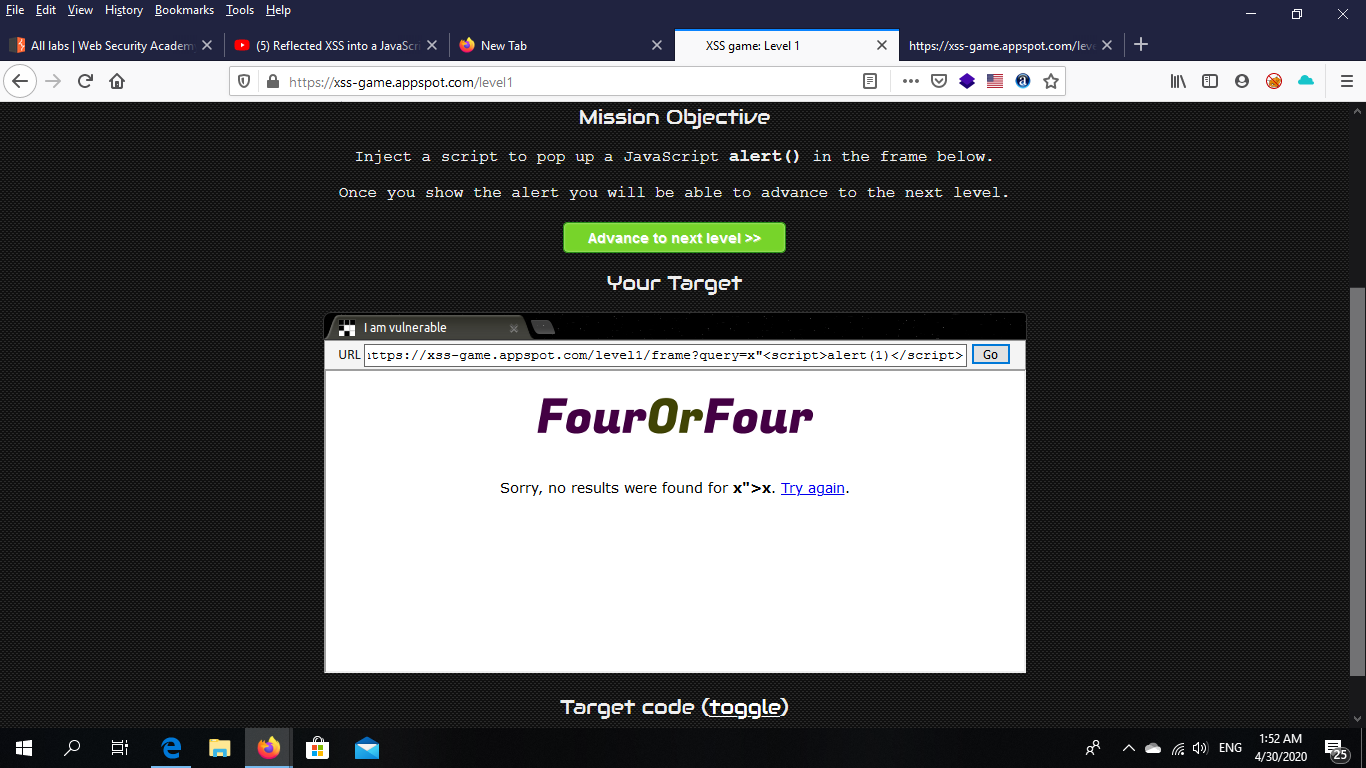
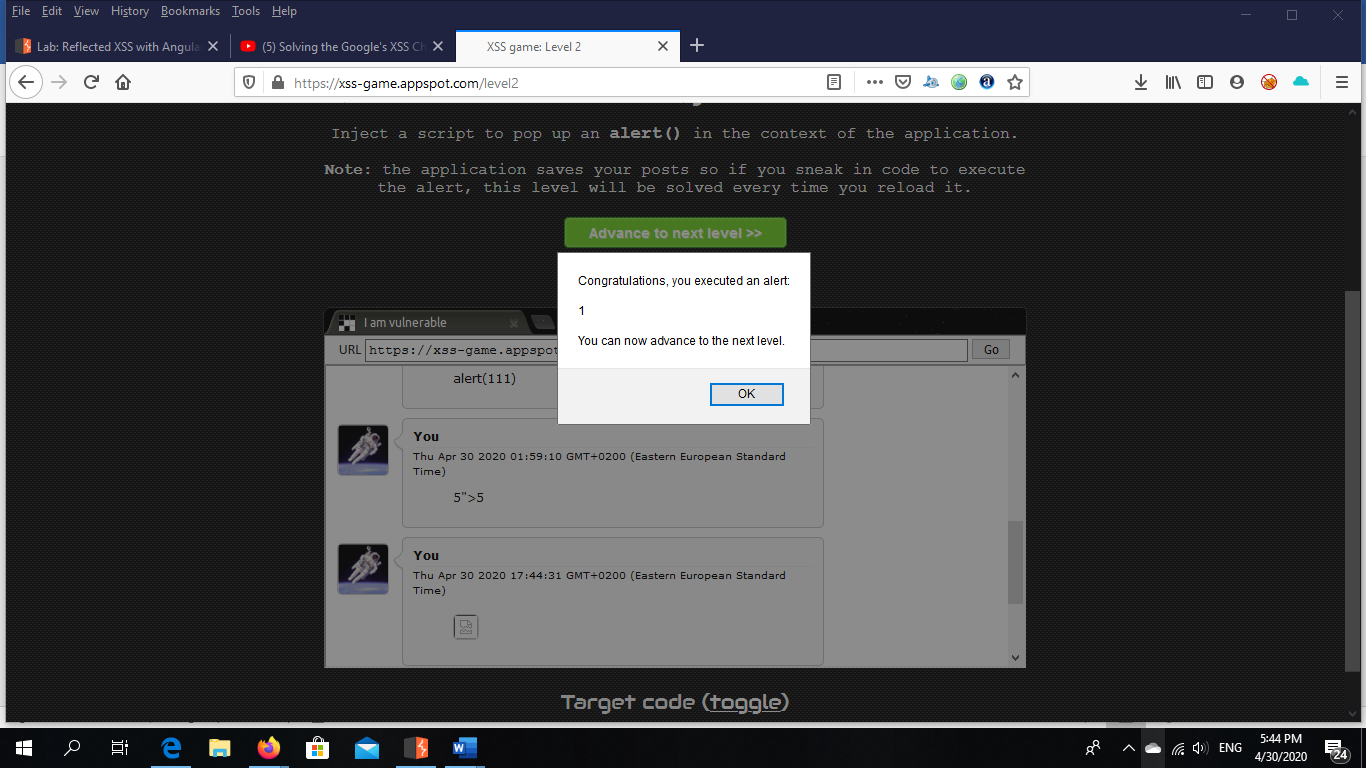
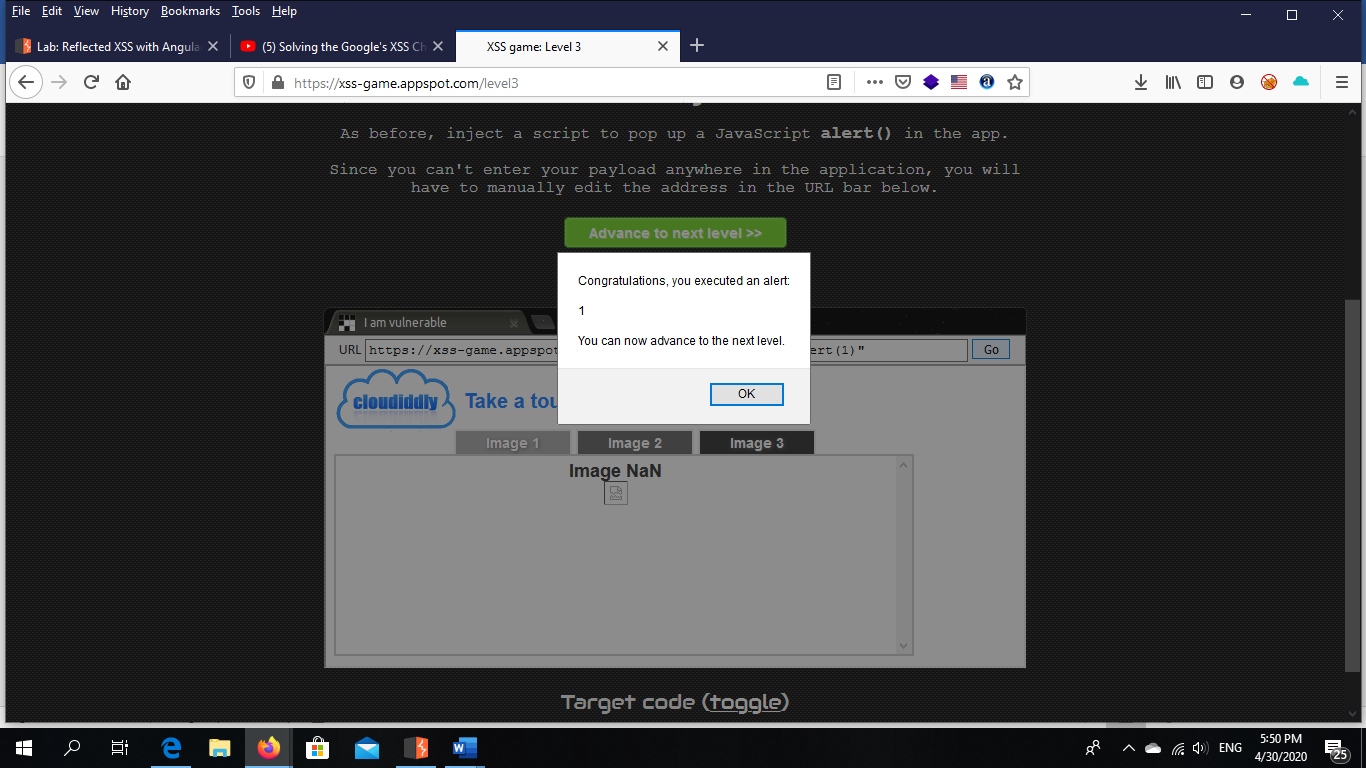
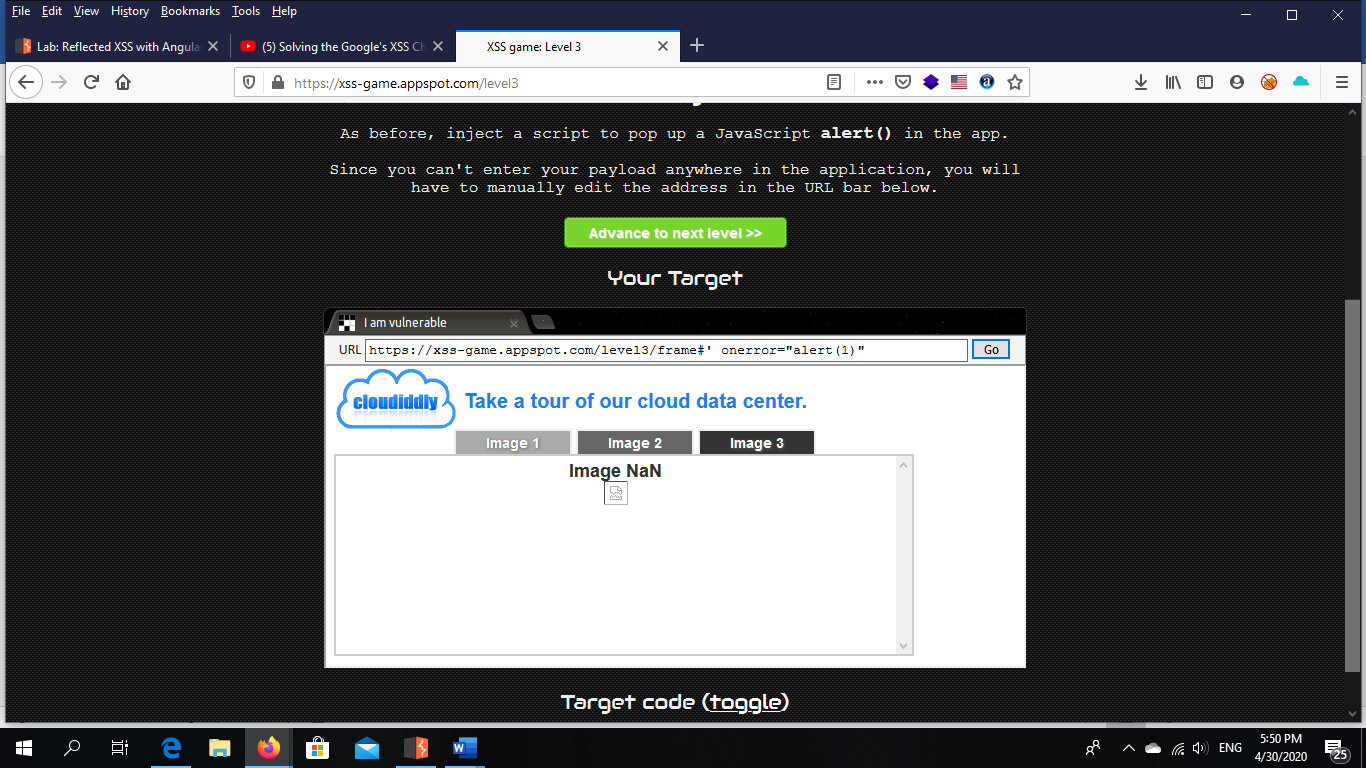
**Google XSS game**

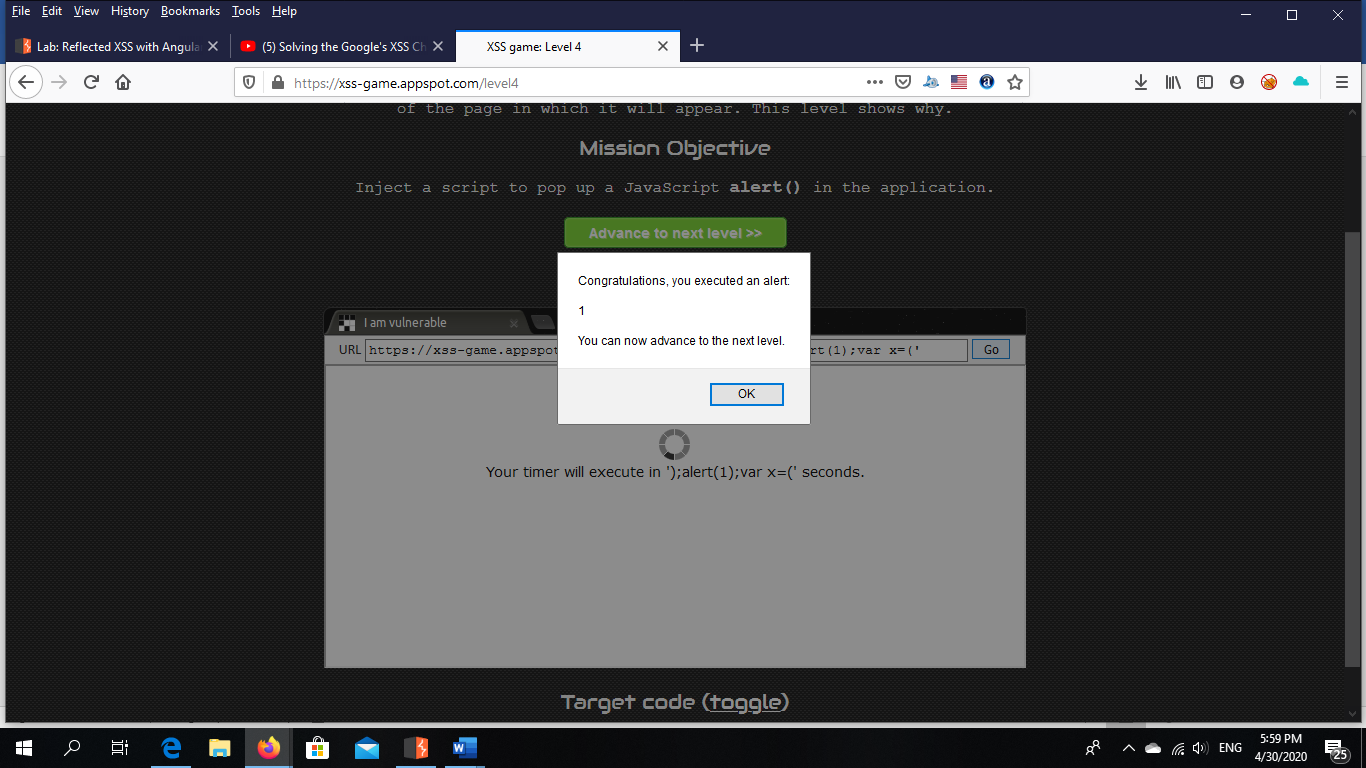
**Task 2**



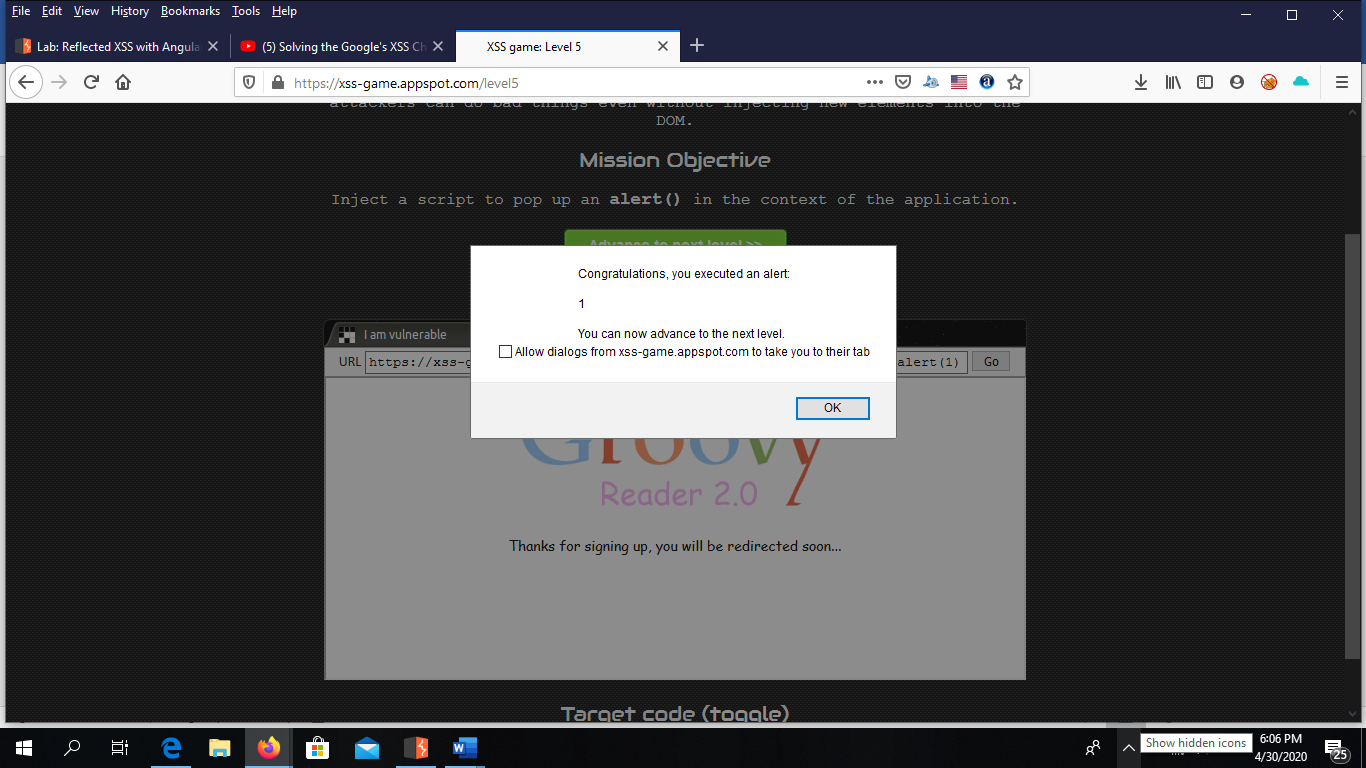




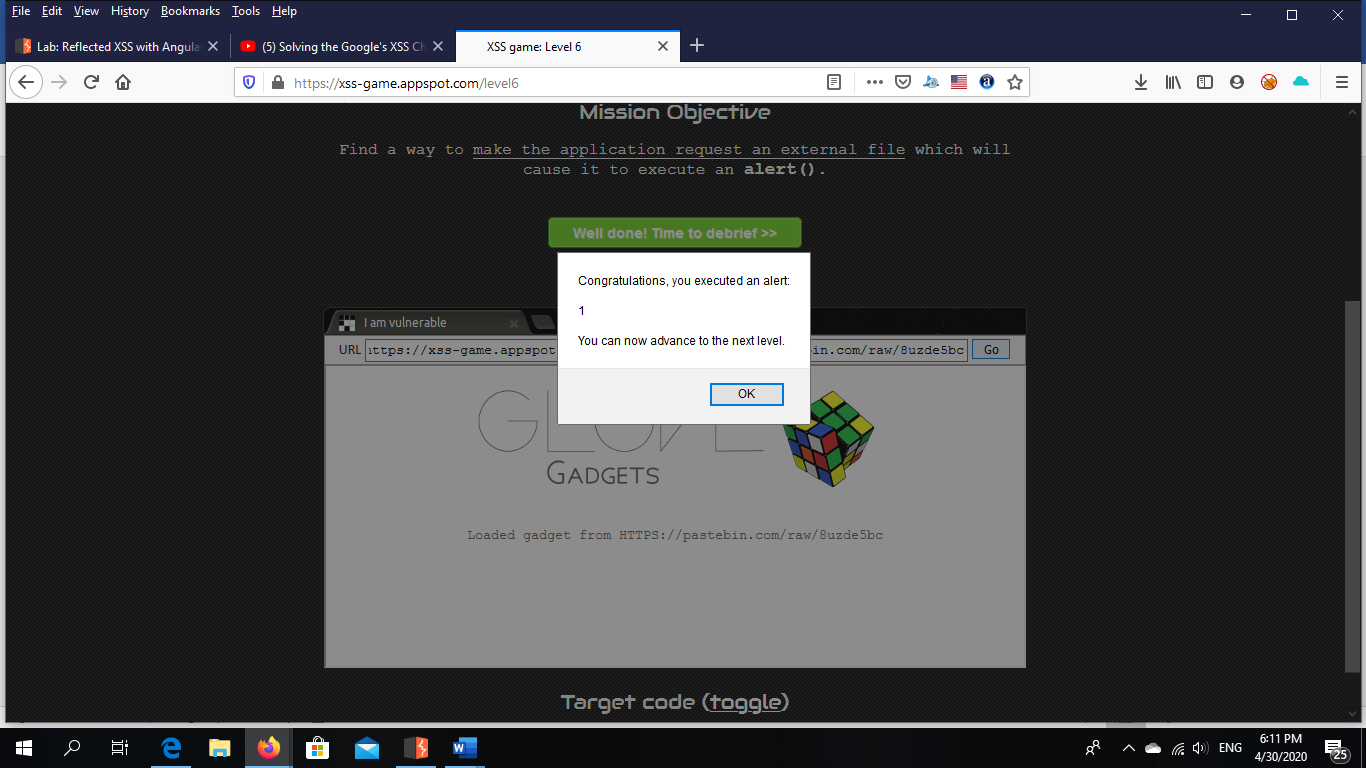
**(Level 3) **

****

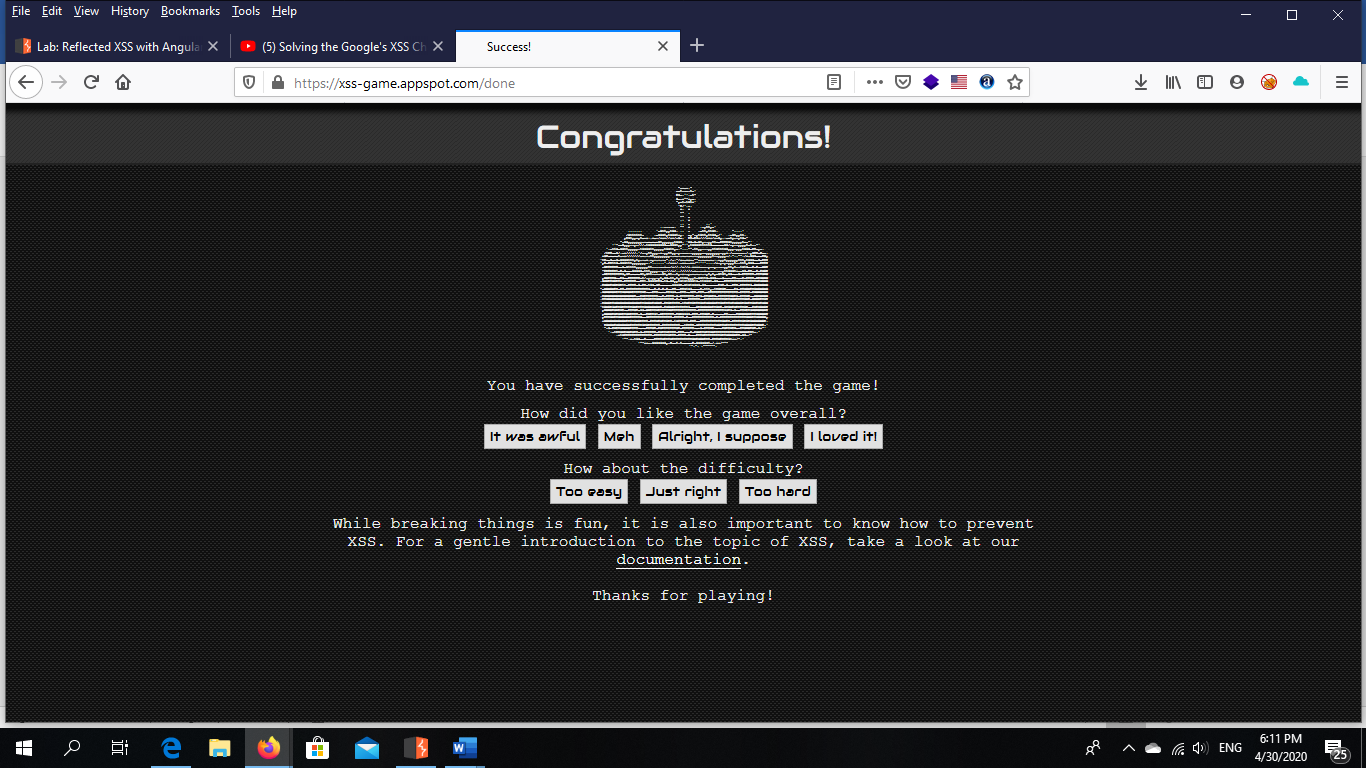
**(Level 4)**

****

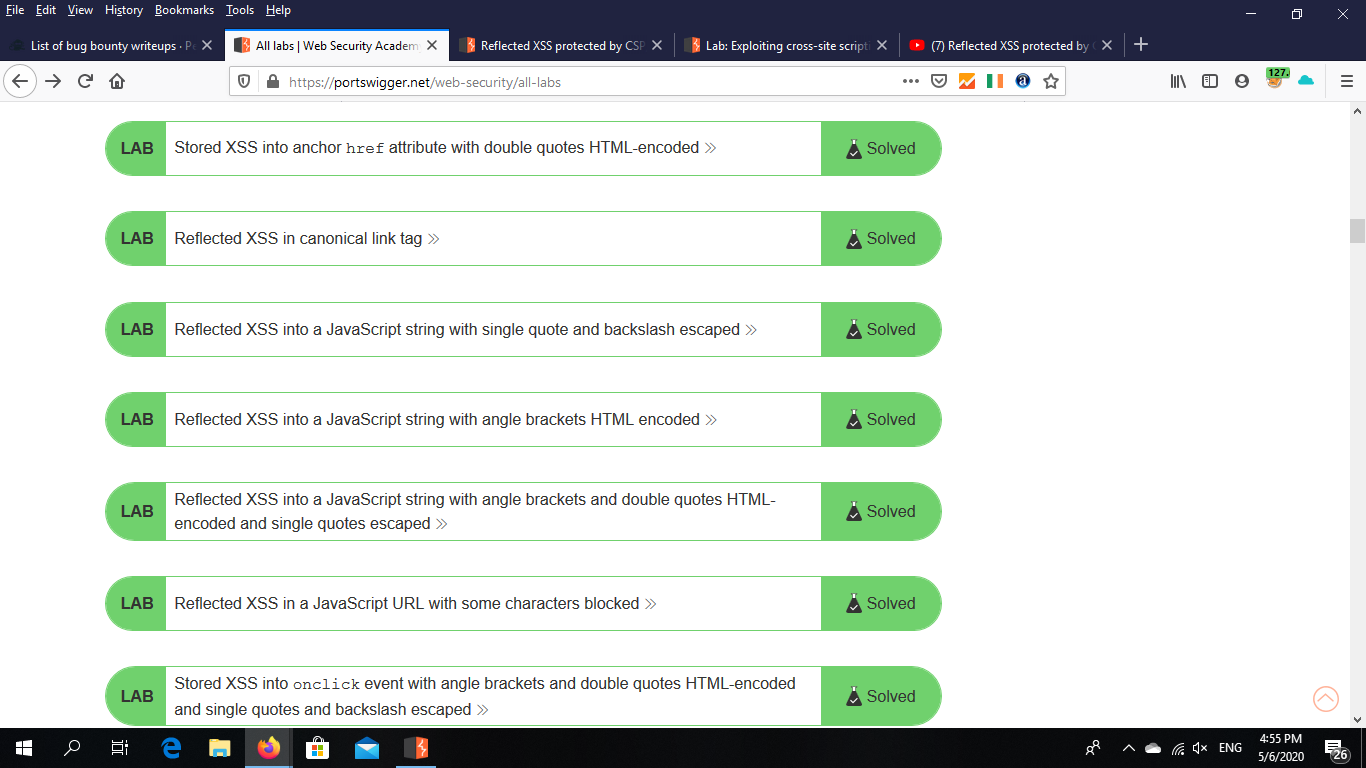
**(Level 5)**

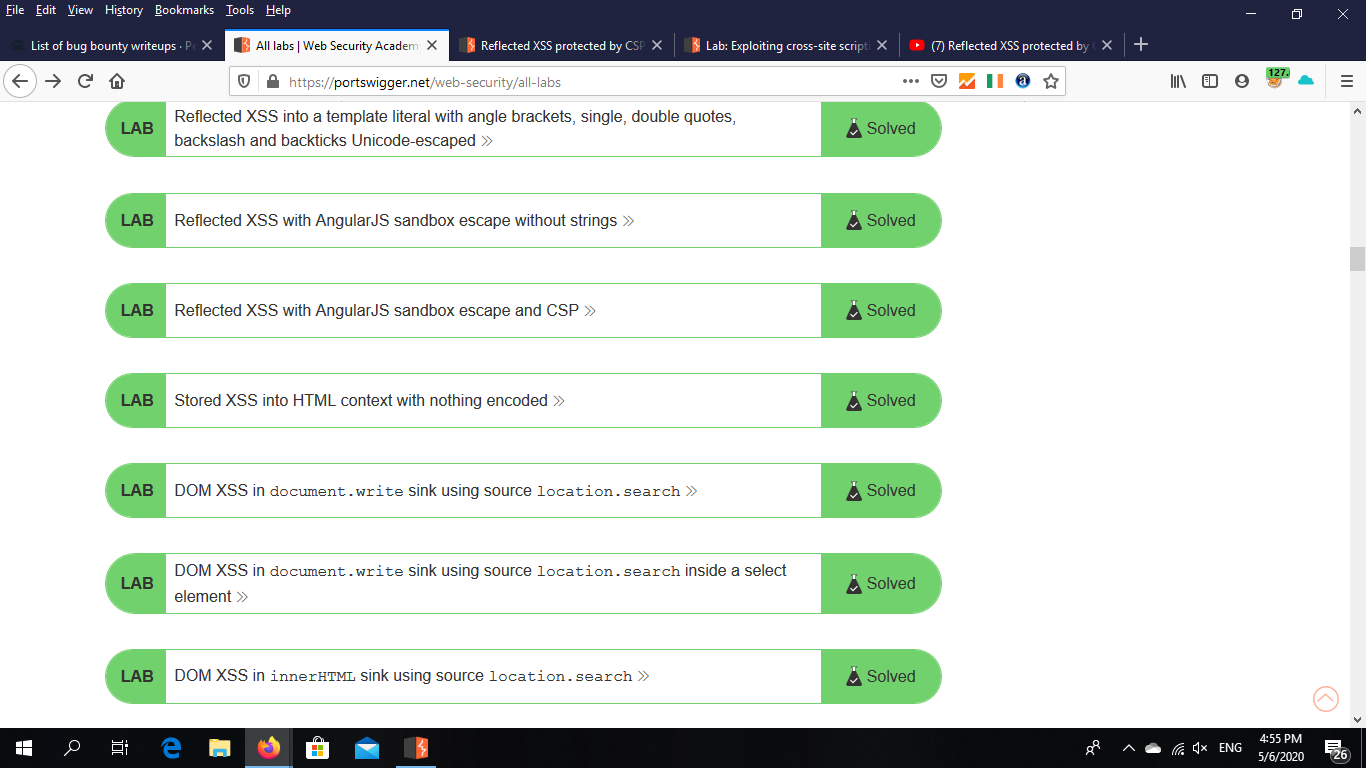


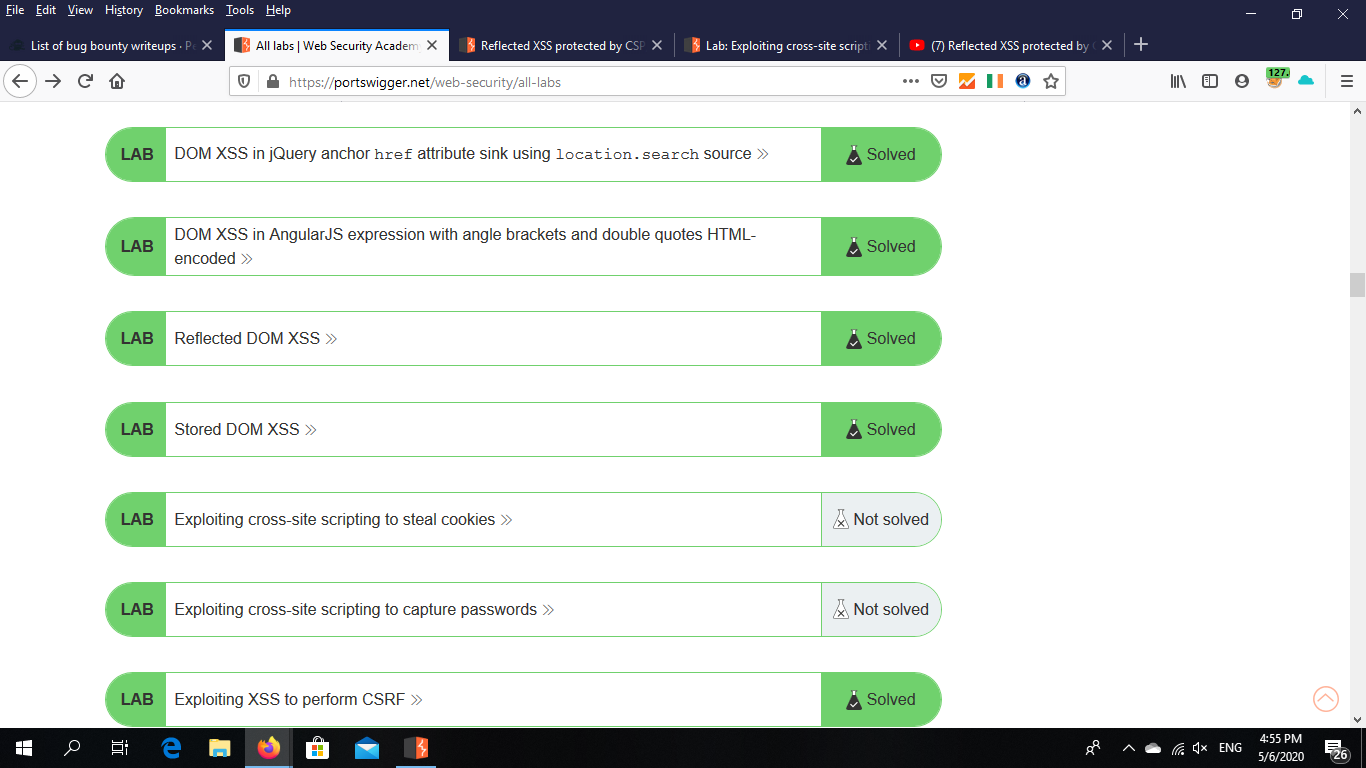
**(Level 6)**

****

**Cross site scripting**







**Writeups about XSS**

- <https://0x65.dev/blog/2020-03-30/cve-2019-17004-semi-universal-xss-affecting-firefox-for-ios.html> .

- <https://payatu.com/blog/nikhil-mittal/executing-scripts-in-safari-reader-mode--to-csp-bypass> .

- <https://smaranchand.com.np/2020/02/the-tricky-xss/> .

- <https://www.mohamedharon.com/2018/03/reflected-xss-moogaloop-swf-version-62x.html> .

- <https://www.mohamedharon.com/2018/03/xss-in-subdomain-httpsyefgrantsyahoocom.html> .

- <https://www.mohamedharon.com/2018/03/xss-in-sportstwcampaignyahoonet.html> .

- <https://blog.securitybreached.org/2018/02/02/how-i-was-able-to-bypass-xss-protection-on-hackerones-private-program/> .

- <https://www.noob.ninja/2017/11/local-file-read-via-xss-in-dynamically.html> .

- <https://www.ansariosama.com/2017/11/how-i-pwned-company-using-idor-blind-xss.html> .

- <https://www.guptashubham.com/multiple-vulnerabilities-in-oracle-ebs/> .

- <https://wesecureapp.com/2017/07/10/how-we-tookover-shopify-accounts-with-one-single-click/> .

- <https://buer.haus/2017/06/29/escalating-xss-in-phantomjs-image-rendering-to-ssrflocal-file-read/> .

- <https://know.bishopfox.com/blog/2017/06/how-i-built-an-xss-worm-on-atmail> .

**Dom XSS**

-<https://jinone.github.io/bugbounty-a-dom-xss/> .

-<https://hacknpentest.com/dom-based-xss-bug-bounty-writeup/> .

- <https://websecblog.com/vulns/clickjacking-xss-on-google-org/> .

- <https://mike-n1.github.io/Chain_XSS> .

**Stored XSS**

* <https://www.rcesecurity.com/2019/09/H1-4420-From-Quiz-to-Admin-Chaining-Two-0-Days-to-Compromise-an-Uber-Wordpress/> .
* <https://m0chan.github.io/2020/02/04/Arbitary-File-Upload-Too-Stored-XSS.html> .
* <https://learn.hackersid.com/2019/08/stored-xss-on-laporbugid.html> .
* <https://learn.hackersid.com/2019/08/stored-xss-on-laporbugid.html> .

**Writeup about CSRF**

<https://haiderm.com/how-i-was-able-to-delete-13k-microsoft-translator-projects/> .

<https://kongwenbin.com/fastest-fix-on-open-bug-bounty-platform/> .

<https://www.sec-down.com/wordpress/?p=809> .

<https://nirmaldahal.com.np/r-xss-csrf-bypass-to-account-takeover/?__cf_chl_jschl_tk__=1c20259fe0ca7ae6bc2b80e501e07d10e14caea1-1588509618-0-AewTuG_RsSTaDuP4kzGzHGGvIke36SEznPP5l8IGmaszAaggCgrWgEbwLBk7mxSJ3s9iHPqsYl9Qwzhr1gbBMxelr-nkfg1dpaLRlh6H9hBZO1b6fFafo9qTjQtuMQEeRowVd0SY2zDgfnKNniq61kTm6IpC_DEOD6_q5mKWK9QlHwxd0S5zd7_BNK063VpEEDWjvAUlHahjCh4qRVRUFzY33PvzNjCXCZXlkr0ad_3OVcSgP5hktqB5bYnNozvBQ0j7KB7mZIKKT8xCNd8I9hkE4GQWD40Yljs7ppGNYltXQeEbXEH3aX1mw4VL8ADksctFtjUlwytG4shZzbYbPHQ> .

<https://mike-n1.github.io/Chain_XSS> .

<https://blog.scrt.ch/2018/08/24/remote-code-execution-on-a-facebook-server/>

<https://whitton.io/articles/instagrams-one-click-privacy-switch/> .

<https://whitton.io/articles/obtaining-tokens-outlook-office-azure-account/> .

<https://www.rcesecurity.com/2016/02/ubiquiti-bug-bounty-unifi-v3-2-10-generic-csrf-protection-bypass/> .

<https://blog.darabi.me/2015/04/bypass-facebook-csrf.html> .

<https://buer.haus/2015/02/03/flickr-api-explorer-force-users-to-execute-any-api-request/> .

<https://www.josipfranjkovic.com/blog/hacking-facebook-csrf-device-login-flow> .

<https://www.arneswinnen.net/2017/06/authentication-bypass-on-airbnb-via-oauth-tokens-theft/> .

<https://seekurity.com/blog/2017/06/11/mahmoud-gamal/general/lets-steal-some-tokens> .

<https://whitton.io/articles/messenger-site-wide-csrf/> .

<https://ahussam.me/Amazon-leaking-csrf-token-using-service-worker/> .

<https://philippeharewood.com/facebook-graphql-csrf/> .

<https://bughunt1307.herokuapp.com/googlebugs.html> .

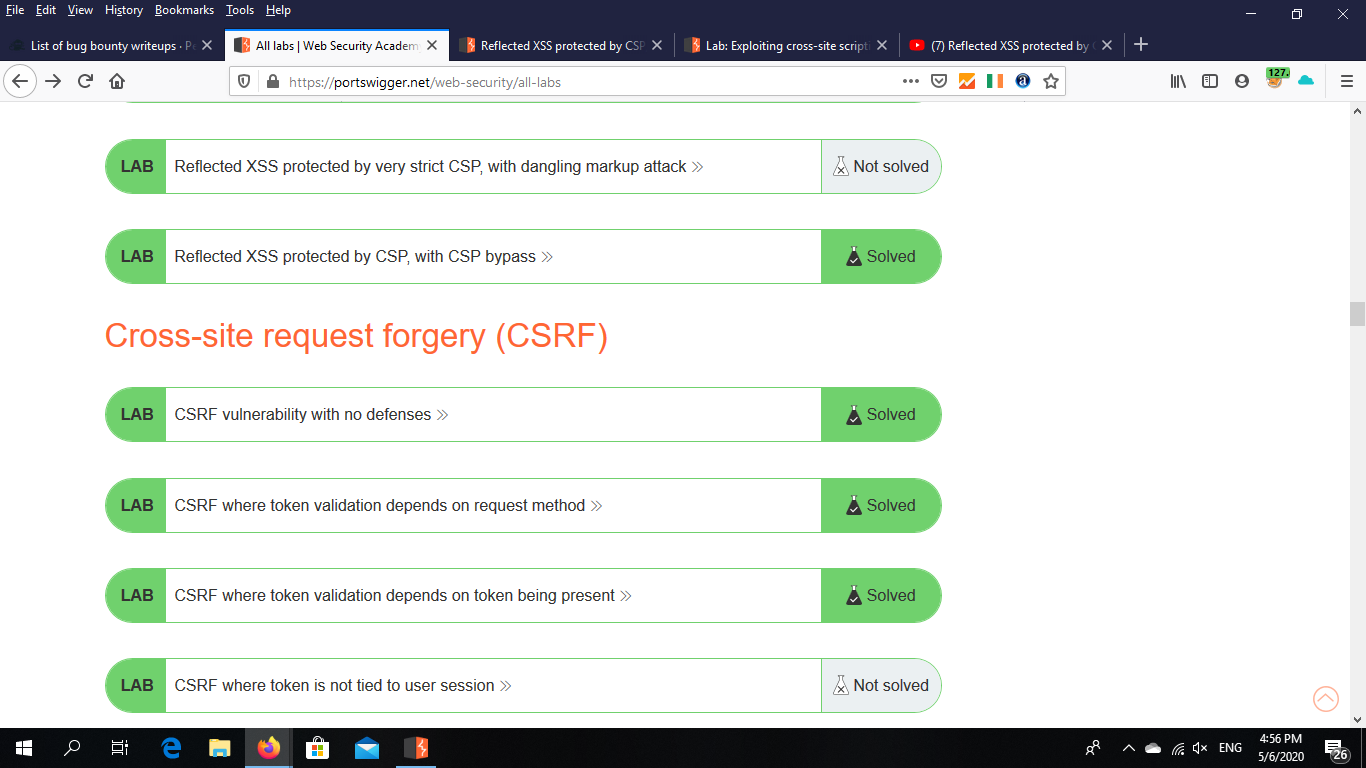
<https://blog.yappare.com/2018/01/1800-in-less-than-hour.html> .

<https://ahussam.me/Leaking-WordPress-CSRF-Tokens/> .

<https://whitton.io/articles/stealing-facebook-access-tokens-with-a-double-submit/> .

<https://whitton.io/archive/my-experience-with-the-paypal-bug-bounty-programme/> .

**Labs:- CSRF**



**Summary about disclosure tips**

-Backup files (Zip,tar,tgz,sql,rar,gz,….).

Ex:- [www.site.com/backup.sql](http://www.site.com/backup.sql). (this is form of disclosure ).

**Other form of disclosure :-**

-Hidden files (.file name)

(The black hacker prefer this way to attack any source code or data .)

-source code repositories (.git ,.svn)

(git :- this is famous file ,it help developers in their modifications ,if hacker get this file ,that mean his enable to see the source code and he success in attack.)

-source code files (.old ,.back ,.php~ ,.swp).

**NOT:- from types disclosure Java script files and this more dangerous**