Agenda

1. First up: grants (MWDS, D8 Accelerate sponsorship of hours)
2. Goals
3. Issue status/solution review (see below)

Goals

The critical is "remove or document every safemarkup::set() call".
Until that statement is done, the critical is not resolved.

The "how" of it should focus on not bloating the safe string list and using the updated filtering API. alexpott has an outstanding todo to document this.

- update the meta with the current best practices assumptions for deciding how to resolve each (which proposed resolution to use).
    - TLDR:
        - Evaluate where the string is coming from and whether the SafeMarkup::set() is even needed in the first place. Check for what markup or user input might be in it. Look at the calling code.
        - Consider #markup whenever there is a render array or in the theme layer
        - Let Twig escape stuff that should be escaped
        - Consider whether the intent is to escape or filter
- update the meta with a how to review section.
- tag issues that are child of the meta (because we don't have an advanced search like result for "child of meta") : "safemakup critical blocker" ?

Next steps / order of and solutions for issues

https://www.drupal.org/project/issues/search/drupal?project_issue_followers=&status[0]=1&status[1]=13&status[2]=8&status[3]=14&status[4]=4&priorities[0]=300&version[0]=8.0.x-dev&issue_tags_op=%3D&issue_tags=SafeMarkup&text=&assigned=&submitted=&&&order=created&sort=asc

1. Get dsm() working in https://www.drupal.org/node/2505497 Support render arrays for drupal_set_message(). **Probably "easy", just needs to be done** -- maybe eff commit.
    a. Get hook_requirements() working in install phase and fix usage in drupal_check_module() in https://www.drupal.org/node/2505499 Explicitly support render arrays in hook_requirements() **Probably "easy", just needs to be done**
        i. test drush with patch once it's updated / dsm is fixed and file drush PR if needed
        ii. xjm to post updated patch once the main issue is fixed
    b. Then we can fix all these simply: (@todo xjm all three issues, roll patches for)
        i. https://www.drupal.org/node/2501683 Remove or document SafeMarkup::set in _update_message_text() **Probably "easy", just needs to be done**
        ii. https://www.drupal.org/node/2296929 Remove system_requirements() SafeMarkup::set() use **Probably "easy", just needs to be done**
        iii. https://www.drupal.org/node/2501827 followup to remove the early render **Probably "easy", just needs to be done**
2. Comma-separated item lists (inline template or item list or a method) @todo lauriii create an issue to make a comma separator item list template.
    a. (*) https://www.drupal.org/node/2501937 Remove SafeMarkup::set in ViewsUIController::reportFields() -- **Probably "easy", just needs to be done** pending decision on templating
        i. inline template plus semantic join

    ii. item list, make a template that is comma separated. (themer could change the format of the list? - Lauriii to create, joelpittet to investigate.
  b. https://www.drupal.org/node/2505931 Remove SafeMarkup::set in ViewListBuilder -- **Probably "easy", just needs to be done** pending decision on templating but *be careful about test coverage and differing code paths*
  c. (*) https://www.drupal.org/node/2501971 Remove or document SafeMarkup::set in FieldStorageConfigListBuilder -- **Probably "easy", just needs to be done** pending decision on templating
  d.
3. SafeString / internal usage conversions
  a. https://www.drupal.org/node/2296101 Remove SafeMarkup::set() use in \Drupal\Core\Render\Element\HtmlTag::preRenderHtmlTag() -- rumblings about html tag in general but probably just needs tests/final review/etc. alexpott and I thought the proposed resolution looked okay so **Probably "easy", just needs to be done**
    i. @todo pwolanin document where test coverage is
  b. https://www.drupal.org/node/2501931 Remove SafeMarkup::set in twig_render_template() and ThemeManager and FieldPluginBase:advancedRender -- **Needs thorough review -- dawehner, joelpittet, effulgentsia?**
    i. could be ready (rtbc)
    ii. could do some profiling…
    iii. alexpott to post updated patch **DONE**
    iv. pwolanin seems to understand, maybe to do review.
  c.
4. Template conversions (grants?)
  a. https://www.drupal.org/node/2363423 views-view-fields.html.twig gets escaped -- looking good; needs more work -- **Grant** to Twig folks? (Blocked on performance -JP)
    i. need to find the related issue with performance testing. https://www.drupal.org/node/2348747 #70 & #69. if it is a 10% penalty on a miss.. vs dx and security benefit. now views caching more effective so might not need to keep this optimized. views render caching making it 2-tiered went in 2 months ago… might make it worth redoing the performance test. @todo profile joel or david (#d8accelerate) then @todo catch to make the call
    ii. D8 Accelerate grant: maybe joël; reach out to Cottser, Fabianx, dawehner
  b. https://www.drupal.org/node/2502089 #2502089: Remove SafeMarkup::set() in template_preprocess_views_view_table() -- part of **Grant** for (a) ? JP
  c. (*) https://www.drupal.org/node/2506485 Header label + customized label wrapper of a Views table display is double escaped -- not a part of the critical; should probably be postponed or merged back in
  d. (currently unpublished) https://www.drupal.org/node/2501737 Remove or document SafeMarkup::set in theme_system_modules_details() -- **Needs technical direction and sec review**
    i. come back to this once issue is (probably) republished
    ii. alexpott to talk to secteam
5. Tag assembly, inline template, tag wrapping, etc.
  a. https://www.drupal.org/node/2501697 Remove SafeMarkup::set in rdf_preprocess_comment() -- **Probably "easy", just needs to be done** or **Grant**
  b. https://www.drupal.org/node/2501711 Remove or document SafeMarkup::set in template_preprocess_ckeditor_settings_toolbar -- **Needs technical direction**; alexpott commented because "that's hard". Also what about https://www.drupal.org/node/2306515 ?
    i. look into and implement alexpott suggestions
      1. @pwolanin or @alexpott **DONE**
    ii. ping the issue to wim once the patch is updated **DONE**
  c.
6. Error handling

a. https://www.drupal.org/node/2501319 Remove SafeMarkup::set in Error::renderExceptionSafe and _drupal_log_error And improve backtrace formatting consistancy in _drupal_log_error, Error::renderExceptionSafe, and DefaultExceptionSubscriber::onHtml
    i. figure out why the patch is not failing on the first line
    ii. markup should be escaped in error messages, should not be expecting a browser to be recipient of error message
    iii. missing test coverage. it pases and it should not. patch depends on the assumption things get added to the safe string list, but changes earlier this year change it so strings are not added.
    iv. file an issue for 9.0.x to remove markup in/around error messages.
    v. note change in https://www.drupal.org/node/2506195 effects things.
b. (*) https://www.drupal.org/node/2501835 Remove SafeMarkup::set in Drupal\Core\Database\Install\Tasks::runTasks() and ensure multiple messages are printed
    i. trying different ways to test manually to get multiple failures
    ii. alexpott to review / post a comment **DONE**
    iii. needs installer tests updated
    iv. @todo david seems to understand this
    v. @todo stefan.r is on it **DONE**
        ~~1. if not, bother @alexpott (non-working installer test stuffs)~~
            ~~a. will post a link to another test to see how to test a broken installer.~~
c. api safemarkup format, @ % !, using ! guarantees it *will* b escaped cause it has not been marked safe. print raw stuff in other ways. whaa. deprecate !, and use @ cause it is smart, if it is safe, skip over it, or do a checkplain. https://www.drupal.org/node/2506445

7. Other
a. https://www.drupal.org/node/2544156 / https://www.drupal.org/node/2501455 Deprecate drupal_render_children() and remove all usages in Drupal core -- just needs to be done. However, this *is* one we could just document if push comes to shove if we also add the deprecation. #3/internal - JP?
    i. SafeString::create() -- **This should be done in https://www.drupal.org/node/2501455**
    ii. Deprecated/internal only -- we actually don't have strategy to replace all the current usages, so we can't do this yet
    iii. Remove postponed to D9 issue -- **joël to find it / child of https://www.drupal.org/node/2544156 ? split that one into two?**
b. https://www.drupal.org/node/2399261 Remove SafeMarkup::set and Recheck and Mark Safe the Output of Unicode::truncate() in DbLog -- **Probably "easy", just needs to be done** (Needs tests)
c. (*) https://www.drupal.org/node/2501757 Remove SafeMarkup::set in NodeSearch::prepareResults() -- **Probably "easy", just needs to be done**
d. https://www.drupal.org/node/2502025 Remove SafeMarkup::set() in core/modules/dblog/src/Tests/Views/ViewsIntegrationTest.php -- **RTBC, NR from xjm**.
e. (*) https://www.drupal.org/node/2502781 Remove SafeMarkup::set in template_preprocess_file_widget_multiple()
f. need to work out where it was previously printed? further up in the same function. "easy" to fix? move the hide after we do the copy
    i. alexpott to repost comment DONE (thanks @cilefen)
g. Needs review: Attribute class to check safe strings before escaping -JP https://www.drupal.org/node/2531824
    i. alexpott and maybe pwolanin to look at it
    ii.

Pre-meeting notes

Things to discuss

- How to join two strings? eg. https://www.drupal.org/node/2501757 and https://www.drupal.org/node/2501683
- What to do about https://gist.github.com/Berdir/ad89316e3c0d4722d11b XssAdminFilter removes the data- attribute
- See list of open issues down further

Examples of nice fixes

1. document set() #2501823: Document SafeMarkup::set in FormCache::loadCachedFormState
2. document set() #2501447: Document SafeMarkup::setMultiple in _batch_page()
3. document set() #2501451: Document SafeMarkup::set in drupal_get_messages()
4. document set() #2501441: Document SafeMarkup::set in AllowedTagsXssTrait::fieldFilterXss
5. document set() #2501403: Document SafeMarkup::set in Xss::filter
6. document set() #2539300: Remove SafeMarkup::set in \Drupal\Tests\Core\Form\FormCacheTest::testSetCacheWithSafeStrings()
7. remove code #2501933: Remove dead code in ViewUI::getDefaultAJAXMessage()
8. refactor using t() #2501639: Remove SafeMarkup::set in drupal_check_module()
9. refactor string concatenation using format() #2280963: Refactor use of SafeMarkup in HWLDFWordAccumulator
10. refactor using format() #2502009: Remove SafeMarkup::set in SearchExtraTypeSearch::execute()
11. refactor using format(), adds test for escaping #2501705: Remove SafeMarkup::set() in LinkGenerator and document SafeMarkup::set() in LinkGeneratorTest
12. refactor string concatenation using #markup, has manual testing steps for XSS and double escaping #2501827: Remove SafeMarkup::set() in file_save_upload() and allow render/template code to control a single-item list
13. refactor using #markup #2501819: Remove SafeMarkup::set in search_embedded_form_preprocess_search_result()
14. refactor using #markup #2501947: Remove SafeMarkup::set in ViewUI::renderPreview()
15. refactor using #markup, adds a santitizing test #2501701: Remove SafeMarkup::set in ViewUI::renderPreview()
16. refactor using htmlspecialcharacters() and document set() #2505701: Document SafeMarkup::set and Use htmlspecialchars() directly in Attribute() so we don't bloat the list of safe strings
17. refactor using instanceOf SafeStringInterface, adds tests for escaping #2506133: Replace SafeMarkup::set() in \Drupal\Core\Template\Attribute
18. casts to (string or instanceOf SafeStringInterface #2506581: Remove SafeMarkup::set() from Renderer::doRender
19. refactor using Xss::filter() #2501747: Remove SafeMarkup::set in search_excerpt
20. refactor using checkAdminXss() #2501749: Remove SafeMarkup::set in SimpletestResultsForm.php

21. document and refactor using replace() and checkAdminXss(), and add tests to ensure script tag stripped out #2273925: Ensure #markup is XSS escaped in Renderer::doRender()
22. refactor Xss::filterAdmin() using #markup and xssFilter(), adds escaping tests #2506195: Remove SafeMarkup::set() from Xss::filter()
23. refactor by not using template preprocess and use a twig template #2502095: Remove SafeMarkup::set in template_preprocess_views_ui_view_info()template_preprocess_color_scheme_form()
24. refactor to use twig templates #2501481: form_select_options() is a theme function in disguise and should not use SafeMarkup::set *NICE EXAMPLE*

Open issues: (nb: this was incorporated into the list above)

1. Needs a decision on direction: #2501711: Remove or document SafeMarkup::set in template_preprocess_ckeditor_settings_toolbar lots of overlap with #2306515: SafeMarkup in CKEditor toolbar configuration UI — fix by not generating markup in PHP but using Twig Macros
    - worked on by: cwells and joelpittet
    - looked at by: aneek, xjm, chx
2. Needs a decision on direction: #2501697: Remove SafeMarkup::set in rdf_preprocess_comment()
    - worked on/working on: Les Lim (and earlier by: hestenet, pfrenssen, leslieg)
    - has a #markup solution
        - (if go this way, need more whitelisting of attributes and touches `Xss::filter()` internals)
    - has a inline template solution
        - which needs work, and may not let through the rdf attributes
    - needs tests
3. needs guidance: #2501835: Remove SafeMarkup::set in Drupal\Core\Database\Install\Tasks::runTasks() and ensure multiple messages are printed
    - worked on by: kgoel (but not lately), davidhernandez, xjm, YesCT, crowdcg, joelpittet, Cottser
    - installer can be tricky
    - test not sure how to write
4. needs work: #2501737: Remove or document SafeMarkup::set in theme_system_modules_details()
    - worked on by: lauriii, cilefen, joelpittet, sclapp
    - needs tests
    - needs test coverage evaluation and documented in the issue summary
    - needs a call as to if escaping the module info description is ok See #25
5. needs work: #2544262: Refactor use of SafeMarkup::set in \Drupal\Core\Render\Element\HtmlTag::preRenderConditionalComments()
    - worked on by: akalata, YesCT
    - needs test - tricky test, render prefix and suffix sent in via element array for the prefix and suffix which do have tests.
6. needs work: #2501319: Remove SafeMarkup::set in Error::renderExceptionSafe and _drupal_log_error And improve backtrace formatting consistancy in _drupal_log_error, Error::renderExceptionSafe, and DefaultExceptionSubscriber::onHtml
    - worked on by: YesCT, cmanalansan, cwells, joelpittet, Cottser
    - could be too much in one, or out of scope changes, but otoh might be fine
    - there is a whole call to set() that has not been attempted to be removed
7. needs work: #2296929: Clean up system_install() SafeMarkup::set() use
    - worked on by xjm, pwolanin, YesCT, codemonkie, David_Rothstein, alexpott, herved, lauriii, aneek
    - stalled
    - **update:** xjm working on it again now
8. needs work: #2501931: Remove SafeMarkup::set in twig_render_template() and ThemeManager and FieldPluginBase:advancedRender
    - being actively worked on by alexpott
    - could be a testbot issue, passed on new, failed on old

    - **update**: need to consider carefully the use of SafeStringInterface in Views
9. rtbc: #2399261: Remove SafeMarkup::set and Recheck and Mark Safe the Output of Unicode::truncate() in DbLog
    - rtbc by: genjohnson and mdrummond (with assistance from YesCT)
    - this issue summary didn't have the template to note if there was test coverage and document it.
    - effulgentsia did make a call in #72 on what direct to take.
10. rtbc: #2502781: Remove SafeMarkup::set in template_preprocess_file_widget_multiple()
    - rtbc by: YesCT
    - maybe not the most confident in this rtbc
11. rtbc: #2501757: Remove SafeMarkup::set in NodeSearch::prepareResults()
    - rtbc by: YesCT
    - fairly confident rtbc aside from a small concern about test assertion
12. NR (from RTBC): #2501683: Remove or document SafeMarkup::set in _update_message_text
    - rtbc by: lauriii
    - **updated by xjm** to convert to a render array and remove unneeded code complexity
    - https://www.drupal.org/node/2505499#comment-10181922 (comment #4) is germane
13. NW (from RTBC): #2505931: Remove SafeMarkup::set in ViewListBuilder
    - rtbc by: joelpittet
    - **nw by alexpott & xjm** -- the current patch now mixes in filtering along with escaping, and there is an untested code path (using %) that is not handled properly in the current patch.
    - recommended solution: switch it to an item list and add a Twig template that joins item lists with a comma.
14. rtbc: #2488304: Add more docs that translate() also marks strings as safe
    - rtbc by: jhodgdon
15. rtbc #2502025: Remove SafeMarkup::set() in core/modules/dblog/src/Tests/Views/ViewsIntegrationTest.php
    - rtbc by: YesCT
    - worked on by: dsnopek, geertvd, cilefen, xjm, davidhernandez, joelpittet
    - looked at by: alexpott, effulgentsia (and not sure if they agree)
16. needs testing #2296101: Remove SafeMarkup::set() use in \Drupal\Core\Render\Element\HtmlTag::preRenderHtmlTag()
    - needs test coverage evaluation and documented in the issue summary
17.