



**Trinity College Dublin**  
Coláiste na Tríonóide, Baile Átha Cliath  
The University of Dublin

School of Engineering  
Department of Electronic & Computer Engineering

# **An overview on the Web/DNS/TLS testers**

Author: Hlib Fedchuk

Supervisor: Stephen Farrell

A thesis submitted in partial fulfilment of the degree of BAI in  
Computer & Electronic Engineering

May 2018

## **Table of Contents (needs fixing):**

Abstract.....	3
Background.....	XX
- crap web sites	
-getting less crap	
Methods.....	XX
- internet measurement, now practical wasn't before	
- loadsa text about specific tests done (heartbleed, hsts,...)	
- initial list of possible testers	
= reduce list based on scriptability	
= try include most commonly used (sslabs, moz,..)	
- reproducible: what hlib does needs to be re-doable by all	
Design/implementation.....	XX
- set of test sites	
- set of testers	
- scripting/screen-scraping	
Results.....	XX
Conclusion and future work.....	XX
- it's great but could be better, here's how	
- ask testers to do X,Y,Z to improve commonality	
Acknowledgements.....	XX
References.....	XX
Appendices.....	XX

## ***Abstract:***

This project is about comparing and contrasting different web site testers. During the period of this project's progress, a list of tester and test sites will be picked in order to come up with results. The aim of this project is to differentiate between the tester's results output in order to see and pick out the key differences between them. A set of web testers will be broken into three different categories: DNS testers, TLS (mail) testers and overall website testers. This separation was introduced in order to have a set of results that would relate to each other and get rid of confusion, where it would be very impractical to compare a TLS tester with a DNS tester, where there may be some similarities between them, but we want to obtain results of the same lookup area. During this project, the results would depend on the:

1. Overall score:

Typically, a tester would provide the overall score to the user that would indicate how well or bad their website/mail server is implemented in terms of security aspects. This result value cannot be discarded and should be taken very seriously, as it is the final score that the tester provides on how well the security features are implemented in this website, whether they are coming from a DNS/TLS or overall web tester.

2. Security and privacy issues:

A majority of the web testers would provide a detailed description on how they came up with the end score (privacyscore doesn't). This description will provide the information on the points (that this specific tester thinks are important), whether they are implemented or not. For example, 2 different test may consider the same feature differently, some might penalize for it, giving it a negative mark, and some may just leave it and give a 0 mark for it.

3. Scope of implemented features:

This aspect will consider the current amount of implemented features that the web site has. We can consider a small web site and a much bigger one, but the smaller one can get more points depending on the implementation, if more measures are implemented – it wouldn't be a surprise that the score will be higher.

## ***Background:***

### ***Bad Websites:***

There was a need to do some research and find some bad websites that aren't good regarding the results that the testers would provide. This had to be done in order to see the vast difference that the tester would provide between the results of a tester. It would be rather interesting to see what results will be present in a good test site compared to what will be shown for a bad site.

A way to choose if a web site is badly implemented was to:

1. Surf the internet with a query for "bad sites" or something similar. There are many blog pages that would provide us with a list where these sites are discussed and some pictures are also provided. Mostly these sites are ranked by aesthetics and the way they look, but there are some outliers that actually talk about a website not being secure and these guys are the ones to definitely look into.
2. When the research was done and a list of "bad" websites was created, the next step would be to actually check if this website is bad security wise or it's just bad aesthetically. To check it, there is a simple way – creating a batch file with that list and running it through Privacyscore tester. It's rather easy and simple, because there will only be around 20 lines of a script and this script will be copy-paste, but the name of the test sites will be changed.
3. In order to pick a bad web site, a certain threshold had to be created to be able to call this web site bad, when the result comes back. For myself, I didn't think that long and decided to go for a score that is less than 40 (taking 40 as a pass mark). This would mean that all the test sites that undergo Privacyscore 's test and fail it are considered bad and will be kept in order to have the comparison that would help to understand how the testers work and what aspects they consider important.

## ***Methods:***

### ***Internet measurement:***

Internet has become a huge aspect of human lives for the past ten years. It includes different branches like: international commerce, communication and technological development. It is important that various groups that affect and use internet, like researches, entrepreneurs, service providers and other members of internet community understand the growth characteristics and its limitations.

At early stages internet measurement was neglected giving it a low priority to increasing network's speed, capacity and coverage. The increase in interest towards the internet only come pretty recently and it is a logical outcome as internet has expanded, which led to an increase in the number of users and malicious behavior. In order to counter these malicious elements, there needs to be a huge investment into Internet measurement and data analytics. Merit Network operated the NSFnet backbone in its various forms, measured the backbone's traffic volumes and produced summary statistics through April 1995. But these were primarily oriented toward short-term operational requirements or periodic simplistic traffic reports for funding agencies. As such, they weren't conducive to workload or performance characterization, much less network-dynamics modeling. As the NSFnet and attached regional infrastructures exploded in popularity among academic and commercial sectors, operators acutely focused on increasing link speeds and router/switch-traffic capacities. Developers worked on improving protocols and inventing new ones to support emerging services. The evolutionary context of the infrastructure left little room for more than mild interest in network measurement. For ordinary people, the Internet has become an integral part of everyday life; it is now used continually to find information, buy products, meet people, do our jobs, and play. As if these circumstances weren't sufficiently revolutionary, the pervasive adoption of mobile computing expectations and requirements is now prompting service providers to take a strong interest in more strategic measurement and charging schemes.

With its ever-growing user community, the Internet has gradually been forced over the past decade to deal with the "real world." Like chemical pollutants from industrial production processes, infrastructural pollution — such as viruses, worms, and spam traffic — has become significant in

volume and impact on user productivity. Protective technologies such as firewalls and NAT gateways have changed the Internet's simple end-to-end connectivity model. Although these devices can effectively block some malignant packets, they do so by filtering packets according to access control lists (ACLs), which can prevent many applications from working properly.

The Challenges Collection, interpretation, and modeling of empirical Internet data remains challenging. The technologies and protocols involved in generating and delivering Internet traffic were designed for technical expediency, architectural clarity, and functionality, rather than for measurement and analysis. New developments often introduce specifications that are independent of their predecessors; technology developers often deploy them as rapidly as possible, without concerted systematic testing on the vast set of heterogeneous components encountered on the Internet. Indeed, it would be impossible to test certain behaviors against all possible combinations of equipment, software, and configuration. Furthermore, many who develop technologies and protocols contend that the Internet has evolved splendidly thus far without extensive measurement and modeling. Others believe that we should not begin measurement and modeling efforts until doing so proves cheaper than simply expanding the currently available bandwidth. To make matters harder, a variety of legal and privacy issues serve as active disincentives to measurement research and development activity. Nonetheless, every constituency of the Internet (providers, vendors, policymakers, and users) realizes that we need a better understanding of Internet structure and behavior, including the influence of various components and functionalities on macroscopic dynamics. Floyd and Paxson's landmark paper provided several insights into why the Internet is hard to measure, and thus hard to simulate, making it resistant to modeling and predictive insight.<sup>2</sup> The first big challenge is that everything keeps changing. For example, HTTP traffic grew from zero in 1995 to more than 80 percent of the network traffic at many sites by the early 2000s. Yet, HTTP's proportion of total traffic is now dropping on most links, and peer-to-peer traffic is steadily rising as developers find more ways to use P2P technology. The Internet's global scale also complicates measurement efforts, as does the fact that many aspects of traffic and behavior change from location to location. Thus, statistics gathered at one location often prove unrepresentative of the global Internet. Instead, we need to make measurements at many sites and correlate the results to derive a comprehensive view. Finally, few Internet protocols and applications were designed to inherently support fine-grained measurement. Instead, researchers have had to find indirect ways to measure network phenomena. For example, traffic-flow measurements rely on data collected from packet headers as they pass across links; counting packets and bytes and classifying them into flows

on the basis of values taken from the headers is easy but yields limited insight into higher-layer behavior. Measuring application performance generally remains a challenge, since applications differ as to how they transport application-specific data. For example, while effective tools exist for measuring Web server performance, such tools are often not effective at measuring performance of other applications.

## ***Reproducibility:***

This section is important, as the following text will be about recreating my work up to date in order to generate the results.

Installation instructions for SSLabs, Mozilla-observatory and privacy score.

### **Windows:**

#### **SSLabs:**

Before installing SSLabs, Go has to be of version, which is at least 1.3 or higher should be installed.

<https://golang.org/doc/install?download=go1.10.windows-amd64.msi> -> use this link to download go.

To ensure that Go was installed properly: go build command should be typed when in C://go/src directory from cmd.

When that has worked out, next step would be to clone the repo of SSLabs by using gitbash with a simple command: git clone <https://github.com/ssllabs/ssllabs-scan.git>

Next step is to change directory to C://users/go/src/ssl-labs and use the command to build it again: "go build"

When that was done, we go to cmd from the directory above, we use a command: SSLabs-scan --json-flat jell.ie (or other test site)

There is at least 3-4 delay for me until a json would appear.

On the next run of the same tester, there result output is almost instant.

A command for SSLabs-scan --json-flat --host file (that would allow to test multiple test sites from a file where they are separated by a line)

### **Mozilla Observatory:**

Before installing Mozilla-observatory, Npm or node.js that has Npm in it has to be installed by following: <https://www.npmjs.com/get-npm>

Next step: in command line use the command Npm install -g observatory-cli. Before doing the installation, a directory should be created for example C://user/"..."/Mozilla-obs.

We clone the repository by using git clone <https://github.com/mozilla/observatory-cli.git> into the above directory.

The command "npm install -g observatory-cli" is used to install Mozilla-obs.

When that command went through, observatory jell.ie --zero --format=report command is used to generate a report that includes 0 scores also. The output here is json format.

A command observatory some.site.name --rescan is used to force a rescan. This could be used as fetching results from cache.

### **Privacyscore:**

Privacyscore also uses go, so the same procedure is followed. The only difference is just creating a new directory for privacyscore in C://users/"..."/go/

Then we clone the repo <https://github.com/asciimoo/privacyscore> and then use the command in this directory: go build.

When build succeeds, privacyscore.exe appears in the directory.

To run it in cmd, a command privacyscore.exe some.site.name is used to run the scan.



## Virtual Machine:

That scan only provides a score for the test site, thus a command created by my project supervisor is used.

This command is used for Ubuntu, thus VM is installed.

This command is: `" cat index.html | sed -e 's/<span/\n<span/g' | sed -e 's/<span .*">/' | sed -e 's/</span>/' | sed -e 's/"/"/g' | grep -v "<" | grep -v ">" | head -1652 | tail -1629 | json_pp "`

To get this file, a filename.html was saved when results were generated and this script gets rid of "spans" and "quotes" and json\_pp is used to get the json from this.

For some reason this doesn't work for me and i get an error. If json\_pp (pretty print) is not used, i get the required information for the results, but not in json format.

## ***List of testers:***

The list of testers was created after the research was done. This list is a good help later on when the installation process will occur. This list will then be the end list that would show which tester will actually be used to generate the results from the scripts run from the command line.

## ***DNS testers:***

Tester name	JSON export available from tester
<a href="http://dnsviz.net/">http://dnsviz.net/</a>	No
<a href="https://manytools.org/network/query-dns-records-online/go">https://manytools.org/network/query-dns-records-online/go</a>	No
<a href="https://www.ultratools.com/domainHealthReport">https://www.ultratools.com/domainHealthReport</a>	No
<a href="https://www.zonemaster.fr">https://www.zonemaster.fr</a>	Possible to get results from HTML, because there is iFrame present
<a href="https://mxtoolbox.com">https://mxtoolbox.com</a> Domain Health --- possibility of getting rid of it just because mxbox is used as a mail tester.	No, has commands to use but only on their web 🗨
<a href="http://www.dnsstuff.com">http://www.dnsstuff.com</a>	Allows export of a .pdf file
<a href="https://dnschecker.org">https://dnschecker.org</a>	Yes <a href="https://dnschecker.org/dns-tool.php">https://dnschecker.org/dns-tool.php</a>
<a href="http://dnscheck.pingdom.com">http://dnscheck.pingdom.com</a>	No
<a href="https://observatory.mozilla.org">https://observatory.mozilla.org</a> -> from your list	Yes

Tester name	JSON export available from tester
<a href="https://pingability.com">https://pingability.com</a> IP stuff	Yes, Report of results in email though: /
<a href="https://mxtoolbox.com">https://mxtoolbox.com</a> SMTP	No
<a href="http://www.dnsstuff.com/mstc">http://www.dnsstuff.com/mstc</a>	Needs code to get it from HTML
<a href="https://www.ultratools.com">https://www.ultratools.com</a>	Code to get JSON format, not a lot of results there
<a href="https://www.wormly.com/test-smtp-server">https://www.wormly.com/test-smtp-server</a> SMTP	No
<a href="http://emailsecuritygrader.com">http://emailsecuritygrader.com</a> Web and mail, a pretty good one, stay for sure.	No

Tester name	JSON export available for export
<a href="https://website.grader.com">https://website.grader.com</a>	Looks like it requires a subscription
<a href="https://www.dareboost.com">https://www.dareboost.com</a>	Yes allows export of CSV
<a href="https://www.uptrends.com">https://www.uptrends.com</a>	Yes <a href="https://api.uptrends.com/v3/checkpointservices?format=json">https://api.uptrends.com/v3/checkpointservices?format=json</a>
<a href="https://testmysite.withgoogle.com">https://testmysite.withgoogle.com</a>	Yes F-12 audits
<a href="https://privacyscore.org">https://privacyscore.org</a> --- a pretty good one for results	<a href="https://github.com/PrivacyScore/PrivacyScore">https://github.com/PrivacyScore/PrivacyScore</a> Data goes on the their disk and could be pulled after
<a href="https://www.ssllabs.com">https://www.ssllabs.com</a>	Yes

From this list, we can see that the list is reduced to only those testers that can only be scripted in order to automate the result fetching process.

### ***Set of test sites:***

Initially, the set of test sites was composed of mainly 4 sites. 2 of these sites were run by my supervisor and the other 2 are trinity sites, tcd.ie and scss.tcd.ie. A simple text file was created and pushed to GitHub in order to keep track, either adding or getting rid of some sites, which didn't happen throughout the project. The results could be written in a table at the end, which can be seen below.

<b>Supervisor Sites</b>	<b>TCD sites</b>	<b>My site</b>	<b>Other Irish test sites</b>
Jell.ie	Tcd.ie	Herdwatch.ie	Heanet.ie
Responsible.ie	scss.tcd.ie	Jamilin.com	iedr.ie
		Pennyjuice.com	inex.ie
		007museum.com	
		Arngren.net	
		georgermartin.com	
		theroommovie.com	
		electrifyingtimes.com	

## **Some background on different tests:**

### **Heartbleed:**

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

#### ***What is being leaked?***

Encryption is used to protect secrets that may harm your privacy or security if they leak. In order to coordinate recovery from this bug we have classified the compromised secrets to four categories: 1) primary key material, 2) secondary key material and 3) protected content and 4) collateral.

#### ***What is leaked primary key material and how to recover?***

These are the crown jewels, the encryption keys themselves. Leaked secret keys allow the attacker to decrypt any past and future traffic to the protected services and to impersonate the service at will. Any protection given by the encryption and the signatures in the X.509 certificates can be bypassed. Recovery from this leak requires patching the vulnerability, revocation of the compromised keys and reissuing and redistributing new keys. Even doing all this will still leave any traffic intercepted by the attacker in the past still vulnerable to decryption. All this has to be done by the owners of the services.

#### ***What is leaked secondary key material and how to recover?***

These are for example the user credentials (user names and passwords) used in the vulnerable services. Recovery from this leak requires owners of the service first to restore trust to the service according to steps described above. After this users can start changing their passwords and

possible encryption keys according to the instructions from the owners of the services that have been compromised. All session keys and session cookies should be invalidated and considered compromised.

### ***What is leaked protected content and how to recover?***

This is the actual content handled by the vulnerable services. It may be personal or financial details, private communication such as emails or instant messages, documents or anything seen worth protecting by encryption. Only owners of the services will be able to estimate the likelihood what has been leaked and they should notify their users accordingly. Most important thing is to restore trust to the primary and secondary key material as described above. Only this enables safe use of the compromised services in the future.

### ***What is leaked collateral and how to recover?***

Leaked collateral are other details that have been exposed to the attacker in the leaked memory content. These may contain technical details such as memory addresses and security measures such as canaries used to protect against overflow attacks. These have only contemporary value and will lose their value to the attacker when OpenSSL has been upgraded to a fixed version.

## **HSTS:**

HTTP Strict Transport Security (HSTS) is a web server directive that informs user agents and web browsers how to handle its connection through a response header sent at the very beginning and back to the browser.

This sets the Strict-Transport-Security policy field parameter. It forces those connections over HTTPS encryption, disregarding any script's call to load any resource in that domain over HTTP. HSTS is but one arrow in a bundled sheaf of security settings for your web server or your web hosting service.

You never close your physical store or home without locking the doors, right? You may even have metal detectors at the door to control shrinkage. Data can be just as valuable as physical items in your shop or house, so it's just as important to keep them locked up and secure. Padlocking your website is sometimes not enough as people will still find a way to reach your website over http://. HSTS forces browsers and app connections to use HTTPS if that is available. Even if someone just types in the www or http://.

HTTPS is a small ranking factor in Google and is categorized as a 'site quality' score along with many other factors such as page speed and mobile responsiveness.

Setting up 301 redirects from http:// to https:// is not enough to completely secure your domain name. The window of opportunity still exists in the insecure redirection of HTTP.

The hacker(s) are still able to capture site cookies, session ID (usually sent as a URL parameter) or force a redirection to their phishing site that looks exactly like your website.

By having a Strict-Transport-Security header installed, it will be nearly impossible for the bad guys to glean any information at all!



## **Results:**

### ***Privacyscore:***

Jell.ie	Respobnsble.ie	Scss.tcd.ie	Tcd.ie	Herdwatch.ie	Heanet.ie	Iedr.ie	Inex.ie
100	91	65	53	50	85	51	58

Jamilin.com	Pennyjuice.com	007museum.com	Argngren.net	Georgematin.com	Theroommovie.com	Electrifyingtimes.com
11	35	-33	-22	63	28	8

# HTTPObservatory:

## 007museum:

[httpobs007museum.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File	Search	View	Tools	Snippets	Configuration	Help
Text	1	Score: 0 [F]				
Tree	2	Modifiers:				
List	3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers				
	4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla				
	5	[ 0] HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain				
	6	[ 0] No cookies detected				
	7	[ 0] Referrer-Policy header not implemented				
	8	[ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https				
	9	[ -5] X-Content-Type-Options header not implemented				
	10	[ -10] X-XSS-Protection header not implemented				
	11	[ -20] Does not redirect to an https site				
	12	[ -20] HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain				
	13	[ -20] X-Frame-Options (XFO) header not implemented				
	14	[ -25] Content Security Policy (CSP) header not implemented				
	15					

## Arngren.net:

[httpobsArngren.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File	Search	View	Tools	Snippets	Configuration	Help
Text	1	Score: 0 [F]				
Tree	2	Modifiers:				
List	3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers				
	4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla				
	5	[ 0] HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain				
	6	[ 0] Referrer-Policy header not implemented				
	7	[ 0] Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin				
	8	[ -5] X-Content-Type-Options header not implemented				
	9	[ -10] X-XSS-Protection header not implemented				
	10	[ -20] Cookies set without using the Secure flag or set over http				
	11	[ -20] Does not redirect to an https site				
	12	[ -20] HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain				
	13	[ -20] X-Frame-Options (XFO) header not implemented				
	14	[ -25] Content Security Policy (CSP) header not implemented				
	15					

## Electrifyingtimes.com:

[httpobselectrifyingtimes.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File	Search	View	Tools	Snippets	Configuration	Help
Text	1	Score: 0 [F]				
Tree	2	Modifiers:				
List	3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers				
	4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla				
	5	[ 0] HTTP Public Key Pinning (HPKP) header can't be implemented without https				
	6	[ 0] Referrer-Policy header not implemented				
	7	[ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https				
	8	[ -5] X-Content-Type-Options header not implemented				
	9	[ -10] X-XSS-Protection header not implemented				
	10	[ -20] Cookies set without using the Secure flag or set over http				
	11	[ -20] HTTP Strict Transport Security (HSTS) header cannot be set for sites not available over https				
	12	[ -20] Redirects, but final destination is not an https URL				
	13	[ -20] X-Frame-Options (XFO) header not implemented				
	14	[ -25] Content Security Policy (CSP) header not implemented				
	15					

## Georgermartin.com:

[httpbsgeorgermartin.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
1 Score: 0 [F]
2 Modifiers:
3 [ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
4 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
5 [ 0] HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain
6 [ 0] No cookies detected
7 [ 0] Referrer-Policy header not implemented
8 [-5] X-Content-Type-Options header not implemented
9 [-10] X-XSS-Protection header not implemented
10 [-20] Does not redirect to an https site
11 [-20] HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain
12 [-20] X-Frame-Options (XFO) header not implemented
13 [-25] Content Security Policy (CSP) header not implemented
14 [-50] Subresource Integrity (SRI) is not implemented, and external scripts are loaded over http
15
```

## Heanet.ie

[httpbsheanetie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
1 Score: 15 [F]
2 Modifiers:
3 [ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
4 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
5 [ 0] HTTP Public Key Pinning (HPKP) header not implemented
6 [ 0] Initial redirection is to https on same host, final destination is https
7 [ 0] No cookies detected
8 [ 0] Referrer-Policy header not implemented
9 [-5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
10 [-5] X-Content-Type-Options header not implemented
11 [-10] X-XSS-Protection header not implemented
12 [-20] HTTP Strict Transport Security (HSTS) header not implemented
13 [-20] X-Frame-Options (XFO) header not implemented
14 [-25] Content Security Policy (CSP) header not implemented
15
```

## Herdwatch.ie:

[httpbsherdwatch.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
1 Score: 15 [F]
2 Modifiers:
3 [ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
4 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
5 [ 0] HTTP Public Key Pinning (HPKP) header not implemented
6 [ 0] Initial redirection is to https on same host, final destination is https
7 [ 0] No cookies detected
8 [ 0] Referrer-Policy header not implemented
9 [-5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
10 [-5] X-Content-Type-Options header not implemented
11 [-10] X-XSS-Protection header not implemented
12 [-20] HTTP Strict Transport Security (HSTS) header not implemented
13 [-20] X-Frame-Options (XFO) header not implemented
14 [-25] Content Security Policy (CSP) header not implemented
15
```

## ledr.ie:

[httpobsiedrie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
Text 1 Score: 0 [F]
2 Modifiers:
3 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
4 [ 0] HTTP Public Key Pinning (HPKP) header not implemented
5 [ 0] Initial redirection is to https on same host, final destination is https
6 [ 0] Public content is visible via cross-origin resource sharing (CORS) Access-Control-Allow-Origin header
7 [ 0] Referrer-Policy header not implemented
8 [ 0] X-Frame-Options (XFO) header set to SAMEORIGIN or DENY
9 [ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
10 [ -5] X-Content-Type-Options header not implemented
11 [ -10] X-XSS-Protection header not implemented
12 [ -20] HTTP Strict Transport Security (HSTS) header not implemented
13 [ -25] Content Security Policy (CSP) header not implemented
14 [ -40] Session cookie set without using the Secure flag or set over http
15
```

## Inex.ie:

[httpobsinexie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
Text 1 Score: 35 [D]
2 Modifiers:
3 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
4 [ 0] HTTP Public Key Pinning (HPKP) header not implemented
5 [ 0] HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
6 [ 0] Initial redirection is to https on same host, final destination is https
7 [ 0] No cookies detected
8 [ 0] Public content is visible via cross-origin resource sharing (CORS) Access-Control-Allow-Origin header
9 [ 0] Referrer-Policy header not implemented
10 [ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
11 [ -5] X-Content-Type-Options header not implemented
12 [ -10] X-XSS-Protection header not implemented
13 [ -20] X-Frame-Options (XFO) header not implemented
14 [ -25] Content Security Policy (CSP) header not implemented
15
```

## Jamiliin.com:

[httpobsjamiliin.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
Text 1 Score: 0 [F]
2 Modifiers:
3 [ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
4 [ 0] Contribute.json isn't required on websites that don't belong to Mozilla
5 [ 0] HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain
6 [ 0] No cookies detected
7 [ 0] Referrer-Policy header not implemented
8 [ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
9 [ -5] X-Content-Type-Options header not implemented
10 [ -10] X-XSS-Protection header not implemented
11 [ -20] Does not redirect to an https site
12 [ -20] HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain
13 [ -20] X-Frame-Options (XFO) header not implemented
14 [ -25] Content Security Policy (CSP) header not implemented
15
```

## Jell.ie:

[httpobsjellie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	1	Score: 105 [A+]
	2	Modifiers:
	3	[ +5] Preloaded via the HTTP Strict Transport Security (HSTS) preloading process
Tree	4	[ +5] Referrer-Policy header set to "no-referrer", "same-origin", "strict-origin" or "strict-origin-when-cross-origin"
	5	[ +5] X-Frame-Options (XFO) implemented via the CSP frame-ancestors directive
List	6	[ 0] All hosts redirected to are in the HTTP Strict Transport Security (HSTS) preload list
	7	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
	8	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla
	9	[ 0] HTTP Public Key Pinning (HPKP) header not implemented
	10	[ 0] No cookies detected
	11	[ 0] Subresource Integrity (SRI) is not needed since site contains no script tags
	12	[ 0] X-Content-Type-Options header set to "nosniff"
	13	[ 0] X-XSS-Protection header set to "1; mode=block"
	14	[ -10] Content Security Policy (CSP) implemented, but allows 'unsafe-eval'
	15	

## PennyJuice.com:

[httpobsPennyjuice.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	1	Score: 0 [F]
	2	Modifiers:
	3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
Tree	4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla
	5	[ 0] HTTP Public Key Pinning (HPKP) header can't be implemented without https
List	6	[ 0] Referrer-Policy header not implemented
	7	[ -5] X-Content-Type-Options header not implemented
	8	[ -10] X-XSS-Protection header not implemented
	9	[ -20] Does not redirect to an https site
	10	[ -20] HTTP Strict Transport Security (HSTS) header cannot be set for sites not available over https
	11	[ -20] X-Frame-Options (XFO) header not implemented
	12	[ -25] Content Security Policy (CSP) header not implemented
	13	[ -40] Session cookie set without using the Secure flag or set over http
	14	[ -50] Subresource Integrity (SRI) is not implemented, and external scripts are loaded over http
	15	

## Responsible.ie:

[httpobsresponsibleie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	1	Score: 100 [A+]
	2	Modifiers:
	3	[ +5] Referrer-Policy header set to "no-referrer", "same-origin", "strict-origin" or "strict-origin-when-cross-origin"
Tree	4	[ +5] X-Frame-Options (XFO) implemented via the CSP frame-ancestors directive
	5	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
List	6	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla
	7	[ 0] HTTP Public Key Pinning (HPKP) header not implemented
	8	[ 0] HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
	9	[ 0] Initial redirection is to https on same host, final destination is https
	10	[ 0] No cookies detected
	11	[ 0] Subresource Integrity (SRI) is not needed since site contains no script tags
	12	[ 0] X-Content-Type-Options header set to "nosniff"
	13	[ 0] X-XSS-Protection header set to "1; mode=block"
	14	[ -10] Content Security Policy (CSP) implemented, but allows 'unsafe-eval'
	15	

## Scss.tcd.ie:

[httpobsscscstcdie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1	Score: 20 [F]	
2	Modifiers:	
3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers	
4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla	
5	[ 0] HTTP Public Key Pinning (HPKP) header not implemented	
6	[ 0] Initial redirection is to https on same host, final destination is https	
7	[ 0] No cookies detected	
8	[ 0] Referrer-Policy header not implemented	
9	[ 0] Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	
10	[ -5] X-Content-Type-Options header not implemented	
11	[ -10] X-XSS-Protection header not implemented	
12	[ -20] HTTP Strict Transport Security (HSTS) header not implemented	
13	[ -20] X-Frame-Options (XFO) header not implemented	
14	[ -25] Content Security Policy (CSP) header not implemented	
15		

## Tcd.ie:

[httpobstcdie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1	Score: 0 [F]	
2	Modifiers:	
3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers	
4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla	
5	[ 0] HTTP Public Key Pinning (HPKP) header not implemented	
6	[ 0] No cookies detected	
7	[ 0] Referrer-Policy header not implemented	
8	[ -5] Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https	
9	[ -5] X-Content-Type-Options header not implemented	
10	[ -10] X-XSS-Protection header not implemented	
11	[ -20] Does not redirect to an https site	
12	[ -20] HTTP Strict Transport Security (HSTS) header not implemented	
13	[ -20] X-Frame-Options (XFO) header not implemented	
14	[ -25] Content Security Policy (CSP) header not implemented	
15		

## Theroommovie.com:

[httpobstheroommovie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\HTTPOBS\2018-05-01-11-31-32] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1	Score: 0 [F]	
2	Modifiers:	
3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers	
4	[ 0] Contribute.json isn't required on websites that don't belong to Mozilla	
5	[ 0] HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain	
6	[ 0] Referrer-Policy header not implemented	
7	[ 0] Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	
8	[ -5] X-Content-Type-Options header not implemented	
9	[ -10] X-XSS-Protection header not implemented	
10	[ -20] Cookies set without using the Secure flag or set over http	
11	[ -20] Does not redirect to an https site	
12	[ -20] HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain	
13	[ -20] X-Frame-Options (XFO) header not implemented	
14	[ -25] Content Security Policy (CSP) header not implemented	
15		




# SSLLabs:

007museum:

[ssl007museum.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```
Text 1 [
2   = {
3     "host": "www.007museum.com",
4     "port": 443,
5     "protocol": "HTTP",
6     "isPublic": false,
7     "status": "READY",
8     "startTime": 1525170620765,
9     "testTime": 1525170628223,
10    "engineVersion": "1.31.0",
11    "criteriaVersion": "2009p",
12    "cacheExpiryTime": 1525171228223,
13    "endpoints": [
14      = {
15        "ipAddress": "194.9.94.213",
16        "serverName": "s368.loopia.se",
17        "statusMessage": "Certificate not valid for domain name",
18        "progress": -1,
19        "duration": 6848,
20        "eta": -1,
21        "delegation": 2,
22        = {
23          "hostStartTime": 1525170620765,
24          "key": {},
25          "cert": {},
26          "chain": {},
27          "protocols": [
28            = {
29              "id": 769,
30              "name": "TLS",
31              "version": "1.0"
32            },
33            = {
34              "id": 770,
35              "name": "TLS",
36              "version": "1.1"
37            },
38            = {
39              "id": 771,
40              "name": "TLS",
41              "version": "1.2"
42            }
43          ],
44          "suites": {},
45          "prefixDelegation": true,
46          "nonPrefixDelegation": false
47        }
48      ]
49    ],
50    "certHostnames": [
51      "*.loopiasecure.com",
52      "loopiasecure.com"
53    ]
54  }
55 ]
56
57
```

 [sslArngren.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSON

File Search View Tools Snippets Configuration Help

```

1  [
2  = {
3      "host": "www.Arngren.net",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1525170634776,
9      "testTime": 1525170639215,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "cacheExpiryTime": 1525171239215,
13     "endpoints": [
14     = {
15         "ipAddress": "67.195.61.46",
16         "serverName": "pl0pn-i.geo.vip.gql.yahoo.com",
17         "statusMessage": "Certificate not valid for domain name",
18         "progress": -1,
19         "duration": 4284,
20         "eta": -1,
21         "delegation": 2,
22     = {
23         "details": {
24             "hostStartTime": 1525170634776,
25             "key": {},
26             "cert": {},
27             "chain": {},
28             "protocols": [
29             = {
30                 "id": 769,
31                 "name": "TLS",
32                 "version": "1.0"
33             },
34             = {
35                 "id": 770,
36                 "name": "TLS",
37                 "version": "1.1"
38             },
39             = {
40                 "id": 771,
41                 "name": "TLS",
42                 "version": "1.2"
43             }
44         ],
45         "suites": {},
46         "prefixDelegation": true,
47         "nonPrefixDelegation": false
48     }
49     ],
50     "certHostnames": [
51         "secure.hostingprod.com",
52         "*.secure.hostingprod.com"
53     ]
54 }
55 ]
56

```



🔍 [sslelectrifyingtimes.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1		[
2		= {
3		"host": "www.electrifyingtimes.com",
4		"port": 443,
5		"protocol": "HTTP",
6		"isPublic": false,
7		"status": "READY",
8		"startTime": 1525170676723,
9		"testTime": 1525170692020,
10		"engineVersion": "1.31.0",
11		"criteriaVersion": "2009p",
12		"cacheExpiryTime": 1525171292020,
13		"endpoints": [
14		= {
15		"ipAddress": "66.175.58.9",
16		"serverName": "hostedc38.carrierzone.com",
17		"statusMessage": "Unable to connect to the server",
18		"statusDetails": "TESTING_PROTO_2_0",
19		"statusDetailsMessage": "Testing SSL 2.0",
20		"progress": -1,
21		"duration": 15014,
22		"eta": -1,
23		"delegation": 2,
24		= "details": {
25		"hostStartTime": 1525170676723,
26		"key": {},
27		"cert": {},
28		"chain": {},
29		"protocols": [],
30		"suites": {},
31		"prefixDelegation": true,
32		"nonPrefixDelegation": false
33		}
34		}
35		]
36		}
37		]
38		
39		

🔍 [sslgeorgermartin.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1	[	
2	= {	
3	"host": "www.georgermartin.com",	
4	"port": 443,	
5	"protocol": "HTTP",	
6	"isPublic": false,	
7	"status": "READY",	
8	"startTime": 1525170643224,	
9	"testTime": 1525170653905,	
10	"engineVersion": "1.31.0",	
11	"criteriaVersion": "2009p",	
12	"cacheExpiryTime": 1525171253905,	
13	"endpoints": [	
14	= {	
15	"ipAddress": "185.53.178.7",	
16	"statusMessage": "No secure protocols supported",	
17	"statusDetails": "TESTING_PROTO_3_4",	
18	"statusDetailsMessage": "Testing TLS 1.3",	
19	"progress": -1,	
20	"duration": 10283,	
21	"eta": -1,	
22	"delegation": 2,	
23	= "details": {	
24	"hostStartTime": 1525170643224,	
25	"key": {},	
26	"cert": {},	
27	"chain": {},	
28	"protocols": [],	
29	"suites": {},	
30	"prefixDelegation": true,	
31	"nonPrefixDelegation": false	
32	}	
33	}	
34	]	
35	}	
36	]	
37		

🔍 [sslheanetie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```

Text
Tree
List
1  [
2  = {
3      "host": "www.heanet.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1525170092828,
9      "testTime": 1525170276827,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13     =
14         {
15             "ipAddress": "2001:770:18:2:0:0:c101:db51",
16             "serverName": "iconia.heanet.ie",
17             "statusMessage": "Ready",
18             "grade": "A",
19             "gradeTrustIgnored": "A",
20             "hasWarnings": false,
21             "isExceptional": false,
22             "progress": 100,
23             "duration": 91450,
24             "eta": 1,
25             "delegation": 2,
26             "details": {
27             =
28                 "key": {
29                     "size": 2048,
30                     "alg": "RSA",
31                     "debianFlaw": false,
32                     "strength": 2048
33                 },
34                 "cert": {
35                     "subject": "CN=*.heanet.ie, O=HEAnet Ltd, L=Dublin, ST=Dublin, C=IE",
36                     "commonNames": [
37                         "*.heanet.ie"
38                     ],
39                     "altNames": [
40                         "*.heanet.ie",
41                         "heanet.ie"
42                     ],
43                     "notBefore": 1454371200000,
44                     "notAfter": 1549454400000,
45                     "issuerSubject": "CN=TERENA SSL CA 3, O=TERENA, L=Amsterdam, ST=Noord-Holland, C=NL",
46                     "issuerLabel": "TERENA SSL CA 3",
47                     "sigAlg": "SHA256withRSA",
48                     "revocationInfo": 3,
49                     "crlURIs": [
50                         "http://crl3.digicert.com/TERENASSLCA3.crl"
51                     ],
52                     "ocspURIs": [
53                         "http://ocsp.digicert.com"
54                     ],
55                     "revocationStatus": 2,
56                     "crlRevocationStatus": 2,
57                     "ocspRevocationStatus": 2,
58                     "sgc": 0,
59                     "issues": 0,
60                     "sct": false,
61                     "mustStaple": 0,
62                     "sha1Hash": "25fe4da0b24d82494468753f174d529187d030f8",
63                     "pinSha256": "TavGGBnA66M4Ro9ZdAKbR/lw8Mi6a0s3l938HRnYKwg="
64                 },
65                 "chain": {
66                 =
67                     "certs": [
68                     =
69                         {
70                             "subject": "CN=*.heanet.ie, O=HEAnet Ltd, L=Dublin, ST=Dublin, C=IE",
71                             "label": "*.heanet.ie",
72                             "notBefore": 1454371200000.

```

## Herdwatch.ie:

[sslherdwatch.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-04-14-18-09-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
1  [
2  = {
3      "host": "www.herdwatch.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1523726819028,
9      "testTime": 1523726962624,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13     = {
14         "ipAddress": "34.251.142.107",
15         "serverName": "ec2-34-251-142-107.eu-west-1.compute.amazonaws.com",
16         "statusMessage": "Ready",
17         "grade": "B",
18         "gradeTrustIgnored": "B",
19         "hasWarnings": true,
20         "isExceptional": false,
21         "progress": 100,
22         "duration": 143220,
23         "eta": 0,
24         "delegation": 2,
25     = {
26         "hostStartTime": 1523726819028,
27         = {
28             "size": 4096,
29             "alg": "RSA",
30             "debianFlaw": false,
31             "strength": 4096
32         },
33     = {
34         "cert": {
35             "subject": "CN=www.herdwatch.ie, OU=PositiveSSL, OU=Domain Control Validated",
36             "commonNames": [
37                 "www.herdwatch.ie"
38             ],
39             "altNames": [
40                 "www.herdwatch.ie",
41                 "herdwatch.ie"
42             ],
43             "notBefore": 1496966400000,
44             "notAfter": 1591660799000,
45             "issuerSubject": "CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB",
46             "issuerLabel": "COMODO RSA Domain Validation Secure Server CA",
47             "sigAlg": "SHA256withRSA",
48             "revocationInfo": 3,
49             "crlURIs": [
50                 "http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl"
51             ],
52             "ocspURIs": [
53                 "http://ocsp.comodoca.com"
54             ],
55             "revocationStatus": 2,
56             "crlRevocationStatus": 2,
57             "ocspRevocationStatus": 2,
58             "sgc": 0,
59             "validationType": "D",
60             "issues": 0,
61             "sct": false,
62             "mustStaple": 0,
63             "sha1Hash": "722e7bd0a238900b3735dad9ad3ee119df9ad83",
64             "pinSha256": "TDGzN3nbWiFE0eRHILe7JCIUcGFHxbfCZNNtkzHwkkw="
65         },
66     = {
67         "chain": {
68             "certs": [
69                 {
70                     "subject": "CN=www.herdwatch.ie, OU=PositiveSSL, OU=Domain Control Validated",
71                     "label": "www.herdwatch.ie".
```

## iedr.ie:

🔍 [sslredrie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-04-14-18-09-32] - JSONedit

File Search View Tools Snippets Configuration Help

```
Text
Tree
List
1  [
2  = {
3    "host": "www.iedr.ie",
4    "port": 443,
5    "protocol": "HTTP",
6    "isPublic": false,
7    "status": "READY",
8    "startTime": 1523727163834,
9    "testTime": 1523727287512,
10   "engineVersion": "1.31.0",
11   "criteriaVersion": "2009p",
12   "endpoints": [
13     = {
14       "ipAddress": "2a01:4b0:0:6:0:0:0:19",
15       "serverName": "www2.iedr.ie",
16       "statusMessage": "Ready",
17       "grade": "A",
18       "gradeTrustIgnored": "A",
19       "hasWarnings": false,
20       "isExceptional": false,
21       "progress": 100,
22       "duration": 61741,
23       "eta": 6,
24       "delegation": 2,
25       = {
26         "hostStartTime": 1523727163834,
27         = {
28           "key": {
29             "size": 4096,
30             "alg": "RSA",
31             "debianFlaw": false,
32             "strength": 4096
33           },
34           "cert": {
35             "subject": "CN=*.iedr.ie, OU=COMODO SSL Wildcard, OU=Domain Control Validated",
36             "commonNames": [
37               "*.iedr.ie"
38             ],
39             "altNames": [
40               "*.iedr.ie",
41               "iedr.ie"
42             ],
43             "notBefore": 1491782400000,
44             "notAfter": 1527983999000,
45             "issuerSubject": "CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB",
46             "issuerLabel": "COMODO RSA Domain Validation Secure Server CA",
47             "sigAlg": "SHA256withRSA",
48             "revocationInfo": 3,
49             "crlURIs": [
50               "http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl"
51             ],
52             "ocspURIs": [
53               "http://ocsp.comodoca.com"
54             ],
55             "revocationStatus": 2,
56             "crlRevocationStatus": 2,
57             "ocspRevocationStatus": 2,
58             "sgc": 0,
59             "validationType": "D",
60             "issues": 0,
61             "sct": false,
62             "mustStaple": 0,
63             "sha1Hash": "82942elf4f50c57c25087fca197fb32383010358",
64             "pinSha256": "+Od8qULvd2Y8IIG3d7UIqCGvn/x8eXn9zSGN7jXv/oc="
65           },
66         = {
67           "subject": "CN=*.iedr.ie, OU=COMODO SSL Wildcard, OU=Domain Control Validated",
68           "label": "*.iedr.ie".
69         }
70       }
71     ]
72   }
73 ]
```

## Inex.ie:

[sslinexie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-04-14-18-09-32] - JSONedit

File Search View Tools Snippets Configuration Help

```

1  [
2  = {
3      "host": "www.inex.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1523727291904,
9      "testTime": 1523727476865,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13         {
14             "ipAddress": "2001:7f8:18:2:0:0:0:183",
15             "serverName": "webproxy.inex.ie",
16             "statusMessage": "Ready",
17             "grade": "A+",
18             "gradeTrustIgnored": "A+",
19             "hasWarnings": false,
20             "isExceptional": true,
21             "progress": 100,
22             "duration": 92688,
23             "eta": 1,
24             "delegation": 2,
25             "details": {
26                 "hostStartTime": 1523727291904,
27                 "key": {
28                     "size": 4096,
29                     "alg": "RSA",
30                     "debianFlaw": false,
31                     "strength": 4096
32                 },
33                 "cert": {
34                     "subject": "CN=www.inex.ie, OU=PositiveSSL, OU=Domain Control Validated",
35                     "commonNames": [
36                         "www.inex.ie"
37                     ],
38                     "altNames": [
39                         "www.inex.ie",
40                         "inex.ie"
41                     ],
42                     "notBefore": 1487116800000,
43                     "notAfter": 1589155199000,
44                     "issuerSubject": "CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB",
45                     "issuerLabel": "COMODO RSA Domain Validation Secure Server CA",
46                     "sigAlg": "SHA256withRSA",
47                     "revocationInfo": 3,
48                     "crlURIs": [
49                         "http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl"
50                     ],
51                     "ocspURIs": [
52                         "http://ocsp.comodoca.com"
53                     ],
54                     "revocationStatus": 2,
55                     "crlRevocationStatus": 2,
56                     "ocspRevocationStatus": 2,
57                     "sgc": 0,
58                     "validationType": "D",
59                     "issues": 0,
60                     "sct": false,
61                     "mustStaple": 0,
62                     "sha1Hash": "852fe993c7c3dcc30167db849e657ad57e4ebd9a",
63                     "pinSha256": "cJDaz1VUPcvmjzJQxgYngl0ubJom4y92T23F2iyxRwo="
64                 },
65                 "chain": {
66                     "certs": [
67                         {
68                             "subject": "CN=www.inex.ie, OU=PositiveSSL, OU=Domain Control Validated",
69                             "label": "www.inex.ie".

```

🔍 [ssljamilin.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] -

File Search View Tools Snippets Configuration Help

Text	Tree	List
1	[	
2	= {	
3	"host": "www.Jamilin.com",	
4	"port": 443,	
5	"protocol": "HTTP",	
6	"isPublic": false,	
7	"status": "READY",	
8	"startTime": 1525170603777,	
9	"testTime": 1525170608642,	
10	"engineVersion": "1.31.0",	
11	"criteriaVersion": "2009p",	
12	"cacheExpiryTime": 1525171208642,	
13	"endpoints": [	
14	= {	
15	"ipAddress": "50.116.70.236",	
16	"serverName": "box6141.bluehost.com",	
17	"statusMessage": "Certificate not valid for domain name",	
18	"progress": -1,	
19	"duration": 4604,	
20	"eta": -1,	
21	"delegation": 2,	
22	= "details": {	
23	"hostStartTime": 1525170603777,	
24	"key": {},	
25	"cert": {},	
26	"chain": {},	
27	"protocols": [	
28	= {	
29	"id": 769,	
30	"name": "TLS",	
31	"version": "1.0"	
32	},	
33	= {	
34	"id": 770,	
35	"name": "TLS",	
36	"version": "1.1"	
37	},	
38	= {	
39	"id": 771,	
40	"name": "TLS",	
41	"version": "1.2"	
42	}	
43	],	
44	"suites": {},	
45	"prefixDelegation": true,	
46	"nonPrefixDelegation": false	
47	}	
48	}	
49	],	
50	"certHostnames": [	
51	"bluehost.com",	
52	"*.bluehost.com"	
53	]	
54	}	
55	]	
56	--	

## Jell.ie:

[ssljellie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-04-14-18-09-32] - JSONedit

File Search View Tools Snippets Configuration Help

```

1  [
2  = {
3      "host": "www.jell.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1523725776405,
9      "testTime": 1523726144117,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13     = {
14         "ipAddress": "2a04:2e00:1:3:0:0:0:2",
15         "statusMessage": "Ready",
16         "grade": "A+",
17         "gradeTrustIgnored": "A+",
18         "hasWarnings": false,
19         "isExceptional": true,
20         "progress": 100,
21         "duration": 175105,
22         "eta": 2,
23         "delegation": 2,
24     = {
25         "hostStartTime": 1523725776405,
26     = {
27         "size": 2048,
28         "alg": "RSA",
29         "debianFlaw": false,
30         "strength": 2048
31     },
32     = {
33         "subject": "CN=jell.ie",
34         "commonNames": [
35             "jell.ie"
36         ],
37         "altNames": [
38             "jell.ie",
39             "www.jell.ie"
40         ],
41         "notBefore": 1518811571000,
42         "notAfter": 1526587571000,
43         "issuerSubject": "CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US",
44         "issuerLabel": "Let's Encrypt Authority X3",
45         "sigAlg": "SHA256withRSA",
46         "revocationInfo": 2,
47         "crlURIs": [
48             ""
49         ],
50         "ocspURIs": [
51             "http://ocsp.int-x3.letsencrypt.org"
52         ],
53         "revocationStatus": 2,
54         "crlRevocationStatus": 4,
55         "ocspRevocationStatus": 2,
56         "sgc": 0,
57         "issues": 0,
58         "sct": false,
59         "mustStaple": 0,
60         "sha1Hash": "b0d5f119f658a7fb3dad55485dc58637a50107bd",
61         "pinSha256": "1D8rF+NH41kB59I1/d6We3QmjxuqgBDVKU1MUaL6/ak="
62     },
63     = {
64         "chain": {
65         = {
66             "subject": "CN=jell.ie",
67             "label": "jell.ie",
68             "notBefore": 1518811571000,
69             "notAfter": 1526587571000.

```



## PennyJuice.com:

🔍 [sslPennyjuice.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

Text	Tree	List
1		[
2		= {
3		"host": "www.Pennyjuice.com",
4		"port": 443,
5		"protocol": "HTTP",
6		"isPublic": false,
7		"status": "READY",
8		"startTime": 1525170612274,
9		"testTime": 1525170613870,
10		"engineVersion": "1.31.0",
11		"criteriaVersion": "2009p",
12		"cacheExpiryTime": 1525171213870,
13		"endpoints": [
14		= {
15		"ipAddress": "205.147.88.151",
16		"statusMessage": "Failed to communicate with the secure server",
17		"statusDetails": "TESTING_PROTO_3_4",
18		"statusDetailsMessage": "Testing TLS 1.3",
19		"progress": -1,
20		"duration": 1508,
21		"eta": -1,
22		"delegation": 2,
23		= "details": {
24		"hostStartTime": 1525170612274,
25		"key": {},
26		"cert": {},
27		"chain": {},
28		"protocols": [],
29		"suites": {},
30		"prefixDelegation": true,
31		"nonPrefixDelegation": false
32		}
33		}
34		] }
35		}
36		]
37		

## Responsible.ie:

🔍 [sslresponsibleie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```

1  [
2  = {
3      "host": "www.responsible.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1525169428067,
9      "testTime": 1525169756825,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13     = {
14         "ipAddress": "2a04:2e00:1:67:0:0:0:a",
15         "statusMessage": "Ready",
16         "grade": "A+",
17         "gradeTrustIgnored": "A+",
18         "hasWarnings": false,
19         "isExceptional": true,
20         "progress": 100,
21         "duration": 164617,
22         "eta": 1,
23         "delegation": 2,
24     = "details": {
25         "hostStartTime": 1525169428067,
26     = "key": {
27         "size": 2048,
28         "alg": "RSA",
29         "debianFlaw": false,
30         "strength": 2048
31     },
32     = "cert": {
33         "subject": "CN=responsible.ie",
34         "commonNames": [
35             "responsible.ie"
36         ],
37         "altNames": [
38             "responsible.ie",
39             "www.responsible.ie"
40         ],
41         "notBefore": 1521352036000,
42         "notAfter": 1529128036000,
43         "issuerSubject": "CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US",
44         "issuerLabel": "Let's Encrypt Authority X3",
45         "sigAlg": "SHA256withRSA",
46         "revocationInfo": 2,
47         "crlURIs": [
48             ""
49         ],
50         "ocspURIs": [
51             "http://ocsp.int-x3.letsencrypt.org"
52         ],
53         "revocationStatus": 2,
54         "crlRevocationStatus": 4,
55         "ocspRevocationStatus": 2,
56         "sgc": 0,
57         "issues": 0,
58         "sct": false,
59         "mustStaple": 0,
60         "sha1Hash": "13a8860f2c5e8fdca0a6a7009c08dlfeaa607",
61         "pinSha256": "6y0Urbjwa3ddiCK1CLjJMbE0+FxvB9MLnv5lkP7zyGc="
62     },
63     = "chain": {
64         "certs": [
65         = {
66             "subject": "CN=responsible.ie",
67             "label": "responsible.ie",
68             "notBefore": 1521352036000,
69             "notAfter": 1529128036000.

```

## Scss.tcd.ie:

[sslscstcdie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```
1  [
2  = {
3    "host": "www.scss.tcd.ie",
4    "port": 443,
5    "protocol": "HTTP",
6    "isPublic": false,
7    "status": "READY",
8    "startTime": 1525169764161,
9    "testTime": 1525169934447,
10   "engineVersion": "1.31.0",
11   "criteriaVersion": "2009p",
12   "endpoints": [
13     = {
14       "ipAddress": "134.226.56.2",
15       "serverName": "discovery.scss.tcd.ie",
16       "statusMessage": "Ready",
17       "grade": "A",
18       "gradeTrustIgnored": "A",
19       "hasWarnings": false,
20       "isExceptional": false,
21       "progress": 100,
22       "duration": 154160,
23       "eta": 0,
24       "delegation": 2,
25       "details": {
26         "hostStartTime": 1525169764161,
27         "key": {
28           "size": 2048,
29           "alg": "RSA",
30           "debianFlaw": false,
31           "strength": 2048
32         },
33         "cert": {
34           "subject": "CN=*.scss.tcd.ie, OU=School of Computer Science and Statistics, O=\"Trinity College, Dublin\", L=Dublin, ST=Dublin, C=IE",
35           "commonNames": [
36             "*.scss.tcd.ie"
37           ],
38           "altNames": [
39             "*.scss.tcd.ie",
40             "scss.tcd.ie"
41           ],
42           "notBefore": 1456963200000,
43           "notAfter": 1552046400000,
44           "issuerSubject": "CN=TERENA SSL CA 3, O=TERENA, L=Amsterdam, ST=Noord-Holland, C=NL",
45           "issuerLabel": "TERENA SSL CA 3",
46           "sigAlg": "SHA256withRSA",
47           "revocationInfo": 3,
48           "crlURIs": [
49             "http://crl3.digicert.com/TERENASSLCA3.crl"
50           ],
51           "ocspURIs": [
52             "http://ocsp.digicert.com"
53           ],
54           "revocationStatus": 2,
55           "crlRevocationStatus": 2,
56           "ocspRevocationStatus": 2,
57           "sgc": 0,
58           "issues": 0,
59           "sct": false,
60           "mustStaple": 0,
61           "sha1Hash": "c30b4dd9f3fcf783e410f58d667503bb7c32088a",
62           "pinSha256": "SBzH4ar8du3kwt7hJ5bfaKF0VsGM/qvyUPb6ZH2Vyw="
63         },
64         "chain": {
65           "certs": [
66             = {
67               "subject": "CN=*.scss.tcd.ie, OU=School of Computer Science and Statistics, O=\"Trinity College, Dublin\", L=Dublin, ST=Dublin, C=IE",
68               "label": "*.scss.tcd.ie",
69               "notBefore": 1456963200000.
```

## Tcd.ie:

ssltdie.json - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```

1  [
2  = {
3      "host": "www.tcd.ie",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1525169939130,
9      "testTime": 1525170077703,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "endpoints": [
13     = {
14         "ipAddress": "134.226.14.234",
15         "serverName": "www.tcd.ie",
16         "statusMessage": "Ready",
17         "grade": "B",
18         "gradeTrustIgnored": "B",
19         "hasWarnings": true,
20         "isExceptional": false,
21         "progress": 100,
22         "duration": 138059,
23         "eta": 0,
24         "delegation": 2,
25         "details": {
26             "hostStartTime": 1525169939130,
27             "key": {
28                 "size": 2048,
29                 "alg": "RSA",
30                 "debianFlaw": false,
31                 "strength": 2048
32             },
33             "cert": {
34                 "subject": "CN=*.tcd.ie, OU=IT Services, O=\"Trinity College, Dublin\", L=Dublin, ST=Dublin, C=IE",
35                 "commonNames": [
36                     "*.tcd.ie"
37                 ],
38                 "altNames": [
39                     "*.tcd.ie",
40                     "tcd.ie"
41                 ],
42                 "notBefore": 1484697600000,
43                 "notAfter": 1579780800000,
44                 "issuerSubject": "CN=TERENA SSL CA 3, O=TERENA, L=Amsterdam, ST=Noord-Holland, C=NL",
45                 "issuerLabel": "TERENA SSL CA 3",
46                 "sigAlg": "SHA256withRSA",
47                 "revocationInfo": 3,
48                 "crlURIs": [
49                     "http://crl3.digicert.com/TERENASSLCA3.crl"
50                 ],
51                 "ocspURIs": [
52                     "http://ocsp.digicert.com"
53                 ],
54                 "revocationStatus": 2,
55                 "crlRevocationStatus": 2,
56                 "ocspRevocationStatus": 2,
57                 "sgc": 0,
58                 "issues": 0,
59                 "sct": false,
60                 "mustStaple": 0,
61                 "sha1Hash": "8f080610299c8c204c80d3550009dd36ed1a9671",
62                 "pinSha256": "o+DUU8UcFWfXpgNdrol7zJu2v3V69bzC5Xlcagc3Sec="
63             },
64             "chain": {
65                 "certs": [
66                 = {
67                     "subject": "CN=*.tcd.ie, OU=IT Services, O=\"Trinity College, Dublin\", L=Dublin, ST=Dublin, C=IE",
68                     "label": "*.tcd.ie",
69                     "notBefore": 1484697600000.

```

[ssltheroommovie.json] - [C:\Users\Gleb.DESKTOP-KSUIH87\go\src\ssllabs-scan\2018-05-01-11-08-56] - JSONedit

File Search View Tools Snippets Configuration Help

```

Text 1  [
2  = {
3      "host": "www.theroommovie.com",
4      "port": 443,
5      "protocol": "HTTP",
6      "isPublic": false,
7      "status": "READY",
8      "startTime": 1525170662728,
9      "testTime": 1525170667991,
10     "engineVersion": "1.31.0",
11     "criteriaVersion": "2009p",
12     "cacheExpiryTime": 1525171267991,
13     "endpoints": [
14     = {
15         "ipAddress": "67.195.197.76",
16         "serverName": "pllats-i.geo.vip.bfl.yahoo.com",
17         "statusMessage": "Certificate not valid for domain name",
18         "progress": -1,
19         "duration": 5116,
20         "eta": -1,
21         "delegation": 2,
22     = {
23         "details": {
24             "hostStartTime": 1525170662728,
25             "key": {},
26             "cert": {},
27             "chain": {},
28             "protocols": [
29             = {
30                 "id": 769,
31                 "name": "TLS",
32                 "version": "1.0"
33             },
34             = {
35                 "id": 770,
36                 "name": "TLS",
37                 "version": "1.1"
38             },
39             = {
40                 "id": 771,
41                 "name": "TLS",
42                 "version": "1.2"
43             }
44             ],
45             "suites": {},
46             "prefixDelegation": true,
47             "nonPrefixDelegation": false
48         }
49     },
50     "certHostnames": [
51         "secure.hostingprod.com",
52         "*.secure.hostingprod.com"
53     ]
54 }
55 ]
56

```

## **Discussion:**

### **SSL Labs:**

If we are to look through the generated results for the SSL Labs, we can see that this tester provides a lot of detail. This detail varies whether the test was passed or not. If the test wasn't passed, it's simple 60 lines of json, which says that the progress of the test is -1 and doesn't provide the detail why the test was failed, but rather gives the versions of TLS that are supported in this specific website. On the other hand if the test is passed, the tester generates around 2000 lines of json, which says how and why the result was obtained. The main aspects to look at here is that this tester provides a type of algorithm used e.g. RSA and the strength of encryption, which varies from weak to strong.

In terms of detail, this tester is the best for detail and would prove to be very useful for the web developers or website testers as they would easily spot the aspects they would need to look through, considering all ports used and detailed description of provided certs.

On the other hand, this tester is providing way too much information for someone who just wants to see what is wrong with their website and things that need to be changed are not clearly seen and may actually confuse someone by providing this much of detail in their results.

## **HTTPSObservatory:**

Overall this tester has proven to be very good in terms of their results. This tester provides a set of rules that one should follow in order to succeed with their website. It doesn't matter for this tester whether a test site fails or passes the test, as the results have a template, which can be seen below.

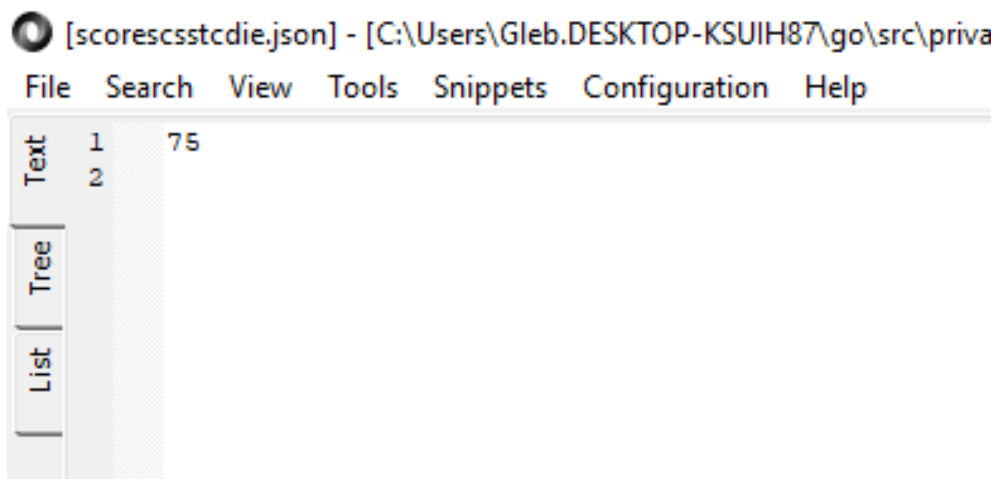
Te	2	Modifiers:
	3	[ 0] Content is not visible via cross-origin resource sharing (CORS) files or headers
	4	[ 0] <b>Contribute.json isn't required on websites that don't belong to Mozilla</b>
	5	[ 0] HTTP Public Key Pinning (HPKP) header not implemented
	6	[ 0] Initial redirection is to https on same host, final destination is https
	7	[ 0] No cookies detected
	8	[ 0] Referrer-Policy header not implemented
	9	[ 0] Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
	10	[ -5] X-Content-Type-Options header not implemented
	11	[ -10] X-XSS-Protection header not implemented
	12	[ -20] HTTP Strict Transport Security (HSTS) header not implemented
	13	[ -20] X-Frame-Options (XFO) header not implemented
	14	[ -25] Content Security Policy (CSP) header not implemented
	15	

The only thing that could be unclear with this tester is that, a test site may score over 100 points, which could be very unclear, because one might think that the max points possible would be 100, but if all the requirements were met, the user will get over 100. This is due to this tester starts their testing with an initial 100 points and depending on what is implemented or not present, the score is modified. It would be a good way to encourage users to get a better grade and implement more features to secure their sites as much as possible.

## **Privacyscore:**

In my opinion, this tester is not great, because it only provides the overall score for the test site, without giving any detail what so ever. This makes this tester very incommensurate, because if the user will want to check their site and will only get a bad result, they wouldn't know what is wrong and what needs to be changed in order to enhance the security of their website. An example of the result that is obtained for a random test.

On the other hand, this tester may prove to be good, because it is rather quick to run the tests in. One could come up with a list of websites and run them on a periodic basis to check for a change and then report to the site owners that their site is not doing that good.





## **Conclusion and future work:**

It was great to see and test how the testers function themselves and the variety of results gathered and worked with from those testers. It was seen that all of them provide different results and amount of detail. A great thing to see would be if all testers would provide some scheme, of course it will be different depending on the tester, whether they are DNS, TLS or overall web testers. Mozilla observatory actually have some sort of a template that encourages users to do better and sets a list of milestones a user should follow in order to be sorted for security. My opinion on this is that, all testers should do it and to encourage the testers to set rules in order for people to see what steps they should follow in order to enhance their security. To do that, a good idea would be to actually contact the testers themselves and ask what their take on this is and what can they offer as a solution for this matter.

It was a pity that not all testers on the list were scripted and not so many results were seen and not a lot of different behaviors were observed. I was very interested in this project and I would like to research and find more testers like that that are scripted and see what type of results that would output and it would be great to compare them with my current testers. It was seen throughout this project that 3 well knows testers are fully different between each other and even the way they decide to go about outputting their results, the detail varies a lot.

## **Acknowledgments:**

I would like to thank my friends for accepting nothing less than excellence from me. Last but not the least, I would like to thank my family: my parents and to my brothers and sister for supporting me spiritually throughout writing this thesis and my life in general.

I would also like to thank my supervisor, Professor Stephen Farrell for bearing with me throughout the project duration and guiding me through the project. Thanks to him, I have a much better understanding of web security and testing in general as this is the area I see myself in near future.

## **References:**

<https://observatory.mozilla.org>

<https://privacyscore.org/>

<https://mxtoolbox.com/dnscheck.aspx>

<https://www.namecheap.com/support/knowledgebase/article.aspx/9711/how-to-check-if-hsts-is-enabled>

<https://github.com/mozilla/http-observatory/blob/master/httpobs/docs/api.md>

<https://www.ssllabs.com/ssltest>

<http://dnscheck.pingdom.com/>

<https://en.wikipedia.org/wiki/Heartbleed>

[https://en.wikipedia.org/wiki/Network\\_Security\\_Services](https://en.wikipedia.org/wiki/Network_Security_Services)

[https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)

[https://en.wikipedia.org/wiki/Cryptographic\\_protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol)

## **Appendices:**

The following a script written in order to generate the json results seen in the results section:

```
cd go

cd src

cd sslabs-scan

@echo off

cls

echo Date format = %date%

echo dd = %date:~0,2%

echo mm = %date:~3,2%

echo yyyy = %date:~6,4%

echo.

echo Time format = %time%

echo hh = %time:~0,2%

echo mm = %time:~3,2%

echo ss = %time:~6,2%

echo.

set "Timestamp=%date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%"

echo %Timestamp%

:: = %date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%

md %Timestamp%

ssllabs-scan.exe www.jell.ie >> "%Timestamp%/ssljellie.json"
```

```
ssllabs-scan.exe www.responsible.ie >> "%Timestamp%/sslresponsibleie.json"

ssllabs-scan.exe www.scss.tcd.ie >> "%Timestamp%/sslscsstcdie.json"

ssllabs-scan.exe www.tcd.ie >> "%Timestamp%/ssltcdie.json"

ssllabs-scan.exe www.herdwatch.ie >> "%Timestamp%/sslherdwatch.json"

ssllabs-scan.exe www.heanet.ie >> "%Timestamp%/sslheanetie.json"

ssllabs-scan.exe www.iedr.ie >> "%Timestamp%/ssliedrie.json"

ssllabs-scan.exe www.inex.ie >> "%Timestamp%/sslinexie.json"

ssllabs-scan.exe www.Jamilin.com>> "%Timestamp%/ssljamilin.json"

ssllabs-scan.exe www.Pennyjuice.com >> "%Timestamp%/sslPennyjuice.json"

ssllabs-scan.exe www.007museum.com >> "%Timestamp%/ssl007museum.json"

ssllabs-scan.exe www.Arngren.net >> "%Timestamp%/sslArngren.json"

ssllabs-scan.exe www.georgermartin.com >> "%Timestamp%/sslgeorgermartin.json"

ssllabs-scan.exe www.theroommovie.com >> "%Timestamp%/ssltheroommovie.json"

ssllabs-scan.exe www.electrifyingtimes.com >> "%Timestamp%/sslelectrifyingtimes.json"
```

```
cd ..
```

```
cd ..
```

```
cd ..
```

```
cd HTTPOBS
```

```
@echo off
```

```
cls
```

```
echo Date format = %date%
```

```
echo dd = %date:~0,2%
```

```
echo mm = %date:~3,2%
```

echo yyyy = %date:~6,4%

echo.

echo Time format = %time%

echo hh = %time:~0,2%

echo mm = %time:~3,2%

echo ss = %time:~6,2%

echo.

set "Timestamp=%date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%"

echo %Timestamp%

:: = %date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%

md %Timestamp%

httpobs.exe www.jell.ie -z >> "%Timestamp%/httpobsjellie.json"

httpobs.exe www.responsible.ie -z >> "%Timestamp%/httpobsresponsibleie.json"

httpobs.exe www.scss.tcd.ie -z >> "%Timestamp%/httpobsscsstcdie.json"

httpobs.exe www.tcd.ie -z >> "%Timestamp%/httpobstcdie.json"

httpobs.exe www.herdwatch.ie -z >> "%Timestamp%/httpobsherdwatch.json"

httpobs.exe www.heanet.ie -z >> "%Timestamp%/httpobsheanetie.json"

httpobs.exe www.iedr.ie -z >> "%Timestamp%/httpobsiedrie.json"

httpobs.exe www.inex.ie -z >> "%Timestamp%/httpobsinexie.json"

httpobs.exe www.Jamilin.com -z>> "%Timestamp%/httpobsjamilin.json"

httpobs.exe www.Pennyjuice.com -z >> "%Timestamp%/httpobsPennyjuice.json"

httpobs.exe www.007museum.com -z >> "%Timestamp%/httpobs007museum.json"

httpobs.exe www.Arngren.net -z >> "%Timestamp%/httpobsArngren.json"

httpobs.exe www.georgermartin.com -z >> "%Timestamp%/httpobsgeorgermartin.json"

```
httpobs.exe www.theroommovie.com -z >> "%Timestamp%/httpobstheroommovie.json"
```

```
httpobs.exe www.electrifyingtimes.com -z >> "%Timestamp%/httpobselectrifyingtimes.json"
```

```
cd ..
```

```
cd go
```

```
cd src
```

```
cd privacyscore
```

```
@echo off
```

```
cls
```

```
echo Date format = %date%
```

```
echo dd = %date:~0,2%
```

```
echo mm = %date:~3,2%
```

```
echo yyyy = %date:~6,4%
```

```
echo.
```

```
echo Time format = %time%
```

```
echo hh = %time:~0,2%
```

```
echo mm = %time:~3,2%
```

```
echo ss = %time:~6,2%
```

```
echo.
```

```
set "Timestamp=%date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%"
```

```
echo %Timestamp%
```

```
:: = %date:~6,4%-%date:~3,2%-%date:~0,2%-%time:~0,2%-%time:~3,2%-%time:~6,2%
```

```
md %Timestamp%
```

```
privacyscore.exe www.jell.ie >> "%Timestamp%/scorejellie.json"
```

privacyscore.exe www.responsible.ie >> "%Timestamp%/scorerresponsibleie.json"

privacyscore.exe www.scss.tcd.ie >> "%Timestamp%/scorescsstcdie.json"

privacyscore.exe www.tcd.ie >> "%Timestamp%/scoretcdie.json"

privacyscore.exe www.herdwatch.ie >> "%Timestamp%/scoreherdwatch.json"

privacyscore.exe www.heanet.ie >> "%Timestamp%/scoreheanetie.json"

privacyscore.exe www.iedr.ie >> "%Timestamp%/scoreiedrie.json"

privacyscore.exe www.inex.ie >> "%Timestamp%/scoreinexie.json"

privacyscore.exe www.Jamilin.com>> "%Timestamp%/scorejamilin.json"

privacyscore.exe www.Pennyjuice.com >> "%Timestamp%/scorePennyjuice.json"

privacyscore.exe www.007museum.com >> "%Timestamp%/score007museum.json"

privacyscore.exe www.Arngren.net >> "%Timestamp%/scoreArngren.json"

privacyscore.exe www.georgermartin.com >> "%Timestamp%/scoregeorgermartin.json"

privacyscore.exe www.theroommovie.com >> "%Timestamp%/scoretheroommovie.json"

privacyscore.exe www.electrifyingtimes.com >> "%Timestamp%/scoreelectrifyingtimes.json"