Code merged with nmap main repo :

1. http-cve2017-1001000.nse : Made a vulnerability detection script which attempts to detect a privilege escalation vulnerability in Wordpress 4.7.0 and 4.7.1 that allows unauthenticated users to inject content in posts. The vulnerability became very widespread and affected great number of websites using Wordpress API.

   Github commit link :

https://github.com/nmap/nmap/commit/aedd40ced55cee033adb1819999afc8b2efcedbb

2. Closed a bug in the Issues tab #878 (https://github.com/nmap/nmap/issues/878) The bug was due to indexing of a variable without checking whether its nil or not.

   Github commit link :

https://github.com/nmap/nmap/commit/be66ffd38a3759d395d1ebe6251cb5a0d2eaaa5b

3. http-security-headers.nse : This is a discovery script which checks for the HTTP response headers related to security given in OWASP Secure Headers Project and shows if they are configured. It also gives a brief description of the header and its configuration value.

   Github commit link :

https://github.com/nmap/nmap/commit/bd9ad1223d76315cc4327d0838cda02cc26208ba

4. Found a bug in the relative URL handling of the http-library. I was working on http-xss-scanner script and found the bug when I was unable to get the expected output in the script.

   Github commit link:

https://github.com/nmap/nmap/commit/2c98b309a81c0e04f04d5ecb55b5e34ef84bb1b5

5. Added the detection of Express Server in http-devframework-fingerprint.lua. Express is a very popular Nodejs Web application framework and it was good to have its detection in nmap.

   Github commit link:

https://github.com/nmap/nmap/commit/706fd7c130ed321bdb61a4874f2e00941981d6a6

6. Makes improvements to do http-sitemap-generator.nse by improving the normalise_path function.

   Github commit link:

https://github.com/nmap/nmap/commit/21992c9c7c8006cf2160db67ba1b9c1289666227

7. Added http-jsonp-detection.nse : Added the jsonp-detection script which attempts to discover JSoNP endpoints in web servers. JSONP endpoints can be used to bypass same-origin policy restrictions in web browsers. The vulnerability is relatively new and not many other network-security-scanners detect JSoNP endpoints.

   Github commit link:

https://github.com/nmap/nmap/commit/995988ea8c1968bb566680def8297691db97565d

8. Added the detection of Jenkins header to http-dev-frameworks-fingerprint. This also returns a lot of information about the Jenkins if the service is detected.

   Github commit link:

https://github.com/nmap/nmap/commit/7c833b933e771923e660077cf33bbc9d3b3b233d

Uncommitted Code(not merged with nmap main):

httpcookies.lua and http-cookie-alert.nse : On testing http-xss-scanner, I figured out that nmap wasn't handling cookies as expected. So, I first thought of implementing the support in http.lua and httpspider.lua . On submitting those changes and getting reviewed by the community, we all decided on a library that will be made for handling cookies. A documentation of the library was made (https://secwiki.org/w/Nmap/Cookies_library) and then I committed. Further decision was made to add a httpcookies argument in http.lua and httpspider.lua library. Also, automatic parsing of cookies was done in httpspider using a new argument called 'enable_cookies'.

Github commit link:

https://github.com/nmap/nmap/pull/963

Things left to do:

- More testing from the community is required before merging.

- Update existing scripts to use the new library.
- Add keywords to the script http-cookies-alert.
- Add support for cookies in string format via library arguments.
- Update/Improve library documentation.

TR069 vulnerability script : TR-069 (Technical Report 069) is a technical specification that defines an application layer protocol for remote management of end-user devices. "New NTP Server" feature in this can be used to execute arbitrary commands. The vulnerability became very popular but enough testing of the script couldn't be done. Once tested properly with enough number of devices, the script will be added to nmap.

Github commit link:

https://github.com/vinamrabhatia/nmap/commit/b4bea9c67c45f6a57474b5d67a6a797ad2eebde0

http-xss-scanner and xss payloads database file : Earlier xss scripts in nmap detects XSS using GET and another one using POST by detecting the forms. An effort was made to combine both the methods into one script called http-xss-scanner. Besides, a comprehensive list of payloads were also taken from various sources and put in together to make xss scanner very efficient. Again, the script needed quite a lot more testing and ample time was spent on it. So, we decided to move on with other parts of the project for then.

Github commit link:

https://github.com/nmap/nmap/compare/master...vinamrabhatia:http-xss-scanner

Tasks left to complete(will be done after GSoC) :

1. Refactor all the code related to cookies present in http library and shift it to httpcookies library. Also, modifications have to be made in old scripts which are using http library for cookies.

2. Work on http-iss-shortname-scanner : The iss-shortname-scanner got a few new modifications lately. The current nmap iss-shortname-scanner script doesn’t incorporate these changes, and hence needs to be updated.

Here is the github link to the repository which contains all the code that was added to nmap during GSoC 2017.

https://github.com/vinamrabhatia/nmap-gsoc2017