONZ4qeMq8xmeCHX03IlgIYE4MEXVfVL6oj05IbuXTDM/edit#gid=0 ; this is the set of projects we'll offer MFA tokens to
- Overall process:
  - We notify critical OSS projects that they're eligible for free MFA tokens, they tell us if they want them (& how many of each).
  - We distribute "coupon codes" (Google Titan) and "validation codes" (GitHub Yubikeys) to the projects. Each is a use-once code that lets people "buy" the token at no charge from the Google Store / GitHub Shop (respectively).
  - Note: OpenSSF *never* has physical possession of the tokens, nor do we have to ship them - the stores handle this.
- CRITICAL ISSUE: MUST distribute Google tokens by the end of December, as their coupon codes expire then. We might get more later, but we LOSE any we don't distribute this time around.
- David A. Wheeler has done a "trial run" with the Linux kernel & curl
  - Linux kernel doesn't need any (they have their own supply), but Greg K-H did provide some helpful feedback

    - curl is interested, they’d like at least 4 (still working details).
- We NEED NOTIFIERS. NOW.
    - Notifiers contact projects, share our invitation <https://github.com/ossf/great-mfa-project/blob/main/invitation.txt>, report back if they want tokens, how many, & where to send the info.
    - Ideally a notifier is already known to the project - not always possible, but please tell us of those who know you, so we can prefer you!
    - If we have 5 notifiers, that means each notifier will have to notify 100/5 = 20 projects, so more notifiers are better.
- VOLUNTEER NOTIFIERS ARE:
    - David A. Wheeler - dwheeler@linuxfoundation.org
    - Xavier Rene-Corail
    - Marta Rybczynska
    - CRob
    - John Naulty - john.naulty@coinbase.com
    - Arnaud J Le Hors
    - Glenn ten Cate
    - Georg Kunz
- Notifiers: Please let us know which projects know you
    - Editable copy of crit project list, put your notifier name in column H, https://docs.google.com/spreadsheets/d/1sO_tJ_B7_2I-TUx23pnBoIRJIqaOm8yBnKAwqs7DwBw/edit#gid=0
    - By end of TODAY, put your name in column H of any project who knows you. After that, we’ll assign the rest.
    - Tomorrow+, please start sending invitations. Text of invitations: https://github.com/ossf/great-mfa-project/blob/main/invitation.txt (e.g., email) https://github.com/ossf/great-mfa-project/blob/main/invitation.md (e.g,. GitHub issues)
- We also need help improving our “how to” documents on how to use them - EVERYONE, please keep creating pull requests to improve them!!
- Next round Marta suggests adding bootloaders to list
    - David A. Wheeler: Good idea! Please mention this to Amir
    - David A. Wheeler has added a stub to the critical OSS projects WG’s list, so that they will at least consider this.

CII Best Practices Badge (David A. Wheeler)

- Discussing rename from “CII”. I’ve been busy on Great MFA Distribution, but intend to get back to that & complete it.

edX Course (David A. Wheeler)

- No new news.

SKF(Glenn)

- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    - https://github.com/ossf/wg-best-practices-os-developers/pull/44
- Creating stories and project definition

Inventory

-

Scorecard

-

OSS supply-chain security best practice WIP

- [Laurent]: introduction of project https://docs.google.com/spreadsheets/d/1cf7A5hBA7fgtnNd-_XJJOmm2rRGTWxHpkqR9ihind48/edit?resourcekey=0-AsSqhE8APC9GyR6vwN2nLQ#gid=0
- Can be used for project omega
- GCC flags for C/C++:
- Q: What’s the connection to SLSA?
- Yotam suggests the “MITRE-attack framework” to look at/refer to

Future WG collaboration:

- “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20211123

Attendees:

- CRob (Intel)
- David A. Wheeler (Linux Foundation)
- Xavier Rene-Corail (GitHub) - Sub - Jose Palafox (GitHub)
- Dave Russo (Red Hat)
- Glenn ten Cate(SKF)
- Azeem Shaikh (Google)
- Arnaud J Le Hors (IBM)

New friends:

- Jose Palafox (GitHub) - can give more context on MFA

Meeting Notes:

- Introduce any new friends
- Great MFA Distribution Project
    - Big issue: Google's coupon codes expire at the END OF THIS YEAR, so we need to HURRY if we want to use them. The set is worth about $15K, so it'd be a shame to lose them.
    - David A. Wheeler has made changes to repo that propose a schedule to meet this hurried date <https://github.com/ossf/great-mfa-project>. It's very aggressive, but it seems possible - we should at least try. Even if we only get some distributed, that's more than 0.
    - WE NEED YOUR HELP. We need help in completing a list of critical projects & docs on how to use them by 2021-12-02, volunteer "notifiers" to notify projects, etc. See below. If there are other jobs to be done, please let us know!!
    - Proposed schedule:
        - We'll use a list of about 100 critical open source software (OSS) projects as identified by the OpenSSF Securing Critical Projects Working Group; see their current list. We'll use the version as of 2021-12-02, since the Google coupon codes expire on 2021-12-31.
        - We'll also develop a set of simple documents on how to use these tokens for common OSS cases, by 2021-12-02
        - Identified critical OSS projects will be sent at invitation by one of the great-mfa-plan notifiers (e.g., John Naulty, David A. Wheeler), typically by filing an issue, in 2021-12-02..09.
        - When a project accepts, the notifier will tell a sender (David A. Wheeler or Jory Burson) key information: the project who has accepted, the email address to send private information to, and how the project accepted. The sender will then send the project the coupon codes and validation codes using the coupon_sending.md template. This is 2021-12-03..31.
        - Projects distribute the codes. Receivers use them to get the tokens from the Google Store or GitHub shop. Then the tokens get used!
        - Projects send back some information, that we combine with other data and determine whether or not we've had a positive effect (hopefully we have!).
    - Minor issue, we think resolved: Learned that GitHub doesn't want to send us coupon codes directly, to ensure that they're really distributed to different people. Worked with Xavier; GitHub will send "validation codes"; each user will use a GitHub web page to convert a validation code into a coupon code. The purpose is to ensure legal compliance & getting metrics.
    - GitHub wants a short blurb from the project. Proposed text:
        - The Great Multi-factor Authentication (MFA) project, a project of the Open Source Security Foundation (OpenSSF), is intended to

prevent supply chain attacks involving weak or compromised credentials (passwords) of developers of open source software. The "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attack" by Ohm et al noted that this is one way to subvert open source software (OSS), e.g., its source code (in a force) or its package (in a package repository). For example, Malware found in coa and rc, two npm packages with 23M weekly downloads", 2021-11-05 and the Popular NPM package UA-Parser-JS poisoned with cryptomining, password-stealing malware".

-

- Issue: are we measuring enough? The right things?
  - Current requirements:
    - How many of recipients didn't have an MFA hardware token before, and
    - How many people used the Google coupon codes to receive an MFA token (we can separately get the total counts for the GitHub validation codes)
  - Probably should ask for slightly different numbers. Do we anticipate giving at most 1 token from each source to an individual (if not, how do we reword)? The Google & GitHub tokens may be sent at different times, and we should probably just ask for all the numbers we need (even from GitHub). E.g.:
    - How many people received a token from just Google, just GitHub, and from both (3 numbers)?
    - How many people didn’t have any tokens before who received a token from just Google, just GitHub, and from both (3 more numbers)?
  - If we just plan to distribute tokens to projects (multiple tokens per person possible, because people are more likely to depend on tokens if they have backup tokens), maybe we instead ask for:
    - How many tokens did you distribute from just Google? From just GitHub?
    - How many people received tokens from just Google? From just GitHub? From both?
    - How many people didn’t have hardware tokens they used for OSS who received tokens from just Google? From just GitHub? From both?
  - Any other suggestions/volunteers?
    - CRob will create a comm plan - draft by EOD tomorrow
    - Token docs: Titan easy with tokens - please add PRs!
    - Arnaud: GitHub setup Titan key - Arnaud will add links as PRs
      - https://www.yubico.com/github for Github config

        - https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/configuring-two-factor-authentication#configuring-two-factor-authentication-using-a-security-key
        - Good to have both text and videos
        - Video “Connect to GitHub without a password”: Anchor to 10:22 https://www.youtube.com/watch?v=D2gXo-T4wqA
    - CRob will add some software token data
    - David will work to help critical projects
    - Glenn ten Cate: We had talked about Q&A, e.g., backup/recovery when the token breaks. Will write up something on backup/recovery.
        - For GitHub: https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/recovering-your-account-if-you-lose-your-2fa-credentials
    - Notifiers (of projects):
        - David A. Wheeler
        - Xavier
        - Jose
        - CRob
        - Arnaud

- Status reports

Project Updates
(please enter and speak to anything interesting)

CII Best Practices Badge (David A. Wheeler)

-

edX Course (David A. Wheeler)

- No new news.

SKF(Glenn)

- Testing the Kraken and Keycloak
- Draft of interactive design for website
- Azure credits - open source initiative
- ING Announcement
    - Going to help create 3 learning paths

Inventory

-

Scorecard

- GitHub actions almost ready
- Working on badges
- Best practice for package manager, especially pinning (will share in a few weeks)

Future WG collaboration:

- “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20211109

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Dave Russo (Red Hat)
- Matt Rutkowski (IBM)
- Azeem Shaikh (Google)
- Marta Rybczynska (OSTC)
- Arnaud J Le Hors (IBM)
- Jeff Mendoza (Google)
- Arlen Baker (Wind River)

Meeting Notes:

- @CROB reach out to GitLab contacts to get re-engagement
- New Friends?
- Opens
- Town Hall Next week!
- SECOM “Adoption”/endorsement
    - https://tqrg.github.io/sec-commits/
- Great MFA Giveaway collab
    - https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit
    - Giveaway - Google will give Titan keys - give coupon codes, order on Google.
    - CRob volunteers to help with Yubikeys
    - GitHub - verbal commit - talk with Xavier - can give 500 Yubikeysk, coupon tokens to order them on GitHub shop.

    - Can't give to places forbidden by export controls
    - Plan to work on "most critical projects" - as identified by project Alpha, Harvard analysis, criticality score
    - Perhaps we could use them as reward for improving Scorecard or CII BP badge score (secondarily)
    - "Don't want this to be a token effort" (GB)
    - Xavier: We want this to go even bigger. If the first phase works well, we can provide more. It's super-important to align on success measures.
    - Need to measure "this person wasn't using MFA & now they are & they are a contributor to an OSS project"
        - Maybe ask contributors to give us GitHub / GitLab handles - GitHub & GitLab can then check before/after (didn't have 2FA before, had 2FA after)
        - OpenSSF could track coupon codes & accounts
        - GitHub could make queries before & after on accounts and report % of accounts that use 2FA at end & percentage that used at start of those users
        - Need to develop a draft proposal for measuring results, e.g., capturing account names, & run by legal
    - Laurent: This information is available within GitHub if they use GitHub, but not public
    - There's a debate on whether or not to publicly show "this user uses MFA" via API
    - What are Alpha/Omega timelines (when do we need to be ready?)

New friends:

- Arlen Baker (Wind River)

We have a new OpenSSF Governing Board (GB), lots of additional money allocated.

Project Updates
(please enter and speak to anything interesting)

CII Best Practices Badge (David A. Wheeler)

- Presented today at Open Source Experience, Paris, went well
- Rename: "CII Best Practices Badge" to "OpenSSF Best Practices Badge" (GitHub badge would show "ossf passing" et al.? https://github.com/coreinfrastructure/best-practices-badge/issues/1515
    - Generally agree, eliminates confusion
    - What about scorecard? "OpenSSF ScoreCard Badge" if it has a badge
- We're getting a HUGE number of queries of the form GET path="/projects.json?url=https%3A%2F%2Fgithub.com%2Fpoppinss%2Fmodule-methods-extractor" host=bestpractices.coreinfrastructure.org fwd="34.72.136.33, 34.72.136.33,167.82.161.45" - they *appear* to be from Google IP ranges (not a single

system). They aren’t taking us down but they sure create log entries. Anyone know what’s going on?
    - Azeem Shaikh - analyzing a million repos a week.

edX Course (David A. Wheeler)

- No new news.

SKF (Glenn)

-

Inventory

-

Scorecard (Laurent)

- Working on a tighter collaboration with AllStar.
- Scorecard GitHub Actions should be rolling out soon. Thanks to Laurent!
- Exploring Scorecard + SLSA collaboration. azeems@ will present some high-level ideas in the coming weeks at this meeting if anything materializes here.
- Pinning & Dependabot discussion:
    - Dependabot doesn’t look for malicious components before notifying an update currently. Have separate work to look for that.
    - (Long discussion)
    - Wheeler: Think GitHub would be willing to tweak the matching comment (“COMMENT-SYMBOL pin NUMBER”) ?:
    - # the naming convention of https://github.com/mheap/pin-github-action
    - - - uses: actions/checkout@1e204e9a9253d643386038d443f96446fa156a97 # pin @v2.3.4
    - + - uses: actions/checkout@1e204e9a9253d643386038d443f96446fa156a97 # pin @v2.3.5
    -

Future WG collaboration:

- “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20211026

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Dave Russo (Red Hat)
- Matt Rutkowski (IBM)
- Azeem Shaikh (Google)
- Arnaud J Le Hors (IBM)
- Patricia Tarro (Dell)

Meeting Notes:

-

New friends:

- Georg Kunz (Ericsson)
- Jack (ControlPlane/nix)

Project Updates

CII Best Practices Badge (David A. Wheeler)

- We'd love to have more reviewers of pull requests! Currently we're trying to update our style checker, which requires various minor code changes. Just watch: https://github.com/coreinfrastructure/best-practices-badge & occasionally review a pull request

edX Course

- No new news.

SKF

-

Inventory

-

Scorecard

- V3 release presentation:
  - Numeric scoring and risk categories replace Pass/Fail.
  - New repo interface to simplify the future integration of other code versioning systems besides GitHub.
  - Weekly scans for 200k (now 600k) GitHub repos with critical ecosystems dependencies.
- Community contribution guidelines - Scorecard is working on improving their contribution guidelines and looking for input from other experienced maintainers.

WG collaboration:

- Great MFA Giveaway
  a. “Great MFA Distribution” Plan https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit
- “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
  a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20211012

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Dave Russo (Red Hat)
- Glenn ten Cate(SKF)
- Marta Rybczynska (OSTC)
- Arnaud Le Hors (IBM)

Meeting Notes:

- NIST SSDF - SP800-218 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218-draft.pdf
  - Public comment period: September 30, 2021 through November 5, 2021
- Arnaud talks about the hyperledger project
  - Block-chain based
  - Immutable
  - Challenges working across different languages
  - Looking to implement OSSF’s Vuln. Disclosure guide
  - Steering committee looking to create welcoming, consistent environment for projects to work in
  - Enforces presence checking at commit, but this is just a string & not bullet-proof
  - Some contributors have reasons to not disclose their identities
    - How can we respect those needs but also ensure quality/integrity/security of the commits

New friends:

Project Updates

CII Best Practices Badge (David A. Wheeler)

-

edX Course

- No new news.

SKF

- New release done, Portmapping Labs -> Subdomain labs, MASVS fully implemented
- Started with the SSO implementation using KrakenD, KeyCloak
- Azure deployment how to PR received
- Mentoring student: rebuilding the Python labs NodeJs
- Todo: Lab Editor release

Inventory

-

Scorecard

- Recent v3 release
- Working with them to imply users don't HAVE TO use Github (more generic implementation)
    - Would be nice to have examples for other repo implementations (GitLab, etc)

WG collaboration:

- Great MFA Distribution project
    a. https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit
    b. Need to collect use cases
        i. Why MFA?
            1. Credential theft
            2. ...
        ii. You just got a token! What now? (OS differences, device differences)
        iii. How to use token to log in and sign git commits: given token type, forge (GitHub, GitLab), platform
        iv. How do I use it to execute a release
        v. What if it is lost or broken? Recovery mechanism / path
    c. Talk to Git* about sharing process & access to giveaway to their users
    d.
- "Existing Guidelines for Developing and Distributing Secure Software" - Existing Guidelines for Developing and Distributing Secure Software
- Next project will be "newbies view" for secure coding and practices - will leverage our SKF "one-pager" as a reference to structure the deck.

a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20210928

Attendees:

- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Matt Rutkowski (IBM)
- Azeem Shaikh (Google)
- Marta Rybczynska (OSTC)
- Arnaud J Le Hors (IBM)
- Eric Cornelissen (Cobalt.io)

Meeting Notes:

-

New friends:

- Sofia Reis

Project Updates

CII Best Practices Badge (David A. Wheeler)

-

edX Course

- No new news.

SKF

-

Inventory

-

Scorecard

- V3 Release upcoming; providing 0-10 scoring; enabling as a github action
    - Xav asks why shift to one score? - team got some user feedback, also looking for way to show users if a project is compliant with policies.
    - Score is a policy view of the results (Xav - changes seem directed to make tool more actionable for users)
    - Team will do demo for WG in ~ 2wks

WG collaboration:

- Any updates for our “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
- Great 2FA giveaway project
    a.
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0
- SECOM Convention
    - Best practices for security commits messages
        - Sofia presented her work on SECOM
            - Details/Website: https://tqrg.github.io/sec-commits/
            - Survey: https://forms.gle/YADhxoe7d4nqLHnQ8
            - Presentation: https://drive.google.com/file/d/1_UFPRDD9jvmlARxWshSu9WNV1ib_kCid/view?usp=sharing
            - E-mail: sofiareis1994@gmail.com // sofia.o.reis@tecnico.ulisboa.pt

        - Working to teach ML how to detect sec vulns in JavaScript source code
            - Ned more data
        - Using Natural Language Processing to scrub ~8000 commits
        - “Are security-relevant commits informative?” - YES!§
            - See 3 patterns - Poorly documented, misspelling issues, & non-security related notes
                - Practices & templates to create better security commit messages would be helpful
        - “How to write a good security commit message? Are there sources/guidelines available?”
            - For general commits, yes, security not so much
            - Created SECOM template to help solve this problem
            -
- Next call Arnaud will talk about Hyperledger & WG intersection

20210914

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)

- Ryan Ware (Intel)
- Glenn ten Cate(SKF)
- Azeem Shaikh (Google)
- Chris Horn (Secure Decisions)

Meeting Notes:

-

New friends:

-

Project Updates

CII Best Practices Badge (David A. Wheeler)

- Working on implementing Scorecards and also feeding comments back
  - Implemented pinned dependencies - asked to change pinning so it only applies to applications (not automated, not clear it can do that)
  - Updated Scorecards description of CII Best Practices
  - Need to work through yes

edX Course

- Have added a number of issues for things to do for a later update. See: https://github.com/ossf/secure-sw-dev-fundamentals/issues - if there's more, please add an issue!

SKF

- Making final changes to the SKF Lab Editor feature
- Testing SubDomain based deployments
- After this testing Azure deployment

Inventory

-

Scorecard

- Increased repo count analyzed by Scorecard to 100k.
- Recently realized Project Thoth is using Scorecard - https://github.com/ossf/scorecard/issues/978#issuecomment-917955571.
- V2 version of result format coming. Scores of 0-10 instead of Pass/Fail.
- Design completion of Scorecard GitHub Actions and GitHub badge.

WG collaboration:

- "Existing Guidelines for Developing and Distributing Secure Software" - Existing Guidelines for Developing and Distributing Secure Software

- Discussion of https://kompar.tools - extends CCR to record weakness coverage for various techniques. Are building these mappings for other techniques, various tools, etc.
    a. Could be really useful for Scorecard - given the tools used, what weaknesses are covered or not?
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0
- 2FA tokens - think OpenSSF will get a number of Yubikeys to distribute - need some hands-on video tutorials, etc., on hardware tokens so people will know how to use them well.
    a. John Naulty has past experience training on tokens
    b. Craft some training materials on how to install and use + tips & tricks (videos, etc)
    c. Need to collect use cases
        i. You just got a token! What now? (OS differences, device differences)
        ii. How to use token to log in and sign git commits: given token type, forge (GitHub, GitLab), platform
        iii. How do I use it to execute a release
        iv. What if it is lost or broken? Recovery mechanism / path
    d. Others interested: Chris Horn, Ryan Ware, David A. Wheeler, Glenn ten Cate
    e. Yubikey packaging information: YubiKey packaging - Yubico
- NIST Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software
    a. https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot
    b. One reference cited NIST SSDF - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf

20210831

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Matt Rutkowski (IBM)
- Glenn ten Cate(SKF)
- Marta Rybczynska (OSTC)

Meeting Notes:

- To spread the word - conference talks & blog posts
    - Fosdem cfp soon (feb 6 &7)
        - https://fosdem.org/2021/

        - Glenn has deck that he uses that could potentially be modified to add in WG materials - https://www3.dbmaestro.com/blog/21-essential-devops-events-of-2021
    - DevOpsDays
        - https://devopsdays.org/
    - B-Sides (assorted)
        - https://infosec-conferences.com/category/bsides/
    - David A. Wheeler will present at “Open Source Experience” Paris, France
    - David’s been trying to do some of this, see: https://dwheeler.com/presentations.html - but more is better!

New friends:

-

Project Updates

CII Best Practices Badge (David A. Wheeler)

- We now have over 4,000 participating projects (4029 as of August 30), see https://bestpractices.coreinfrastructure.org/en/project_stats
- As always, update dependencies. This included updating Rails 6.1.3.2->6.1.4.1, which addressed actionpack vulnerability CVE-2021-22942, <https://groups.google.com/g/rubyonrails-security/c/wB5tRn7h36c> "Possible Open Redirect in Host Authorization Middleware".
- We point to the edX course, but edX’s text makes it appear you must pay to take the lessons. We now point to the OpenSSF page, clarified that you “audit” to take the free course, and make the same changes on the OpenSSF website page about the course. That should make it easier for people to understand the difference between paid & free, and then easier to choose their preferred option.

edX Course

- No new news.

SKF

- Finalizing gsoc implementation of editor (fixing window resizing)
- Will next modify SKF to launch editor
- Adding KB descriptions & guidance on implementation for MASVS (Mobile application security verification standard) + expert system
- Working on CII Best Practices Badging process - Glenn may create a blog post. It wasn’t bad, learned some things (e.g., didn’t have a way to report vulnerabilities). Needed to have license in GitHub, etc. Could have boilerplate best practices template
- Best Practice Badge “starter kit” of templates to jumpstart new projects with examples for them to leverage

    - David: I’ve talked with others before. One challenge is that it’s more work than it appears at first. Maybe with very simple text instructions to start with, and then later try to automate some things.

Inventory

-

Scorecard

-

C/C++ recommendations for compiler flags

- Marta has a similar thing
- In general, it’s agreed to be a good idea.
- Start on Google docs, then transition to GitHub doc Markdown within the Best Practices WG - https://docs.google.com/document/d/1SslnJuqbFUyTFnhzkhC_Q3PPGZ1zrG89COrS6LV6pz4/edit

WG collaboration:

1. “Existing Guidelines for Developing and Distributing Secure Software” - Existing Guidelines for Developing and Distributing Secure Software
    a. Will talk with the Tooling group on 8/24. - check - they will be reviewing their existing docs
    b. Will review Tooling feedback as a group 8/31 - - Tools not prepared at this time
    c. Target 9/14 for publication of guidance - ***Q to group - do we publish without Tooling Group input or do we wait?***
    d.
2. Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.
    a. Suggested format - https://docs.google.com/presentation/d/1iyReG5FtJT5YPm5ZyFM_obWqkUGFGuRqVg5gkJ7Z3_Q/edit#slide=id.ged18471c8b_0_0

20210817

Attendees:

- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Dave Russo (Red Hat)
- Matt Rutkowski (IBM)
- Glenn ten Cate(SKF)
- Marta Rybczynska (OSTC)

Meeting Notes:

- Very special Joint call with Tooling group NEXT TUESDAY @12pm EST - https://meet.google.com/nid-mxeg-xwt
- David A. Wheeler sends his regrets, he has a conflicting meeting on 2021-08-17! He's written notes below that report his status.

New friends:

-

Project Updates

CII Best Practices Badge (David A. Wheeler)

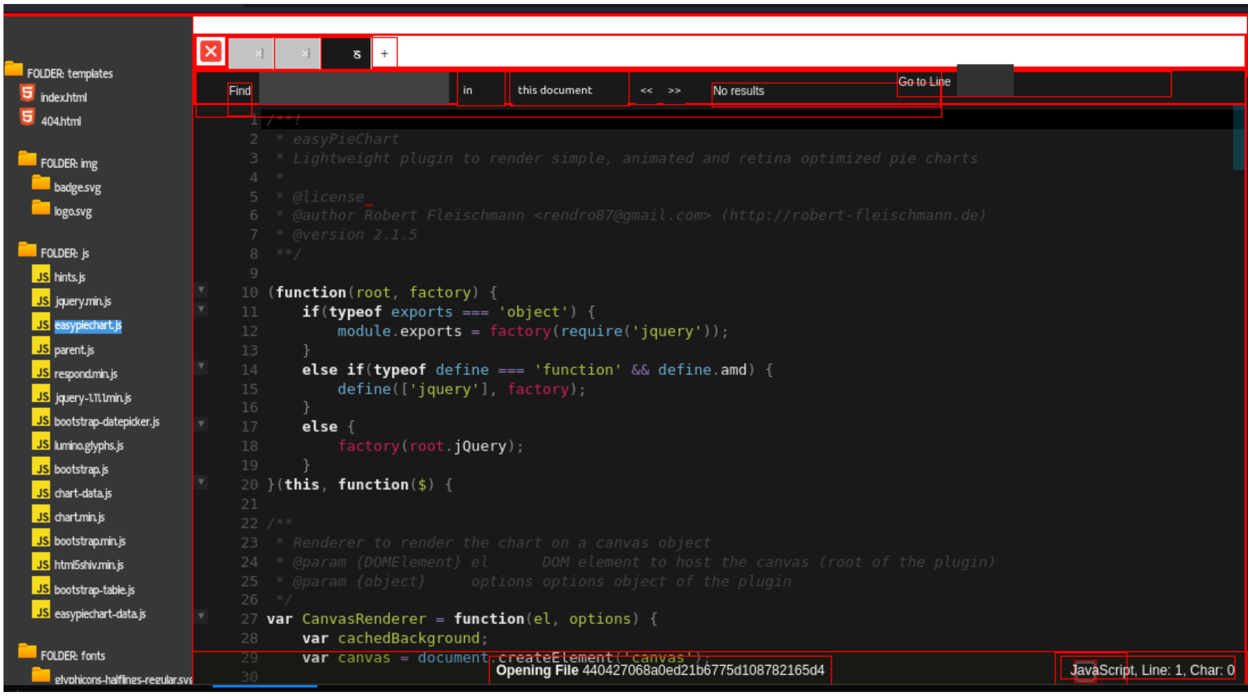
- As of 2021-08-15 we have 3,997 participating projects. We expect to break 4,000 by today or tomorrow.
- Minor updates continue. E.g., we've updated many transitive dependencies & have improved various natural language translations

edX Course

- "You're Doing IoT RNG" presentation showed that 35 BILLION IoT devices are vulnerable due to bad random number generators:
    - Dan Petro Dan and Allan Cecil's 2021 report "You're Doing IoT RNG" at DEF CON 29 showed that Internet of Things (IoT) devices have a VERY serious problem in that they often don't securely generate random numbers.
    - This leads to vulnerabilities, since many security mechanisms depend on random numbers. They estimate 35 BILLION IoT devices have this serious flaw. That's a lot of devices :-(.
    - Report: https://labs.bishopfox.com/tech-blog/youre-doing-iot-rng
    - Presentation: https://www.youtube.com/watch?v=Zuqw0-jZh9Y
- David A. Wheeler has created a proposed minor modification to the edX course to specifically point this issue out (we already noted the general problem), please comment TODAY:
    - The "Secure Software Development Fundamentals edX courses" already notes that you shouldn't ignore error codes AND it discusses the use of cryptographically secure pseudo-random number generators.
    - Wheeler proposes that we tweak it slightly to really hit this point home, and how to do it. "I've draft a change to do this as this pull request":
    - https://github.com/ossf/secure-sw-dev-fundamentals/pull/6
    - If you object or have further suggestions, please raise them by end of day. We can delay if you think we should, but tell us soon if we should!!

SKF

- Future todo's
    - https://github.com/blabla1337/skf-labs/issues
- The SKF Editor is moving forward:

○ 

No results

```
/**!
 * easyPieChart
 * Lightweight plugin to render simple, animated and retina optimized pie charts
 *
 * @license
 * @author Robert Fleischmann <rendro87@gmail.com> (http://robert-fleischmann.de)
 * @version 2.1.5
 **/

(function(root, factory) {
    if(typeof exports === 'object') {
        module.exports = factory(require('jquery'));
    }
    else if(typeof define === 'function' && define.amd) {
        define(['jquery'], factory);
    }
    else {
        factory(root.jQuery);
    }
}(this, function($) {

/**
 * Renderer to render the chart on a canvas object
 * @param {DOMElement} el       DOM element to host the canvas (root of the plugin)
 * @param {object}     options options object of the plugin
 */
var CanvasRenderer = function(el, options) {
    var cachedBackground;
    var canvas = document.createElement('canvas');
```

Opening File 440427068a0ed21b6775d108782165d4

JavaScript, Line: 1, Char: 0

Inventory

-

Scorecard

-
-

Proposed WG collaboration:

David A. Wheeler proposes that the group working on developing "Recommended GCC and clang option flags for compiling C/C++ programs"; early draft here: https://docs.google.com/document/d/1SsInJuqbFUyTFnhzkhC_Q3PPGZ1zrG89COrS6LV6pz4/edit . Comments from him:

> Maybe someday all software will be written in memory-safe languages, but we need an approach to reduce risks from the large amount of C/C++ written & used today. GCC and clang provide a large number of option flags for compiling C/C++ programs. Many of these flags warn about potential security issues, or harden the software so that vulnerabilities are less likely or have their impacts reduced. For example, the C and C++ specifications have many undefined behaviors (UB) whose accidental use can lead to security vulnerabilities; some flags counter UBs. We can develop many of these recommendations by reviewing existing practices. This could be used by projects & distributions to select options that reduce risks.

The intent would be to collaboratively develop an early draft using Google docs, then transition to markdown on GitHub.

Marta reports recent work on the same topic https://forum.ostc-eu.org/t/compiler-flags-to-be-used-for-all-scenarios-os/94

One-pager

David talked with Glann and connected about funding. Glann wonders if devoting some of that funding to the one-pager would be worthwhile.

WG collaboration:

“Existing Guidelines for Developing and Distributing Secure Software” - Google docs to start, once we get it going we can convert to GitHub.
https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit

- Will talk with the Tooling group on 8/24.
- Will review Tooling feedback as a group 8/31
- Target 9/14 for publication of guidance
- Next project will be “newbies view” for secure coding and practices - will leverage our SKF “one-pager” as a reference to structure the deck.

~~~~~~~~~~~~~~

20210803

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Dave Russo (Red Hat)
- Glenn ten Cate(SKF)
- Marta Rybczynska (OSTC)

Meeting Notes:

- [Project Leads] Review any project updates

New friends:

-

Project Updates

CII Best Practices Badge (David A. Wheeler)
~~~~~~~~~~~~~~

- I proposed a talk at the Linux Security Summit (I'm on the program committee), but we had a HUGE number of proposals & I think it's unlikely mine will be accepted. So if you didn't get yours in, don't feel bad, it was extremely competitive.
- My talk about the CII Best Practices badge *WAS* just accepted by the "Open Source Experience 2021" conference in Paris, France, Nov 9-10. This is a big OSS conference in Europe; they're expecting 200 speakers, 70 exhibitors, and 4500 attendees <https://www.opensource-experience.com/en/exhibit/why-exhibit/>.
- We now have over 600 passing projects, and are very close to having 4,000 participating projects. Stats here: https://bestpractices.coreinfrastructure.org/project_stats

edX Course (David A. Wheeler)

- No new news.
- Page https://openssf.org/edx-courses/ now includes direct link to GitHub page with content (for comments (file issues) and reuse by others)
- If you want changes to the edX course (for an update), please post as issues (or pull requests): https://github.com/ossf/secure-sw-dev-fundamentals

SKF (Glenn ten Cate)

- Editor making good progress, with the student from GSOC
- GSOC ending in August and we plan for a release of this new feature
- Examples available in Nodejs, Python, Ruby
- Request for help: Someone expert on Kubernetes?
  - Currently run as 2 Kubernetes clusters
  - David W: Not an expert, but not sure that wildcards really make sense. Why not just have separate pods for everything, provides more separation & simplifies deployment. I think you're trying to do things the hard way. IP address limitations: Consider using IPv6.

Inventory (CRE)

- No update recently

Scorecard

- No update
- Version 2 released recently

Updates to the TAC (from CRob)

- [CRob] - TAC updates
  - Funding (no news yet, missed call last week) - GB approved - talk to John Mertic & David A. Wheeler, once GB approves we (the LF) can get that moving
    - SKF project funding - Glenn
  - Proposed cross-WG doc (will talk about next week)
  - Newly created Government Policy committee to provide feedback on OSS-impacting government things (like the recent WH EO)
    - Will be talking about DevSec best practices, vuln disclosure best practices and others

- [CRob] will be meeting with Tools WG lead to try and coordinate joint call between our groups in Aug/Sept
- “Post-Approval LF Security Funding” - this is the typical process
  - https://docs.google.com/document/d/1iIDAWRY_xBatKsbrXUe4iR0a_VTxqYCYJ40ZCrhlOKg/edit

- Next steps: Need to identify other person to do the SKF work (Glenn)
- Need to get access to Azure credits - Glenn, ask Kay WIlliams (Microsoft)

WG collaboration:

Existing Guidelines for Developing and Distributing Secure Software” - Google docs to start, once we get it going we can convert to GitHub.
https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit
DW - thinking about next steps - do we pull the best ideas out into something once dock is ready
Xav - newbie-view of “where should I start?” - edX course, start with Badge criteria/assessment, use tools ike SKF & CRE to learn new skills or show compliance with Standards
Glenn - one-pager journey to see process overview, see bottlenecks
CRob - take newbie journey + one pager and craft educational presentation

20210720

Attendees:

- David A. Wheeler (Linux Foundation)
- CRob (Intel)
- Xavier Rene-Corail (GitHub)
- Dave Russo (Red Hat)
- Glenn ten Cate(SKF)
- Daniel Silverstone (Codethink)
- Marta Rybczynska (OSTC)

Meeting Notes:

New friends:

- Ax Sharma

Project Updates

CII Best Practices Badge

- Current stats are at https://bestpractices.coreinfrastructure.org/project_stats
    - 3,961 participating projects - anticipate breaking 4,000 soon.
    - 596 passing projects - anticipate breaking 600 soon.
- Continue to update libraries whenever vulnerabilities are found in them. Updated “attributes” gem even we though don’t believe it’s exploitable in this case, because it’s easier to update than determine if it’s vulnerable
- Pattern for not passing?
    - David W: I’ve done that analysis in the past. E.g., a common one is failing to tell people how to report vulnerabilities. I analyzed just projects at 90%+ so they’d already have looked at everything.

edX Course

- Page https://openssf.org/edx-courses/ now includes direct link to GitHub page with content (for comments (file issues) and reuse by others)

SKF

- Small Demo Editor / new labs env- based on ICE coder

Inventory

-

Scorecard

-

WG collaboration:

- Proposed title: “Existing Guidelines for Developing and Distributing Secure Software” - Google docs to start, once we get it going we can convert to GitHub.
    - https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit
    - Above document may not be visible to all.
    - Marta suggests to categorize the General Guidance section into domains
        - General (BSIMM, SAMM, etc)
        - Web dev
        - OS
        - Infrastructure (docker, ci/cd, source code repos)
        - Languages
    - Xav suggests pointing to Tooling group directly for those tools recommendations & we stay focused on development
    - Daniel suggests ONE repo under openssf that collects all different parts as “one book”
- Update on the one pager for our WG -> (S)SDLC HTML / JS

    - Will wait till the next meeting to see how to move forward with this.
- Linux Security Summit
    - Who submitted talks?
        - Glenn, David A. Wheeler, maybe CRob-Jennifer Fenrick
    - Future WG task - look at 2022 Conference Calendar and coordinate submissions to further awareness of WG & Projects @CRob assemble calendar for team to review

20210706

Attendees:

- CRob (Intel)
- Matt Rutkowski (IBM)
- Glenn ten Cate(SKF)
- Daniel Silverstone (Codethink)
- Michael Scovetta (Microsoft / SAFECode)
- Marta Rybczynska (OSTC)

Meeting Notes:

- Welcome new faces
- Take any opens
    -
- Code of Conduct the TAC wants WGs to adopt
- Review any project updates
- WG Collaboration

New friends:

-

Project Updates

CII Best Practices Badge

-

edX Course

-

SKF

- Testing with google cloud & kubes
- Mentoring google summer of code student
-

Inventory

- Glenn talking to CRE about HTML one-page; project very busy atm
-

Scorecard

- 50k projects (everything now collected) added to metrics.openssf.org.
- Google blog post: https://security.googleblog.com/2021/07/measuring-security-risks-in-open-source.html

SAFECode Chat

- Historically have been focused on large enterprises, writing best practices/whitepapers
- Recognized oss is different and thinking about how S.C. can help
- Playbooks on how a small os project can get 80% of the goodness for safe code/practices
- Want to see delta of advocated practices within Openssf & S.C.
- https://github.com/ossf/allstar

WG collaboration:

Proposed title: “Existing Guidelines for Developing and Distributing Secure Software” - Google docs to start, once we get it going we can convert to GitHub. https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit

- Note to DWheeler - can we get this doc opened for public commenting please

20210622

Attendees:

- CRob (Intel)
- Altaz Valani (Security Compass)
- Xavier Rene-Corail (GitHub)
- Matt Rutkowski (IBM)
- David A. Wheeler (Linux Foundation)
- Altaz Valani (Security Compass)
- Dave Russo (Red Hat)
- Glenn ten Cate(SKF)
- Azeem Shaikh (Google)
- Manuel Ifland (SAFECode/Siemens Energy)

Meeting Notes:

New friends:

- Manuel - SAFECode / Siemens Energy, in Germany

- Ben Stoltz

Project Updates

CII Best Practices Badge

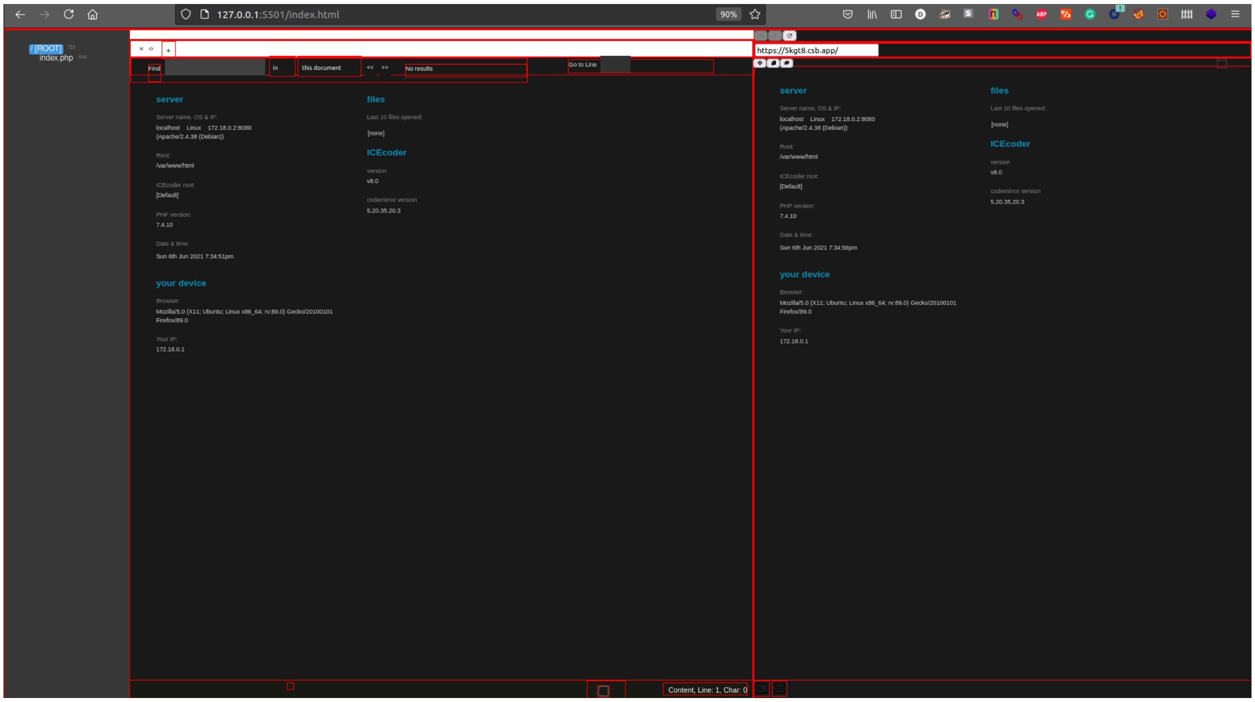
- 3888 projects participating, 583 passing - https://bestpractices.coreinfrastructure.org/en/project_stats
- Pointing to the OpenSSF (website & GitHub) and this WG

edX Course

- No new report

SKF

- https://demo.securityknowledgeframework.org
- Editor Lab updates:

- 

server

Server name, OS & IP:
localhost Linux 172.18.0.2:8080
(Apache/2.4.38 (Debian))

Root:
/var/www/html

ICEcoder root:
[Default]

PHP version:
7.4.10

Date & time:
Sun 6th Jun 2021 7:34:51pm

your device

Browser:
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101
Firefox/89.0

Your IP:
172.18.0.1

files

Last 10 files opened:
[none]

ICEcoder

version
v8.0

codemirror version
5.20.35.20.3

server

Server name, OS & IP:
localhost Linux 172.18.0.2:8080
(Apache/2.4.38 (Debian))

Root:
/var/www/html

ICEcoder root:
[Default]

PHP version:
7.4.10

Date & time:
Sun 6th Jun 2021 7:34:56pm

your device

Browser:
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101
Firefox/89.0

Your IP:
172.18.0.1

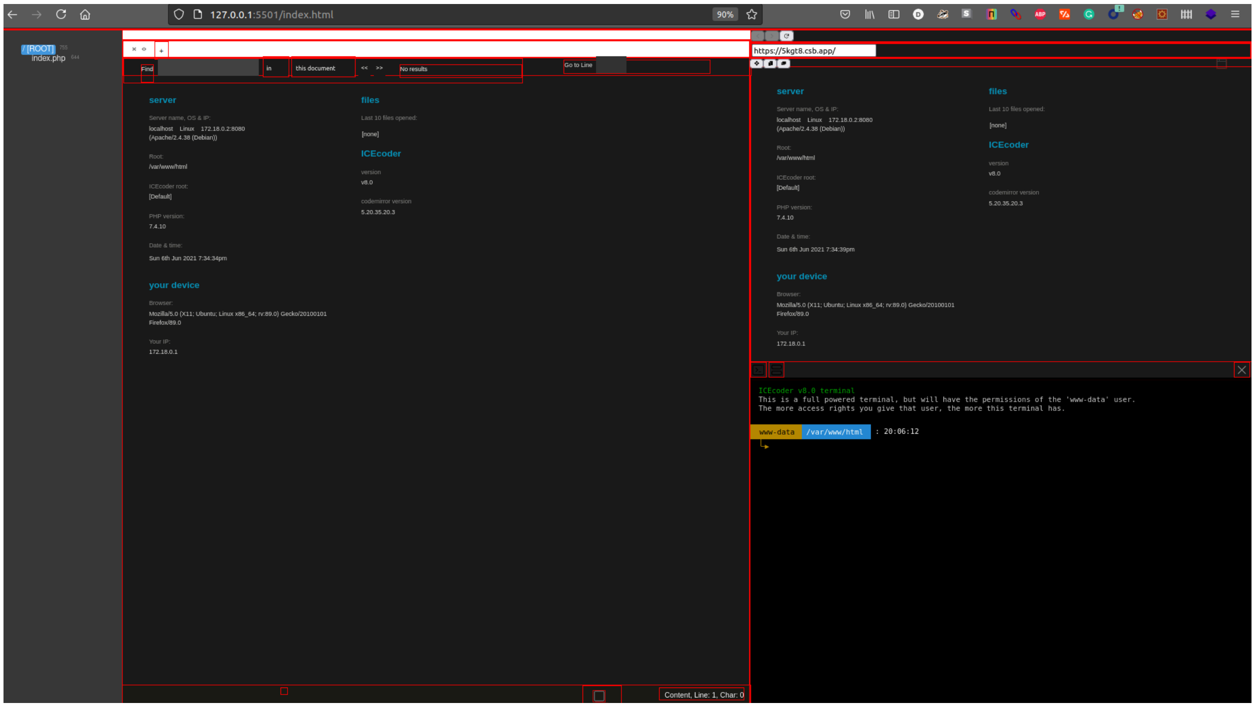
files

Last 10 files opened:
[none]

ICEcoder

version
v8.0

codemirror version
5.20.35.20.3



server

Server name, OS & IP:
localhost Linux 172.18.0.2:8080
(Apache/2.4.38 (Debian))

Root:
/var/www/html

ICEcoder root:
[Default]

PHP version:
7.4.10

Date & time:
Sun 6th Jun 2021 7:34:34pm

Date & time:
Sun 6th Jun 2021 7:34:39pm

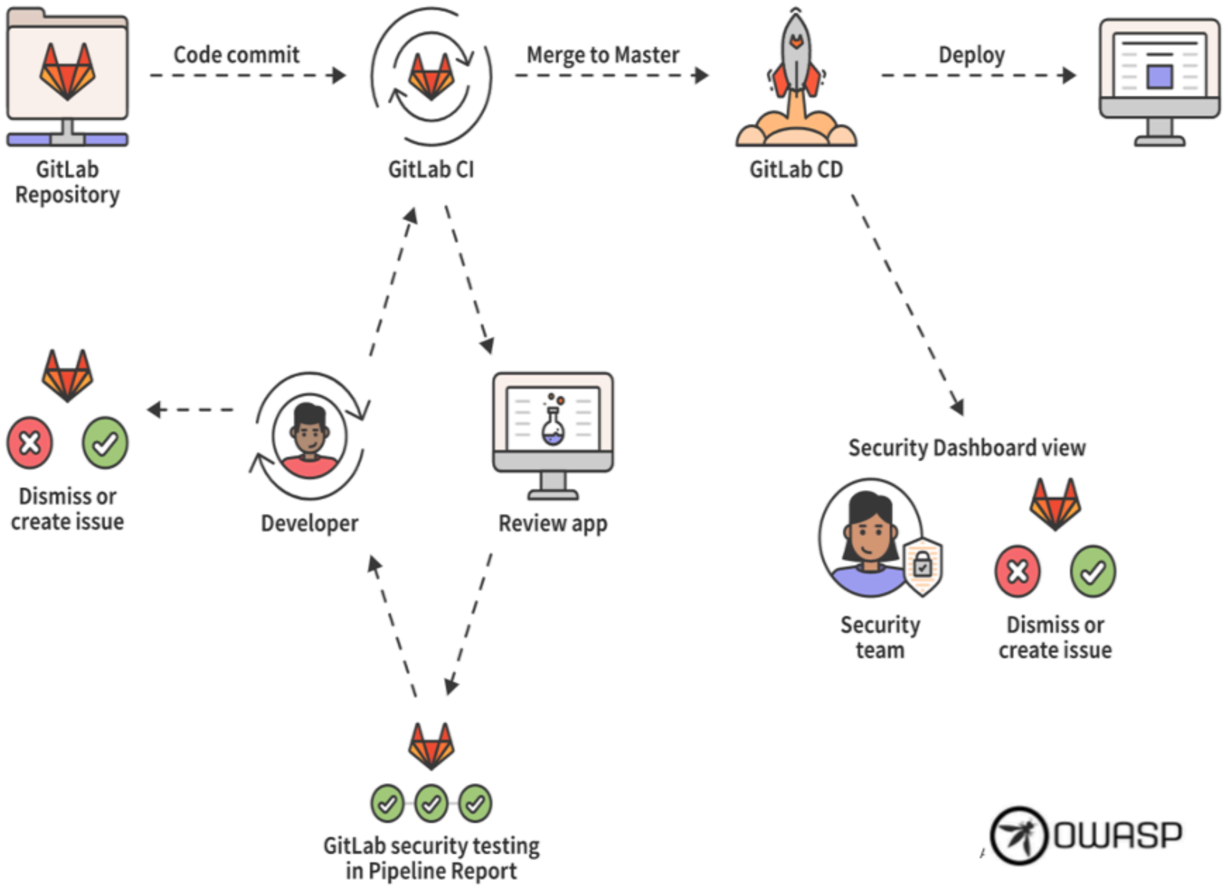
```
ICEcoder v8.0 terminal
This is a full powered terminal, but will have the permissions of the 'www-data' user.
The more access rights you give that user, the more this terminal has.

 www-data  /var/www/html  : 20:06:12
 ↳
```

- Github sec vulns db - want to take snippets from it and provide as examples
- Looking at codeql engine also
- TAC Update (voting in progress - https://github.com/ossf/tac/issues/60)

Inventory

- Met with SKF team and are designing HTML page for the OSSF Welcome page:



-
- We used the Gitlab image as an idea of the different steps and phases
- And some data for populating the different phases:
- Training

TedEx course
OWASP SKF Labs
OWASP JuiceShop
OWASP SAMM

Code repo

Sonarcube
TruffleHog
Badge Project
OWASP Dependency check

CI

CodeQL
OWASP ZAP
FindAllBugs
Anchore
Trivy
...

CD

- OWASP AMASS
- Anchore
- Kube-bench
- Kube-hunter
- key vault hashicorp

- Note: CII Best Practices badge
    - https://bestpractices.coreinfrastructure.org/en/criteria/0
    - https://bestpractices.coreinfrastructure.org/en/criteria
- SAFECode material: https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf
- “Can we do step 1, step 2,....” cookbook & also “why do this?”

Scorecard

- Scaled up to 30,000 repos (should be 50k by end of week)
- Working on integrating with OpenSFF metrics projects

WG collaboration:

- Group interest in submitting papers to linux security summit - https://events.linuxfoundation.org/linux-security-summit-north-america/program/cfp/?utm_content=167184933&utm_medium=social&utm_source=linkedin&hss_channel=lcp-208777
    - Glenn and Altaz expressed interest in collabing
    - David notes it should be a fairly technical audience
- [DaveR] Any further thoughts on composing a list of recommended secure development practices?
    - SAFECode has materials around good practices (Altaz is glad to assist)
        - https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf
    - CII Badge Info - https://bestpractices.coreinfrastructure.org/en/criteria
        - https://bestpractices.coreinfrastructure.org/en/criteria?details=true&rationale=true
    - Aim toward what they value of these practices are (as a long-term goal)
    - Perhaps approach this like an annotated bibliography
        - Example: http://www.devopsbookmarks.com/

Proposed title: “Existing Guidelines for Developing and Distributing Secure Software” - Google docs to start, once we get it going we can convert to GitHub. https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit

Meeting Notes:

- Welcome new faces
- Take any opens
- Review any project updates
- WG Collaboration

Project Updates

EdX Course

- 3888 projects participating - 583 passing

SKF

- TAC Update (voting in progress - https://github.com/ossf/tac/issues/60)
-

CII Best Practices Badge

-

Inventory

-

Scorecard

-

WG collaboration:

- Group interest in submitting papers to linux security summit - https://events.linuxfoundation.org/linux-security-summit-north-america/program/cfp/?utm_content=167184933&utm_medium=social&utm_source=linkedin&hss_channel=lcp-208777