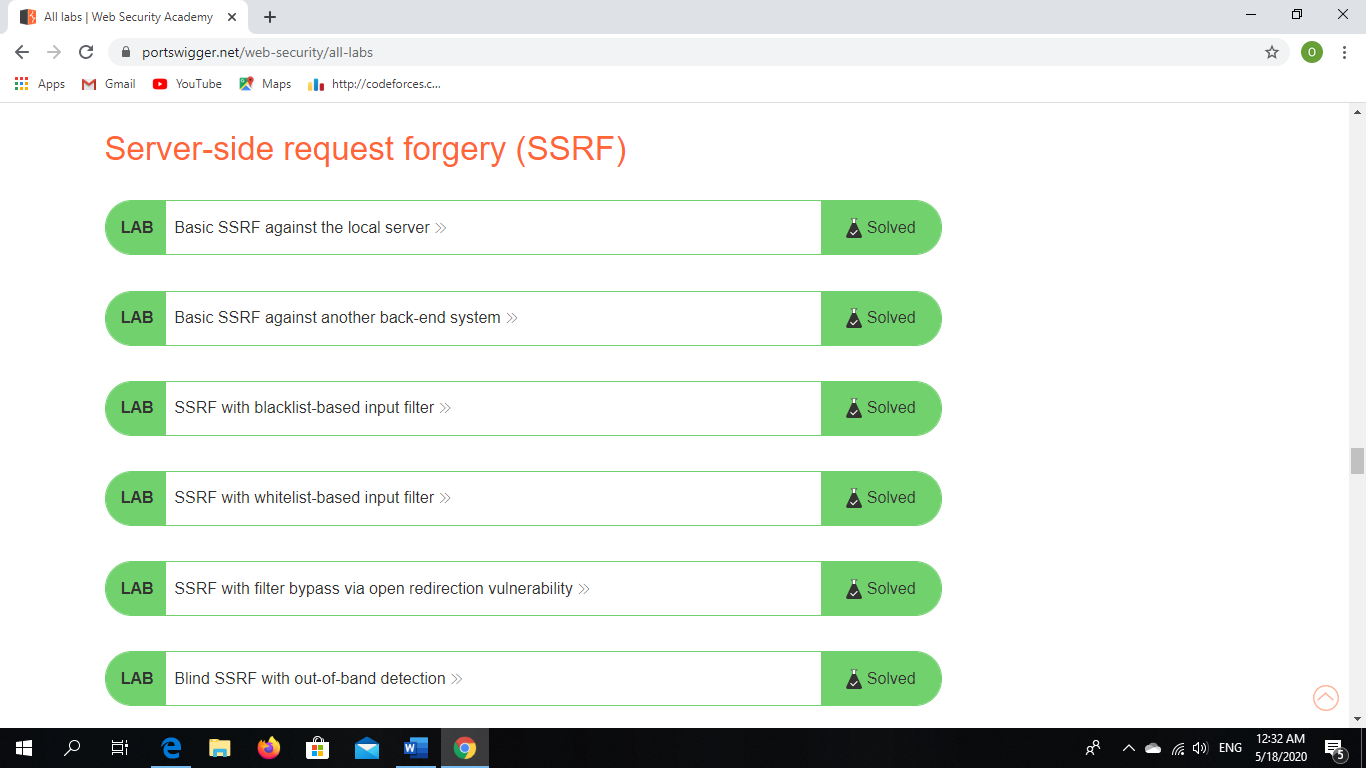
Task 3 :-

Labs :-SSRF



Writeup about SSRF

<https://medium.com/@kurtikleiton/blind-ssrf-on-coda-io-c7063f304455> .

<https://medium.com/@rooterkaustubh/the-story-of-blind-ssrf-leads-to-internal-host-discovery-ee65b9b91e23> .

<https://medium.com/@d0nut/piercing-the-veal-short-stories-to-read-with-friends-4aa86d606fc5> .

<https://www.rtcsec.com/2020/04/01-slack-webrtc-turn-compromise/> .

<https://medium.com/bugbountywriteup/using-vulnerability-analytics-feature-like-a-boss-655fc1f1543b>

<https://medium.com/@michan001/ssrf-on-pdf-generator-36b81e16d67b> .

<https://medium.com/@know.0nix/hunting-good-bugs-with-only-html-d8fd40d17b38> .

<https://ngailong.wordpress.com/2019/12/19/google-vrp-ssrf-in-google-cloud-platform-stackdriver/> .

<https://medium.com/@dPhoeniixx/vimeo-upload-function-ssrf-7466d8630437> .

<https://medium.com/@pflash0x0punk/ssrf-via-ffmpeg-hls-processing-a04e0288a8c5> .

<https://kntx.xyz/Blind-SSRF-due-to-Sentry-Misconfiguration/> .

<https://geleta.eu/2019/my-first-ssrf-using-dns-rebinfing/> .

<https://www.openbugbounty.org/blog/leonmugen/ssrf-reading-local-files-from-downnotifier-server/> .

<https://medium.com/a-bugz-life/the-bugs-are-out-there-hiding-in-plain-sight-12d056613ea3> .

<https://medium.com/@androgaming1912/gain-adfly-smtp-access-with-ssrf-via-gopher-protocol-26a26d0ec2cb> .

<https://medium.com/@w_hat_boy/server-side-request-forgery-ssrf-port-issue-hidden-approch-f4e67bd8cc86> .

<https://medium.com/@logicbomb_1/the-journey-of-web-cache-firewall-bypass-to-ssrf-to-aws-credentials-compromise-b250fb40af82> .

<https://medium.com/@pratiky054/ssrf-to-read-local-files-and-abusing-the-aws-metadata-8621a4bf382>

<https://medium.com/@armaanpathan/pdfreacter-ssrf-to-root-level-local-file-read-which-led-to-rce-eb460ffb3129> .

<https://medium.com/@elberandre/ssrf-trick-ssrf-xspa-in-microsofts-bing-webmaster-central-8015b5d487fb> .

<https://medium.com/@GeneralEG/escalating-ssrf-to-rce-f28c482eb8b9> .

Summary about path traversal &LFD&RFI&LFI :-

* **LOCAL FILE INCLUSION :- (LFI)**

**-this type allow to attacker for include file .(you can read files from server).**

**-php have 4 functions to this type:-**

**-include () / require () /include once () /require once ().**

* **LOCAL FILE DISCLOUSURE :- (LFD)**

**- you can execute file too definition of LFI .**

**(=1 PHP).**

* **REMOTE FILE INCLUSION :- (RFI)**

**-this bug don’t found .**

* **PATH TRAVESAL :-**

**-we exploit bugs with this file .**

**NOTE:-**

**-PHP filter :- this allow to read files .(php://filter).**

**-convert LFI to RCE that happen when we can brought code execution**

**And the technique that we use with this is file upload.**

**-how to fix this bugs (that we identifier file name ).**

Writeups about LFI :-

-<https://nirmaldahal.com.np/lfi-to-10-servers-pwn/> .

-<https://paper.seebug.org/737/> .

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

-<https://www.vesiluoma.com/abusing-mysql-clients/> .

-<https://blog.scrt.ch/2019/01/24/magento-rce-local-file-read-with-low-privilege-admin-rights/> .

-<https://nirmaldahal.com.np/lfi-to-10-servers-pwn/> .

-<https://www.updatelap.com/2019/05/local-file-inclusion-in-peeringgooglecom.html> .

-<https://spenkk.github.io/bugbounty/Local-File-Inclusion/> .

-<https://cyberzombie.in/my-first-lfi/> .

-<https://blog.shashank.co/2013/10/lfi-in-nokia-maps.html> .

-<https://www.rcesecurity.com/2014/04/magix-bug-bounty-magix-com-rce-sqli-and-xara-com-lfi-xss/> .

-<https://josipfranjkovic.blogspot.com/2014/12/reading-local-files-from-facebooks.html> .

-<http://karmainsecurity.com/hacking-magento-ecommerce-for-fun-and-17000-usd> .

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

-<https://www.rcesecurity.com/2017/08/from-lfi-to-rce-via-php-sessions/> .

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

-<http://hassankhanyusufzai.com/RFI_LFI_writeup/> .

-<https://offensi.com/2019/01/31/lfi-in-apigee-portals/> .

Writeups about path traversal :-

-<https://incogbyte.github.io/pathtraversal/> .

-<https://www.inputzero.io/2019/04/evernote-cve-2019-10038.html> .

-<https://ngailong.wordpress.com/2019/04/07/old-but-gold-dot-dot-slash-to-get-the-flag-uber-microservice/amp/> .

-<https://research.checkpoint.com/2019/reverse-rdp-attack-code-execution-on-rdp-clients/> .

-<https://blog.scrt.ch/2019/01/24/magento-rce-local-file-read-with-low-privilege-admin-rights/> .

<http://codegrazer.com/blog/rsftp-to-command-injection.html#.W-Cijl14IJM.twitter> .

-<https://blog.harshjaiswal.com/path-traversal-while-uploading-results-in-rce/> .

<https://hawkinsecurity.com/2018/08/27/traversing-the-path-to-rce/> .

-<https://twitter.com/0x01alka/status/1001763583447969792> .

-<https://buer.haus/2017/03/09/airbnb-chaining-third-party-open-redirect-into-server-side-request-forgery-ssrf-via-liveperson-chat/> .

<https://blog.harshjaiswal.com/path-traversal-while-uploading-results-in-rce/> .

Writeups about LFD and RFI :-

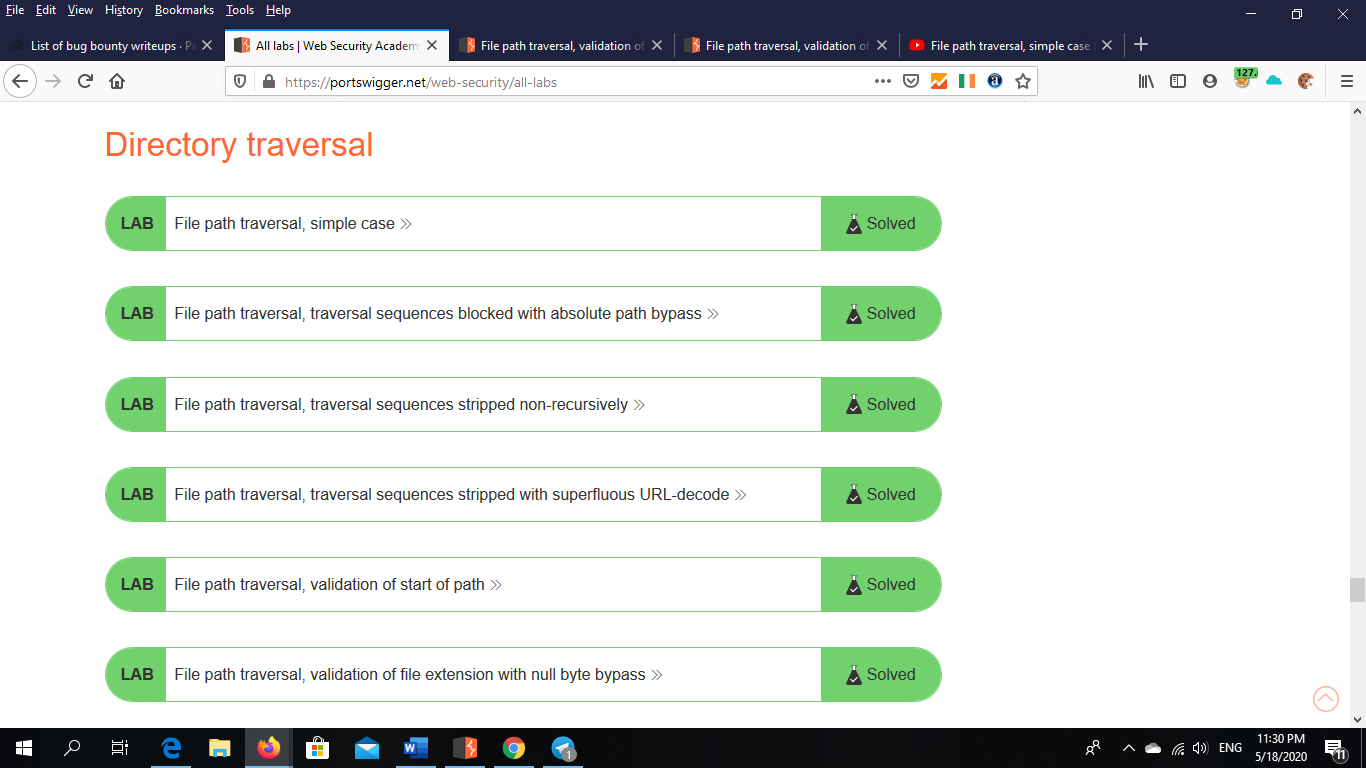
-<https://samcurry.net/reading-asp-secrets-for-17000/> .

-<http://hassankhanyusufzai.com/RFI_LFI_writeup/> .

-<http://karmainsecurity.com/hacking-magento-ecommerce-for-fun-and-17000-usd> .

-<https://bitquark.co.uk/blog/2016/02/09/how_i_got_access_to_millions_of_redacted_accounts> .

Path traversal labs :-



Writeups about host header attacks :-

<https://vict0ni.me/multiple-header-injections-bug-hunting/> .

<https://pethuraj.com/blog/how-i-earned-800-for-host-header-injection-vulnerability/> .

<https://hackerone.com/reports/94637> .

<https://hackerone.com/reports/698416> .

<http://carlos.bueno.org/2008/06/host-header-injection.html> .

<https://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html> .

<https://hackerone.com/reports/698416> .

<https://sites.google.com/site/testsitehacking/10k-host-header> .

<https://www.netsparker.com/blog/web-security/crlf-http-header/> .

<https://hackerone.com/reports/182670> .

<https://nileshsapariya.blogspot.com/2015/10/host-header-injection-at.html> .

<https://hackerone.com/reports/601287> .

<https://hackerone.com/reports/13286> .

<https://hackerone.com/reports/229498> .

<https://hackerone.com/reports/170333> .

<https://hackerone.com/reports/221908> .

<https://hackerone.com/reports/180196> .

<https://hackerone.com/reports/758380> .

<https://hackerone.com/reports/158019> .

<https://hackerone.com/reports/264405> .

<https://hackerone.com/reports/283786> .

<https://hackerone.com/reports/158482> .

<https://hackerone.com/reports/123513> .

<https://hackerone.com/reports/167809> .

<https://hackerone.com/reports/409370> .

<https://hackerone.com/reports/643225> .

<https://hackerone.com/reports/167631> .

<https://hackerone.com/reports/168254> .

<https://hipotermia.pw/bb/http-desync-idor> .

<https://pastebin.com/E6LMFm2w> .

<https://vict0ni.me/multiple-header-injections-bug-hunting/> .

<https://vict0ni.me/multiple-header-injections-bug-hunting/> .

Summary about host header attack:-

**definition :- anyone request site report it on IP .**

**virtual host header name :- when we host most sites on the same server we give its virtual host header name .**

**how that happen ?**

**when request and response any site we can change in hast name with**

**(dev or stage or test or local host ) this give local host of website**

**And this consider attacks .**

Writeups about cache poisoning:-

<https://samcurry.net/abusing-http-path-normalization-and-cache-poisoning-to-steal-rocket-league-accounts/> .

<https://hackerone.com/reports/492841> .

<https://hackerone.com/reports/492841> .

<https://hackerone.com/reports/728664> .

<https://hackerone.com/reports/84601> .

<https://hackerone.com/reports/429747> .

<https://hackerone.com/reports/622122> .

<https://hackerone.com/reports/394016> .

<https://hackerone.com/reports/534297> .

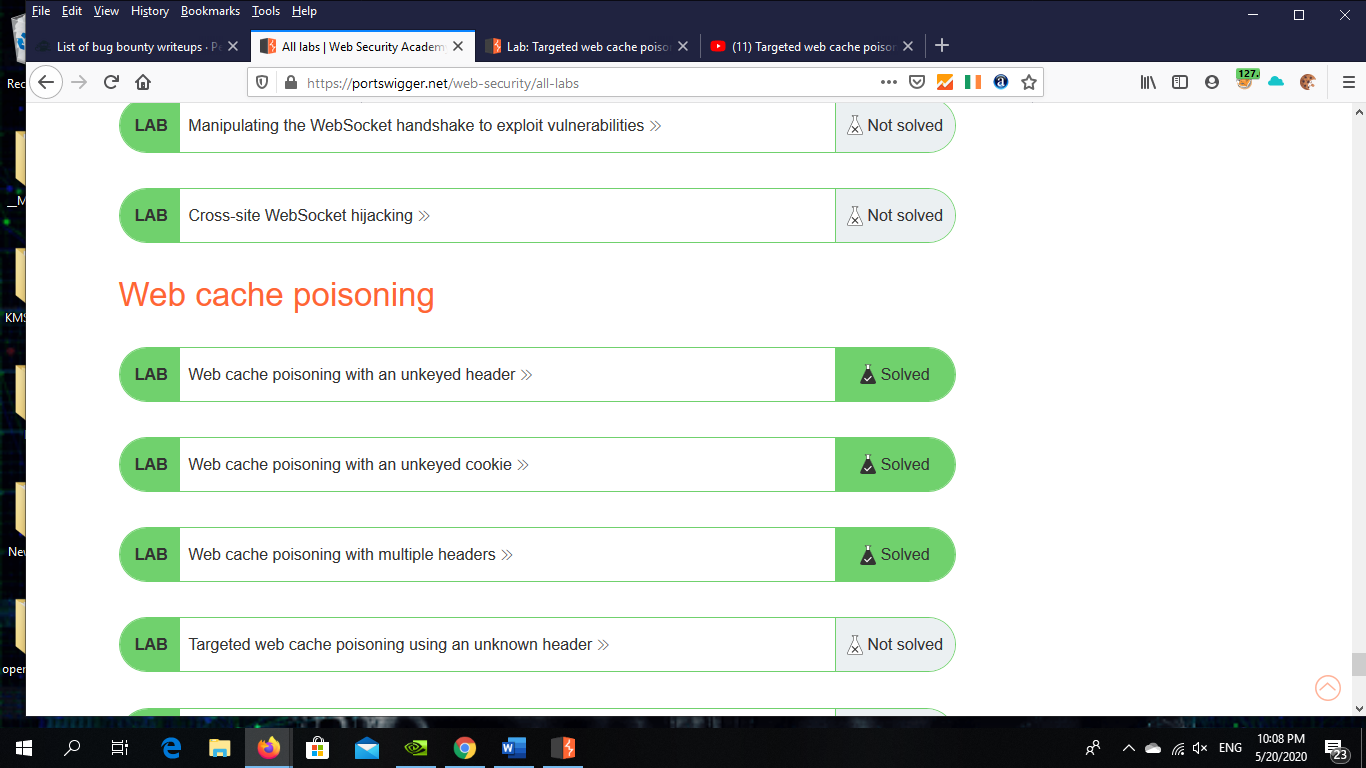
<https://hackerone.com/reports/488147> .

<https://hackerone.com/reports/550266> .

<https://hackerone.com/reports/591302> .

<https://hackerone.com/reports/137756> .

Cache labs:-



Summary about cache poisoning:-

**Web cache poisoning is an advanced technique whereby an attacker exploits the behavior of a web server and cache so that a harmful HTTP response is served to other users.**

**Fundamentally, web cache poisoning involves two phases. First, the attacker must work out how to elicit a response from the back-end server that inadvertently contains some kind of dangerous payload. Once successful, they need to make sure that their response is cached and subsequently served to the intended victims.**

**A poisoned web cache can potentially be a devastating means of distributing numerous different attacks, exploiting vulnerabilities such as XSS, JavaScript injection, open redirection, and so on.**