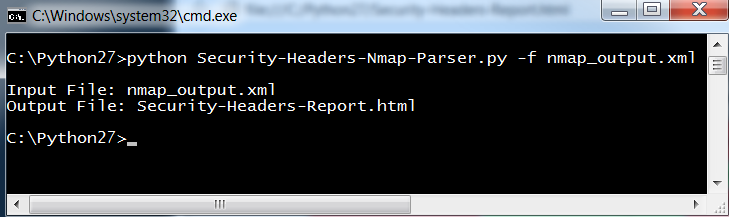
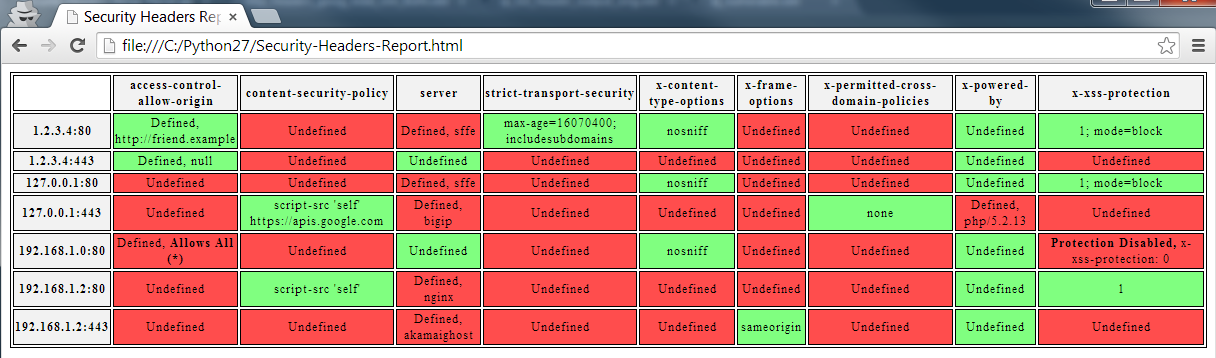
HTTP Security Headers Nmap Parser

A common theme in environments with a lot of web applications is lack of awareness in regards to http headers, especially those which are security-related. In many architectures, these headers can be configured without changing the application, so why not take a look at them? Laziness and ignorance are a few reasons, however the reward for implementing (or removing) some of these headers can be extremely beneficial. It is worth noting that certain headers are only supported by specific browsers and only offer a certain level of protection, so these headers **should not** be solely relied on from a security perspective.

What’s one of the first things we do when we first get on a network? Discovery with Nmap. Nmap has a built in NSE script ‘[http-headers](http://nmap.org/nsedoc/scripts/http-headers.html)’ which will return the headers via a HEAD request of a web server. Manually looking through a large Nmap output file to see which headers are being used can be really difficult, so I wrote a small parser in python which takes in the Nmap .xml output file and generates an html report with only security-related header information.

Steps:

1. Run Nmap with http-headers script and xml output: **nmap --script=http-headers <target> -oX output\_file.xml**
2. Run Security-Headers-Nmap-Parser.py: **python Security-Headers-Nmap-Parser\_done -f output\_file.xml**
3. View generated .html report. This can be copied into :