Linnéuniversitetet
Kalmar Växjö

Bachelor Degree Project

# The status of web security in Sweden

*Author:* Firas Alkhateeb
*Supervisor*: Ola Flygt
*Semester*: Spring 2022
*Discipline*: Computer Science
*Course code*: 2DV50e

## Abstract

Getting incorrect website content has increased in recent years, which is a reflection of the web security status on the Internet. However, when It comes to government and other professional organisations websites, they should have the best security requirements and follow security recommendations. This research will study websites located in the SE zone. The total number of investigated websites is 1166. The testing process was done in two ways. The first way is a Dutch test website tool called Internet.nl. The second is using a tool developed as part of the research. The investigation focus on Swedish websites and nine security extensions. These extensions prevent Man in the middle attack (MITM), downgrade attacks, Cross-Site Scripting (XSS), Click-jacking, and ensure that the correct information is obtained when a client requests a website. The paper evaluated the security between 2014 and 2022. What are the types of security taken and which sector has the best security awareness. The using of security headers had increased in 2022, the total use of tested security standards in the SE zone is around 50%, and banks have the best security awareness.

## Keywords

*DNSsec, HTTPS, HSTS, X-Frame, X-Content-Type-Options, Content-Security-Policy (CSP), Referrer-Policy , Digital certificate (X.509).*

# Preface

I would like to thank my supervisor, Ola Flygt, who gave me the opportunity to complete the study and guided me. Without him, I could not have completed this study. I would also like to thank my English teacher Cordula Hernqvist who supported me during my language journey. My last thanks are to my IT and Math teacher Hatem Alali who showed me how easy and fun Math and IT is.

# Contents

# 1 Introduction

This paper is 15 university credits in Computer science which aim in Cyber security and focus on web security in Sweden. It will study the security standards deployment in the SE zone.

The introduction section explains the study that will be done in this paper, and contains seven subsections. First, an overview of the subject area in the background subsection. It will follow by related works, which are old research and papers in the same field. It will then follow by a problem formulation subsection that describes the problem and presents the research questions that this paper will try to answer. Then comes the motivation subsection. Finally, it is followed by results, scope/selection, target group, and outline.

## 1.1 Background

After the information revolution, communication networks became an essential key in society's development. Networks are expanding, especially the internet, because they are becoming the engine of many technologies that make life easier. All branches like the economy, health care, and education use the Internet. For example, after the Covid-19 epidemic, the need for the internet increased because many students study from their homes. Also, the economy became based on internet usage, and a new type of work started based on online activities. However, extensive Internet usage comes with downsides [1] , including security issues that affect users and organisations like companies, education, and fake news. To avoid these problems, we have rules to follow when building and running websites.

In this thesis, we will study the web security implementation for **(1166)** essential websites (explained in the method) in the **".se"** zone, which are Swedish websites and domains [2]. There are several security extensions aimed to make websites more secure. This study will focus on the degree of implementation of these security standards. Web security is flexible, and it could contain many security standards. The study will focus on the security aspects as the following:DNSsec, HTTPS, HSTS, X-Frame, X-Content-Type-Options, and Content-Security-Policy (CSP). For HTTPS part will also include TLS/SSL (X.509) Certificate.
The choice of the above security mechanism is according to two factors. The first one is Interent.nl which chose these security mechanism to test the websites, and the other factor is the OWASP recommended headers [3].

Jeff Hodges and Andy Steingruebl of PayPal agree on the benefit of the security extension because it reduces the risk of many cyber attacks [4]. This study will help understand the web security in Sweden and allow for future web security development in general. The Previous research in the field did not study the security extinction in Sweden, especially in the SE zone. The state of using security in Sweden as a specific area is unknown.

## 1.2 Related work

Cyber operations have increased in recent years, which also increases the gaps that hackers can use to attack others. The security standards that will study in this paper have been studied before by other researchers. None of the researchers have studied the websites that are located in Sweden. However, Hasan Ahmed and Jawdat Kour studied email security standards in the Swedish zone, and The Swedish Internet foundation studied only DNSsec[5][2]. Therefore, this paper will study the status of web security in Sweden by using the deleted database from the Swedish Internet foundation.

This section discusses the latest previous work related to this thesis area. Moreover, It will show the results that they have obtained. Also, the problem formulation section will discuss the areas that have not covered.

This thesis is based on works from **"The Swedish Internet Foundation"**. In a research they tested 913 websites [2]. It is the organisation responsible for takes care of Sweden's top-level domain **(.SE)**. In 2014, they published a report about the Swedish website healthy "Hälsoläget i .se 2014 – Nåbarhet på nätet". This report examined the quality and accessibility of domains in the (.SE) zone. Furthermore, the examination tested part of the security extensions: DNSsec, HTTPS, and HSTS. The DNSsec deployment was around 29% of the total tested websites. They did not include a test about certificates. Moreover, it does not test the optional security header according to Interent.nl.

In 2018, research investigated HTTP header security. It examined the top one million websites that are ranked by Alexa[6]. The result found by getting HTTP response headers analysis. The research finding indicated that CSP implemented in (3.8%) of total sites. X-Content-Type-Options (24%) of sites. X-Frame-Options Header implemented in (24.86 %) of examined sites. Moreover, the research checked the HTTPS communication based on HTTPS response via port 443. However, 29.1% of the total request had failed based on verification errors such as expired certificates, self-signed, signed by untrusted CA's, malformed, and certificate misconfiguration or installation[6].

Another study done in 2018 by Krit Poonsiri shows the status of DNSsec implantation in Thailand. It found that 6.51% of 1,121 websites have DNSsec extension in their website. The study also found that DNSsec implantation in 2014 was higher than DNSsec deployment in 2019. The two main reasons for the reduction are many domain servers replaced, and change support for domain registrars.[7]

In 2020, a study focused on the Indonesian bank websites security headers by Purwanto Agus and Emanuel Andi Wahju Rahardjo. They found that 51.32% of examined websites have lacking security. The total number of examined websites was 115. Moreover, these sites contain apparent security vulnerabilities [8].

In the same year, 2020, another study was conducted by Haneen Mohialdeen and Johannes Draaijer. They studied the security culture in Sweden, focusing on digital certificate culture in organizations. They created seven certificates according to RFC 5280 [9], RFC 6818 [10], RFC 8398 [11], RFC 8399 [12] and RFC 3161 [13] .They found after test bed for the SSL server that all fields (Authentication of Entity, the integrity of code, authentication of code publisher, and Proof that data existed before a particular time in that exact state) misuse the certificate. However, other fields (Authentication of Domain Confidentiality of data in transit on Transport/Internet layer, and integrity of data in transit on Transport/Internet Layer) have followed the criteria of X.509 [14].

In 2021, Hasan Ahmed and Jawdat Kour investigated the status of email security in Sweden. They collected the essential domains and websites. The total number of domains and websites was 2000. They investigated DNSsec implementation. They divided websites into three groups: Firstly, Swedish public organisations. Secondly, the top 1000 private Swedish organisations. Thirdly, private organisations according to the number of employees. They used the Netherland government online tool "https://internet.nl/". DNSsec deployment for group one were 29%, group two was 5%, and group three was 5% [5].

## 1.3 Problem formulation

The internet has become a part of our daily life that depends mostly on connecting to websites. Many attacks can change, copy, or fabric web content. Man in the middle attack (MITM ) is one of many cyberattacks that can change copy and fabric information, which means MITM breaks Confidentiality [15]. Another cyberattack that affects security is Cross-Site Scripting (XSS). Around 40% of all cyberattacks were XSS in 2019 [16]. According to Internet.nl, two types of security standers can prevent cyberattacks. The first type is the recommended security standards which are DNSsec, HTTPS, X.509 certificates and HSTS. The second type, there are optional standards such as X-Frame, X-Content-Type-Options, and Content-Security-Policy (CSP) [17].

The first security type are required for every website or organisation because they should meet CIA security triangle. However, the other type of security standard is optional standards, which can be used to increase their security. Also, the digital certificate (X.509 v3) is required using TLS/SSL to ensure the secure connection between the server, and the client. Certificate configuration issues and errors have reached a vast number.Certificate configuration issues and errors have reached a vast number. After testing the top one million there were 29100 infected websites [6]. Moreover, Using the above security standards protect the clients from cyber attacks.

However, all related work shows that the usage of these extensions are relatively low. Moreover, websites and domains that do not use this extensions are vulnerable to cyber attacks. In addition, most studies do not cover Sweden as an area and do not study all security standards that this study will do.

This paper investigates the vulnerability of two attacks: MITM and XSS. Also, It will investigate what type of content users receive; by testing if the websites and domains have implemented the extensions. Moreover, the investigation will cover if the websites and domains had implemented these extensions or not. The number of websites that will test is 1166 websites. The study will be affected by sectors.

The investigations in this thesis aim to answer three research questions as the following:

**RQ1- How secure are Swedish websites? Furthermore, has the use of security extension implementations increased since 2014?**

**RQ2- What are the web security standards adopted by Swedish websites? Moreover, what is the situation if websites do not adopt these standards?**

**RQ3-What is the difference in adaption of security mechanisms for websites from different sectors in Sweden and how efficient are these mechanisms for the different sectors?**

## 1.4 Motivation

This paper will enhance the understanding of the status of web security in Sweden, which will help to develop the protection of the information technology infrastructure in the country, where sites are considered the key to entering the internal systems. While writing this thesis, on March 10, 2022, the Swedish Armed Forces **"Försvarsmakten"** announced through a press interview by Chief of Operations Michael Claesson that several Swedish government websites have been under cyber attack. The results will address several points. Firstly, the security level of websites according to the security recommendation. Secondly, security threats that affect society during receiving incorrect information. Thirdly, security awareness that handled by domain owners. Finally, these results will help us to know if Swedish websites can survive after cyber attacks against fabrication and eavesdropping.

## 1.5 Results

The paper presents the security level of Swedish websites. All target websites are processed into two test methods to help evaluate the results. The first method will be the Nederlanden website `www.internet.nl`. The second method is a tool implemented by Python. The second method will also test the certificate. However, the first method has limitations; that can not do the certificate test. Nevertheless, this result warns about needing a solid security approach and following the security recommendations. The Swedish government hid the websites that were under cyber attack and did not publish any report identifying the targeted sectors. However, this paper will identify security levels by sectors.

## 1.6 Scope/Limitation

The research aims to test and examine all domains of the SE zone. However, the collocation of domains included in the SE zone was complex. The reason is that the Swedish Internet Foundation had deleted all of its databases included in the 2014 SE zone healthy report. Therefore, it is impossible to get all domains in the SE zone that the Swedish Internet Foundation handles. This research will not check sub-domains because the test target will be overloaded on manually testing. In addition, the digital certificate has many vulnerabilities and new testing protocols, which will also not be included in this research. In the end, this research will not include any websites that had been under cyber attack, which the Swedish armed forces did not report it on March 10, 2022.

## 1.7 Target group

Fetching the correct web sources and secure communication between client and server are the CIA security triangle goals: confidentiality, integrity, and availability. The misconfiguration or skipping the use of security headers and recommendations leads to security leaking. The paper targets all researchers in Information security and defence, IT students, Information security experts, web developers (Front-back end), and private and government security organisations working in information security. It might also target groups working on security research projects that can help compare the security between different countries.

## 1.8 Outline

This report organised as follows. Chapter 2 discusses the methodological framework, research methods, reliability and validity, and ethical considerations. Chapter 3 discusses the theoretical background. Chapter 4 talk about the implementation of the research project. Chapter 5 discusses the results. Chapter 6 analyses the results and answers the research questions. Chapter 7 discusses the analysis and the writer's view of the results. Finally, chapter 8 is about conclusion and further work.

# 2 Method

This section discusses the methodology used for proceeding with the research. The study is about web security and aims to answer the research questions in section 1.3. To answer thesis questions, the websites in the Swedish zone collected from `www.hardenize.com` via a long searching process.

## 2.1 Research Project

The last information about the Swedish website's security status, was made in 2014. The use of correct certificate implantation is unknown. Therefore, the entire websites studied in this research will be 1166. The study will start by collocating websites according to 11 sectors. The sectors are 95 banks, 63 newspapers, 30 insurance companies, 164 ISPs, 353 municipalities, 18 media, 21 regions, 191 government agencies, 47 state-owned companies, 133 registration domains, and 48 Universities. Then, an advanced tool will be used to test all website security extensions. A statistical study will determine the security extension implementations based on the websites sector. Moreover, the results will be analysed to show an overview of Swedish website security health and possible threats.

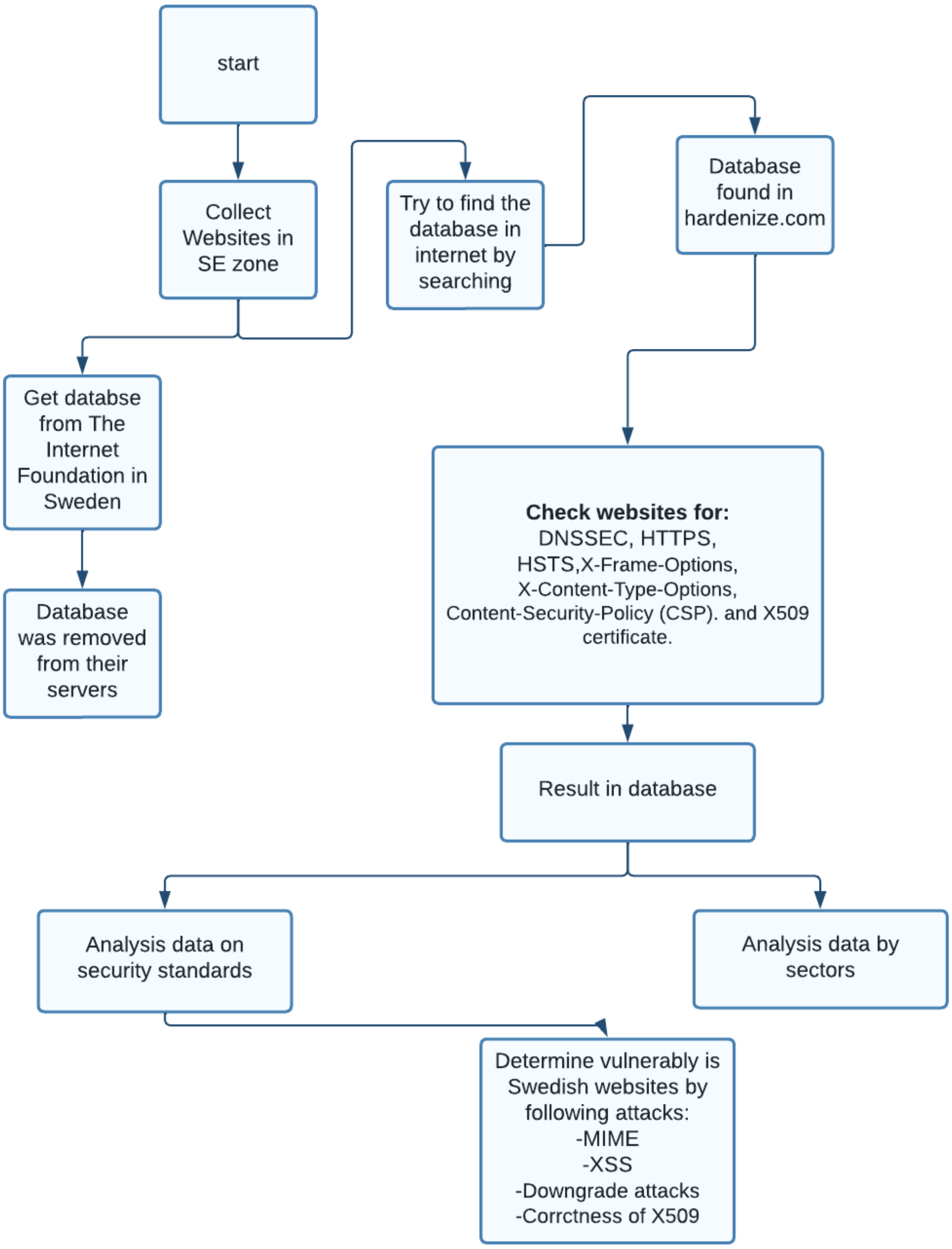

start
Collect Websites in SE zone
Try to find the database in internet by searching
Database found in hardenize.com
Get databse from The Internet Foundation in Sweden
Database was removed from their servers
**Check websites for:** DNSSEC, HTTPS, HSTS,X-Frame-Options, X-Content-Type-Options, Content-Security-Policy (CSP). and X509 certificate.
Result in database
Analysis data on security standards
Analysis data by sectors
Determine vulnerably is Swedish websites by following attacks:
-MIME
-XSS
-Downgrade attacks
-Corrctness of X509

Figure 2.1: shows how the methodology will apply. The experiment chapter will provide more details about the tool that will use to evaluate the websites' security extensions used will be in the experiment chapter.

## 2.2 Research methods

In order to get the correct information about the security situation, the thesis uses two different examination methods. The first method is an implemented tool. This tool uses python programming language and some open source security libraries. The second method is two online websites that can help to evaluate the website online. The first website is www.Internert.nl which has been used before by some papers. The second website is https://www.sslshopper.com/ssl-checker.html. Using both methods will give more reliability to the results. More details provid in the research project – implementation chapter. Finally, this paper uses Kour, J. Ahmed, H. thesis as structure and inspiration [5].

During Interent.nl testing, it shows some wrong values after testing some websites. Therefore, the correct value of each security standard was read, and the websites will test with a new tool which is a Python tool that follows the exact same security standards values. **Internet.nl** did not test all propriety as in Appendix 13 and Appendix 14.

## 2.3 Reliability and Validity

In this study, we will use an online tool https://internet.nl/ to study security extensions and investigate the results. According to their website, this tool created through a collaboration between the Dutch government and the Internet community. The website's source code and the tool are considered open-source because all programs and codes updated to Git. Therefore, the tool can be considered reliable and trusted. However, other online tools can test the same website to check reliability and trustworthiness. The other tools will discuss in the experiment chapter.

Further, All old databases were deleted by the Swedish Internet Foundation. Therefore, there are not possible to get the tested database. However, we could find a database for all Swedish Internet Foundation on the internet at www.hardenize.com. The total number of test websites is 1166, which is more than those tested in 2014, which are 913 websites. This increase is likely due to the 2014 report issued in 2015. Therefore, it is expected that these numbers were for the year 2015. That database from www.hardenize.com has the same sectors.

The internal validity is very high because all websites will be tested in two methods which will give confidence to the results. Moreover, external validity helps to understand the security state and how the security headers apply in Sweden. Moreover, the importance of applying these standards to all websites in the world and especially in Sweden. The ignorance of those standards make the websites vulnerable to many cyber attacks that website administrator must implement.

## 2.4 Ethical Considerations

This thesis includes sensitive information which can use to threat Swedish websites. Significantly, the information about websites in the SE zone was deleted from the Swedish Internet foundation. The data might help organisations to understand the security risk that might occur. On the other hand, this information can use to attack and sabotage these sites. Therefore, instead of showing the website's vulnerabilities, a percentage of results will show for every group by two types of testing. Moreover, all tested websites and the implemented python tool will include in the appendix chapter [5].

# 3 Theoretical Background

After looking to related work especially the Hasan Ahmed and Jawdat Kour, `Interent.nl`, and OWASP security headers show that importance of use the security headers in all websites to avoid Cyber attacks [5] [3].

## 3.1 Domain Name System Security Extensions (DNSsec)

DNS is one of the most important protocols on the Internet. It is necessary to translate the web addresses to the web IP addresses that computers can understand. Unfortunately, DNS does not prevent security issues. DNS has several vulnerabilities, including a man in the middle (MITM), Caching Problems, DDoS attacks, Other significant DNS attacks, and bind Security Considerations.

- (MITM) includes Packet sniffing and transaction ID guessing.
- Caching Problems include Cache Poisoning using Name Chaining and Cache Poisoning using Transaction ID Prediction.
- Other significant DNS attacks include Information Leakage and DNS Dynamic Update Vulnerabilities[18].

DNS does not have origin authentication and integrity. However, to make the DNS safer. An idea comes to create DNSsec[18]. DNSsec is an authentic solution to ensure that it is the correct website [19]. This security supplement helps to avoid several cyber security threats. It solves the DNS spoofing, which leads to the user ending up on the wrong website. Moreover, it protects text records(TXT) and mail records(MX). It is also the foundation that paved the new protection, for example, Certificate records, SSH fingerprints, IPSec public keys, and TLS Trust Anchors. On the other hand, DNSsec supports third parties by preventing the DNS Cache Poisoning and False zone, which allows counterfeit of records and the domain's identity guarantee [18].

DNSsec is a peer of two keys which are public and private. Both keys set to gather to create key pair. The zone has the pair to create secure DNSsec implementation. The validation of DNSsec is to validate DNS requests. It also uses a digital certificate saved with the DNS server to validate the DNS query. There are four points to provide DNSsec. Firstly, assembling DNS records according to group and type. Then sign these records, which are called later RRSIG records. Secondly, every zone that wants to provide DNSsec must have a public and private key in pairs called zone signing key (ZSK). Then add cryptographic sing to Signed RRSIG records and save again with RRSIG records. ZSK public key do verification for the cryptographic signed RRSIG. Then save it in DNS key records. Thirdly, DNS key records contain ZSK and key signed key (KSK), which will use to verify the RRSIG signed records. Finally, a hash function of the DNS key is done to link zones [5] [20] [21] [22].

Since 2005, the .se zone had the first DNSsec implantation by the Swedish internet foundation [19] to solve security issues.

## 3.2 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is an extension of HTTP used in computer networks to create secure communication between server and client. HTTP works in the application layer and does not have security fundamentals: confidentiality, integrity, and authentication. Those security issues can lead to security leaking[23]. There are two types of HTTPS: HTTP over TLS or HTTP over SSL[24][23]. Both are working for the same purpose, which is security achievement. HTTPS protocol meets the security features. To meet the security requirements, it must do encryption to meet confidentiality. The packet does not change during the transmission. It will meet integrity, and the receiver receives the origin message. Finally, it will meet the authentication goal [23].

Establishing HTTPS sessions happens between client and web server. Both parties agree to use cryptographic parameters that will be used later for the session. This process is called TLS handshake [25].

The process of the handshake protocol is as the following:

1. The client sends a “Client Hello” message containing a session ID, random number, and cipher suite list.
2. The server sends a “Server Hello” message containing a session ID, random number, and cipher suite list.
3. The server sends its certificate containing server information, server public key, and hash signature.
4. The server sends a message containing “Server Hello Done”.
5. The client sends Client Key Exchange and uses the server’s public key to encrypt the premaster.
6. The client sends a “Change Cipher Spec” message to the server.
7. The client sends a “Finished” message to end the handshake.
8. The server sends “Change Cipher Spec”.
9. The server sends a “Finished” message to end the handshake.

When the server sends “Change Cipher Spec,” both sides, client and server, agree and conform to the encryption, and then the secure session starts [25] [26].

## 3.3 HTTP STRICT TRANSPORT SECURITY (HSTS)

HSTS is a technique allowing websites to inform clients the way that can be attainable by a secure connection. Announcing mode can be done through web servers via the HTTP response header field. For example, If a web server has the extension **“HSTS”**, it will force the client automatically to connect via a secure connection **“HTTPS”**. Moreover, It will drop the connection if an error happens by an untrusted certificate or TLS. Implementing the HSTS to the top domain will be enforced in all subdomains [27]. HSTS prevents Man in the Middle (**MITM**) attacks by enforcing secure connection HTTPS[28]. Moreover, HSTS prevents users from overriding the invalid certificate message [29].

HSTS extension works between client and server in two steps. In the First step, the client requests a website with HTTP. The server ignores the request. Then the server sends the error message 301. The user asks for the website again with HTTP. The server replay with a secure session. In the second step, the user asks for a website with HTTP. The browser replays with error message 307 **“Internal Redirect”** and forces the request with HTTPS.

## 3.4 X-Frame-Options Header

X-Frame-Options Header, calibrated in **RFC 7034**, is an HTTP header field that declares the policy that shows web content requested by the client and avoids other website contents transmitted in the same frames that are part of different websites. In addition, this header prevents click-jacking [30][6]. This header has three options that define the header: deny, same-origin and allow-from. For the first option, **“Deny”** is the most secure option that prevents using the current frame. The second option, **“SAMEORIGIN”**, is more commonly used. Moreover, it allows frames; however, it limits them to the current domain. The third option, “allow-from” is defined by **RFC 6454** which does not work for modern browsers. Moreover, the browser should not show the other web content’s origin[31]. This policy only applies to a Firefox browser[28]. However, Content-Security-Policy (CSP) offers the same protection [31].

## 3.5 X-Content-Type-Options Header

X-Content-Type-Options is an HTTP header field, which makes the browser more secure by protecting against Multipurpose Internet Mail Extensions or (MITM -type). For example, an attacker can fool the client browser into executing content that is not part of the web application executing [6]. The first use of the header by Microsoft in IE 8 . Then all browsers start to use it [32]. The header has only one value which is **“nosniff”** [6] [32].

## 3.6 Content-Security-Policy (CSP)

(CSP) is a header used by web applications to avoid injection vulnerabilities like cross-site scripting (XSS), which can steal data or distribute malware. Additionally, the header avoids data injection attacks. It decreases clients' prerogative by executing the attacker scripts and applications. Plus, the header contains a safe list that allows secure JavaScript execution and disables all unsafe JavaScript code. CSP aims in deep defining to reduce the injection effect and harm. It is not instead of the other security policy or input validation or encoding[6] [33] [34]. CSP can prevent HTTPS that being related to unexpected HTTP links on the same page of HTTPS [6].

The header must have one value which is **"self"** [34]. The header should not have some other values. Firstly, **"unsafe-inline"**, **"unsafe-eval"**, and **"unsafe-hashes"** allow XSS attacks. Secondly, **"data:"** should not be used in **"default-src"**, **"script-src"**, and **"object-src"**, which allows. Thirdly, **"HTTP:"**, Fourthly, **"*"** should not be used because it allows downloading from other external resources. Filthy, **"127.0.0.1"** should not be used because it enables injection attacks [35].

## 3.7 Referrer-Policy Headers

Referrer-Policy is an HTTP header field that controls the requested addresses header in outgoing HTTP/HTTPS [24] [23]. The server can check if the request originated. This type of header is usually used for analytics and logging, but also it can leak privacy. This type of information can be used for tracking and sending the information via eavesdrop connection by third parties [24]. This header has eight syntaxes according to [24] [36]:

1. **No-referrer:** The "No-referrer" means that the client will send no information to the server and the header will delete or ignore it.

2. **No-referrer-when-downgrade:** The "no-referrer-when-downgrade" means sending origin, path, and query string when the navigation from HTTP to HTTP or HTTPS and from HTTPS to HTTPS. However, the referee must not send less secure communication such as HTTPS to HTTP and HTTPS to file.

3. **Same-origin:** The "same-origin" means that the referee will send to the origin. If their multi-path, the referee will not send it.

4. **Origin:** The "origin" means the referee will send to origin from any request.

5. **Strict-origin:** The "strict-origin" means the referee only will send via secure communication from HTTPS to HTTPS.

6. **Origin-when-cross-origin:** The "origin-when-cross-origin" is sending the referee to the same origin via less secure communication such as HTTPS to HTTP.

7. **Strict-origin-when-cross-origin:** It is the same "origin-when-cross-origin". However, sending will be secure communication HTTPS to HTTPS.

8. **Unsafe-url:** Sending the request without checking the communication security.

9. **The empty string :** the web server does not prefer any specific Referrer-Policy.

The not recommended values are **"origin"**, and **"origin-when-cross-origin"**, because they allow non-secure transmission, which breaks the security goal **"Privacy"**. However, other values such as **"strict-origin"** and **"strict-origin-when-cross-origin"** might be used. To minimise the security issues that come from HTTP and HTTPS, it should use **"no-referrer-when-downgrade"**[36].

## 3.8 Digital Certificate X.509

Digital certificate, identity certificate, or public key certificate is an electronic document used to verify the public key and the certificate owner. The latest version of the certificate is X.509, an ITU-T standard espoused by Internet Engineering Task Force **(IETF)** [9] [37]. X.509 standard still used to control security and identity in internet communications, computer networking, and it is widespread [38]. Moreover, the X.509 certificate architecture consists of a pair of keys which are a private key and a public key. Both keys are used to encrypt / decrypt messages, and secure the identity and message. In addition, X.509 is used by Transport Layer Security **(TLS)** and Secure Socket Layer **(SSL)** to deploy HTTPS protocol [9] [37][38].

Having (**TLS/SLL)** requires a digital certificate from the server that proves the path destination. The client is required to validate the certification path. The validation process is done by checking every certificate value according to X.509 standard [9]. Browsers do the validation process [39]. According to X.509 version 3 standard, the certificate must have the following structure:

1. **Version:** shows which certificate version.

2. **SerialNumber:** shows certificate serial number given by certificate authority (CA).

3. **Signature:** is the cryptographic algorithm that is used to sign the certificate.

4. **Issuer:** is the name of the CA that issued the certificate.

5. **Validity:** is when the certificate starts and ends date.
6. **Subject:** is the name of the organisation that the certificate belongs to.
7. **SubjectPublicKeyInfo:** is subject public key info,
8. **IssuerUniqueIdentifier** is issuer unique identifier.
9. **SubjectUniqueIdentifier** is subject unique identifier.
10. Extensions

The certificate should have a certificate authority **(CA)** that manages and issues the certificate. CA provides certificate chains, verification logic that enables the receiver to verify that the sender and all CA's are trustworthy [9] [40].

# 4 Research project – Implementation

The online tool `www.internet.nl` used to test random websites in the SE zone. The tool was created through a collaboration between the Dutch government and the Internet community. During the experiment, I found some failures in testing some websites. Therefore, a testing program was implemented. These failures are very important so the owner will contacte to get claims verified about the issues. Therefore, the collected websites were tested in implemented tools instead. The internet standards checked in the implemented tool are **DNSsec, HTTPS, HSTS, X-Frame, X-Content-Type-Options, Referrer-Policy, Content-Security-Policy (CSP), and X.509**. The online tool has limitations that one website can test, while the implemented tool can test many websites simultaneously. Also, the test information can be sent to an Excel file, allowing easy analysis. The implemented tool was written in the Python programming language. It works by querying and analysing websites to examine the security mechanisms that are implemented by the organisations.

The first experiment has been done with Google Chrome browser version 103.0.5060.134. The second experiment has been done with Windows 10 operating system.

| | |
|---|---|
| Device name | MSI GL63 8SE - i7 16GB 256GB RTX 2060 |
| Processor | Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz 2.21 GHz |
| Installed RAM | 16.0 GB (15.8 GB usable) |
| System type | 64-bit operating system), x64-based processor |
| Edition | Windows 10 Home |
| Version | 21H2 |
| OS build | 19044.1826 |

Figure 4.1 : illustrates the computer setting.

The implemented tool used **PyCharm 2020.2.2 x64** integrated development environment **"IDE"**. The Python version that have been used is **V 3.9**.

The following table shows the Python libraries that used to implement the tool:

| Library name | The usage |
|---|---|
| **datetime** | counting the date and time. |
| **socket** | open session between client and server. |
| **ssl** | allow accessing to TLS/SSL encryption and authentication. |
| **urllib.request** | allow using the complex URL requests. |
| **dns** | allows to get and apply DNS queries, |
| **requests** | allow URL requests. |
| **xlsxwriter** | allow to create and write on Windows Excel files. |
| **ocspchecker** | test X.509 certificate revocation. |

Figure 4.2 : illustrates Python libraries that used to implement the tool.

The idea behind the program is get the URL from a text file. Every URL get **https://** and **http://** . https://+URL will use only for check **HTTPS**. However https://+URL will use to check other standards.

X-frame-options, X-Content-Type-Options, Strict-transport-security content-security-policy , and Referrer-Policy Headers have the same test mythology, which is to get the website's header and check if the standard is part of the header, then check the value according to figure 4.3. For X.509 certificate, two testing methods will apply. The first one checks the revocation, and the second one tests every field, according to figure 4.3.

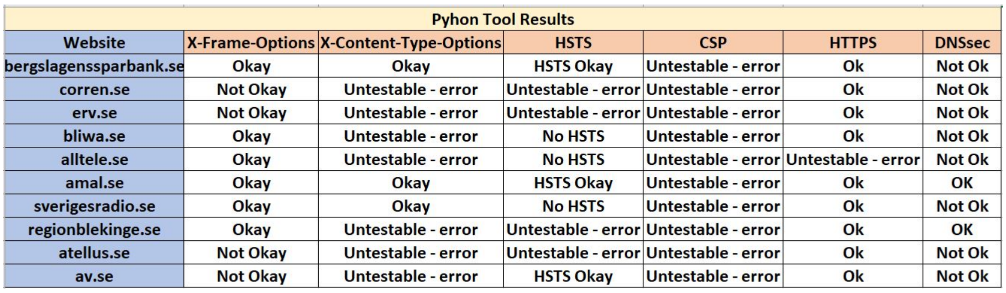
Both tools have the exact testing mechanism by the following table:

| Standard | Checked subset | Test explanation |
|---|---|---|
| **DNSsec** | -RRSIG(DNSKEY)<br>-DNSKEY RECORD | Check domain is signed with a valid DNSSEC signature via answering the DNSKEY Should be DNSKEY and RRSIG(DNSKEY) [5]. |
| **HTTPS** | -HTTP over TLS / SSL. | Check the domain is worked and reachable by HTTPS (valid response) or it will give an invalid response |
| **HSTS** | Get the response header for HSTS. | Check domain is signed with a valid HSTS certificate max-age signature **”max-age<=31536000”**. |
| **X-Frame-Options** | Get the response header for X-Frame-Options | Check the domain is signed with a valid X-Frame-Options signature.<br>-**DENY** (framing not allowed)<br>-**SAMEORIGIN** (only framing by your own website allowed). |
| **X-Content-Type-Options** | Get the response header for X-Content-Type-Options | Check domain is signed with a valid X-Content-Type-Options signature with **nosniff**. |
| **Content-Security-Policy (CSP)** | Get the response header for the CSP | Check domain and is signed with a valid CSP signature.<br>-**Default-src** should be **“none”** or **“self”** signed.<br>-**frame-src** should be **“none”** or **“self”** signed.<br>-**frame-ancestors** should be **“none”** or **“self”** signed<br>- It should not have **unsafe-inline**, **unsafe-eval**, and **unsafe-hashes** |
| **Referrer-Policy Headers** | Get the response header for Referrer-Policy Headers | Check the header should contain **"strict-origin"**, **“strict-origin-when-cross-origin”** and **“no-referrer-when-downgrade"** |
| **X.509 Certificate** | Get the certificate from the target website. | Check all certificate fields according to X.509 standard |

Figure 4.3 : illustrates the testing mechanism.

All sites examined were related to the **SE** zone. The data was tested manually, which means that the information obtained from `www.hardenize.com` was correct. Also, all data were categorised by the appropriate classification, so there is no need to change the website classification.

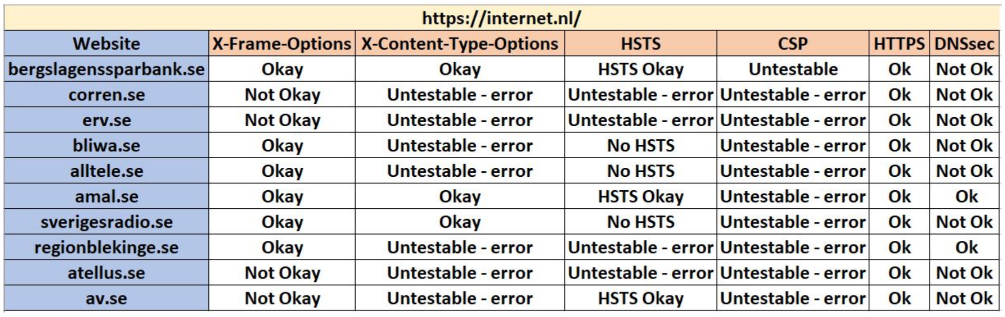
Experiments have been done for both implemented tool and the online tool. Additionally, to compare both tools, more tests have been done using the same online tool used by related work projects, which is `www.securityheaders.com`. In order to verify the tools, Random websites were chosen. The total number of chosen websites is 10.



Pyhon Tool Results

| Website | X-Frame-Options | X-Content-Type-Options | HSTS | CSP | HTTPS | DNSsec |
|---|---|---|---|---|---|---|
| bergslagenssparbank.se | Okay | Okay | HSTS Okay | Untestable - error | Ok | Not Ok |
| corren.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| erv.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| bliwa.se | Okay | Untestable - error | No HSTS | Untestable - error | Ok | Not Ok |
| alltele.se | Okay | Untestable - error | No HSTS | Untestable - error | Untestable - error | Not Ok |
| amal.se | Okay | Okay | HSTS Okay | Untestable - error | Ok | OK |
| sverigesradio.se | Okay | Okay | No HSTS | Untestable - error | Ok | Not Ok |
| regionblekinge.se | Okay | Untestable - error | Untestable - error | Untestable - error | Ok | OK |
| atellus.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| av.se | Not Okay | Untestable - error | HSTS Okay | Untestable - error | Ok | Not Ok |

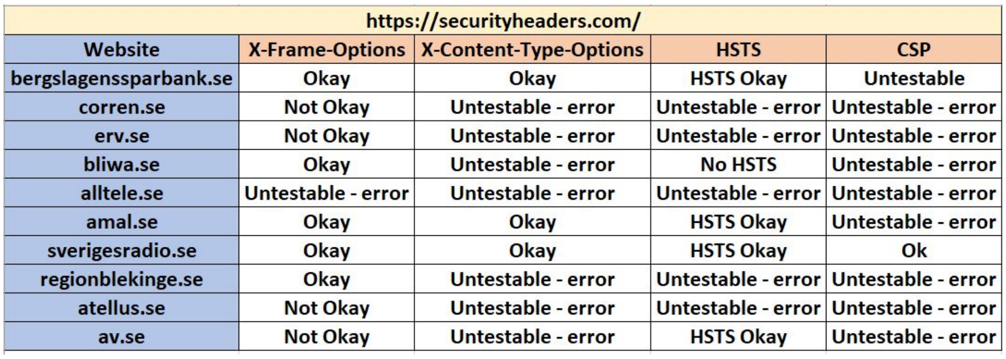
Figure 4.4: illustrates the results of 10 tested websites by the implemented tools.



https://internet.nl/

| Website | X-Frame-Options | X-Content-Type-Options | HSTS | CSP | HTTPS | DNSsec |
|---|---|---|---|---|---|---|
| bergslagenssparbank.se | Okay | Okay | HSTS Okay | Untestable | Ok | Not Ok |
| corren.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| erv.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| bliwa.se | Okay | Untestable - error | No HSTS | Untestable - error | Ok | Not Ok |
| alltele.se | Okay | Untestable - error | No HSTS | Untestable - error | Ok | Not Ok |
| amal.se | Okay | Okay | HSTS Okay | Untestable - error | Ok | Ok |
| sverigesradio.se | Okay | Okay | No HSTS | Untestable - error | Ok | Not Ok |
| regionblekinge.se | Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Ok |
| atellus.se | Not Okay | Untestable - error | Untestable - error | Untestable - error | Ok | Not Ok |
| av.se | Not Okay | Untestable - error | HSTS Okay | Untestable - error | Ok | Not Ok |

Figure 4.5: illustrates the results of 10 tested websites by Interent.nl.



https://securityheaders.com/

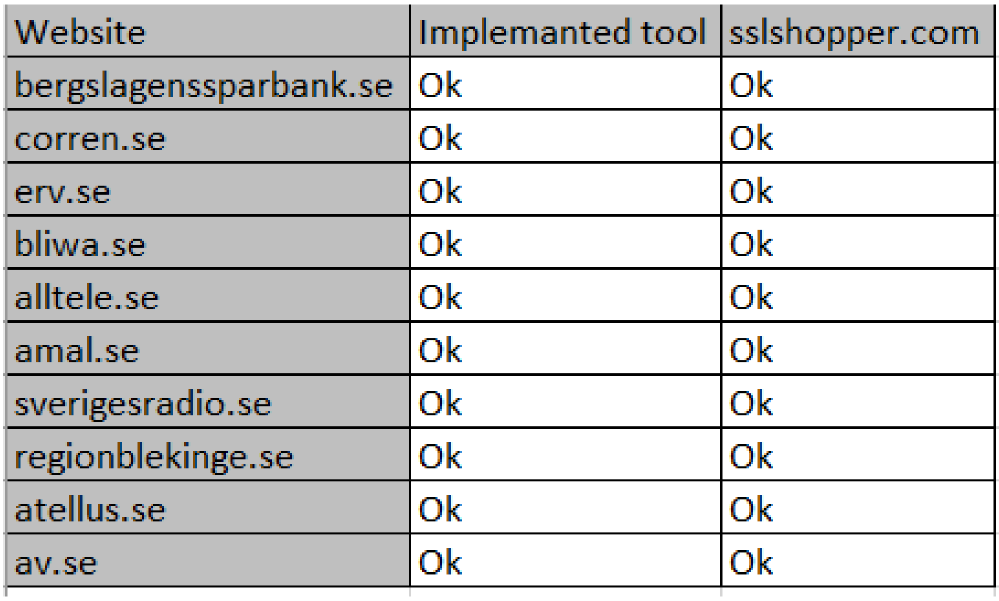
| Website | X-Frame-Options | X-Content-Type-Options | HSTS | CSP |
|---|---|---|---|---|
| bergslagenssparbank.se | Okay | Okay | HSTS Okay | Untestable |
| corren.se | Not Okay | Untestable - error | Untestable - error | Untestable - error |
| erv.se | Not Okay | Untestable - error | Untestable - error | Untestable - error |
| bliwa.se | Okay | Untestable - error | No HSTS | Untestable - error |
| alltele.se | Untestable - error | Untestable - error | Untestable - error | Untestable - error |
| amal.se | Okay | Okay | HSTS Okay | Untestable - error |
| sverigesradio.se | Okay | Okay | HSTS Okay | Ok |
| regionblekinge.se | Okay | Untestable - error | Untestable - error | Untestable - error |
| atellus.se | Not Okay | Untestable - error | Untestable - error | Untestable - error |
| av.se | Not Okay | Untestable - error | HSTS Okay | Untestable - error |

Figure 4.6: illustrates the results of 10 tested websites by secuirtyheaders.com.

Collecting data from `www.internet.nl`, and `www.securityheaders.com` has been done manually.

By analysing previous results, a difference was observed at a single website, which `www.isaltele.se`. Thus, the error rate is one in ten. This indicates that the implemented test program is effective by 90%. Therefore, the implemented test program was used in all tests.

Also, another test examines the X.509 certificate using a website called `https://www.sslshopper.com/ssl-checker.html` and the implemented tool. Both results show 100% of correctness.



| Website | Implemanted tool | sslshopper.com |
|---|---|---|
| bergslagenssparbank.se | Ok | Ok |
| corren.se | Ok | Ok |
| erv.se | Ok | Ok |
| bliwa.se | Ok | Ok |
| alltele.se | Ok | Ok |
| amal.se | Ok | Ok |
| sverigesradio.se | Ok | Ok |
| regionblekinge.se | Ok | Ok |
| atellus.se | Ok | Ok |
| av.se | Ok | Ok |

Figure 4.7: illustrates the results of 10 tested websites by implemented tool and sslshopper.com.

# 5 Results

The results section talks about the results that get from two experiments which are the automatic test and the manual test, where the first test is a tool implemented via python using security libraries. However, a second test is two online websites that can test the security standards. For the X.509 test, a website called `www.sslshopper.com/ssl-checker.html` was involved in testing the digital certificate. `www.internet.nl` is used to test the other standards. The first experiment refers to the automatic tool, and the second experiment refers to manual testing.

## 5.1 The total tested websites for implemented tool and manual tasting.

The first test shows that 36% of websites implemented DNSsec, 77.06% is for HTTPS, 33.59% for HSTS, 48.28% is for X-Frame header, 32.73% is for X-content-Type, 0.17% is for CSP, 17.61% is for Referrer-Policy header, and 89.00% is for X.509 certificate.

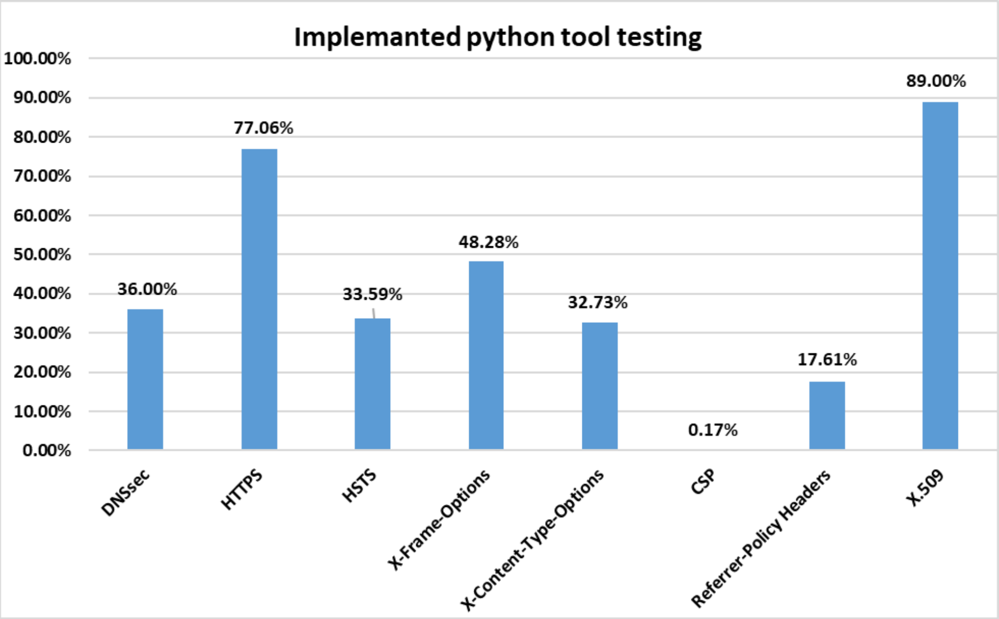


Figure 5.1 (a) : The average of implemented security standards for 1166 tested websites by the automated test.

The second test shows that 26.50% of websites implemented DNSsec, 78.30% is for HTTPS, 19.21% for HSTS, 19.21% is for X-Frame header, 17.32% is for X-content-Type, 0.09% is for CSP, 7.29% is for Referrer-Policy header and 74.79% is for X.509. certificate.

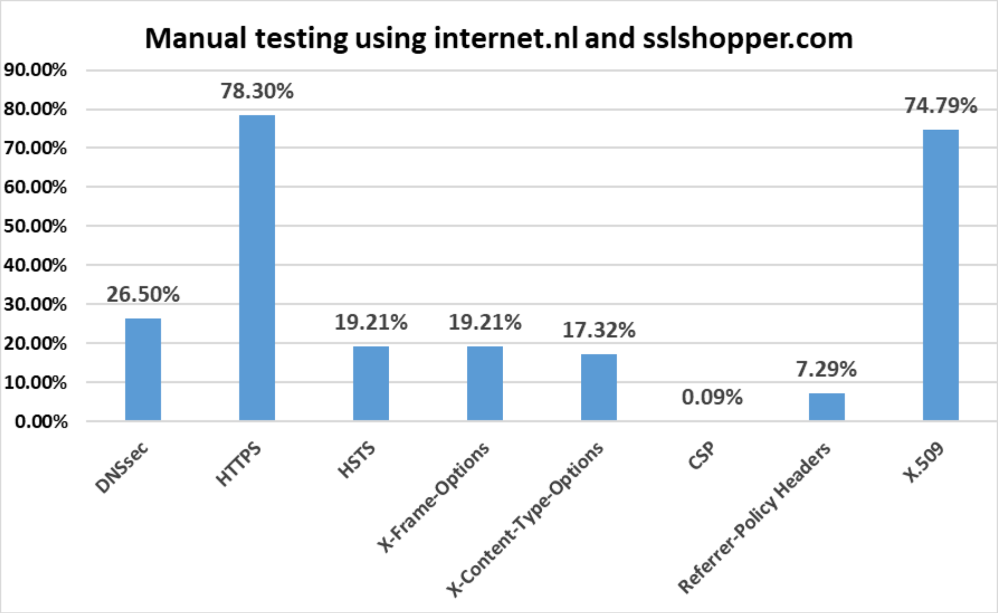


Figure 5.1 (b) : The average of implemented security standards for 1166 tested websites by the manual test.

## 5.2 The situation of implemented security standards for banks' website branch

The first test shows that 14.89% of websites implemented DNSsec, 85.11% is for HTTPS, 87.23% for HSTS, 80.85% is for X-Frame header, 79.79% is for X-content-Type, 0.00% is for CSP, 8.51% is for Referrer-Policy header, and 98.94% is for X.509 certificate.

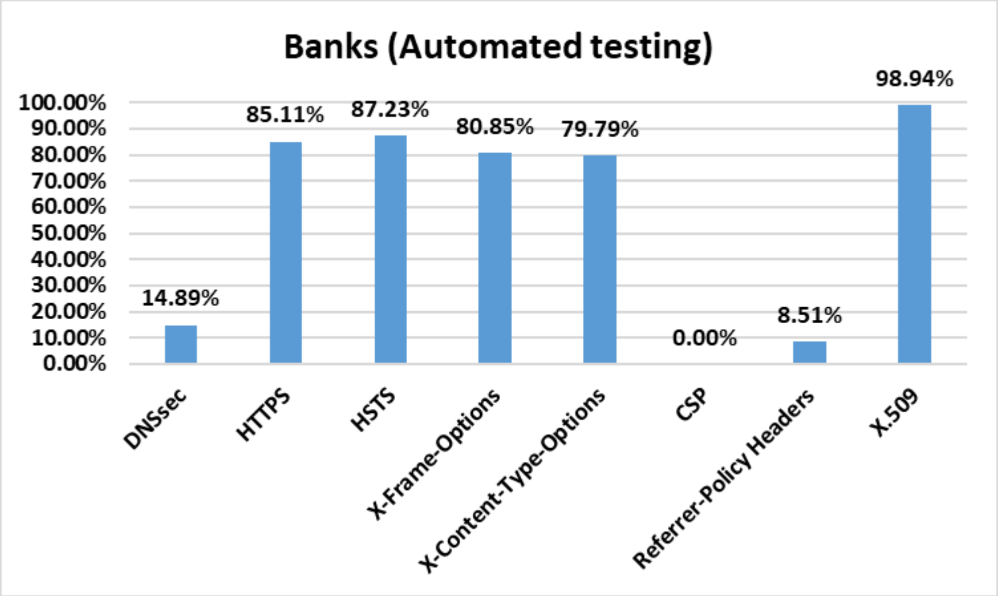


Figure 5.2 (a): The average of implemented security standards for 95 tested websites by the automated test.

The second test shows that 18.09% of websites implemented DNSsec, 70.21% is for HTTPS, 70.21% for HSTS, 65.96% is for X-Frame header, 64.89% is for X-content-Type, 0.00% is for CSP, 3.19% is for Referrer-Policy header and 98.94% is for X.509 certificate.

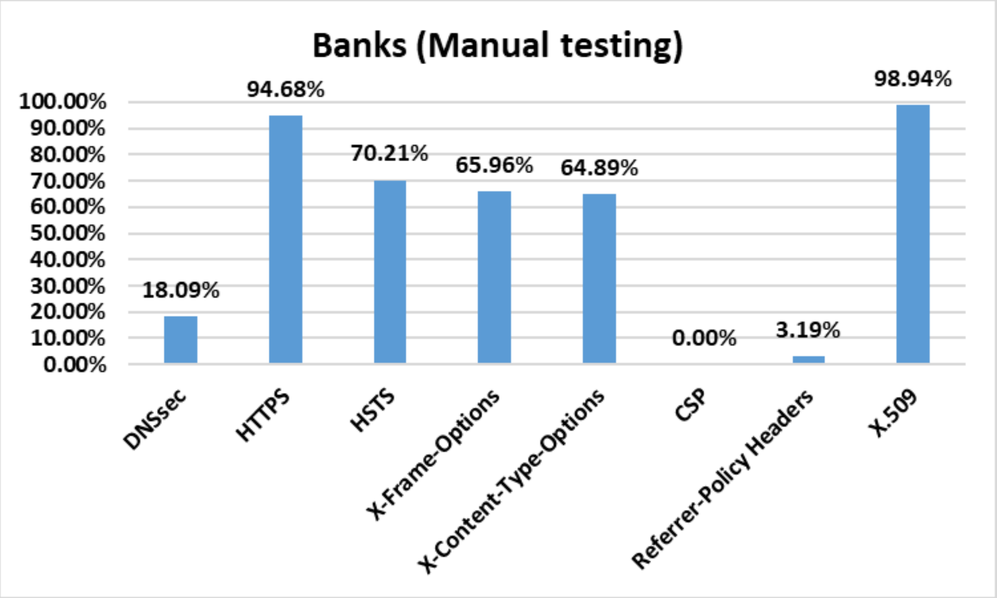


Figure 5.2 (b) : The average of implemented security standards for 95 tested websites by the manual test.

## 5.3 The situation of the implemented security standards for the insurance companies branch

The first test shows that 36.67% of websites implemented DNSsec, 76.67% is for HTTPS, 20.00% for HSTS, 46.67% is for X-Frame header, 46.67% is for X-content-Type, 0.00% is for CSP, 6.67% is for Referrer-Policy header, and 96.67% is for X.509 certificate.

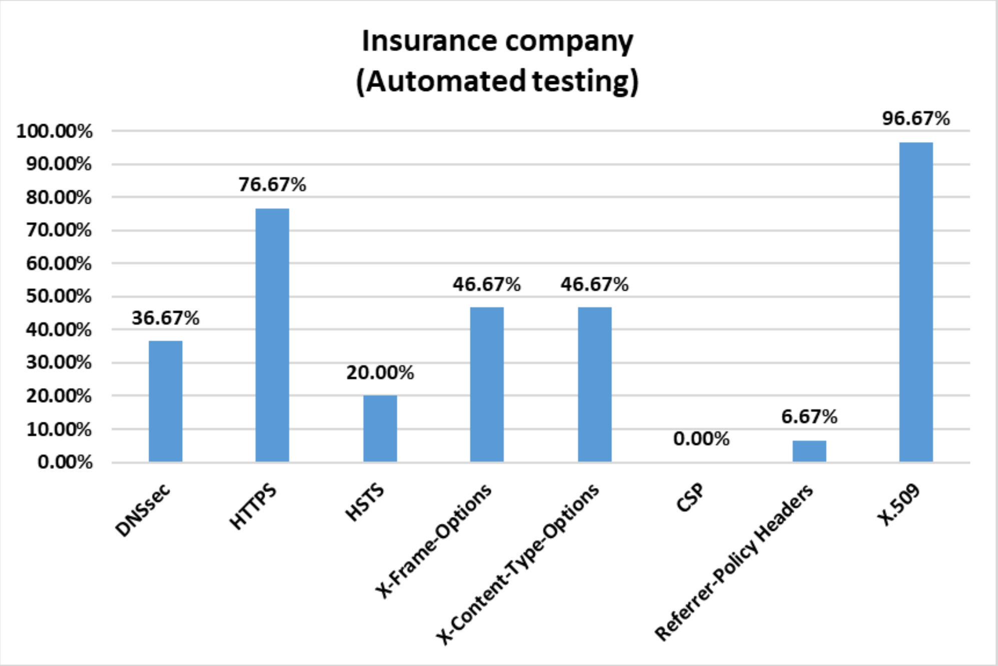


Figure 5.3 (a): The average of implemented security standards for 30 tested websites by the automated test.

The second test shows that 33.33% of websites implemented DNSsec, 93.33% is for HTTPS, 10.00% for HSTS, 23.33% is for X-Frame header, 13.33% is for X-content-Type, 0.00% is for CSP, 3.33% is for Referrer-Policy header and 90.00% is for X.509 certificate.

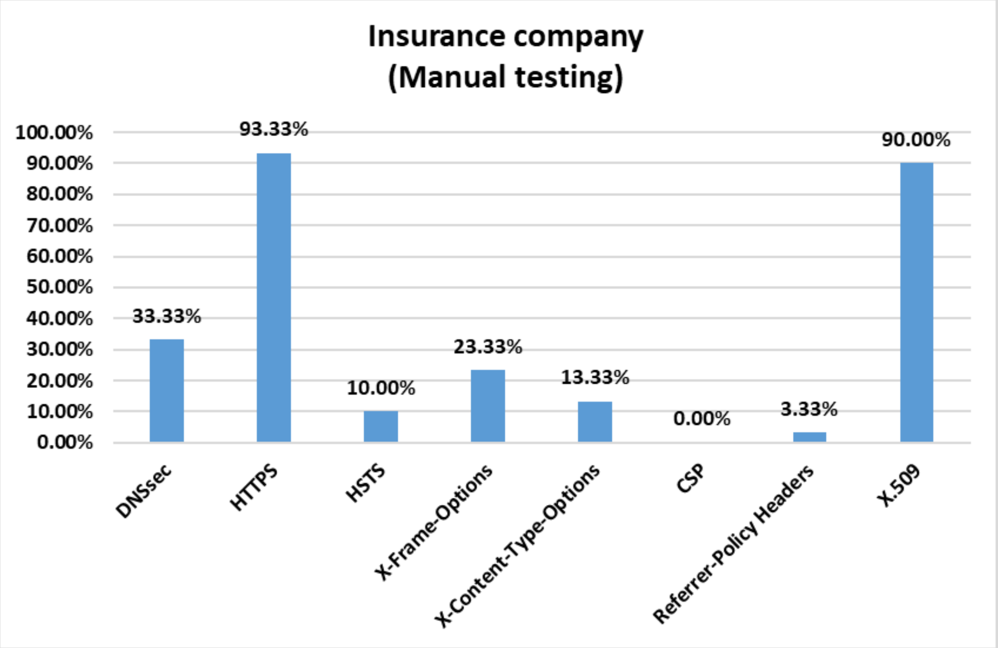


Figure 5.3 (b) : The average of implemented security standards for 30 tested websites by the manual test.

## 5.4 The situation of implemented security standards for the ISP branch

The first test shows that 22.61% of websites implemented DNSsec, 82.32% is for HTTPS, 19.51% for HSTS, 15.85% is for X-Frame header, 19.51% is for X-content-Type, 0.00% is for CSP, 12.80% is for Referrer-Policy header and 90.24% is for X.509 certificate.

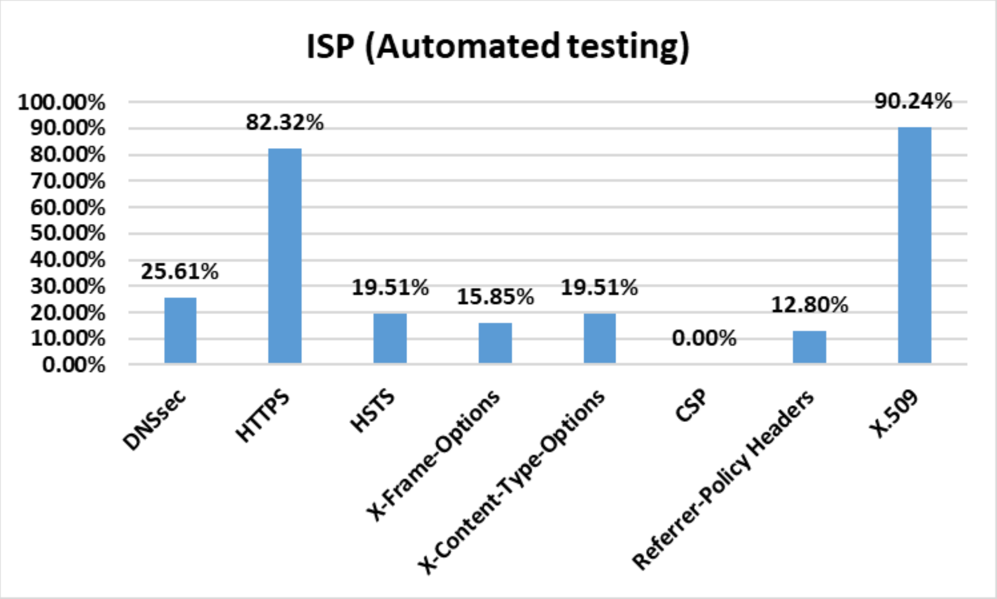


Figure 5.4 (a): The average of implemented security standards for 164 tested websites by the automated test.

The second test shows that 20.73% of websites implemented DNSsec, 92.68% is for HTTPS, 15.24% for HSTS, 13.41% is for X-Frame header, 13.41% is for X-content-Type, 0.00% is for CSP, 7.93% is for Referrer-Policy header and 88.41% is for X.509 certificate.

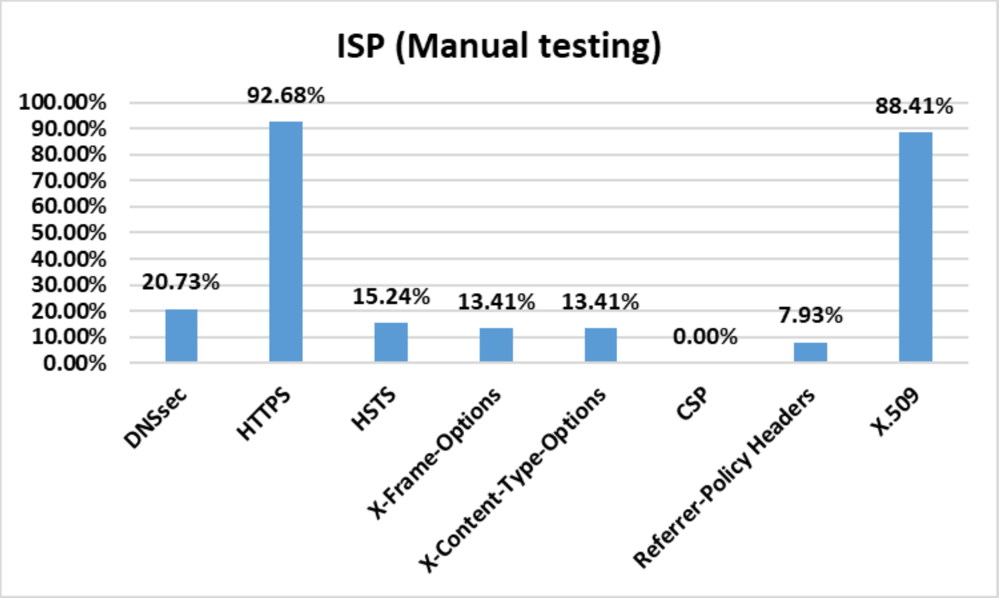


Figure 5.4 (b) : The average of implemented security standards for 164 tested websites by the manual test.

## 5.5 The situation of implemented security standards for the Media branch

The first test shows that 0.0% of websites implemented DNSsec, 55.56% is for HTTPS, 16.67% for HSTS, 33.33% is for X-Frame header, 66.67% is for X-content-Type, 0.0% is for CSP, 22.22% is for Referrer-Policy header, and 72.22% is for X.509 certificate.

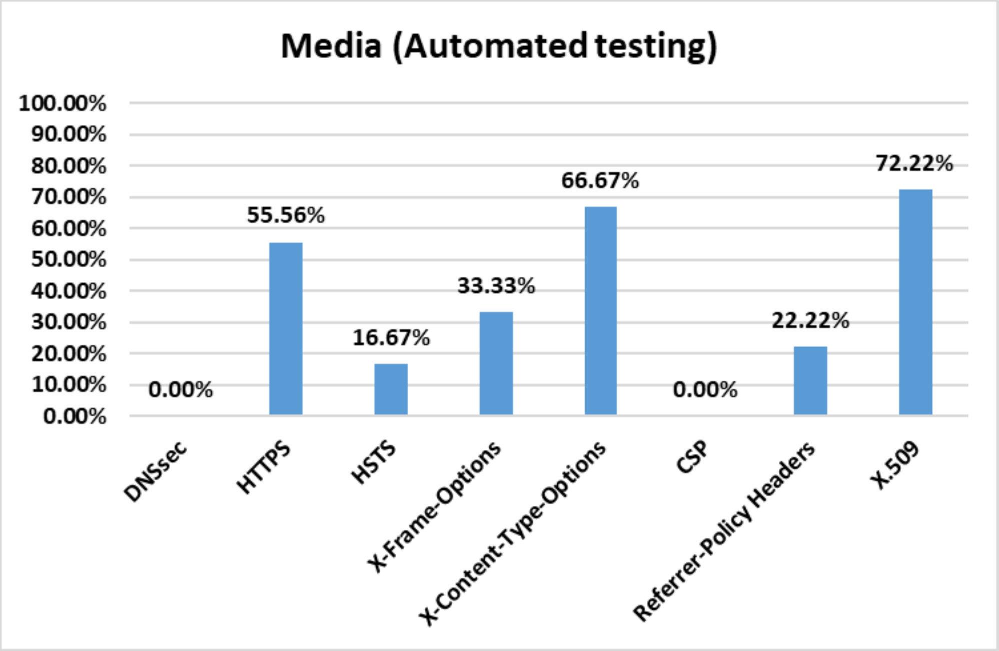


Figure 5.5 (a): The average of implemented security standards for 18 tested websites by the automated test.

The second test shows that 0.00% of websites implemented DNSsec, 77.78% is for HTTPS, 5.56% for HSTS, 11.11% is for X-Frame header, 11.11% is for X-content-Type, 0.00% is for CSP, 0.00% is for Referrer-Policy header and 72.22% is for X.509 certificate.

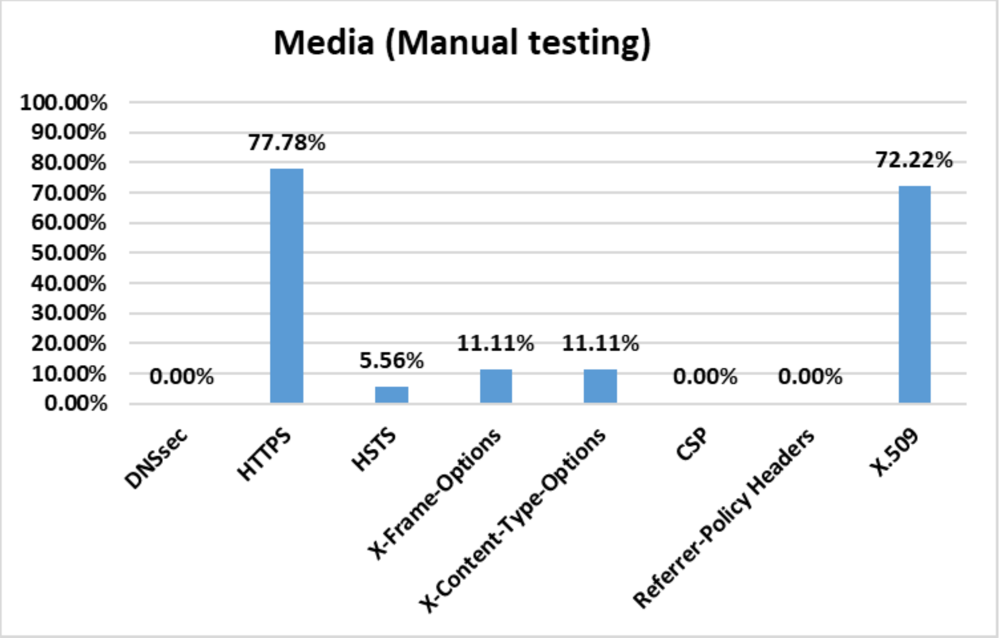


Figure 5.5 (b): The average of implemented security standards for 18 tested websites by the manual test.

## 5.6 The situation of implemented security standards for the municipalities branch

The first test shows that 47.44% of websites implemented DNSsec, 78.69% is for HTTPS, 21.59% for HSTS, 67.90% is for X-Frame header, 17.33% is for X-content-Type, 0.00% is for CSP, 22.16% is for Referrer-Policy header, and 84.94% is for X.509 certificate.

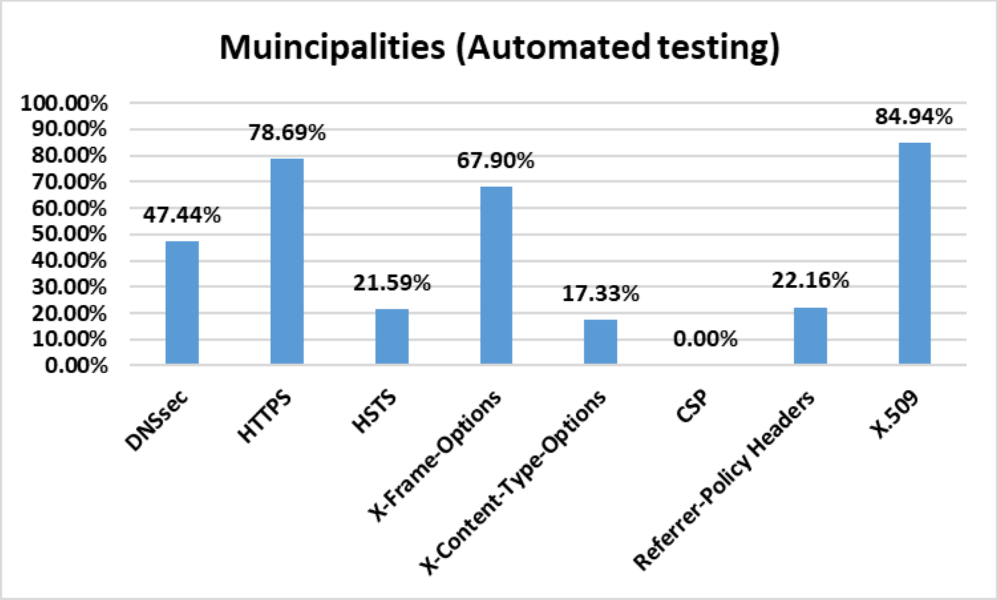


Figure 5.6 (a): The average of implemented security standards for 352 tested websites by the automated test.

The second test shows that 56.25% of websites implemented DNSsec, 88.07% is for HTTPS, 13.64% for HSTS, 32.67% is for X-Frame header, 7.95% is for X-content-Type, 0.00% is for CSP, 11.65% is for Referrer-Policy header and 82.67% is for X.509 certificate.

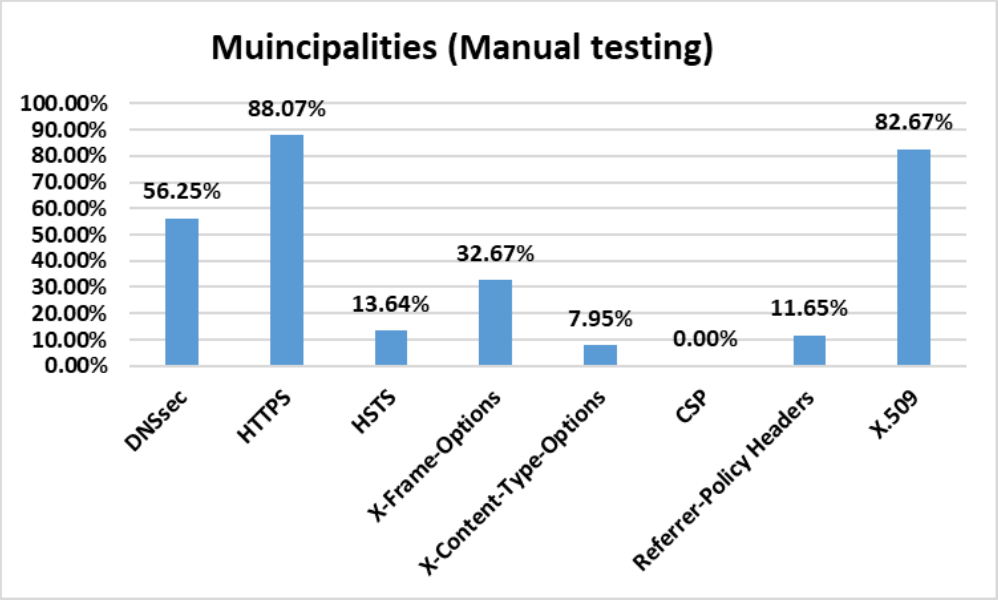


Figure 5.6 (b) : The average of implemented security standards for 352 tested websites by the manual test.

## 5.7 The situation of implemented security standards for the newspapers branch

The first test shows that 1.59% of websites implemented DNSsec, 53.97% is for HTTPS, 50.79% for HSTS, 7.94% is for X-Frame header, 41.27% is for X-content-Type,3.17% is for CSP, 34.92% is for Referrer-Policy header, and 100% is for X.509 certificate.

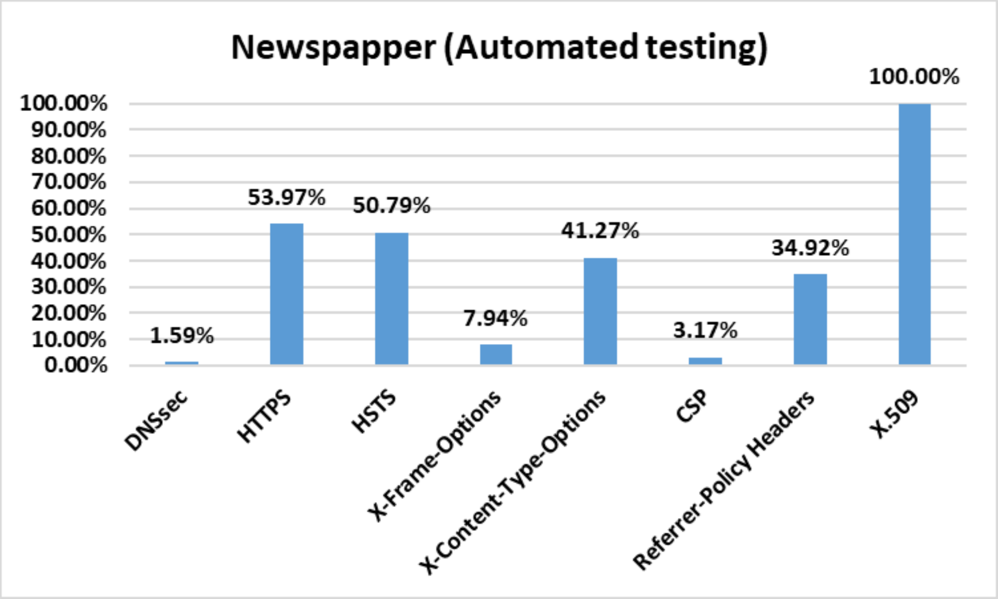


Figure 5.7 (a): The average of implemented security standards for 65 tested websites by the automated test.

The second test shows that 7.94% of websites implemented DNSsec, 96.83% is for HTTPS, 14.29% for HSTS, 0.00% is for X-Frame header, 1.59% is for X-content-Type, 0.007% is for CSP, 0.00% is for Referrer-Policy header and 96.83% is for X.509 certificate.

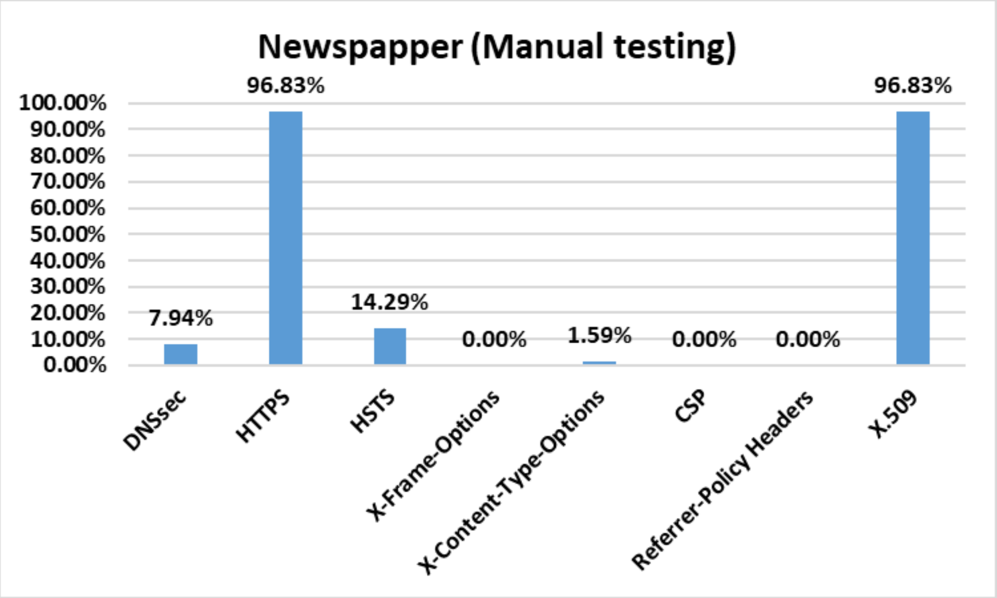


Figure 5.7 (b) : The average of implemented security standards for 65 tested websites by the manual test.

## 5.8 The situation of implemented security standards for the region's branch

The first test shows that 57.14% of websites implemented DNSsec, 85.71% is for HTTPS, 38.10% for HSTS, 52.38% is for X-Frame header, 23.81% is for X-content-Type, 0.00% is for CSP, 23.81% is for Referrer-Policy header, and 95.24% is for X.509 certificate.

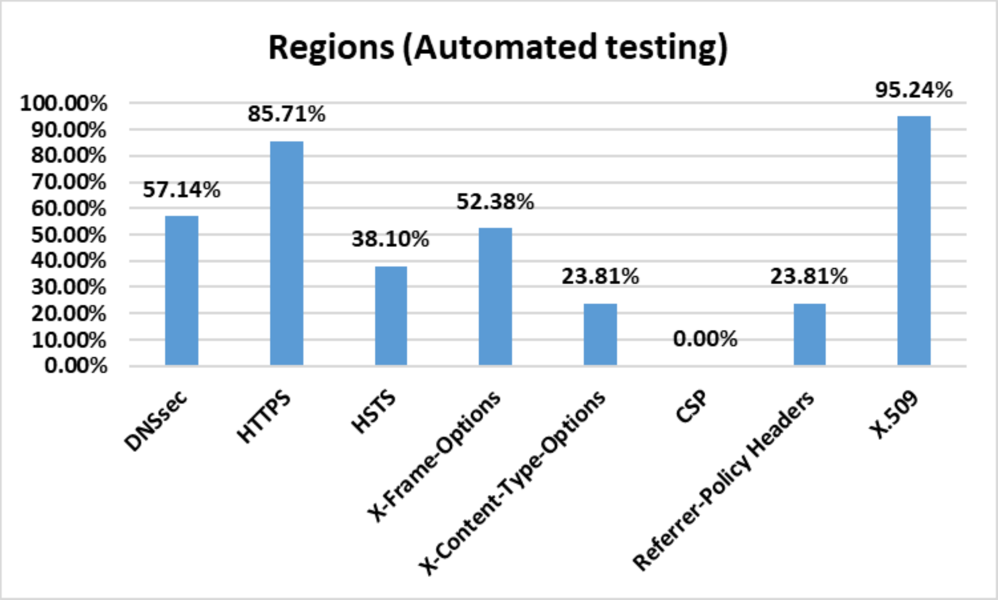


Figure 5.8 (a): The average of implemented security standards for 21 tested websites by the automated test.

The second test shows that 71.43% of websites implemented DNSsec, 95.24% is for HTTPS, 23.81% for HSTS, 23.81% is for X-Frame header, 47.62% is for X-content-Type, 0.00% is for CSP, 19.05% is for Referrer-Policy header and 95.24% is for X.509 certificate.

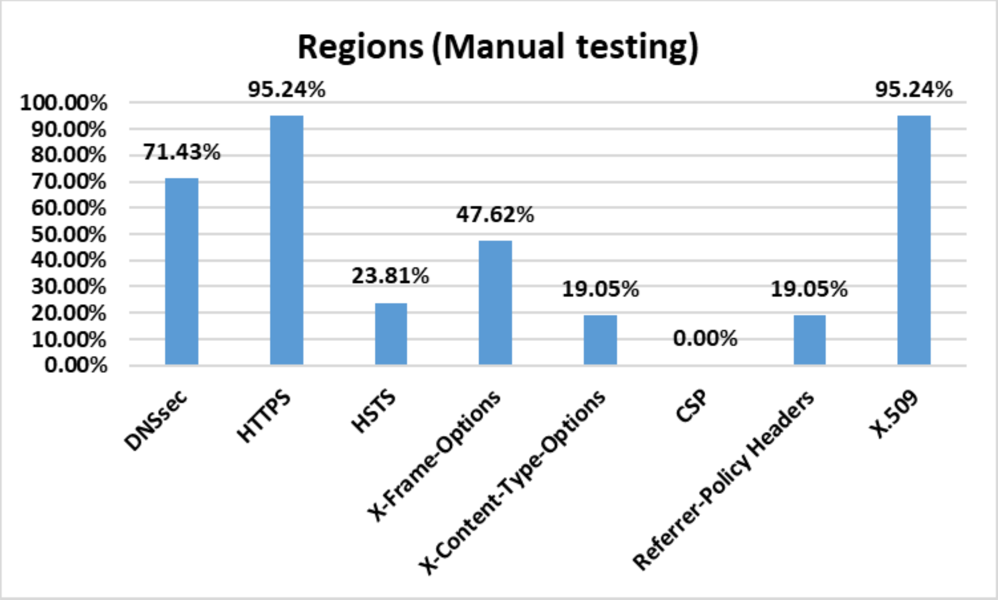


Figure 5.8 (b) : The average of implemented security standards for 21 tested websites by the manual test.

## 5.9 The situation of implemented security standards for the registrars' branch

The first test shows that 28.57% of websites implemented DNSsec, 80.45% is for HTTPS, 33.08% for HSTS, 26.32% is for X-Frame header, 26.32% is for X-content-Type, 0.00% is for CSP, 12.78% is for Referrer-Policy header, and 90.98% is for X.509 certificate.

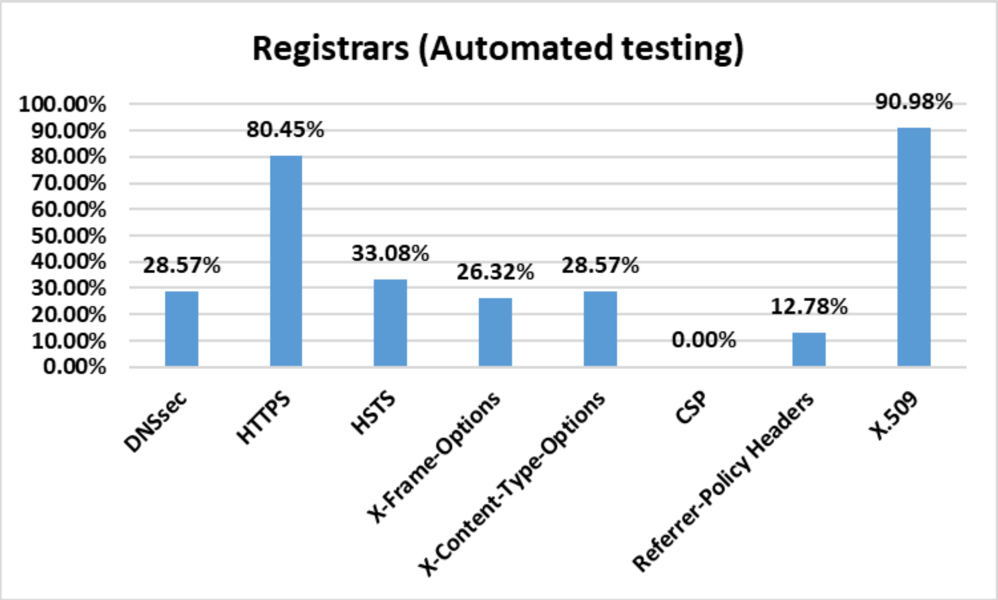


Figure 5.9 (a): The average of implemented security standards for 133 tested websites by the automated test.

The second test shows that 27.82% of websites implemented DNSsec, 93.98% is for HTTPS, 25.56% for HSTS, 32.31% is for X-Frame header, 21.80% is for X-content-Type, 0.00% is for CSP, 13.53% is for Referrer-Policy header and 89.47% is for X.509 certificate.

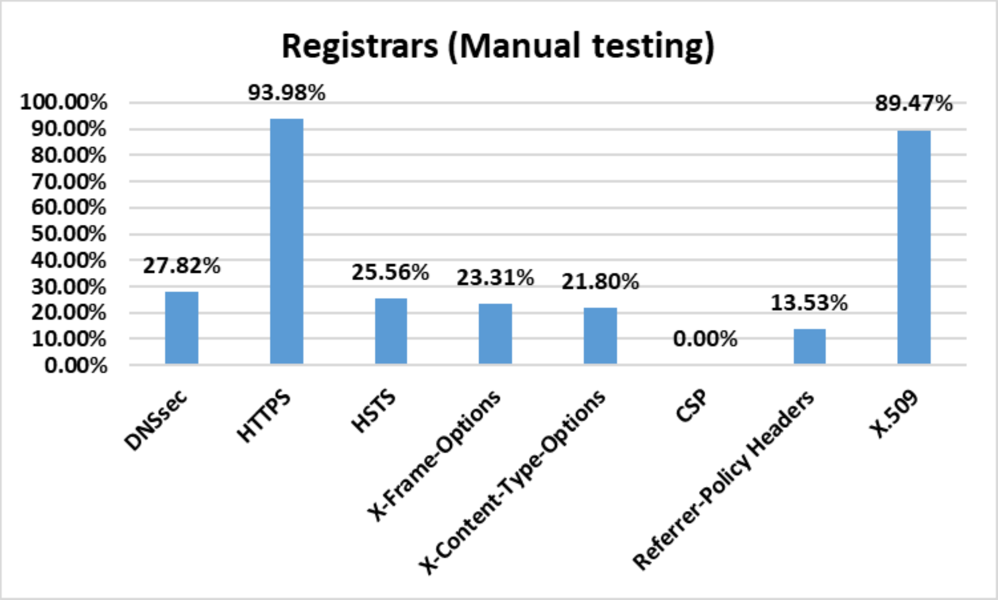


Figure 5.9 (b) : The average of implemented security standards for 133 tested websites by the manual test.

## 5.10 The situation of implemented security standards for the government agencies branch

The first test shows that 49.74% of websites implemented DNSsec, 72.77% is for HTTPS, 40.31% for HSTS, 53.40% is for X-Frame header, 38.74% is for X-content-Type, 0.00% is for CSP, 27.23% is for Referrer-Policy header, and 86.39% is for X.509 certificate.

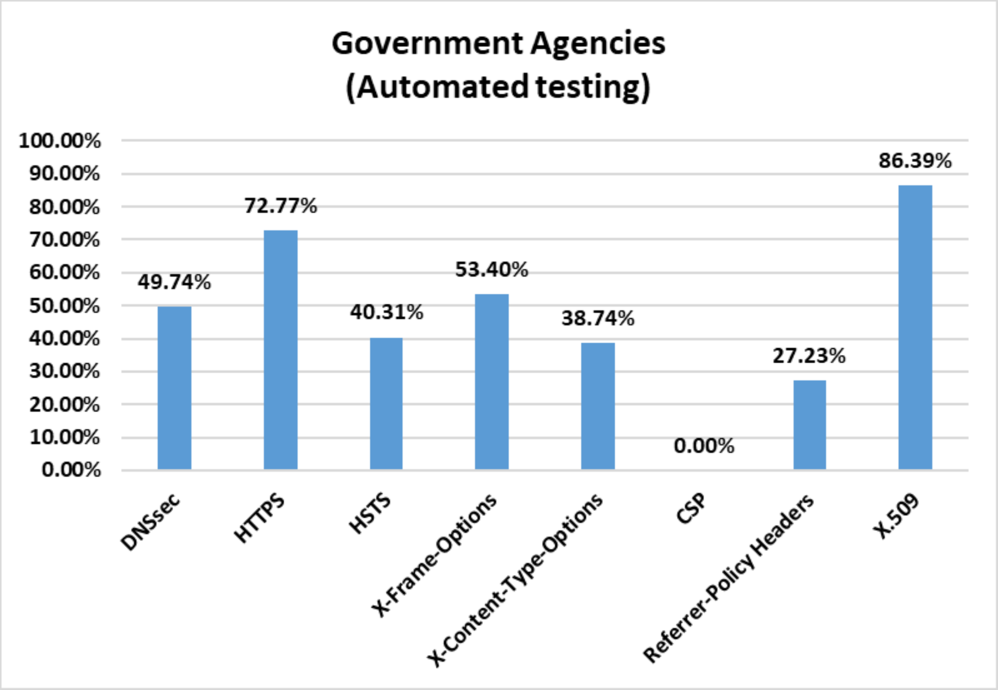


Figure 5.10 (a): The average of implemented security standards for 191 tested websites by the automated test.

The second test shows that 59.16% of websites implemented DNSsec, 68.91% is for HTTPS, 19.90% for HSTS, 22.51% is for X-Frame header, 18.32% is for X-content-Type, 0.00% is for CSP, 12.57% is for Referrer-Policy header and 76.96% is for X.509 certificate.

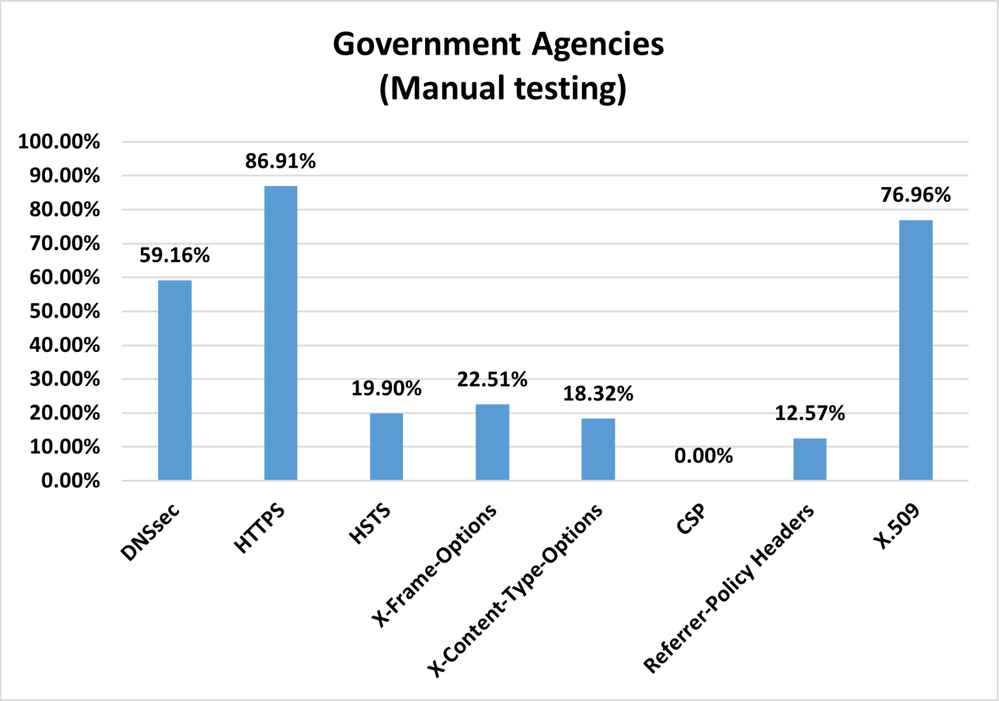


Figure 5.10 (a): The average of implemented security standards for 191 tested websites by the automated test.

## 5.11 The situation of implementing security standards for the State-owned companies branch.

The first test shows that 33.33% of websites implemented DNSsec, 68.75% is for HTTPS, 37.50% for HSTS, 56.25% is for X-Frame header, 58.33% is for X-content-Type, 0.00% is for CSP, 22.92% is for Referrer-Policy header, and 89.58% is for X.509 certificate.

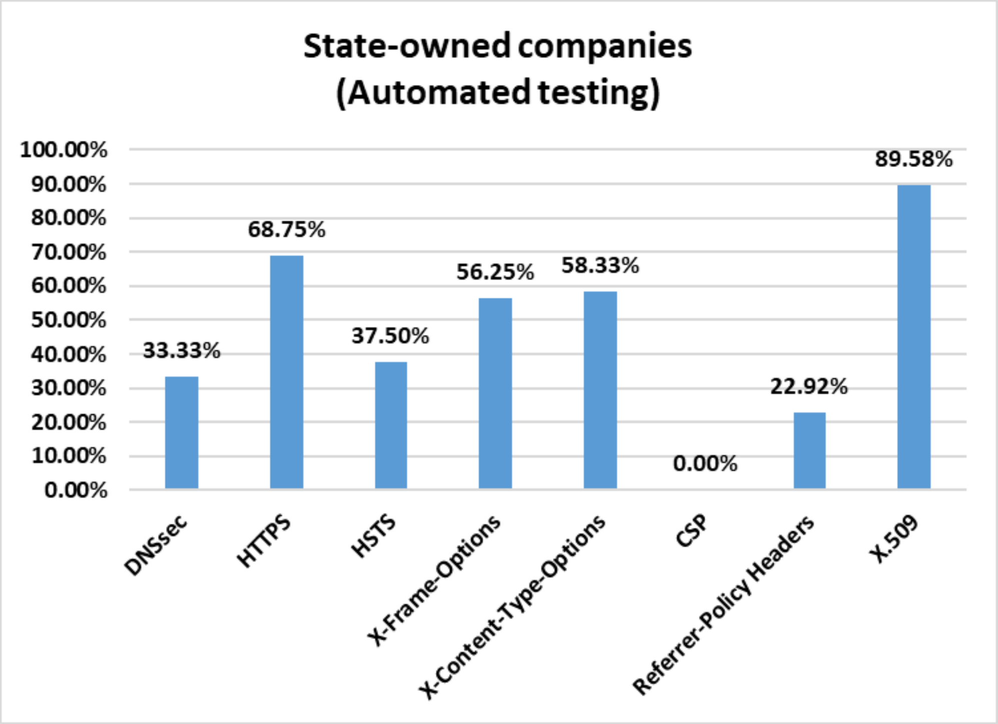


Figure 5.11 (a): The average of implemented security standards for 47 tested websites by the automated test.

The second test shows that 41.67% of websites implemented DNSsec, 14.58% is for HTTPS, 14.58% for HSTS, 20.83% is for X-Frame header, 22.92% is for X-content-Type, 0.00% is for CSP, 6.25% is for Referrer-Policy header and 91.67% is for X.509 certificate.

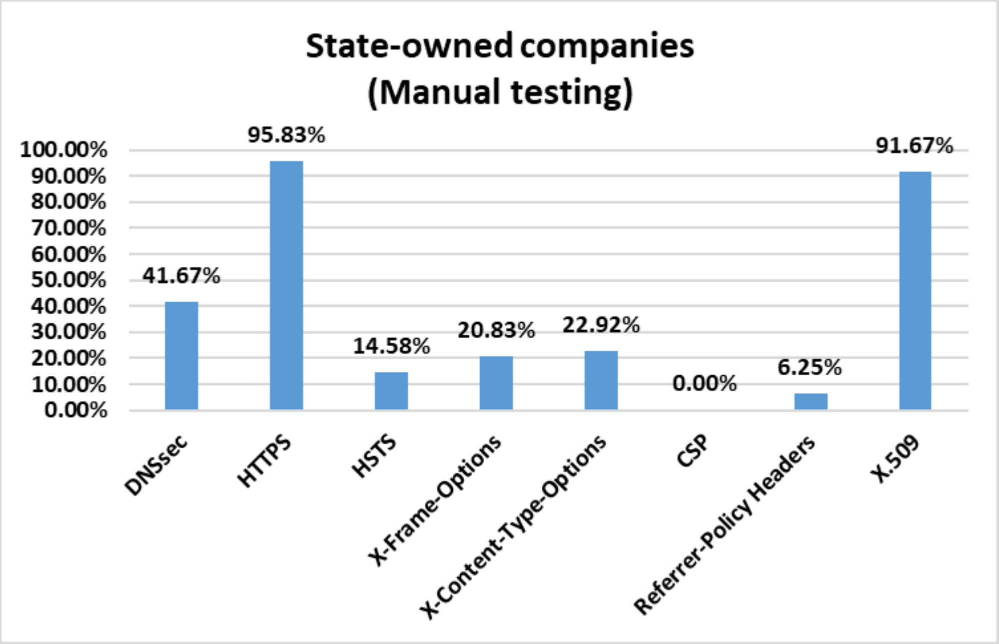


Figure 5.11 (b) : The average of implemented security standards for 47 tested websites by the manual test.

## 5.12 The situation of implemented security standards for the universities branch

The first test shows that 31.25% of websites implemented DNSsec, 85.42% is for HTTPS, 27.08% for HSTS, 43.75% is for X-Frame header, 35.42% is for X-content-Type, 0.00% is for CSP, 25.00% is for Referrer-Policy header, and 93.75% is for X.509 certificate.

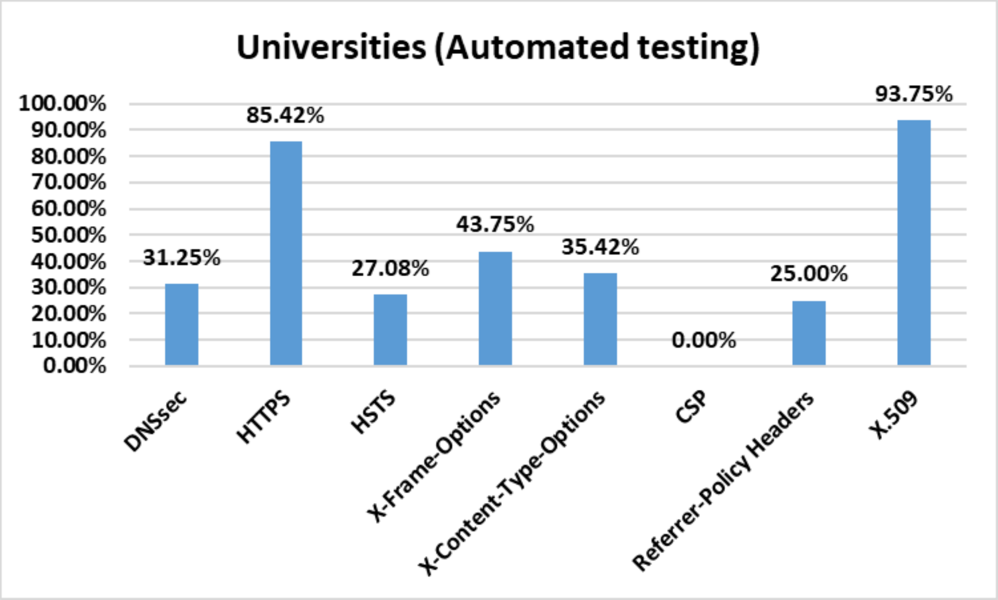


Figure 5.12 (a): The average of implemented security standards for 48 tested websites by the automated test.

The second test shows that 50.00% of websites implemented DNSsec, 95.83% is for HTTPS, 20.83% for HSTS, 27.08% is for X-Frame header, 18.75% is for X-content-Type, 2.08% is for CSP, 12.50% is for Referrer-Policy header and 93.75% is for X.509 certificate.

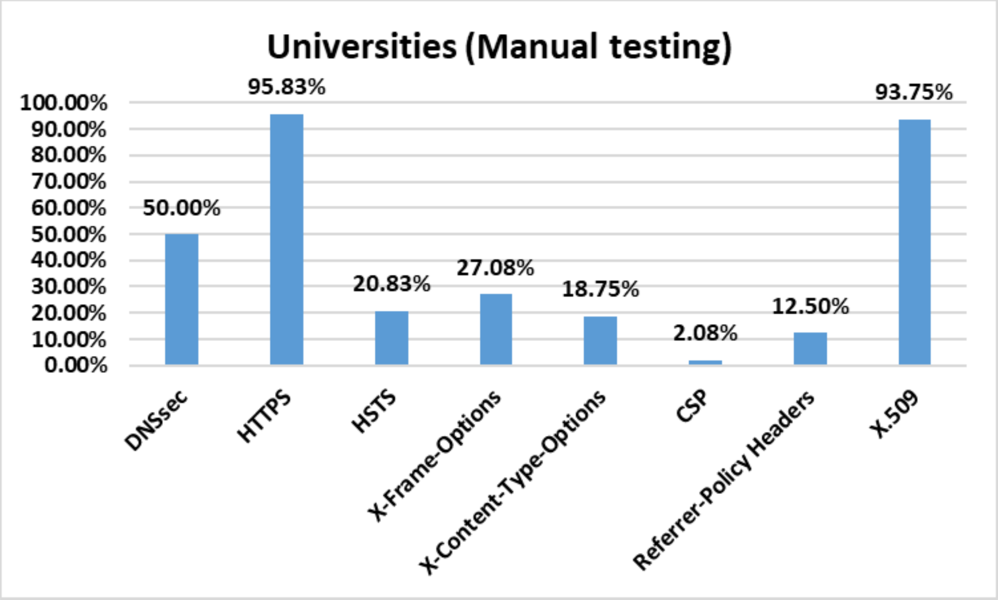


Figure 5.12 (b) : The average of implemented security standards for 48 tested websites by the manual test.

## 5.13 The situation of implemented security standards by branches

The first test shows standards implementation by branches. For universities is 42.71%, state-owned companies is 45.57%, government agencies is 43.78%, registrar is 38.06%, regions is 47.02%, news is 35.58%, municipalities is 42.51%, media is 33.33 %, ISP is 33.23%, insurance company is 44.58%, and banks is 56.91%.

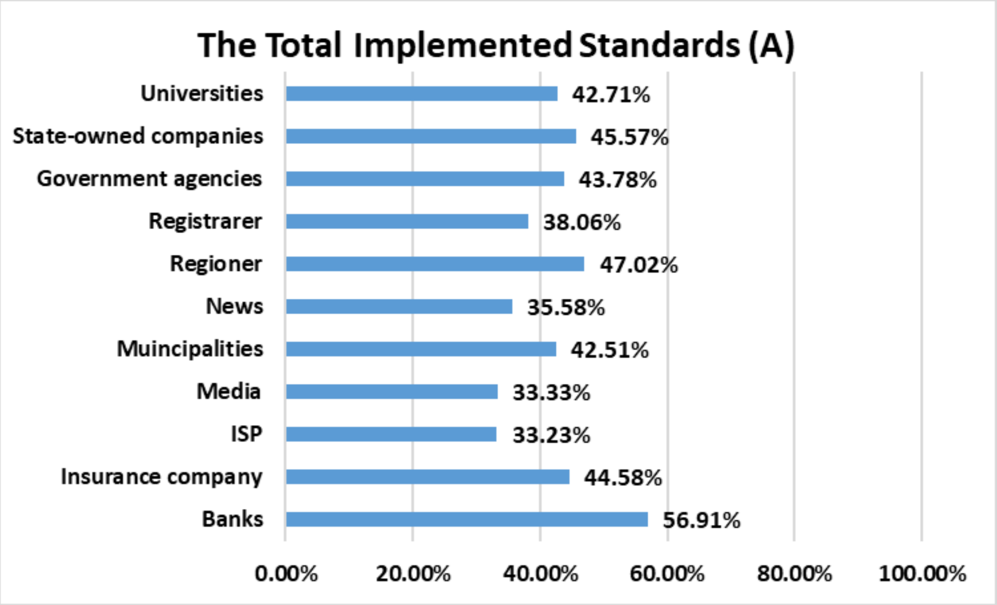


Figure 5.13 (a): The average of implemented security standards for 1166 tested websites by the automated test.

The second test shows standard implementation by branches. For universities is 42.78%, state-owned companies is 40.06%, government agencies is 48.13%, registrar is 41.28%, regions is 48.28%, news is 28.07%, municipalities is 35.21%, media is 30.77 %, ISP is 35.60%, insurance company is 37.04%, and banks is 52.55%.

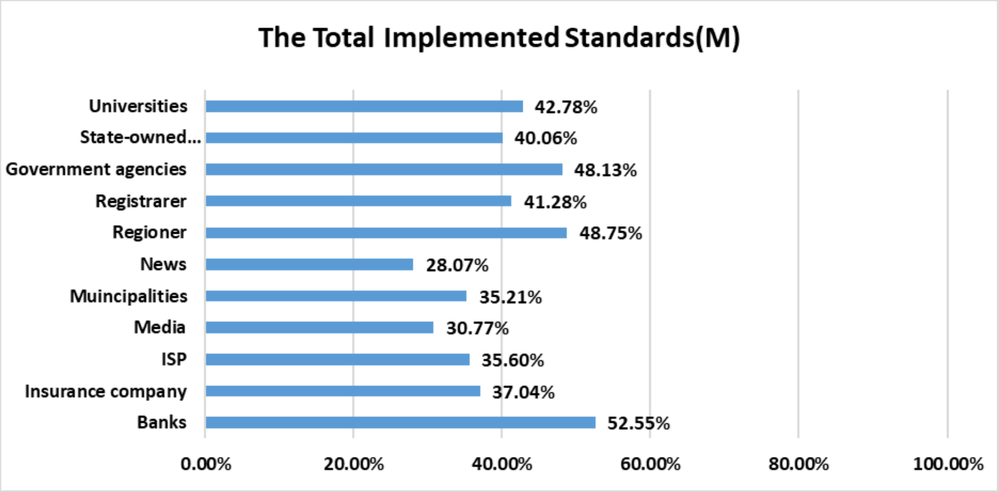


Figure 5.13 (b): The average of implemented security standards for 1166 tested websites by the manual test.

# 6 Analysis and discussion

This chapter is a data analysis that has been taken from both experiments, which showed in the results chapter. Moreover, the answers to the thesis questions will be provided in this chapter. In addition, this chapter will contain discussion.

## 6.1 **RQ1**- How secure are the Swedish websites? Furthermore, Is the security extension implementation in- creased compared to the study in 2014?

The results showed that both experiments had a low rate. For the first experiment, two types of data are obtained. The first type is the significant security mechanisms: DNSsec was 36%, HTTPS was 77,06%, HSTS was 33,59%, and X.509 was 89,00% of all tested websites. These standards are important to get the correct website and secure communication. The rate of this group is 58.9125%. The second type is optional security standards which are X-Frame-Options was 48,25%, X-Content-Type-Options was 32,73%, CSP was 0,17%, and implementation of Referrer-Policy Headers was 17,61%. The rate of this group is 24,69%. However, The assembling of all standards gives a total of 48.80%. The total rate of adoption is 54.35% on all tested websites.

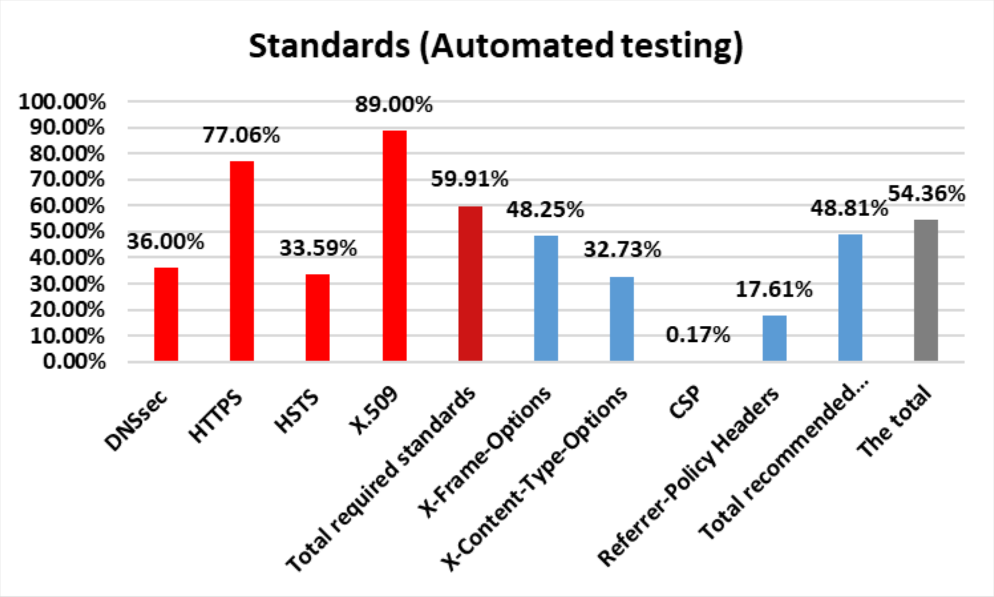


Figure 6.1.1: Average adoption of standards where red is required standards and blue is recommended standards via Automated testing (1166).

On the other hand, the second experiment showed that 26.50% of websites were implementing DNSsec, 78.30% of websites were implementing HTTPS, 19.21% of websites had HSTS, and 74.79% of total tested websites had the correct X.509 certificate. The rate of this group was 49.7%. However, the optional standards X-Frame-Options was 19.21%, X-Content-Type-Options was 17.32%, CSP was 0.09%, and Referrer-Policy Header was implemented by 7.29% of all tested websites. The total average of this group is 10.97%. The assembling of both standards is 30.33%.

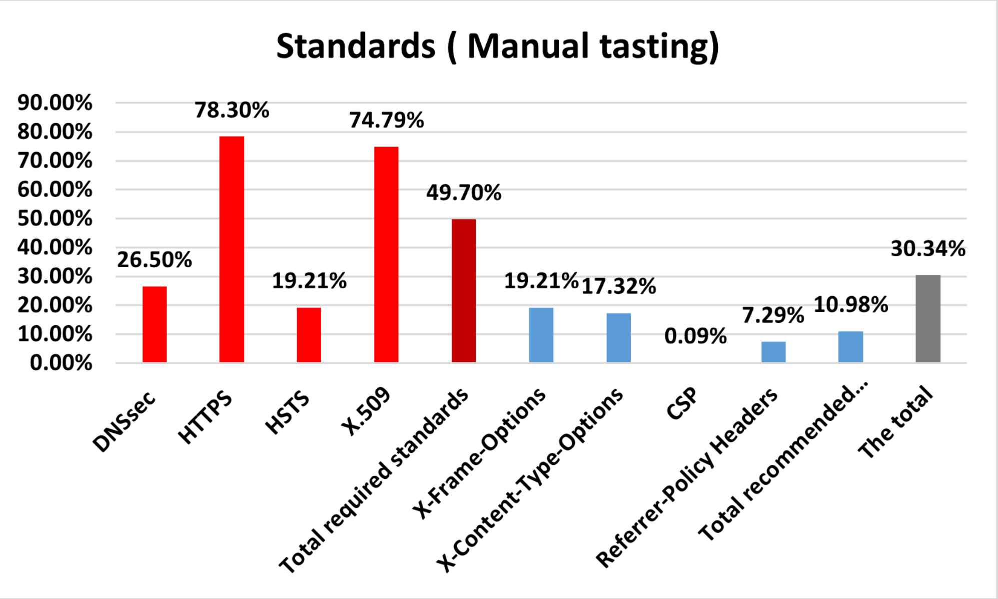
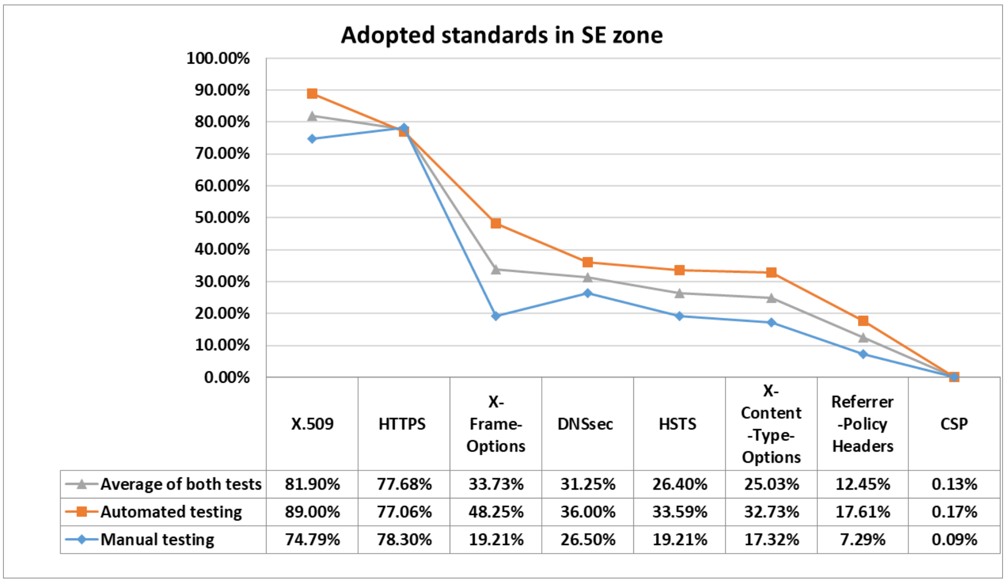


Figure 6.1.2: Average adoption of standards where red is required and blue is recommended by manual testing (1166).

The average of both tests is 43.85%. Therefore, the Swedish websites have high vulnerabilities, which will affect the end-user if attackers try bypassing the security standards. Moreover, a comparison of the results that got from the Swedish Internet Foundation 2014 shows an increase of 6% of websites that added DNSsec in their domains which were 29% and now become 36%. However, the comparison with manual testing shows decreasing in 2.5% of all tested websites.

## 6.2 **RQ2**- What are the web security standards adopted by Swedish web- sites? Moreover, what is the situation if websites do not adopt these standards?

The top deployed Internet standard is X.509, with the average of both tests 81.90%, and automated testing showed 89.00%. However, the manual testing was 74.79%, which is the second topmost standard for the manual group. The second topmost standard is HTTPS, with an average of both tests 77.68% and 77.06% for automated testing. However, the HTTPS was deployed by 78.30% by manual testing, making it the top implemented standard for the manual testing group. X-Frame-Options is the third standard that is implemented in the SE zone. There is a significant difference between the results that can be distinguished clearly between both tests. The difference is around 30%, where the automated testing is 48.25% and the other one 19.21%, with an average of 33.73%. DNSsec, HSTS, and X-Content-Type-Options are implemented between 35% to 25% of all tested websites. The most unimplemented standard is CSP, with an average of 0.13%, and the second most unimplemented standard is Referrer-Policy Headers, with an average of 12.45%. Both standards are optional.



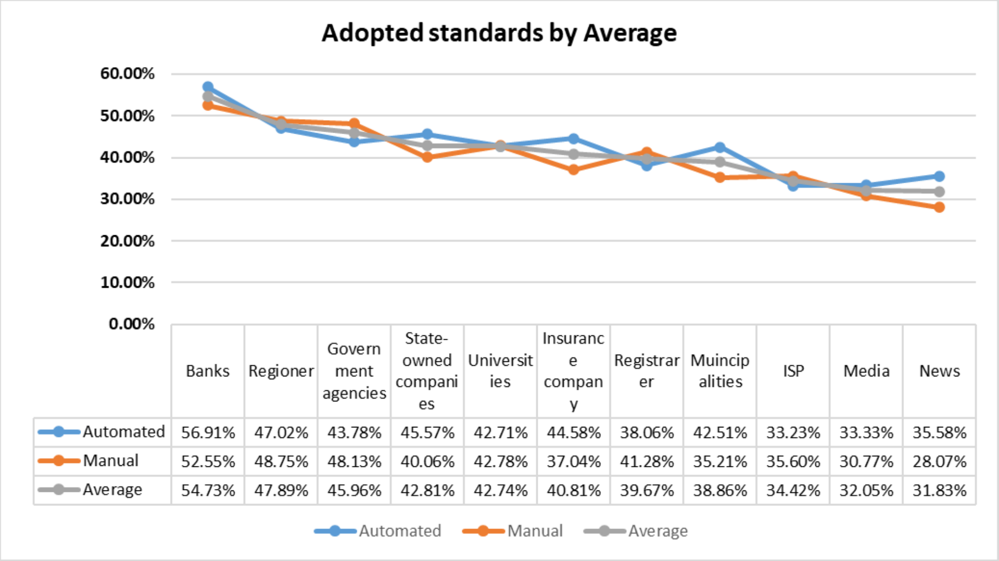
| | X.509 | HTTPS | X-Frame-Options | DNSsec | HSTS | X-Content-Type-Options | Referrer-Policy Headers | CSP |
|---|---|---|---|---|---|---|---|---|
| Average of both tests | 81.90% | 77.68% | 33.73% | 31.25% | 26.40% | 25.03% | 12.45% | 0.13% |
| Automated testing | 89.00% | 77.06% | 48.25% | 36.00% | 33.59% | 32.73% | 17.61% | 0.17% |
| Manual testing | 74.79% | 78.30% | 19.21% | 26.50% | 19.21% | 17.32% | 7.29% | 0.09% |

Figure 6.2.1: Adopted standards in the SE zone. Grey colour is the average of both tests, Orange colour is the automated testing, and manual in a blue one.

All Swedish websites can be affected by cyber-attacks because no one of the standards have been implemented fully by all websites. As a result, websites are safe from man-in-the-middle attack. However, it still hackable by downgrade attacks which change the communication between server and client from HTTPS to HTTP. Furthermore, the average of DNSsec might affect publishing information during the war. Also, the XSS can be dangerous.

## 6.3 **RQ3**-What is the safest sector that has been able to meet all security standards? Are the adoption of web security extensions effective by sector?

No sector has met all test security standards. However, the sector with the highest score is the bank, with 54.73%. The second sector is Regions, with an average of 47.89%. The third sector is State-owned agencies with 45.96%. The results show that security standards deployment is effective by the sectors because the finance branch has the highest average.



| | Banks | Regioner | Government agencies | State-owned companies | Universities | Insurance company | Registrarer | Muincipalities | ISP | Media | News |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Automated | 56.91% | 47.02% | 43.78% | 45.57% | 42.71% | 44.58% | 38.06% | 42.51% | 33.23% | 33.33% | 35.58% |
| Manual | 52.55% | 48.75% | 48.13% | 40.06% | 42.78% | 37.04% | 41.28% | 35.21% | 35.60% | 30.77% | 28.07% |
| Average | 54.73% | 47.89% | 45.96% | 42.81% | 42.74% | 40.81% | 39.67% | 38.86% | 34.42% | 32.05% | 31.83% |

Figure 6.3.1: Adopted standards in the SE zone by average. Grey colour is the average of both tests, Orange colour is the manual testing, and automated in a blue one.

The state of internet standards in the SE zone was undefined. The study is based on many related works that contain both standard types, the recommendations and the optional standards. Using the implemented tool using python language helps to find better results than the **Internet.nl**. However, the certificate test by **shopper.com/ssl-checker.html** gives the same results as the implemented tool.

Adopting Internet standards, both the recommended and optional standards, have a low avarage. Even the Swedish Internet Foundation was the first internet foundation that used DNSsec in their zone. However, the DNSsec adoption is around 36% of the total websites.

The expected results from this research are much higher, but the results prove the opposite expectation. Moreover, 81.90% of tested certificates follow the RFC 5280 standard, but about 20% does not meet the requirements of this standard, which means this is harmful to the client. During the test, all types of certificate failures appeared on exams. For example, when three are X.509 certificates, it finds HTTPS, but the average of HTTPS is 77,68%, which is less than X.509. An example of an unprotected website was one bank website with a correct certificate, but it does not have an HTTPS correct establishment. After a few months, the website has HTTPS now, which is excellent. Man in the middle attack affects about 23% of the visitor. However, HSTS has a low average of 26%. 70% of the websites are vulnerable to downgrade attacks if they use more miniature versions than TLS 1.3. All optional standards have a low average. However, some websites have implemented those standards.

There is a big gap during the test. Internet.nl has some issues, especially during the examination of optional security standards. When the header gets from the server, Internet.nl has no distinction between capital letters and small letters. As a result, some websites have some value that the Internet.nl can not test. During the writeing the paper, An email had been sent to Internet.nl asking if they test case sensitive. The answer was According to (**RFC 7230** and **RFC 7540**) ) HTTP header fields are case-insensitive and Internet.nl check does not check cases. The emails can found in appendices 13, and 14.

In addition, the possibility of getting the correct website content is limited because 36% of websites have DNSsec, which means attackers can fake the website. Attackers can apply DNS spoofing or DNS cache poisoning, targeting cache corruption. Other attacks aimed at X.509 are possible because around 20% of websites do not have the correct structure. Also, the incorrect configuration of X.509 standard effect HTTPS gives attackers the ability to apply Man in the middle attack. The low average of optional standards allows attackers to use XSS against clients. Nevertheless, clients might get incorrect websites. Swedish websites are vulnerable to all attacks mentioned before. X-Frame-Options prevents clickjacking; however, the average of using this optional frame is 33.73%, but the implemented tool shows more value with 48.25%. Therefore, 52% of websites are vulnerable to invisible frames. Again man in the middle attack shows the advantage when the website does not use X-content-Type-options. The total number of vulnerable websites is around 75%. 82.39% of tested websites allow user tracking by not using the Referrer-Policy header. Almost every website has not used CSP, which means users might hack by XSS and injection attacks. However, if the website uses X-Frame-Options Header, it can ignore using CSP because it gives the same protection. Moreover, websites might allow destructive JavaScript code.

Banks are the most secure websites that have used many security standards. The main reason that could answer the question is that banks have the primary credential for financial services, provision of funds and remittance.

The importance of the security standards studied in this research topic can determine by the relationship between the security importance of organizations and the value of distributed information. In addition, cyber operations may be affected by hostile environments where one country threatens another.

# 7 Conclusions

In this thesis, the quality of two types of security standards implemented by 1166 websites and divided into eleven sectors examined by two methods. All examined websites located in the Swedish zone (SE zone). Furthermore, the recommended and optional standards explained in specific. Also, an objectivism fact showed how these standards have an indisputable effect on web security.The research shows insecurity in all sectors, and the average security adoption is around 50%. The automated test shows an increase in deployment for DNSsec compared to 2014. Moreover, the most security deployment is X.509 v3, and the bank sector has the most security deployment. The Swedish websites have more security deployment than the other countries.

The research demonstrates the gap in the SE zone and discusses and determines all expected attacks that may be vulnerable to the websites due to lack of miscommunication and ignorance of the security standards.

In conclusion, the research demonstrated the concern that there is a threat to organizations and an urgent need to re-examine security in general and vulnerable sites according to security mechanisms to be more secure.

## 7.1 Recommendation

Disinformation and cyber-attacks increased after the Russian invasion of Ukraine. According to the Swedish Ministry of Defence, Sweden is subject to major cyber attacks. I believe that these attacks aim at falsifying information and stealing money. Especially when Swedbank lost money, affecting many of the bank's clients. I recommend a comprehensive review of all security systems and the mandatory use of optional headers. This will help access information, avoiding mistakes and cyber-attacks during future wars that are expected to occur. In the end, do not trust the security information that will get by **Internet.nl**.

# 8 Future Work

The research scrutinises website security in the Swedish zone. Especially the communication between the servers and clients. The data used in this research is quite old and is from 2014. Moreover, the Swedish Internet foundation deleted their data. Therefore, I recommend to do the same test with newer versions. Also, it can include more websites that swedes use daily, and subdomian. The thesis checks X.509 correctness structure. However, there are around eight vulnerables that can study. In addition, it should investigate why the recommended standards have a low rate and why the Swedish organisations do not use the optional standards.

# References

[1] R. N. Subudhi, "Impact of internet use during covid lockdown." *Horizon-Jhss*, [Online]. Available: https://horizon-jhssr.com/view-issue.php?id=64. [Accessed: October. 17, 2021].

[2] Internetstiftelsen, "Dnssec - internetstiftelsen," *Internetstiftelsen*, [Online]. Available: https://internetstiftelsen.se/en/domains/tech-tools/dnssec. [Accessed: October. 17, 2021].

[3] "Http security response headers cheat sheet." , [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html . [Accessed: October. 17, 2021].

[4] J. Hodges and A. Steingruebl, "The need for a coherent web security policy framework." web, 2010." , [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.7079&rep=rep1&type=pdf . [Accessed: November 22, 2021].

[5] H. Kour, J. Ahmed, "Mail attacks: Investigation about the vulnerability of the swedish organizations against email threats," *2020 - DIVA*, [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1451915 . [Accessed: 22 November 2021].

[6] A. Lavrenovs and F. J. R. Melón, "Http security headers analysis of top one million websites." *2018 10th International Conference on Cyber Conflict (CyCon), 2018, pp. 345-370*, [Accessed 24 October 2021].

[7] V. Visoottiviseth and K. Poonsiri, "The study of dnssec deployment status in thailand." *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)*, [Online]. Available: https://ieeexplore.ieee.org/abstract/docume . [Accessed: 11 November 2021].

[8] A. Purwanto and A. W. R. Emanuel, "The state of website security response headers in indonesia banking." *AIP Publishing, 16-Nov-2020.*, [Online]. Available: https://aip.scitation.org/doi/abs/10.1063/5.0030359 . [Accessed: 15 November 2021].

[9] S. F. S. B. S. H. R. P. W. Cooper, D. Santesson, "Rfc 5280 - internet x.509 public key infrastructure certificate and certificate revocation list (crl) profileg." *Ietf.org.*, [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280 . [Accessed: 28 February 2022].

[10] P. E. Yee, "Updates to the internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile." *RFC 6818, Jan. 2013*, [Online]. Available: https://rfc-editor.org/rfc/rfc6818.txt . [Accessed: 28 February 2022].

[11] A. Melnikov and W. Chuang, “Internationalized email addresses in x.509 certificates,” rfc 8398, may 2018.” *RFC 6818, Jan. 2013*, [Online]. Available: https://rfc-editor.org/rfc/rfc8398.txt . [Accessed: 28 February 2022].

[12] R. Housley, “Internationalization updates to rfc 5280.” *RFC 8399, May 2018*, [Online]. Available: https://rfc-editor.org/rfc/rfc8399.txt . [Accessed: 28 February 2022].

[13] D. C. A. R. Zuccherato, P. Cain and D. Pinkas, “Internet x.509 public key infrastructure time-stamp protocol (tsp),” *RFC 3161, Aug. 2001*, [Online]. Available: https://rfc-editor.org/rfc/rfc3161.txt . [Accessed: 28 February 2022].

[14] H. Mohialdeen and J. Draaijer, “Security culture in sweden with focus on digital certificate culture in organization,” *2020*, [Online]. Available: http://lnu.diva-portal.org/smash/record.jsf?aq2=%5B%5B%5D%5D . [Accessed: 1 March 2022].

[15] A. Mallik, “Man-in-the-middle-attack: Understanding in simple words,” *Cyberspace: Jurnal Pendidikan Teknologi Informasi 2.2 (2019)*, [Online]. Available: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453 . [Accessed: 23 November 2021].

[16] F. e. a. Mokbal, “An extreme gradient boosting detection framework for cross-site scripting attacks based on hybrid feature selection approach and parameters optimization.” *Journal of Information Security and Applications. (2021)* , [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212621000533?casa_token=EaLrSDqwhfgAAAAA%3AzfBbfWNrurGBGKe1KC9_eCBBhmBse7BPfY2BxxRjdvqfSe320mmMO2QsQ97-0D-qNm2hFqMQWcRK . [Accessed: 23 November 2021].

[17] P. I. . I. S. Platform, “Test for modern internet standards like ipv6, dnssec, https, dmarc, starttls and dane.” *Internet.nl* , [Online]. Available: https://www.internet.nl/ . [Accessed: 8 May 2022].

[18] S. Ariyapperuma and C. J. Mitchell, “Security vulnerabilities in dns and dnssec.” *The Second International Conference on Availability, Reliability and Security (ARES 07), 2007, pp. 335-342, doi: 10.1109/ARES.2007.139 - IEEE.* , [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4159821 . [Accessed: 21 October 2021].

[19] stackexchange, "What problem does dnssec solve?" , [Online]. Available: https://security.stackexchange.com/questions/142604/what-problem-does-dnssec-solve . [Accessed: 21 October 2021].

[20] Cloudflare, "How dnssec works. cloudflare?" , [Online]. Available: https://www.cloudflare.com/dns/dnssec/how-dnssec-works . [Accessed: 20 February 2022].

[21] D. Eastlake, "Domain name system security extensions," *Request for Comments 2535, March 1999*, [Online]. Available: https://tools.ietf.org/html/rfc2535 . [Accessed: 20 February 2022].

[22] B. Networks, "What is dnssec and how does it work?" *BlueCat Networks*, [Online]. Available: https://bluecatnetworks.com/blog/breaking-down-dnssec-how-does-it-work/#:~:text=At%20a%20basic%20level%2C%20DNSSEC,key%20and%20a%20private%20key . [Accessed: 19 May 2022].

[23] W. Hoehlhubmer, "Informational add-on for http over the secure sockets layer (ssl) protocol and/or the transport layer security (tls) protocol," *Datatracker.ietf.org*, [Online]. Available: https://datatracker.ietf.org/doc/draft-hoehlhubmer-https-addon . [Accessed: 24 October 2021].

[24] ——, "Referrer-policy - http | mdn," *Developer.mozilla.org*, [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy . [Accessed: 23 October 2021].

[25] T. Dierks and C. Allen., "The tls protocl ietf rfc 2246, 1999," *In Internet Engineering Task Force (IETF)*, [Online]. Available: http://www.ietf.org/rfc/rfc2246.txt . [Accessed: 20 February 2022].

[26] . R. E. Dierks, T., "Rfc5246: The transport layer security (tls) protocol version 1.2," *In Internet Engineering Task Force (IETF)*, [Online]. Available: https://doi.org/10.17487/rfc5246 . [Accessed: 20 February 2022].

[27] J. C. J.Hodges, PayPal and A.Barth, "Http strict transport security (hsts)," *In Internet Engineering Task Force (IETF)*, [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6797 . [Accessed: 22 October 2021].

[28] S. Helme, "Dhsts - the missing link in transport layer securityg," , [Online]. Available: https://scotthelme.co.uk/hsts-the-missing-link-in-tls . [Accessed: 22 October 2021].

[29] OWASP, "Http strict transport security - owasp cheat sheet serie," , [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_

Strict_Transport_Security_Cheat_Sheet.html . [Accessed: 20 February 2022].

[30] “X-frame-options - http | mdn,” , [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options . [Accessed: 22 October 2021].

[31] D. Ross, “Rfc 7034 - http header field x-frame-option.” *In Internet Engineering Task Force (IETF)*, [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7034 . [Accessed: 22 February 2022].

[32] “X-content-type-options.” , [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options . [Accessed: 22 February 2022].

[33] M. West, “Content security policy level 3.” *W3.org*, [Online]. Available: https://www.w3.org/TR/CSP . [Accessed: 23 October 2021].

[34] “Content security policy (csp).” , [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP . [Accessed: 22 February 2022].

[35] G. Ivanov, I. Marinov, “Current requirements to the safety means for the participants in fire extinguishing for critical infrastructure sites.” , [Online]. Available: https://stumejournals.com/journals/confsec/2019/3/115 . [Accessed: 22 February 2022].

[36] J.Eisinger and E. Stark., “Referrer policy.” , [Online]. Available: https://www.w3.org/TR/referrer-policy/ . [Accessed: 22 February 2022].

[37] N. K. R. Holz, L. Braun and G. Carle, “The ssl landscape: A thorough analysis of the x.509 pki using active and passive measurements.” *In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference - IMC ’11, 2011*, [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/2068816.2068856 . [Accessed: 28 February 2022].

[38] “What an x.509 certificate is how it works?” , [Online]. Available: https://sectigo.com/resource-library/what-is-x509-certificate . [Accessed: 28 February 2022].

[39] C. Heinrich, “Transport layer security (tls),” *In Encyclopedia of Cryptography and Security, Boston, MA: Springer US, 2011, pp. 1316–1317.*, [Online]. Available: https://developer.mozilla.org/en-US/docs/Glossary/TLS . [Accessed: 28 February 2022].

[40] "How certificate chains work." , [Online]. Available: https://knowledge.digicert.com/solution/SO16297.html . [Accessed: 28 February 2022].

# 9 Appendices

## 9.1 The Implemented Tool

Follow the link to find the header tester. https://github.com/Firas-al/Header-tester

## 9.2 Bank websites

```
alemssparbank.se
atvidabergsspb.se
avanza.se
bankgirot.se
bankomat.se
bergslagenssparbank.se
bjursassparbank.se
bluestep.se
carnegie.se
collector.se
coop.se
dalsbank.se
danskebank.se
dnb.se
ekebysparbank.se
ekobanken.se
enablebanking.com
falkenbergssparbank.se
forex.se
fryksdalenssparbank.se
gccab.com
halsinglandssparbank.se
handelsbanken.se
haradssparbanken.se
hogsbysparbank.se
icabanken.se
ikanobank.se
ivetoftasparbank.se
jak.se
kindaydresparbank.se
klarna.com
laholmssparbank.se
landshypotek.se
lansforsakringar.se
lekebergssparbank.se
leksandssparbank.se
ltvsparbank.se
marginalen.se
markarydssparbank.se
mjobackssparbank.se
nordax.se
nordea.se
```

```
nordnet.se
norrbarke-sparbank.se
northmill.com
okq8.se
olandsbank.se
 landsbank .se
orustsparbank.se
penser.se
resursbank.se
roslagenssparbank.se
salasparbank.se
sbab.se
seb.se
sidensjosparbank.se
skandia.se
skurupssparbank.se
smsparbank.se
snapphanebygdenssparbank.se
sodradalarnassparbank.se
sodrahestrasparbank.se
sormlandssparbank.se
sparbankenalingsas.se
sparbankenboken.se
sparbankeneken.se
sparbankenenkoping.se
sparbankengoinge.se
sparbankengotland.se
sparbankenikarlshamn.se
sparbankenlidkoping.se
sparbankennord.se
sparbankenrekarne.se
sparbankensjuharad.se
sparbankenskane.se
sparbankenskaraborg.se
sparbankensyd.se
sparbankentanum.se
sparbankentranemo.se
sparbankenvm.se
svea.com
swedbank.se
tfbank.se
tidaholms-sparbank.se
tjorns-sparbank.se
tjustbanken.se
ulricehamnssparbank.se
vadstenasparbank.se
valdemarsvikssparbank.se
varbergssparbank.se
vimmerbysparbank.se
virserumssparbank.se
volvofinans.se
```

```
sparbank.se
```

Appendix 2 : Bank websites

## 9.3 Insurance Company Website

```
accept.se
agria.se
aktsam.se
alandia.se
atlantica.se
bliwa.se
dina.se
erv.se
folksam.se
gjensidige.se
gouda-rf.se
helaforsakring.se
icaforsakring.se
idunliv.se
if.se
insurify.se
lansforsakringar.se
modernaforsakringar.se
movestic.se
paydrive.se
protectorforsakring.se
skandia.se
solidab.se
svedea.se
sveland.se
swedbank.se
trygghansa.se
vardia.se
villaagarna.se
watercircles.se
```

Appendix 3 : Insurance company websites

## 9.4 ISP Websites

```
1access.se
31173.se
84grams.se
a3foretag.se
aktivit.se
alltele.se
alvsbyn.se
ansluten.net
arkaden.se
asele.se
```

```
awiwo.com
b2b.medianetwork.se
bahnhof.se
bik.nu
bjarekraft.se
bjurholm.se
bktv.se
bluerange.se
bollnasenergi.se
borenet.se
boxer.se
bredband2.com
bredbandsson.se
bredbandsteknik.se
bredbandstjanster.se
carlslid.se
colt.net
comhem.se
connect.se
connectel.io
daladatorer.se
dalakraft.se
datacom.se
dgc.se
doffdata.se
dorotea.se
egonet.se
eidsiva.net
eksjoenergi.se
ember.se
epm.se
excedo.se
excellent-hosting.se
fastbit.se
fiberstaden.se
finet.se
forss.se
fouredge.se
gamma.co.uk
gastabudstaden.se
gavleenergi.se
glesys.se
glocalnet.se
gotanet.se
griffel.se
haboenergi.se
habonet.net
hagnor.se
haparanda.se
hebynet.se
helsingenetovanaker.se
```

```
hjoenergi.se
hogsbynat.se
ide.resurscentrum.se
imegasystem.se
indicate.se
infracomgroup.se
interlan.se
internetport.se
ip-only.se
ip-osteraker.se
ipsweden.se
it-centrum.se
it4u.se
itofsweden.se
itsystem.se
j-fab.net
jarfallaonline.se
jordberga.se
junet.se
karlsborgsenergi.se
karlskogaenergi.se
knivstanet.se
koping.net
kungalvenergi.se
kustbandet.com
lacable.se
layermesh.se
lidendata.se
lidnet.se
ljusdalenergi.se
lyssna-njut.se
mdfnet.se
mediateknik.com
mediateknik.net
microgroup.se
microtec.se
minitel.se
n62.se
nentgroup.com
netatonce.se
netnod.se
nordlo.com
norsjobredband.se
nossebroenergi.se
obenetwork.com
oktv.se
on1call.se
oretel.se
osterlenskraft.se
oversite.se
ownit.se
```

```
perspektivbredband.se
phonera.se
primlight.net
qavat.se
qos.se
quicknet.se
rbcom.se
sandvikenenergi.se
sappa.se
savman.se
servanet.se
skurupselverk.se
soderhamnnara.se
springmobil.se
stockholmsstadsnat.se
straznet.se
sunet.se
sverigesbredband.se
swedavia.se
sydantenn.se
t3.se
tdc.se
teamfront.se
teknorama.se
tele2.se
teleman.se
telenor.se
teleservice.net
teletek.se
teliacompany.com
th1ng.se
tibroenergi.se
tidaholmsenergi.se
tk-data.se
top24.se
tranquillity.se
tre.se
vaggerydsenergi.se
vanerenergi.se
vannas.se
varbergenergi.se
varnamoenergi.se
verizon.com
vilhelmina.se
virserum.com
visolit.se
voicetech.nu
vokby.se
wintherwireless.se
yelles.se
ymex.se
```

```
zedcom.se
```

Appendix 4 : ISP websites

## 9.5 Media Websites

```
cmore.se
dplay.se
ilikeradio.se
kanal5.se
mixmegapol.se
nrj.se
radioplay.se
rixfm.se
sverigesradio.se
svt.se
svtplay.se
tv3.se
tv4.se
tv4play.se
tv6.se
tv8.se
viafree.se
viasat.se
```

Appendix 5 : Media websites

## 9.6 Municipalities Websites

```
ale.se
alingsas.se
almhult.se
alvdalen.se
alvesta.se
alvkarleby.se
 lvkarleby .se
alvsbyn.se
amal.se
aneby.se
ange.se
 nge .se
arboga.se
are.se
 re .se
arjang.se
arjeplog.se
arvidsjaur.se
arvika.se
asele.se
askersund.se
astorp.se
```

```
 storp .se
atvidaberg.se
 tvidaberg .se
avesta.se
bastad.se
b stad.se
bengtsfors.se
berg.se
bjurholm.se
bjuv.se
boden.se
bollebygd.se
bollnas.se
boras.se
borgholm.se
borlange.se
botkyrka.se
boxholm.se
bracke.se
bromolla.se
brom lla.se
burlov.se
dalsed.se
danderyd.se
degerfors.se
dorotea.se
eda.se
ekero.se
eksjo.se
emmaboda.se
engelholm.se
enkoping.se
eskilstuna.se
eslov.se
esl v.se
essunga.se
fagersta.se
falkenberg.se
falkoping.se
falun.se
fargelanda.se
f rgelanda.se
filipstad.se
finspang.se
finsp ng.se
flen.se
forshaga.se
gagnef.se
gallivare.se
gavle.se
gellivare.se
```

```
gislaved.se
gnesta.se
gnosjo.se
gnosj .se
goteborg.se
g teborg.se
gotene.se
g tene.se
gotland.se
grastorp.se
grums.se
gullspang.se
gullsp ng.se
habo.se
h bo.se
habokommun.se
hagfors.se
hallsberg.se
hallstahammar.se
halmstad.se
hammaro.se
haninge.se
haparanda.se
harnosand.se
harryda.se
h rryda.se
hassleholm.se
h ssleholm.se
heby.se
hedemora.se
hellefors.se
helsingborg.se
herjedalen.se
herrljunga.se
hjo.se
hofors.se
hoganas.se
h gan s.se
hogsby.se
hoor.se
h   r.se
horby.se
huddinge.se
hudiksvall.se
hultsfred.se
hylte.se
jarfalla.se
j rf lla.se
jokkmokk.se
jonkoping.se
j nk ping.se
```

```
kalix.se
kalmar.se
karlsborg.se
karlshamn.se
karlskoga.se
karlskrona.se
karlstad.se
katrineholm.se
kavlinge.se
kil.se
kinda.se
kiruna.se
klippan.se
knivsta.se
koping.se
k ping.se
kramfors.se
kristianstad.se
kristinehamn.se
krokom.se
kumla.se
kungalv.se
kung lv.se
kungsbacka.se
kungsor.se
kungs r.se
laholm.se
landskrona.se
laxa.se
lekeberg.se
leksand.se
lerum.se
lessebo.se
lidingo.se
lidkoping.se
lidk ping.se
lillaedet.se
lindesberg.se
linkoping.se
link ping.se
ljungby.se
ljusdal.se
ljusnarsberg.se
lomma.se
ludvika.se
lulea.se
lule .se
lund.se
lycksele.se
lysekil.se
mala.se
```

```
malmo.se
malung-salen.se
mariestad.se
mark.se
markaryd.se
mellerud.se
mjolby.se
molndal.se
m lndal.se
monsteras.se
m nster s.se
morakommun.se
morbylanga.se
m rbyl nga.se
motala.se
mullsjo.se
mullsj .se
munkedal.se
munkfors.se
nacka.se
nassjo.se
n ssj .se
nora.se
norberg.se
nordanstig.se
nordmaling.se
norrkoping.se
norrk ping.se
norrtalje.se
norrt lje.se
norsjo.se
norsj .se
nybro.se
nykoping.se
nyk ping.se
nykvarn.se
nynashamn.se
ockelbo.se
ockero.se
  cker  .se
odeshog.se
  deshg  .se
olofstrom.se
olofstr m.se
orebro.se
orkelljunga.se
ornskoldsvik.se
orsa.se
orust.se
osby.se
oskarshamn.se
```

```
osteraker.se
  sterker  .se
ostersund.se
osthammar.se
ostragoinge.se
ovanaker.se
ovan ker.se
overkalix.se
overtornea.se
oxelosund.se
pajala.se
partille.se
perstorp.se
pitea.se
ragunda.se
rattvik.se
r ttvik.se
robertsfors.se
ronneby.se
saffle.se
s ffle.se
sala.se
salem.se
sandviken.se
sater.se
s ter.se
savsjo.se
sigtuna.se
simrishamn.se
sjobo.se
sj bo.se
skara.se
skelleftea.se
skinnskatteberg.se
skovde.se
sk vde.se
skurup.se
smedjebacken.se
soderhamn.se
s derhamn.se
soderkoping.se
s derk ping.se
sodertalje.se
s dert lje.se
solleftea.se
sollefte .se
sollentuna.se
solna.se
solvesborg.se
s lvesborg.se
sorsele.se
```

```
sotenas.se
staffanstorp.se
stenungsund.se
stockholm.se
storfors.se
storuman.se
strangnas.se
str ngn s.se
stromstad.se
stromsund.se
sundbyberg.se
sundsvall.se
sunne.se
surahammar.se
svalov.se
sval v.se
svedala.se
svenljunga.se
taby.se
tanum.se
tibro.se
tidaholm.se
tierp.se
timra.se
tingsryd.se
tjorn.se
tomelilla.se
toreboda.se
torsas.se
torsby.se
tranas.se
tranemo.se
trelleborg.se
trollhattan.se
trosa.se
tyreso.se
tyres .se
uddevalla.se
ulricehamn.se
umea.se
ume .se
upplands-bro.se
upplandsvasby.se
upplandsv sby.se
uppsala.se
uppvidinge.se
vadstena.se
vaggeryd.se
valdemarsvik.se
vallentuna.se
vanersborg.se
```

```
v nersborg.se
vannas.se
vansbro.se
vara.se
varberg.se
vargarda.se
varmdo.se
v rmd .se
varnamo.se
v rnamo.se
vasteras.se
v ster s.se
vansbro.se
vara.se
varberg.se
vargarda.se
varmdo.se
v rmd .se
varnamo.se
v rnamo.se
vasteras.se
v ster s.se
vingaker.se
ving ker.se
ydre.se
ystad.se
```

Appendix 6 : Municipalities websites

## 9.7 Newspaper Websites

```
aftonbladet.se
allehanda.se
arbetarbladet.se
barometern.se
blt.se
corren.se
dagen.se
dagenssamhalle.se
dalademokraten.se
di.se
dn.se
dt.se
ekuriren.se
eposten.se
expressen.se
falukuriren.se
folkbladet.nu
folket.se
gd.se
gp.se
```

```
hallandsposten.se
hallekis.com
hd.se
helagotland.se
helahalsingland.se
hn.se
ht.se
jnytt.se
jp.se
kkuriren.se
kristianstadsbladet.se
kuriren.nu
lt.se
ltz.se
metromode.se
mvt.se
na.se
norran.se
norrteljetidning.se
nsd.se
nt.se
nwt.se
nynashamnsposten.se
olandsbladet.se
op.se
ostrasmaland.se
pt.se
salaallehanda.com
skd.se
sla.se
smp.se
sn.se
st.nu
svd.se
sydostran.se
sydsvenskan.se
ttela.se
unt.se
ut.se
vf.se
vimmerbytidning.se
vk.se
vlt.se
vt.se
ystadsallehanda.se
```

Appendix 7 : Newspaper websites

## 9.8 Regioner websites

```
gotland.se
```

```
norrbotten.se
regionblekinge.se
regiondalarna.se
regiongavleborg.se
regionhalland.se
regionjh.se
regionkalmar.se
regionkronoberg.se
regionorebrolan.se
regionostergotland.se
regionsormland.se
regionuppsala.se
regionvarmland.se
regionvasterbotten.se
regionvastmanland.se
rjl.se
rvn.se
skane.se
sll.se
vgregion.se
```

Appendix 8 : Regioner websites

## 9.9 Registrarer websites

```
100procent.com
101domain.com
1198.cn
123domain.eu
1and1.com
1api.net
28kdigital.com
ascio.com
atellus.se
ballou.se
beebyte.se
bgpm.se
bluesnap.io
buildit.net
buildit.se
comlaude.com
corehub.net
cps-datensysteme.de
crossnet.net
crossnet.se
crystone.se
cscglobal.com
dn.ee
dnr.emea.verizonbusiness.com
domaindiscount24.com
domains.rackfish.com
```

```
domanregister.se
domanservice.se
domanshop.se
dotkeeper.com
drs.knipp.de
edomains.com
edoms.com
egensajt.se
ember.se
enom.com
epag.de
eurodns.com
excedodms.se
forss.se
frobbit.se
fsdata.se
ftech.se
gandi.net
gotanet.se
gratisdns.com
griffel.se
groth.se
hertigtorulf.se
hostnet.nl
ilait.com
inbrand.se
indukon.se
infracom.se
inleed.se
instra.com
internetsrs.com
internetstiftelsen.se
internetvikings.com
internetx.com
intripid.com
inwx.com
itconnect.se
itkoncept.se
joker.com
koneo.se
kontorsspecial.se
levonline.com
lexsynergy.com
loopia.se
lopnet.se
markmonitor.com
metaregistrar.com
mono.net
mrdomain.com
name.com
nameisp.com
```

```
namesrs.com
nameweb.biz
netim.com
neware.se
nicsell.com
nmugroup.com
nominate.com
nordichosting.com
nunames.nu
oderland.se
odibo.se
one.com
openprovider.com
ovh.com
pixel.se
portsgroup.com
proisp.no
quicknet.se
readydigital.se
realtimeregister.com
redsnapper.nu
register.eu
registrar-proxy.nl
registrar.nl
registrera-doman.se
regit.nu
rymdweb.se
safebrands.fr
safenames.net
sarek.fi
scandinavianhosting.se
secure.nameshield.net
servercentralen.se
simply.com
sircon.no
space2u.com
spacedump.se
standardbolaginternet.se
sveabyran.se
svenskadomaner.se
svenskaexportmedia.com
telia.se
theregistrarcompany.com
united-domains.de
variomedia.de
vmi.se
wannafind.dk
web-solutions.eu
webb.se
webhotellet.net
weblovers.com
```

```
wiredequity.com
wk.se
wopsa.se
yamito.se
yask.se
```

Appendix 9 : Registrarer websites

## 9.10 Government agencies website

```
aklagare.se
arbetsdomstolen.se
arbetsformedlingen.se
arbetsgivarverket.se
arkdes.se
arn.se
av.se
barnombudsmannen.se
bfn.se
bo.se
bolagsverket.se
boverket.se
bra.se
br .se
brottsoffermyndigheten.se
cert.se
csn.se
delmos.se
digg.se
do.se
dom.se
domstol.se
ehalsomyndigheten.se
ei.se
ekn.se
ekobrottsmyndigheten.se
elsakerhetsverket.se
energimyndigheten.se
epn.se
esf.se
esv.se
etikprovningsmyndigheten.se
fba.se
fi.se
finanspolitiskaradet.se
fmi.se
fmv.se
foi.se
folkhalsomyndigheten.se
formas.se
forsakringskassan.se
```

```
forsvarsmakten.se
f rsvarsmakten.se
forte.se
fortifikationsverket.se
fortv.se
fra.se
havkom.se
havochvatten.se
iaf.se
ifau.se
imy.se
irf.se
isf.se
isof.se
isp.se
ivo.se
jamstalldhetsmyndigheten.se
jk.se
jo.se
jordbruksverket.se
justitiekanslern.se
kammarkollegiet.se
karnavfallsfonden.se
kb.se
kemi.se
ki.se
kkv.se
kommerskollegium.se
konj.se
konkurrensverket.se
konstfack.se
konstnarsnamnden.se
konstn rsn mnden.se
konsumentverket.se
kriminalvarden.se
kronofogden.se
kulturanalys.se
kulturradet.se
kulturr det.se
kungahuset.se
kustbevakningen.se
lakemedelsverket.se
l kemedelsverket.se
lansstyrelsen.se
lantmateriet.se
levandehistoria.se
lfv.se
livsmedelsverket.se
lm.se
mfd.se
mfof.se
```

```
mi.se
migrationsverket.se
mil.se
modernamuseet.se
mpa.se
mprt.se
msb.se
mtm.se
mucf.se
musikverket.se
myh.se
mynak.se
myndighetensst.se
nai.uu.se
nationalmuseum.se
naturvardsverket.se
naturv rdsverket.se
nrm.se
oks.se
onep.se
oredlighetsprovning.se
pensionsmyndigheten.se
pliktverket.se
polar.se
polisen.se
prv.se
pts.se
raa.se
regeringen.se
regeringskansliet.se
revisorsinspektionen.se
riksarkivet.se
riksdagen.se
riksgalden.se
riksrevisionen.se
rmv.se
rymdstyrelsen.se
sakerhetspolisen.se
sakint.se
sameskolstyrelsen.se
sametinget.se
sbu.se
scb.se
sfhm.se
sfv.se
sgi.se
sgu.se
shm.se
si.se
sida.se
sieps.se
```

```
siun.se
sjofartsverket.se
sj fartsverket.se
skatteverket.se
skogsstyrelsen.se
skolfi.se
skolinspektionen.se
skolverket.se
slv.se
smhi.se
smtm.se
snsb.se
socialstyrelsen.se
spelinspektionen.se
sprakochfolkminnen.se
spr kochfolkminnen.se
spsm.se
spv.se
ssm.se
stat-inst.se
statenskonstrad.se
statensmedierad.se
statenssc.se
statskontoret.se
stralsakerhetsmyndigheten.se
str ls kerhetsmyndigheten.se
sva.se
svk.se
swedac.se
tillvaxtanalys.se
tillvaxtverket.se
tillv xtverket.se
tlv.se
trafa.se
trafikverket.se
transportstyrelsen.se
tullverket.se
uhr.se
uka.se
uk .se
undom.se
upphandlingsmyndigheten.se
vardanalys.se
v rdanalys.se
varldskulturmuseerna.se
vinnova.se
vr.se
vti.se
```

Appendix 10 : Government agencies websites

## 9.11 State-owned Companies Websites

```
akademiskahus.se
almi.se
apl.se
apoteket.se
arlandabananinfrastructure.se
bilprovningen.se
dramaten.se
eurofima.org
gotakanal.se
greencargo.se
industrifonden.se
infranord.se
jernhusen.se
lernia.se
lkab.com
metria.se
norrlandsfonden.se
operan.se
orio.com
postnord.se
ri.se
samhall.se
saminvest.se
sas.se
sbab.se
sbo.se
sek.se
sj.se
sosalarm.se
specialfastigheter.se
sscspace.com
svanen.se
sveaskog.se
svedab.se
svenskaskeppshypotek.se
svenskaspel.se
svevia.se
swedavia.se
swedesurvey.se
swedfund.se
systembolaget.se
telia.se
teracom.se
vasallen.se
vattenfall.se
visitsweden.com
voksenaasen.no
voksenaasen.se
```

Appendix 11 : State-owned companies websites.

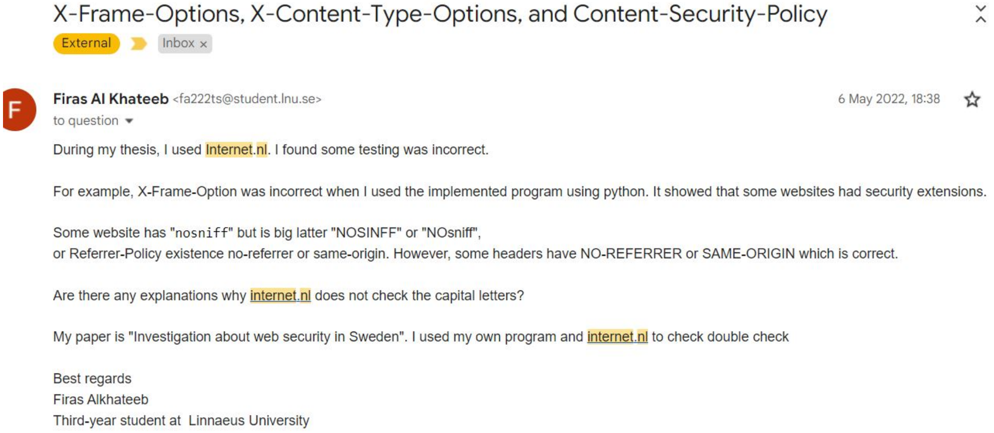
## 9.12 Universities Websites

```
altutbildning.se
beckmans.se
bth.se
cbti.se
chalmers.se
du.se
ericastiftelsen.se
esh.se
evidens4u.se
fhs.se
gammelkroppa.se
gih.se
gu.se
hb.se
hh.se
hhs.se
hig.se
his.se
hkr.se
hv.se
johannelund.nu
ju.se
kau.se
ki.se
kkh.se
kmh.se
konstfack.se
kth.se
liu.se
lnu.se
ltu.se
lu.se
mau.se
mdh.se
miun.se
newman.se
oru.se
rkh.se
sapu.se
sh.se
shh.se
slu.se
smi.se
su.se
ths.se
umu.se
```

```
uniarts.se
uu.se
```

Appendix 12 : Universities websites.

## 9.13 Case Sensitive Email question



X-Frame-Options, X-Content-Type-Options, and Content-Security-Policy

**Firas Al Khateeb** <fa222ts@student.lnu.se>    6 May 2022, 18:38

to question

During my thesis, I used Internet.nl. I found some testing was incorrect.

For example, X-Frame-Option was incorrect when I used the implemented program using python. It showed that some websites had security extensions.

Some website has "nosniff" but is big latter "NOSINFF" or "NOsniff",
or Referrer-Policy existence no-referrer or same-origin. However, some headers have NO-REFERRER or SAME-ORIGIN which is correct.

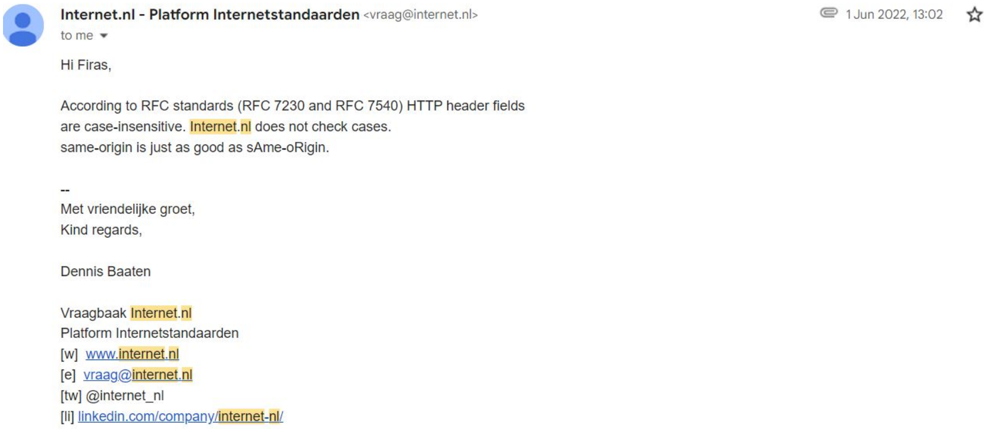
Are there any explanations why internet.nl does not check the capital letters?

My paper is "Investigation about web security in Sweden". I used my own program and internet.nl to check double check

Best regards
Firas Alkhateeb
Third-year student at  Linnaeus University

Appendix 13 : The email that sent asking about case sensitive.

## 9.14 Case Sensitive Email reply



**Internet.nl - Platform Internetstandaarden** <vraag@internet.nl>    1 Jun 2022, 13:02

to me

Hi Firas,

According to RFC standards (RFC 7230 and RFC 7540) HTTP header fields
are case-insensitive. Internet.nl does not check cases.
same-origin is just as good as sAme-oRigin.

--
Met vriendelijke groet,
Kind regards,

Dennis Baaten

Vraagbaak Internet.nl
Platform Internetstandaarden
[w]  www.internet.nl
[e]  vraag@internet.nl
[tw] @internet_nl
[li] linkedin.com/company/internet-nl/

Appendix 14 : The reply email about case sensitive.