

TALE OF FORGOTTEN DISCLOSURE

BY

ANANT SHRIVASTAVA

ANANT SHRIVASTAVA

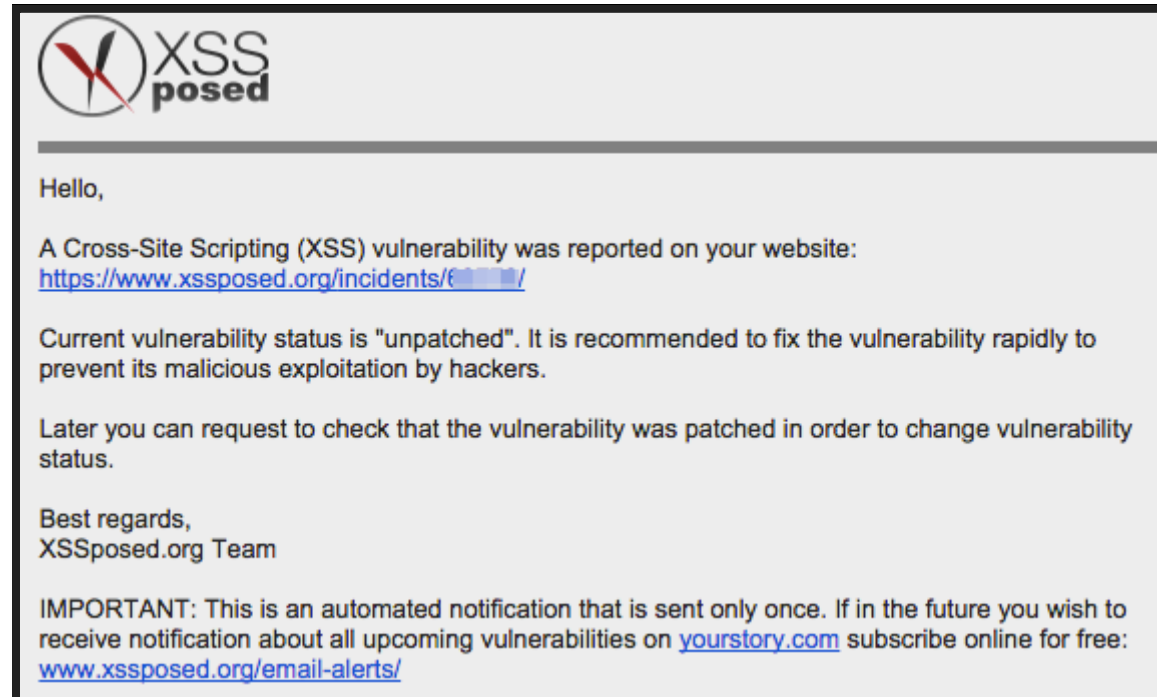
- Information Security Consultant
- Admin - Dev - Security
- null + OWASP + G4H
- <http://anantshri.info> and @anantshri
- Co-Author OWASP Testing Guide 4.0
- Projects



SCENARIO

1. A vulnerability present in code (last updated March 2013)
2. Public disclosure in aug 2014.
3. Interestingly someone posted a pull request in Jan 2013
4. Till may 2015 it was not patched even though there was a new release after the pull request was in place.

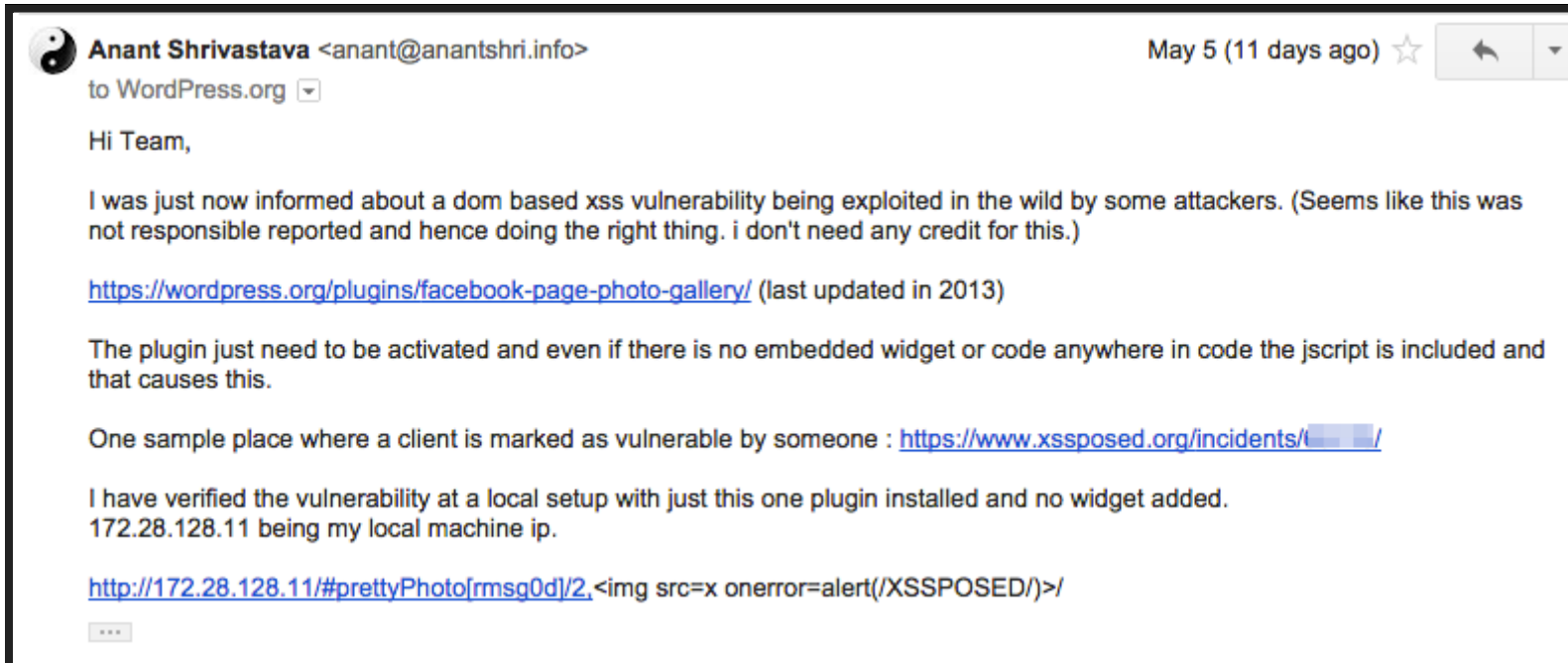
INFORMATION RECIEVED



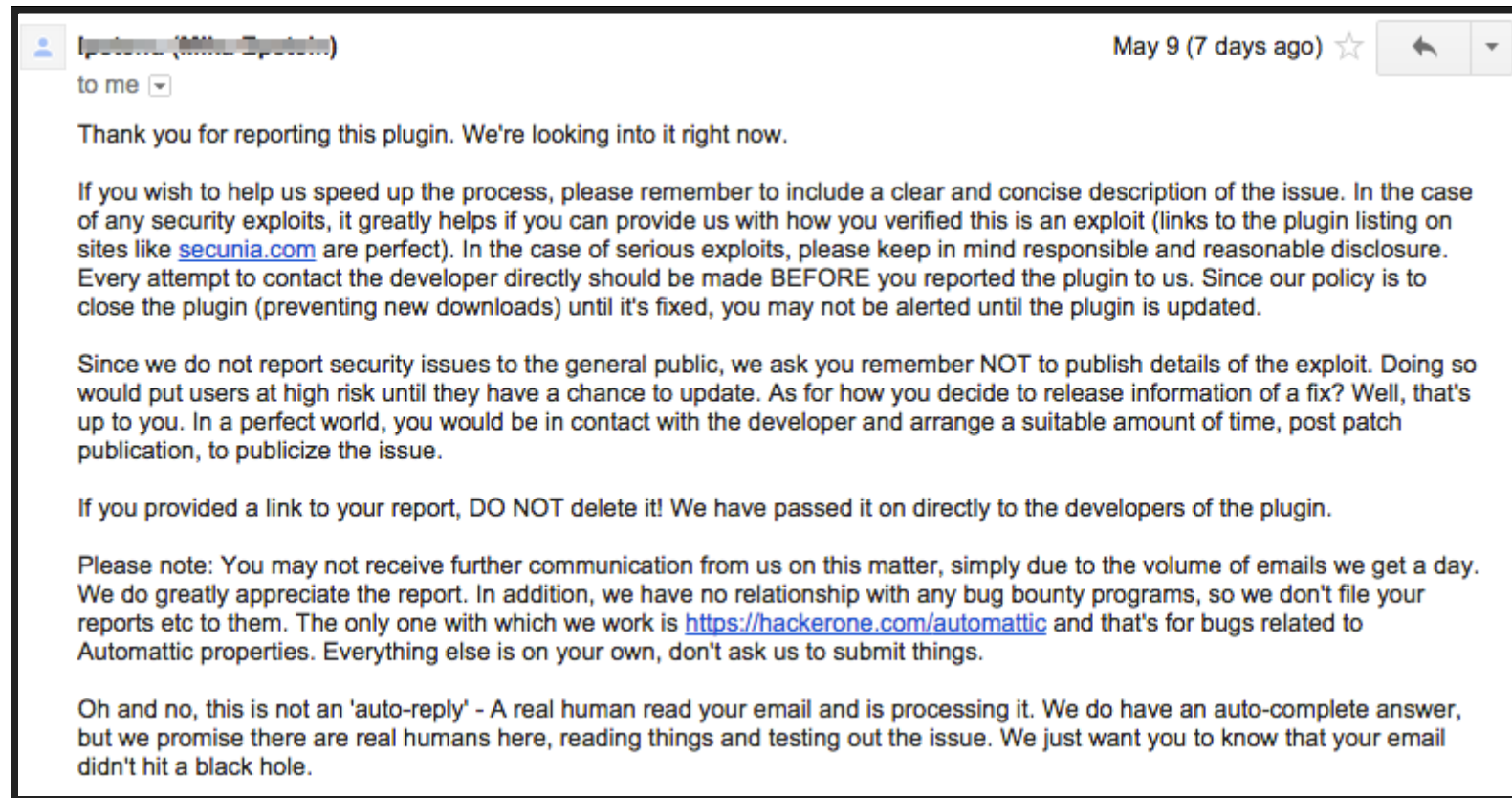
INVESTIGATION RESULT

1. Javascript Based DOM-XSS
2. Culprit identified as facebook-page-photo-gallery wordpress plugin.
3. Remove the plugin
4. XSS Fixed; Issue closed
5. End of Story

EMAIL TO PLUGINS TEAM




RESPONSE FROM PLUGIN TEAM





MEANWHILE


DISCOVERY REQUIRES EXPERIMENTATION

REPOSITORY


 **scaron / prettyphoto**


 Watch ▾ 37

 Star 357


 Fork


branch: master ▾

 Commits on May 7, 2015





Fix post test
scaron authored 9 days ago

4cc502e 





Update v number
scaron authored 9 days ago


3a105aa 




[#149] Filter out chars to prevent XSS
scaron authored 9 days ago


36463d4 

 Commits on Mar 19, 2013




Revert the chnages
scaron authored on 19 Mar 2013

d0a7a04 



Remoed the Y from gallery
scaron authored on 19 Mar 2013

c74a48a 

CRUX OF THE ISSUE

```
function getHashtag(){  
  
    var url = location.href;  
  
    hashtag = (url.indexOf('#prettyPhoto') !== -1) ? decodeURI(url.substring(url.indexOf('#prettyPhoto')+1,url.length)) : false;  
  
    return hashtag;  
  
};
```

GOOGLE AHOY

 www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html

PRINCIPAL SEGURIDAD INFORMATICA NETWORKING SERVIDORES DESCARGAS

Haciendo un XSS en Plugin Prettyphoto

17:03 | [hacking](#), [laboratorio](#), [plugins](#), [xss](#) |


Para explicar este ejemplo de un XSS (Cross Site Scripting) vamos a tener que buscar una web que tenga el plugin prettyphoto, usada en Joomla y Wordpress es muy usado para crear Slides de imagenes, efectos, galerias.



Lo primero seria buscar una web vulnerable, lo mejor es hacerlo mediante un dork, de la siguiente manera:


`inurl:/wp-content/plugins/prettyPhoto`


INTERESTING FACT


 **scaron / prettyphoto**


Watch ▾ 37


fixed xss vulnerability #116

 **Open** Duncaen wants to merge 2 commits into `scaron:master` from `Duncaen:patch-1`

 Conversation 2

 Commits 2

 Files changed 1



Duncaen commented on 15 Jan 2013

Escape hashRel and parse hashIndex as integer.
Example: `http://www.no-margin-for-errors.com/projects/prettyPhoto-jquery-lightbox-clone/#prettyPhoto[pp_gal]/2,/`

CONTACTING AUTHOR

any eta on xss fix #149

 Open

anantshri opened this issue 11 days ago · 5 comments



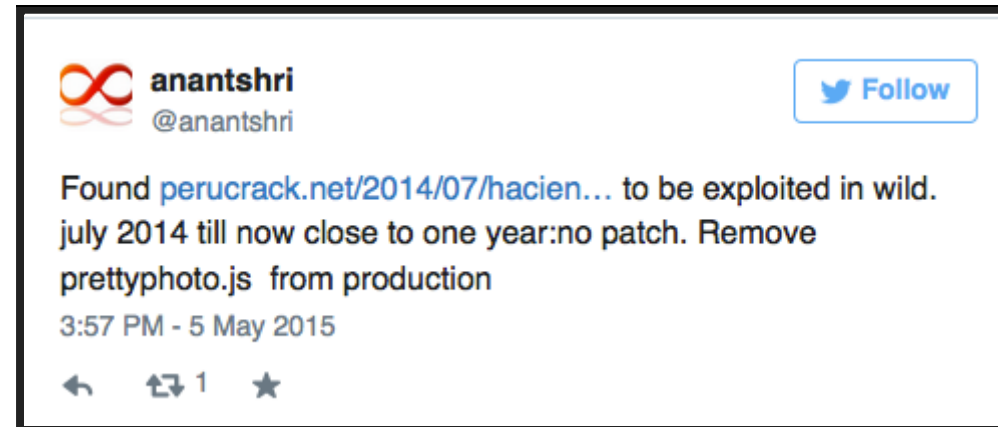
anantshri commented 11 days ago

Someone reported a Dom XSS vector in 07-2014
<http://www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html>

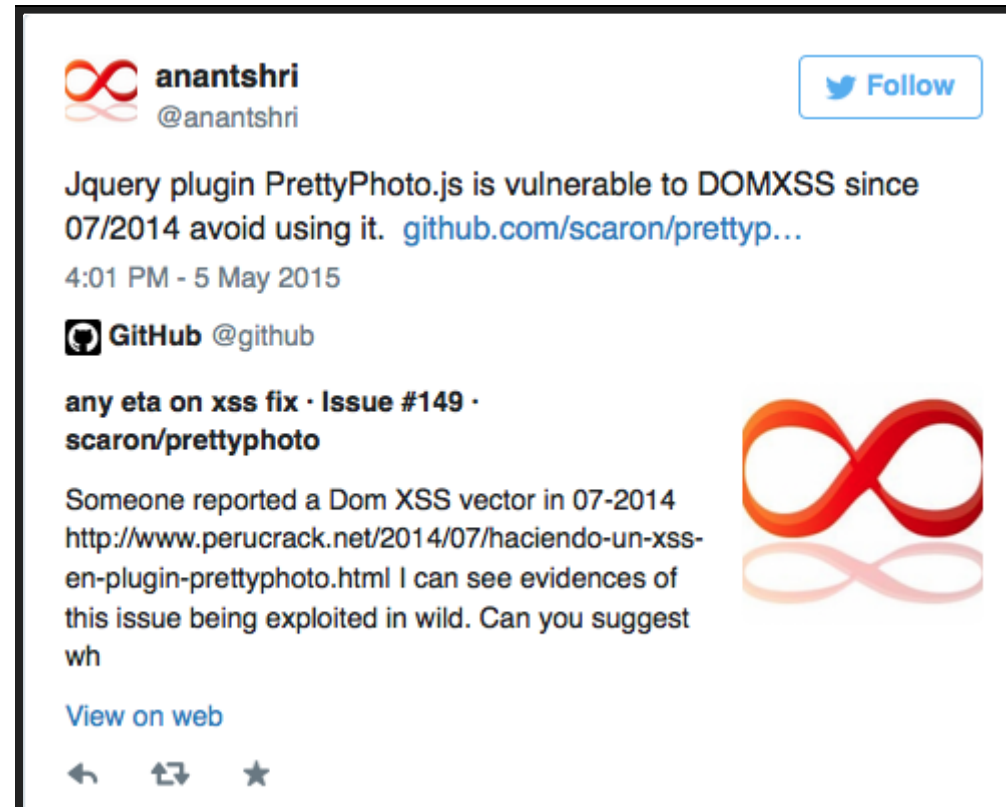
I can see evidences of this issue being exploited in wild. Can you suggest when a fix would be ready.

Created a public issue coz the disclosure was long back but still a lot of people are using this library and all of them are susceptible to this attack.

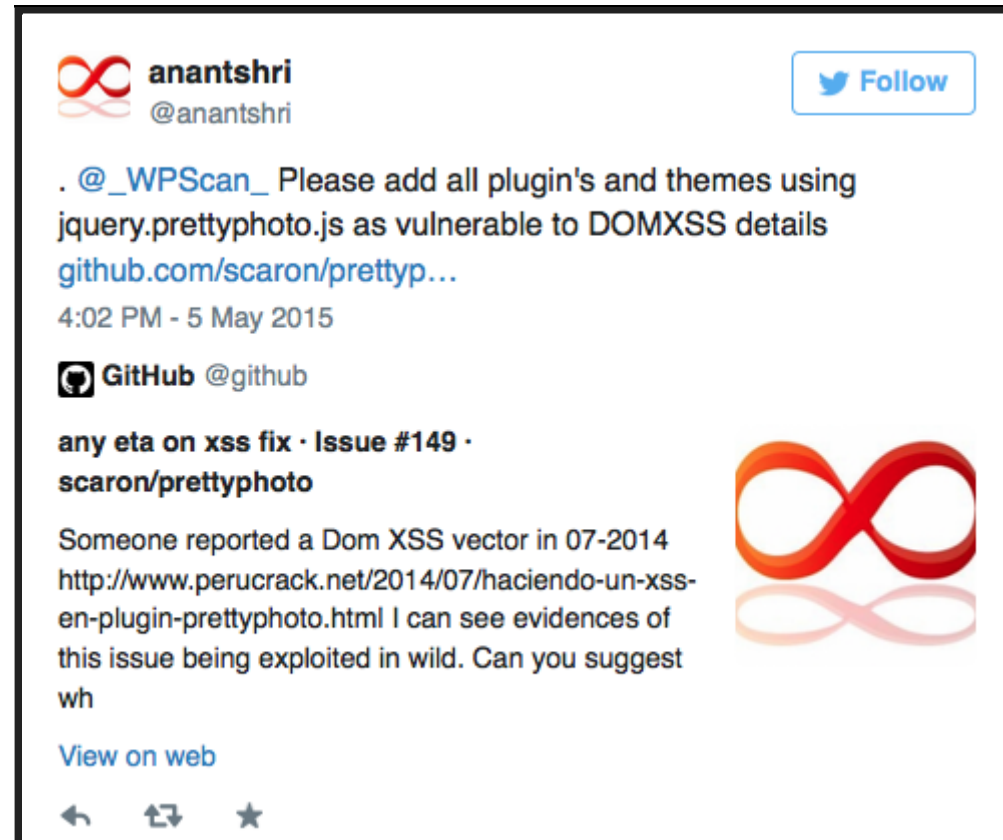
SPREAD THE WORD



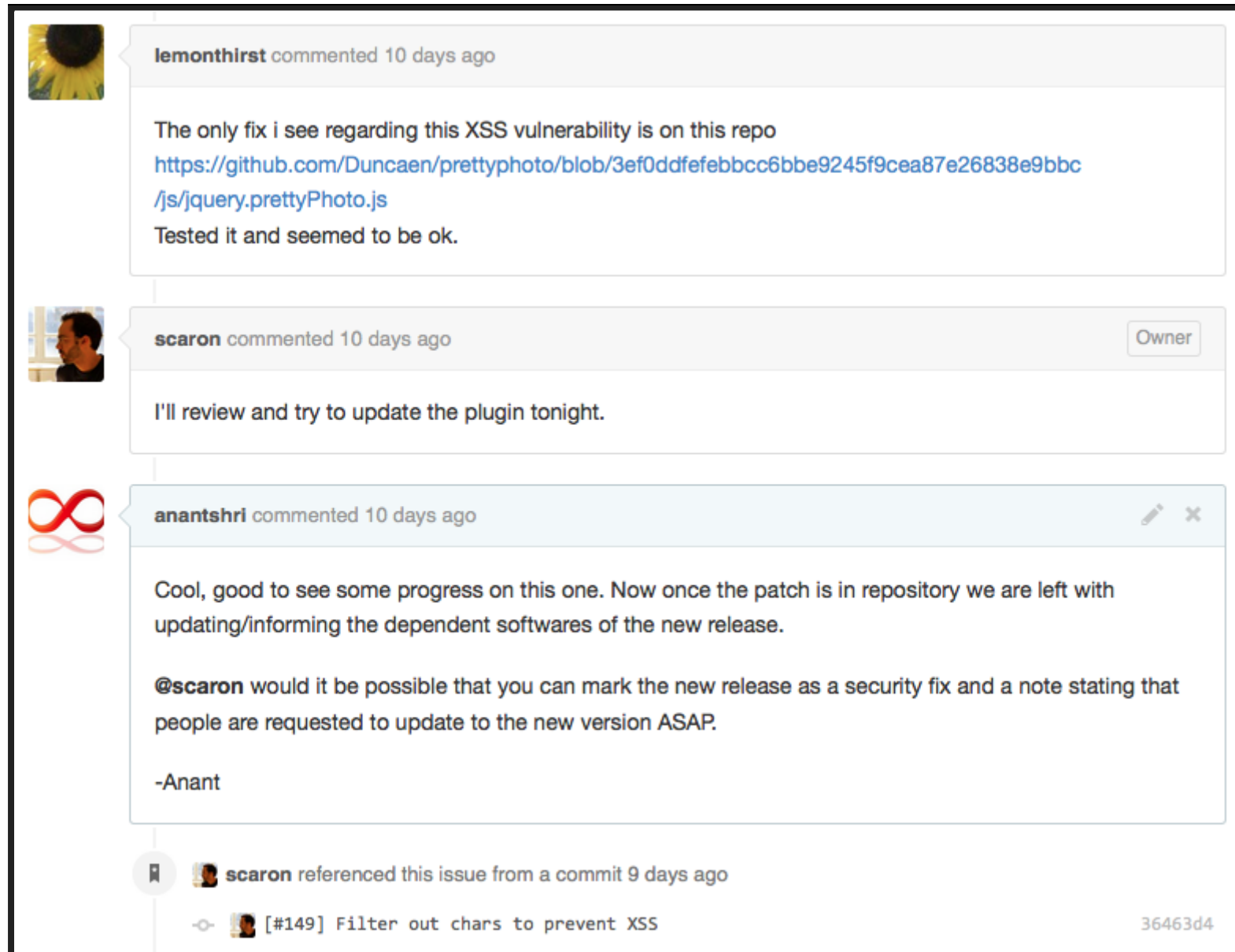
SPREAD THE WORD



SPREAD THE WORD



FINALLY SOME ACTION



A screenshot of a GitHub issue page showing three comments. The first comment is from user 'lemonthirst' with a sunflower profile picture, mentioning a fix for an XSS vulnerability and providing a GitHub link. The second comment is from user 'scaron' with a profile picture of a man, stating they will review and update the plugin. The third comment is from user 'anantshri' with an infinity symbol profile picture, expressing satisfaction with progress and requesting a security fix label and update notice. At the bottom, a commit by 'scaron' is referenced, and the issue title '[#149] Filter out chars to prevent XSS' is visible along with the issue ID '36463d4'.

lemonthirst commented 10 days ago

The only fix i see regarding this XSS vulnerability is on this repo
<https://github.com/Duncaen/prettyphoto/blob/3ef0ddfefebbcc6bbe9245f9cea87e26838e9bbc/js/jquery.prettyPhoto.js>
Tested it and seemed to be ok.

scaron commented 10 days ago Owner

I'll review and try to update the plugin tonight.

anantshri commented 10 days ago

Cool, good to see some progress on this one. Now once the patch is in repository we are left with updating/informing the dependent softwares of the new release.

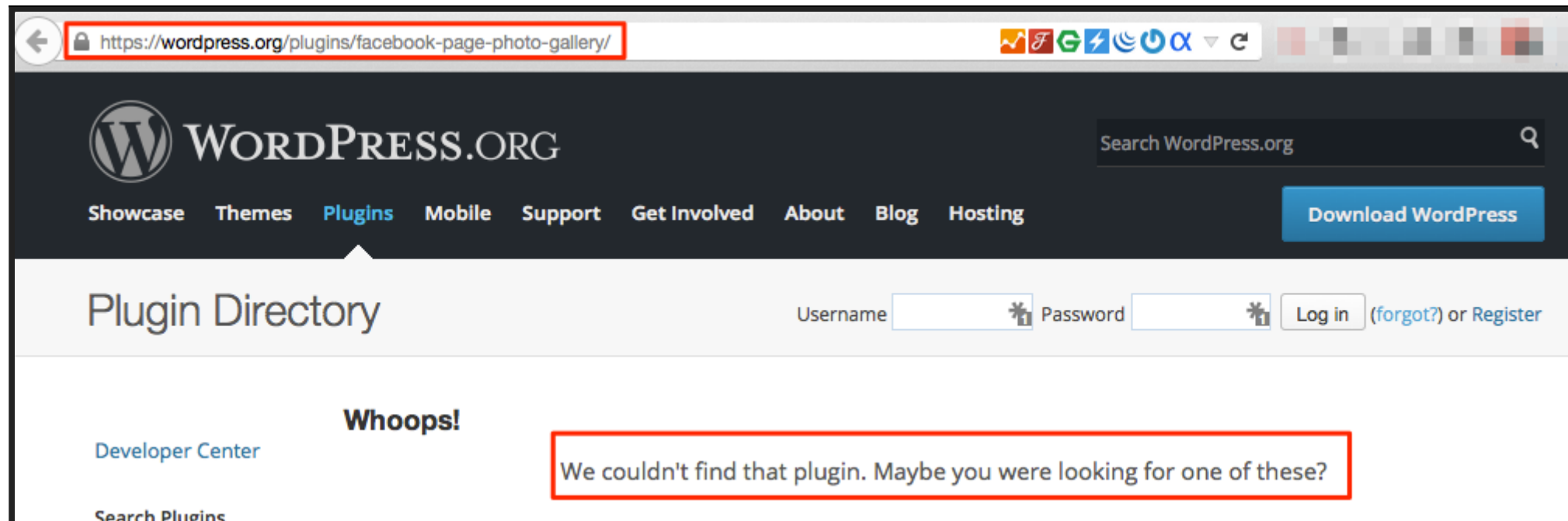
@**scaron** would it be possible that you can mark the new release as a security fix and a note stating that people are requested to update to the new version ASAP.

-Anant

scaron referenced this issue from a commit 9 days ago

[#149] Filter out chars to prevent XSS 36463d4

SOME ACTION



RELIEVED

LET THE WORLD BE IN PEACE

AND

LETS GET BACK TO WORK

AFTER 7 DAYS

WHY YOU NO FIX



WORDPRESS PLUGIN INFO

1. Total 35 Plugins Found

Total Plugin Downloads	Active Install
2882520	3,37,780

NERDY DATA

The screenshot shows a web browser window with the URL `https://search.nerdydata.com/code/?and_code[]=jquery.prettyphoto.js&limit=0,10&rank_min=1&rank_max=1000001`. The page features the Nerdify Data logo on the left, a search bar containing `jquery.prettyphoto.js`, and a green **Search** button. To the right of the search bar is a link for [Advanced](#) search. Below the search bar, a green **Upgrade** button is visible on the left. A red rectangular box highlights the search results summary: **About 1,042,503 results (1.9602 seconds) Page 1 of 104,251**. The browser's address bar and various extension icons are visible at the top of the window.

WHAT IS VULNERABLE

1. Any application / website which has jquery.prettyphoto.js
2. Version 3.1.4 and 3.1.5 are confirmed vulnerable older versions not checked.

WHAT IS A FIX

1. Upgrade to 3.1.6

ENOUGH OF THE PAST

WHAT'S IN IT FOR ME.

LESSONS TO BE LEARNED

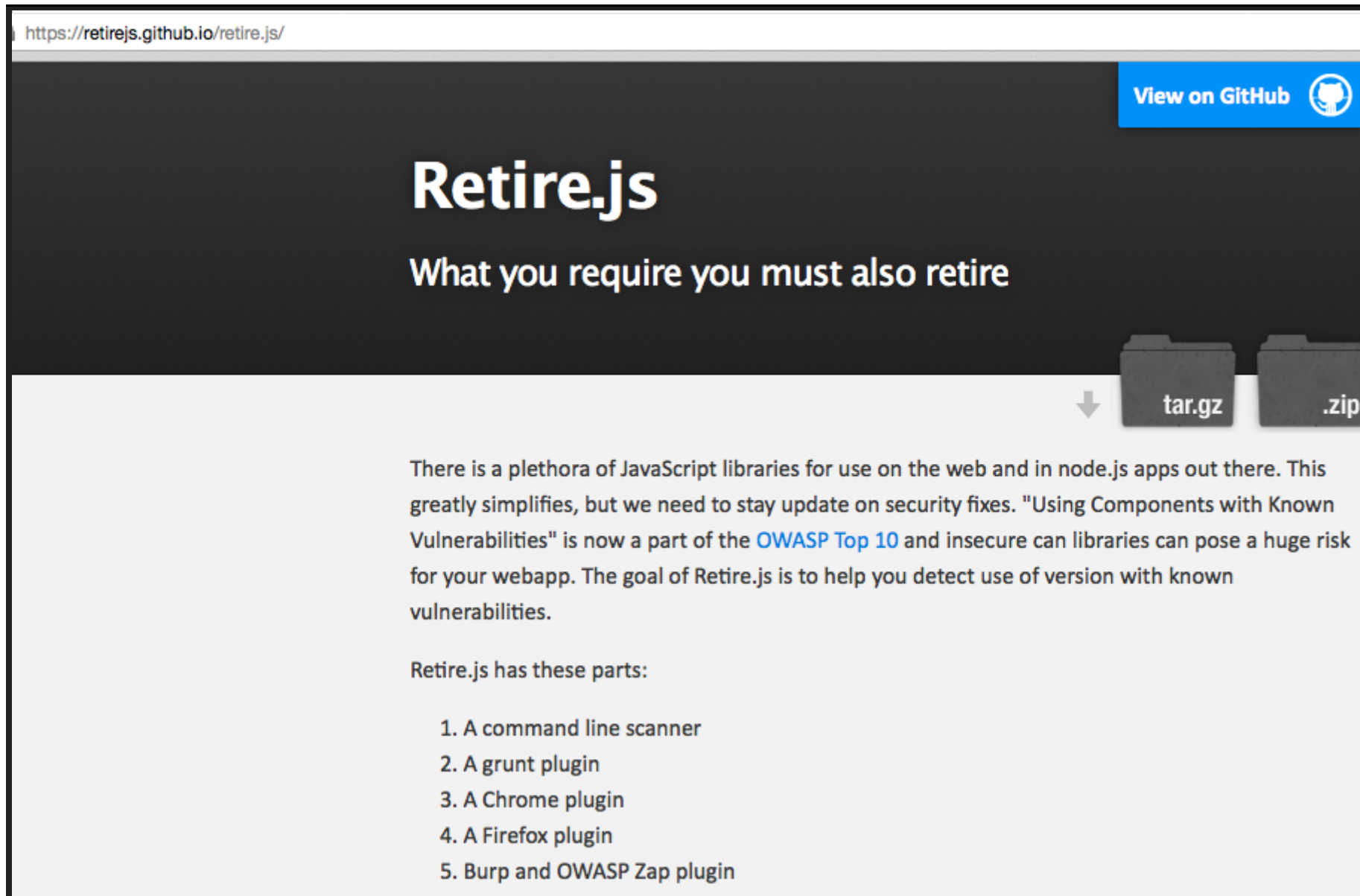
FOR DEVELOPER

1. Never ignore pull requests and security issue bug report.
2. Proactively test software and at-least if a fix is released publicly accept security issue.

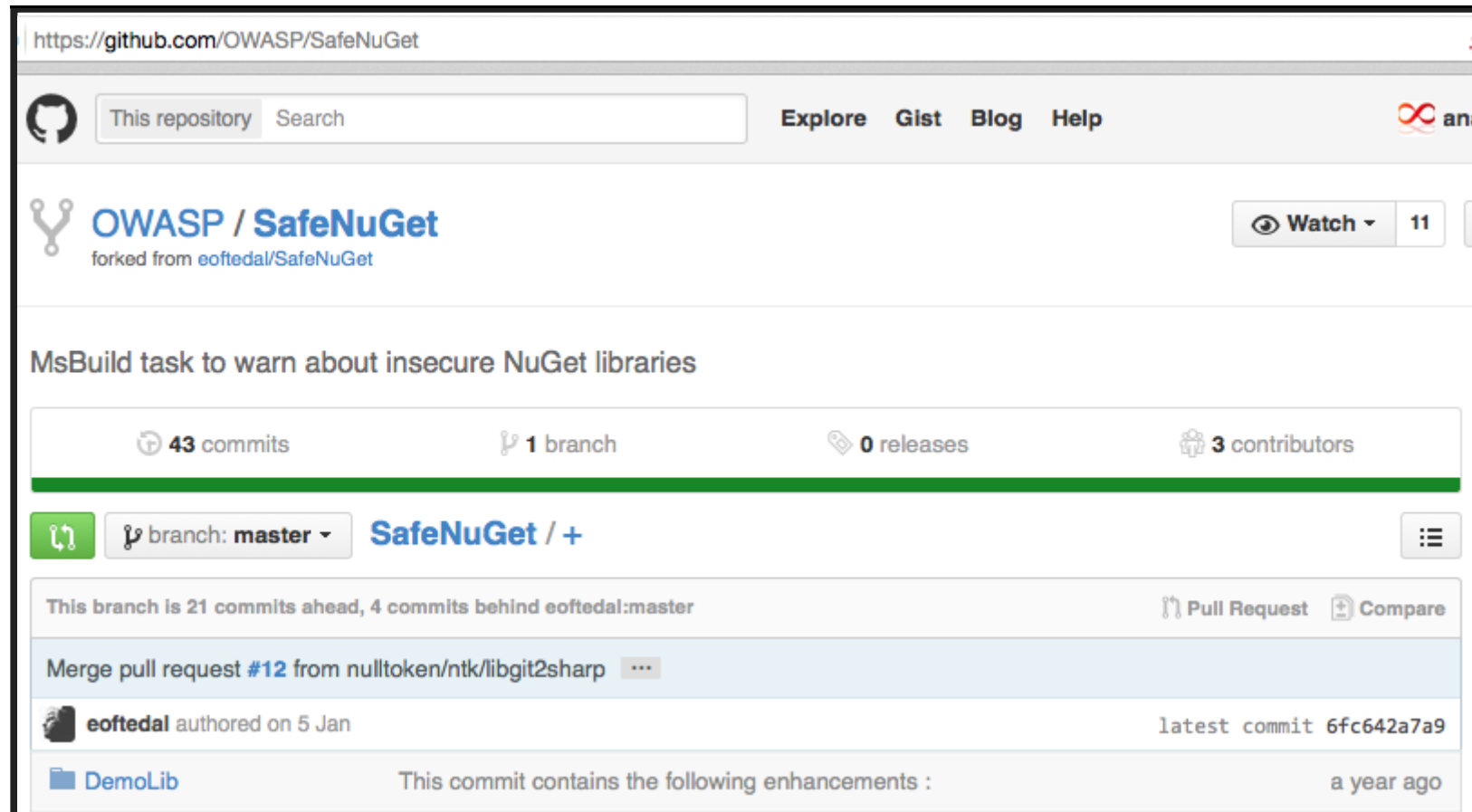
FOR DEVELOPERS / SYSADMIN / DEVOPS

1. never ignore update from shared library
2. Keep an eye on how shared resources are holding up.
3. Monitor your Dependencies

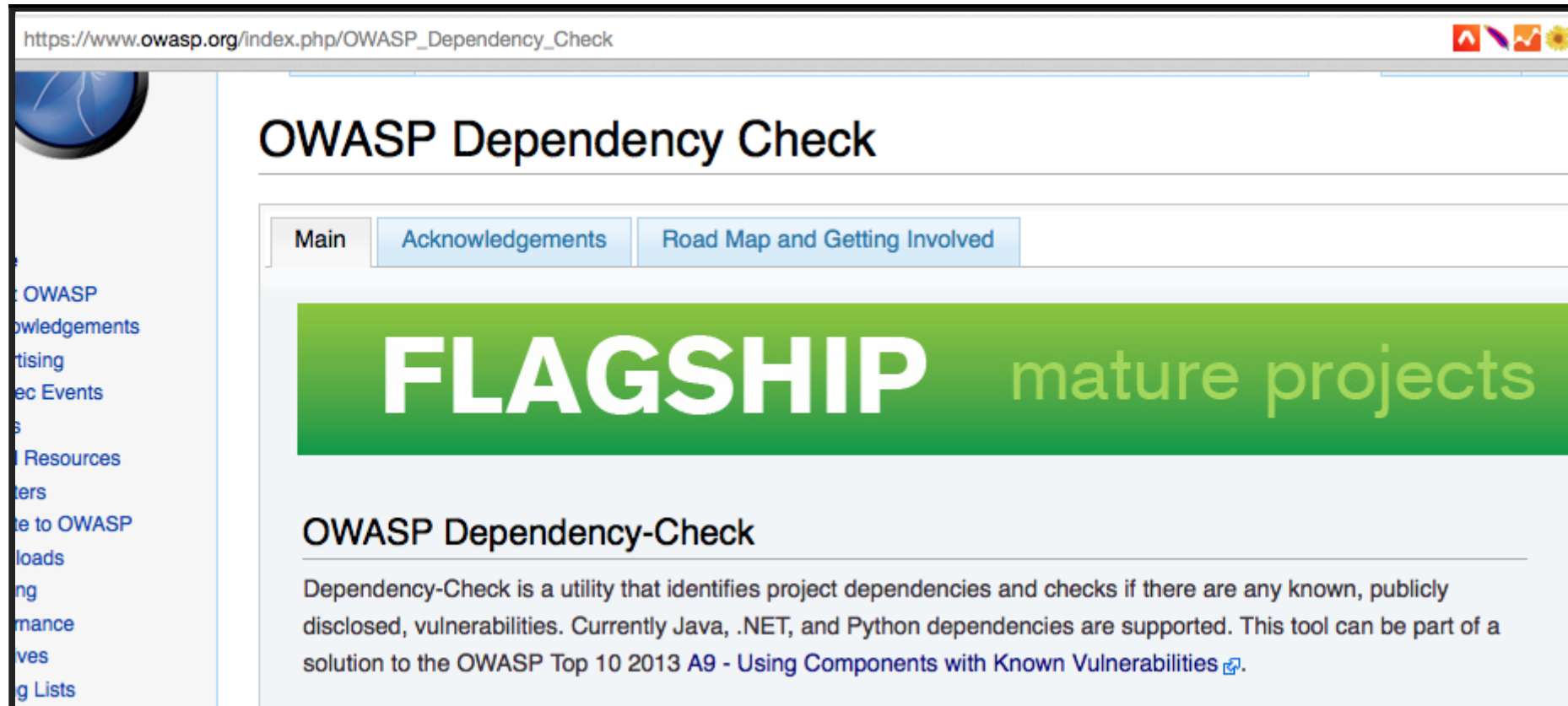
HOW



HOW



HOW



IS THIS ENOUGH

1. Not yet
2. We still lack method to track it for every third party library.
3. Manual tracking is still required.

REFERENCES

1. A9 - Using Components with Known Vulnerabilities
2. https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities

THANKS