

# Sri Lanka Institute of Information Technology



**Sri Lanka Institute of  
Information Technology**

**IE2072 – WEB SECURITY**

**Year 2, Semester 2**

**(Assignment – Individual)-2023**

**\_Bug Bounty vulnerabilities scanning Report 2\_**

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

# LocalTapiola



## • Overview

By combining the businesses of Lähivakuutus and Tapiola Bank, the Finnish finance firm LähiTapiola was created, which offers insurance services. Private, farm, entrepreneur, corporate, and community clients are served by the group firm LähiTapiola, which is owned by its patrons. creatures on the internet.

Scope of the security audit according to <https://hackerone.com/localtapiola?type=team> is as follows,

## Scope and rewards

### In Scope

Asset name ↑	Type	Coverage	CVSS	Bounty
<b>*.lahitapiola.fi</b> This is Category III.	Wildcard	In scope	Medium	Eligible
<b>*.lahitapiolarahoitus.fi</b> This is Category III.	Wildcard	In scope	Medium	Eligible
<b>*.tapiola.fi</b> This is Category III.	Wildcard	In scope	Medium	Eligible
<b>1298908406</b> This is the Terveysheppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer s device. The app can be found here: <a href="https://apps.apple.com/fi/app/terveysheppi/id1298908406">https://apps.apple.com/fi/app/terveysheppi/id1298908406</a>  Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.	iOS: App Store	In scope	Critical	Eligible
<b>1439784468</b> This is the LemmikkiHeppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer s device. The app can be found here: <a href="https://itunes.apple.com/fi/app/lemmikkiheppi/id1439784468">https://itunes.apple.com/fi/app/lemmikkiheppi/id1439784468</a>  Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.	iOS: App Store	In scope	High	Eligible
<b>api.lahitapiola.fi</b> This is a common API gateway that is used by various services in the LähiTapiola ecosystem. Thread carefully - no DoSsing or unnecessary asshattery.	Domain	In scope	Critical	Eligible
<b>asiointi.lahitapiola.fi</b> This service is part of the customer engagement layer - a new customer self service portal.  This site contains customer information which is only accessible to customers. We are primarily interested in issues that are a direct threat to the integrity of our customers or their information - meaning stealing information, modifying information or deleting information. Also privacy issues are high on our list of critical issues.  To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.  No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.  There are no demo or test accounts. F5 BIG-IP ASM	Domain	In scope	Critical	Eligible

<b>ext-gw.lahitapiola.fi</b> This domain contains API's which are part of newly developed services. This domain is used by applications.	Domain	In scope	Critical	Eligible
<b>fi.lahitapiola.lemmikkihelppi</b> This is the LemmikkiHelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer s device. The app can be found here: <a href="https://play.google.com/store/apps/details?id=fi.lahitapiola.lemmikkihelppi&amp;hl=en">https://play.google.com/store/apps/details?id=fi.lahitapiola.lemmikkihelppi&amp;hl=en</a>  Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.	Android: Play Store	In scope	High	Eligible
<b>fi.lahitapiola.mobile</b> This is the TerveysHelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer s device. The app can be found here: <a href="https://play.google.com/store/apps/details?id=fi.lahitapiola.mobile&amp;hl=en">https://play.google.com/store/apps/details?id=fi.lahitapiola.mobile&amp;hl=en</a>  Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.	Android: Play Store	In scope	Critical	Eligible
<b>lisa-sijoitus.lahitapiola.fi</b> This is a service where you can make additional online payments to investment insurance (AOL). Access to this service is through Varainhoidon verkkopalvelu ( <a href="https://www.lahitapiola.fi/henkilo/sijoitukset-ja-varainhoito/kirjautu-rahastojen-ja-varainhoidon-verkkopalveluun">https://www.lahitapiola.fi/henkilo/sijoitukset-ja-varainhoito/kirjautu-rahastojen-ja-varainhoidon-verkkopalveluun</a> ).  Lisätietoa suomeksi: Jotta voisit käyttää tätä palvelua, pitää sinulla olla sijoitusvakuutus <ul style="list-style-type: none"> <li>jossa ei ole sijoituskohteena Kiinteistö-sijoitussalkkua</li> <li>jossa ei ole Korkoetu-sijoituskohdetta</li> </ul>	Domain	In scope	Critical	Eligible
<b>myynti.lahitapiolarahoitus.fi</b> This service is an extranet-service for our partners. This service has a few read-only backend integrations. To be able to log on, you need a partner account. No demo accounts are available. Very limited amounts of customer information is stored in this service. Any issues with confidentiality are interesting to us, as well as <i>cunning and clever</i> spoofing.  Scanning for low value things is not a successful bounty strategy as we will not accept any best practice reports. No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked and put on the naughty list. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.  Other domains on this ip are out of scope.	Domain	In scope	Critical	Eligible
<b>privatetarget-1-www.zigzag</b> Private target: www	Domain	In scope	Medium	Eligible
<b>privatetarget-2-secure.zigzag</b> Private target: secure	Domain	In scope	Critical	Eligible

### secure.lahitapiola.fi

This domain is designed to send emails. It is by design that it accepts all kinds of sender and receiver addresses, including lahitapiola addresses. Because it is an email-service, there is an smtp server. That is also by design. Sending emails to root or other localhost users is not an issue. Also as a reminder - SSL/TLS, DNS and email best practices (DMARC etc.) and all theoretical hardening trick and tips without any real life business case will be closed as n/a.

This service is hosted and segregated outside of any critical infrastructure. Besides any potential data sent between two parties, there is no privacy related personal data stored on the server. The service is not critical for daily operations.

Things that might be interesting to us (not an exhaustive list)

- Using the smtp server to relay spam
- Leaking the actual contents of another users email
- Modifying contents or attachments of another user

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

NOTE: as of May 2018, there will be no public disclosures of any of the reports in this domain.

Domain In scope Critical Eligible

### sijoitusvakuutus.lahitapiola.fi

This is a service for buying "Korkoetu" investment insurance. It is accessed from the Elämänturva mobile application.

Domain In scope Critical Eligible

### tunnistus.lahitapiola.fi

This is a shared SaaS-service. This domain is part of authentication.

Domain In scope Critical Eligible

### verkkopalvelu.tapiola.fi

This is our service portal for customers. This site contains customer information which is only accessible to customers. We are primarily interested in issues that are a direct threat to the integrity of our customers or their information - meaning stealing information, modifying information or deleting information. Also privacy issues are high on our list of critical issues.

To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

There are no demo or test accounts.

F5 BIG-IP ASM

Domain In scope Critical Eligible

### verovelvollisuustiedot.lahitapiola.fi

This application is for reporting Fatca-information. This is a service that can be accessed directly using the URL.

Domain In scope Critical Eligible

### www.lahitapiola.fi

This is our public website. It is built using both customized off-the-shelf tools as well as custom code. This site does (and should not) contain any customer information. We are interested in issues affecting continuity and integrity, misconfigurations that might lead to phishing or other attacks against our customers. Planting misinformation or using our public website for sharing malware would be a serious issue.

### www.lahitapiola.fi

This is our public website. It is built using both customized off-the-shelf tools as well as custom code. This site does (and should not) contain any customer information. We are interested in issues affecting continuity and integrity, misconfigurations that might lead to phishing or other attacks against our customers. Planting misinformation or using our public website for sharing malware would be a serious issue.

If you understand what a public website is, in which country we operate in and the basics of the industry we do business in you will have a better chance of submitting reports successfully. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

F5 BIG-IP ASM

Domain

In scope

Critical

Eligible

### www.tapiola.fi

This is another entry point to our public website <https://www.lahitapiola.fi>. Do NOT copy your report on both domains and always PRIMARILY report on the [www.lahitapiola.fi](https://www.lahitapiola.fi) -asset.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

F5 BIG-IP ASM

Domain

In scope

Critical

Eligible

### yrityspalvelu.tapiola.fi

This is our service portal for corporate users. This site contains customer information which is only accessible to corporate customers. We are primarily interested in issues that are a direct threat to the integrity of our customers their information - meaning stealing information, modifying information or deleting information.

To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

There are no demo or test accounts.

F5 BIG-IP ASM

Domain

In scope

Critical

Eligible

- ✓ .lahitapiola.fi  
This is Category III.
- ✓ \*.lahitapiolarahoitus.fi  
This is Category III.
- ✓ \*.tapiola.fi  
This is Category III.

- ✓ 1298908406  
This is the Terveyshelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer's device. The app can be found here: <https://apps.apple.com/fi/app/terveyshelppi/id1298908406>  
Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.
- ✓ 1439784468  
This is the LemmikkiHelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer's device. The app can be found here: <https://itunes.apple.com/fi/app/lemmikkihelppi/id1439784468>  
Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.
- ✓ api.lahitapiola.fi  
This is a common API gateway that is used by various services in the LähiTapiola ecosystem. Thread carefully - no DoSsing or unnecessary asshattery.
- ✓ asiointi.lahitapiola.fi  
This service is part of the customer engagement layer - a new customer self service portal. This site contains customer information which is only accessible to customers. We are primarily interested in issues that are a direct threat to the integrity of our customers or their information - meaning stealing information, modifying information or deleting information. Also privacy issues are high on our list of critical issues.  
To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.  
No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.  
There are no demo or test accounts.
- ✓ ext-gw.lahitapiola.fi  
This domain contains API's which are part of newly developed services. This domain is used by applications.
- ✓ fi.lahitapiola.lemmikkihelppi  
This is the LemmikkiHelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the

customer s device. The app can be found here:  
<https://play.google.com/store/apps/details?id=fi.lahitapiola.lemmikkihelppi&hl=en>  
Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.

✓ fi.lahitapiola.mobile

This is the Terveysshelppi -application. We are mainly looking for critical information leaks (not version numbers or similar low value) and threats to either the customer or the customer s device. The app can be found here:  
<https://play.google.com/store/apps/details?id=fi.lahitapiola.mobile&hl=en>

Note: If exploitation requires that the device is rooted, the finding is automatically out of scope.

✓ lisasijoitus.lahitapiola.fi

This is a service where you can make additional online payments to investment insurance (AOL). Access to this service is through Varainhoidon verkkopalvelu (<https://www.lahitapiola.fi/henkilo/sijoitukset-ja-varainhoito/kirjaudu-rahastojen-ja-varainhoidon-verkkopalveluun>).

Lisätietoa suomeksi:

Jotta voisit käyttää tätä palvelua, pitää sinulla olla sijoitusvakuutus

jossa ei ole sijoituskohteena Kiinteistö-sijoitussalkkua

jossa ei ole Korkoetu-sijoituskohdetta

✓ myynti.lahitapiolarahoitus.fi

This service is an extranet-service for our partners. This service has a few read-only backend integrations. To be able to log on, you need a partner account. No demo accounts are available. Very limited amounts of customer information is stored in this service. Any issues with confidentiality are interesting to us, as well as cunning and clever spoofing.

Scanning for low value things is not a successful bounty strategy as we will not accept any best practice reports. No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked and put on the naughty list. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

Other domains on this ip are out of scope.

✓ privatetarget-1-www.zigzag

Private target: www

✓ privatetarget-2-secure.zigzag

Private target: secure

✓ secure.lahitapiola.fi

This domain is designed to send emails. It is by design that it accepts all kinds of sender and receiver addresses, including lahitapiola addresses. Because it is an email-service, there is an smtp server. That is also by design. Sending emails to root or other localhost users is not an issue. Also as a reminder - SSL/TLS, DNS and email best practices (DMARC etc.) and all theoretical hardening trick and tips without any real life business case will be closed as n/a.

This service is hosted and segregated outside of any critical infrastructure. Besides any potential data sent between two parties, there is no privacy related personal data stored on the server. The service is not critical for daily operations.

Things that might be interesting to us (not an exhaustive list)

Using the smtp server to relay spam

Leaking the actual contents of another users email

Modifying contents or attachments of another user

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

NOTE: as of May 2018, there will be no public disclosures of any of the reports in this domain.

✓ [sijoitusvakuutus.lahitapiola.fi](#)

This is a service for buying "Korkoetu" investment insurance. It is accessed from the Elämänturva mobile application.

✓ [tunnistus.lahitapiola.fi](#)

This is a shared SaaS-service. This domain is part of authentication.

✓ [verkkopalvelu.tapiola.fi](#)

This is our service portal for customers. This site contains customer information which is only accessible to customers. We are primarily interested in issues that are a direct threat to the integrity of our customers or their information - meaning stealing information, modifying information or deleting information. Also privacy issues are high on our list of critical issues.

To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

There are no demo or test accounts.

✓ [verovelvollisuustiedot.lahitapiola.fi](#)



This application is for reporting Fatca-information. This is a service that can be accessed directly using the URL.

✓ [www.lahitapiola.fi](http://www.lahitapiola.fi)

This is our public website. It is built using both customized off-the-shelf tools as well as custom code. This site does (and should not) contain any customer information. We are interested in issues affecting continuity and integrity, misconfigurations that might lead to phishing or other attacks against our customers. Planting misinformation or using our public website for sharing malware would be a serious issue.

If you understand what a public website is, in which country we operate in and the basics of the industry we do business in you will have a better chance of submitting reports successfully. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

✓ [www.tapiola.fi](http://www.tapiola.fi)

This is another entry point to our public website <https://www.lahitapiola.fi>. Do NOT copy your report on both domains and always **PRIMARILY** report on the [www.lahitapiola.fi](http://www.lahitapiola.fi) - asset.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

✓ [yrityspalvelu.tapiola.fi](http://yrityspalvelu.tapiola.fi)

This is our service portal for corporate users. This site contains customer information which is only accessible to corporate customers. We are primarily interested in issues that are a direct threat to the integrity of our customers or their information - meaning stealing information, modifying information or deleting information.

To be a successful reporter, you need to have an account on this website and understand the basics of the industry we do business in. If you want to understand our reasoning behind assessing reports, read up on risk management to understand the basic concepts of impact and probability.

No automated portscanning or bruteforcing allowed - you will have very limited success and you will be blocked. Copy-pasted reports from vulnerability scanners or Kali-scripts where no business impact is proven will not be awarded.

There are no demo or test accounts.

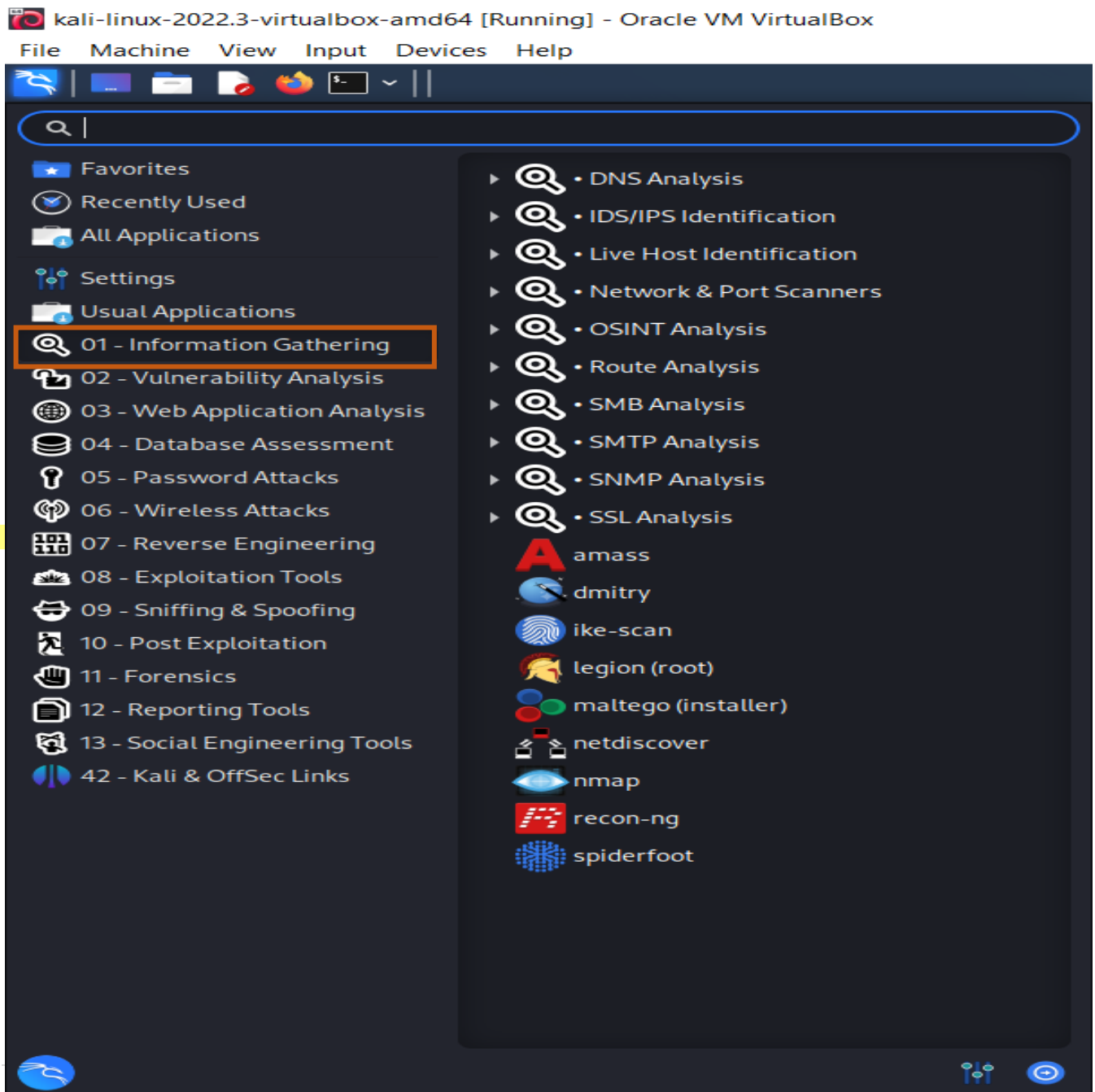
## Out Scope

Asset name ↑	Type	Coverage	CVSS	Bounty
<b>authenticate.lahitapiola.fi</b> This is a shared SaaS-service. This domain is part of authentication but no hacking attempts are allowed.	Domain	Out of scope	None	Ineligible
<b>tandem.lahitapiola.fi</b> DO not report. Reports will be closed as N/A.	Domain	Out of scope	None	Ineligible
<b>toimitilat.lahitapiola.fi</b> The criticality of this domain is medium, meaning scanning for low value things is not a successful bounty strategy. The domain does not contain any sensitive, personal or privacy-related data. If such data would be found - in medium to large quantities, that would be considered serious. Other things we would consider interesting is serious and working phishing schemes as well as using this domain for serious and real life spoofing.  NOTE: We have had previous reports on this domain - both accepted and closed as out of scope. History is in the past - old reports WILL NOT be reopened and they will not have priority - everyone will start from square one and send in new reports.	Domain	Out of scope	None	Ineligible

- ✓ authenticate.lahitapiola.fi
- ✓ This is a shared SaaS-service. This domain is part of authentication but no hacking attempts are allowed.
- ✓ tandem.lahitapiola.fi
- ✓ DO not report. Reports will be closed as N/A.
- ✓ toimitilat.lahitapiola.fi
- ✓ The criticality of this domain is medium, meaning scanning for low value things is not a successful bounty strategy. The domain does not contain any sensitive, personal or privacy-related data. If such data would be found - in medium to large quantities, that would be considered serious. Other things we would consider interesting is serious and working phishing schemes as well as using this domain for serious and real life spoofing.
- ✓ NOTE: We have had previous reports on this domain - both accepted and closed as out of scope. History is in the past - old reports WILL NOT be reopened and they will not have priority - everyone will start from square one and send in new

## Information gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



- Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

- What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: `knockpy <Domain Name>`

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
$ knockpy tapiola.fi

v6.1.0

local: 10757 | remote: 173
Wordlist: 10930 | Target: tapiola.fi | Ip: 193.209.71.143
04:21:52

Ip address      Code Subdomain      Server      Real hostname
-----
20.76.227.250   200 authmigrate.tapiola.fi  Windows-Azure-Web/1.0 Microsoft-HTTPAPI/2.0
193.209.71.79   ahma.tapiola.fi
193.209.71.48   analytics.tapiola.fi
193.209.71.76   ankka.tapiola.fi
217.29.227.115  bl.tapiola.fi
217.29.229.119  srl.tapiola.fi
193.209.71.213  kharon.tapiola.fi
193.209.71.108  kissa.tapiola.fi
193.209.71.200  kuha.tapiola.fi
```

```
kali@kali: ~  
File Actions Edit View Help  
193.209.71.200      kuha.tapiola.fi  
193.209.71.201      lohi.tapiola.fi  
193.209.71.68       mail.tapiola.fi  
193.209.71.69       mail2.tapiola.fi  
193.209.71.84       mmail.tapiola.fi  
193.209.71.85       mmail2.tapiola.fi  
193.209.71.83       mposti.tapiola.fi  
193.209.71.81       mposti1.tapiola.fi  
193.209.71.82       mposti2.tapiola.fi  
193.209.71.67       ns.tapiola.fi  
193.209.71.70       ns2.tapiola.fi  
193.209.71.235      pluto.tapiola.fi  
193.209.71.69       poro.tapiola.fi  
193.209.71.238      satellite.tapiola.fi  
193.209.71.110      siili.tapiola.fi  
193.209.71.1        sonerar.tapiola.fi  
193.209.71.175      st-extranet.tapiola.fi  
193.209.71.188      st-verkkopalvelu2.tapiola.fi  
193.209.71.189      st-webservices.tapiola.fi  
mail2.tapiola.fi
```

```
kali@kali: ~  
File Actions Edit View Help  
193.209.71.189 st-webservices.tapiola.fi  
193.209.71.187 st-verkkopalvelu.tapiola.fi  
193.209.71.183 st-yrityspalvelu.tapiola.fi  
217.29.227.231 stage.tapiola.fi  
217.29.229.88 stagepft.tapiola.fi  
81.22.248.112 tapahtumat.tapiola.fi  
193.209.71.190 200 verkkopalvelu2.tapiola.fi  
193.209.71.182 200 verkkopalvelu.tapiola.fi  
217.29.229.119 test-crl.tapiola.fi  
193.209.71.211 testiverkkopalvelu.tapiola.fi  
193.209.71.166 200 webservices.tapiola.fi  
193.209.71.34 uranus.tapiola.fi  
193.209.71.2 users.tapiola.fi  
193.209.71.208 verkkopalvelut.tapiola.fi  
83.150.127.170 viestinta.tapiola.fi  
83.150.79.5 vuosiraportti.tapiola.fi  
193.209.71.186 yrityspalvelu.tapiola.fi  
193.209.71.143 200 www.tapiola.fi  
83.150.79.5 www.vuosiraportti.tapiola.fi vuosiraportti.tapiola.fi  
193.209.71.206 www.palvelut.tapiola.fi
```


```
193.209.71.208    verkkopalvelut.tapiola.fi
83.150.127.170    viestinta.tapiola.fi
83.150.79.5       vuosisiraportti.tapiola.fi
193.209.71.186    yrittyspalvelu.tapiola.fi
193.209.71.143    200 www.tapiola.fi
83.150.79.5       www.vuosisiraportti.tapiola.fi    vuosisiraportti.tapiola.fi
193.209.71.206    www.palvelut.tapiola.fi
81.17.195.43      www.galleria.tapiola.fi
81.17.195.42      www.teema.tapiola.fi
.
04:30:26
Ip address: 45 | Subdomain: 48 | elapsed time: 00:08:33
```

- Open Ports Enumeration applying with nmap

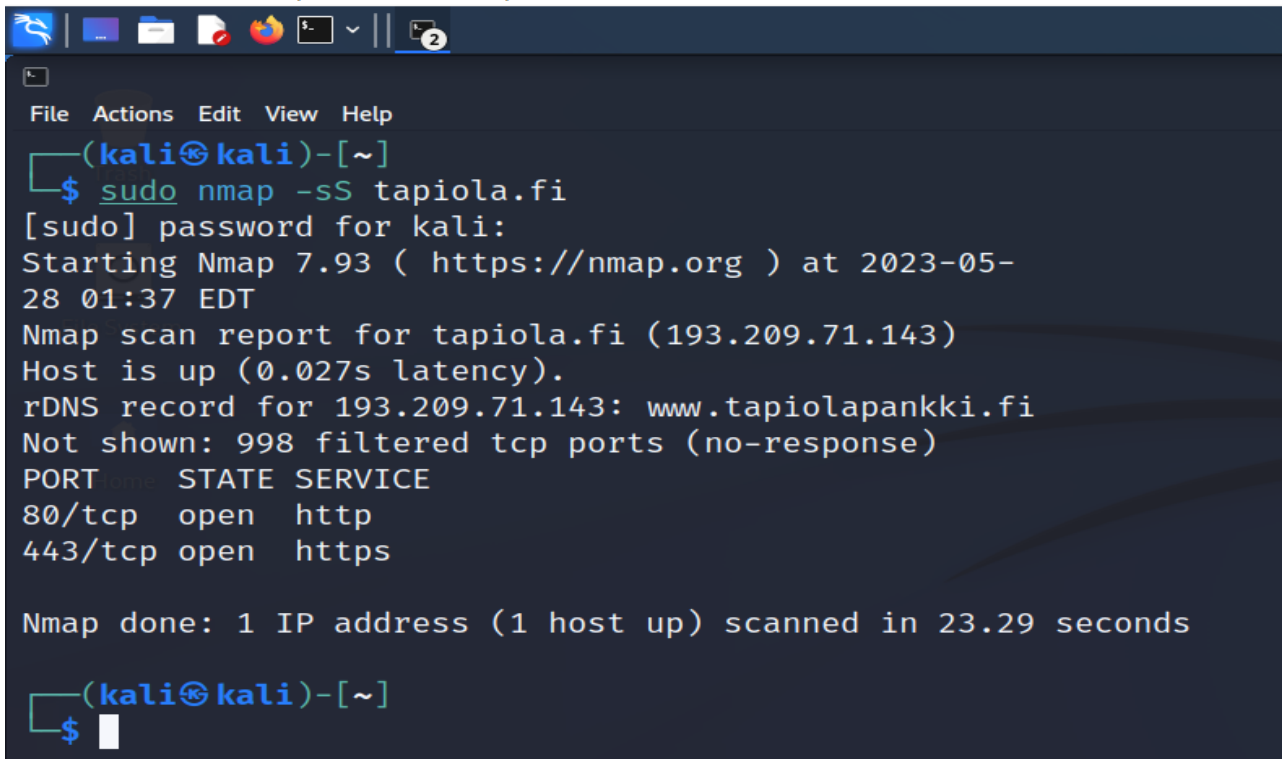
A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

### Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

 kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



```
(kali@kali)-[~]
$ sudo nmap -sS tapiola.fi
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-28 01:37 EDT
Nmap scan report for tapiola.fi (193.209.71.143)
Host is up (0.027s latency).
rDNS record for 193.209.71.143: www.tapiolapankki.fi
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 23.29 seconds

(kali@kali)-[~]
$
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https



## Checking for Vulnerabilities using nikto

vulnerabilities are scanned by Nikto. But not any found vulnerability.

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nikto -h tapiola.fi  
- Nikto v2.5.0  
  
+ Target IP: 193.209.71.143  
+ Target Hostname: tapiola.fi  
+ Target Port: 80  
+ Start Time: 2023-05-28 01:40:36 (GMT-4)  
  
+ Server: BigIP  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Root page / redirects to: http://www.lahitapiola.fi/www/yksityisasiakkaat/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response  
+ ERROR: Error limit (20) reached for host, giving up. Last error:  
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response  
+ Scan terminated: 21 error(s) and 2 item(s) reported on remote host  
+ End Time: 2023-05-28 01:42:25 (GMT-4) (109 seconds)  
  
+ 1 host(s) tested
```

```
(kali@kali)-[~]  
$ sudo nikto -h 193.209.71.143  
- Nikto v2.5.0  
  
+ 0 host(s) tested
```

# Scanned Vulnerabilities Using Netsparker

## 1) Weak Ciphers Enabled

**Weak Ciphers Enabled**  
CONFIRMED MEDIUM

URL : <https://www.tapiola.fi/>

List of Supported Weak Ciphers :

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0041)
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0084)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)

**Vulnerability Details**

Netsparker detected that weak ciphers are enabled during secure communication (SSL).  
You should allow only strong ciphers on your web server to protect secure communication with your visitors.

**Impact**

Attackers might decrypt SSL traffic between your server and your visitors.

**CLASSIFICATION**

PCI DSS 3.2	6.54
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3
CVSS 3.0 SCORE	

Risk type : Medium

URL : <https://www.tapiola.fi/>

List of Supported Weak Ciphers :

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0041)
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0084)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)

- **Vulnerability Details**

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

- **Impact**

Attackers might decrypt SSL traffic between your server and your visitors.

- **Actions to Take**

For Apache, you should modify the SSLCipherSuite directive in the  
httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
```

```
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry.

**Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:  
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

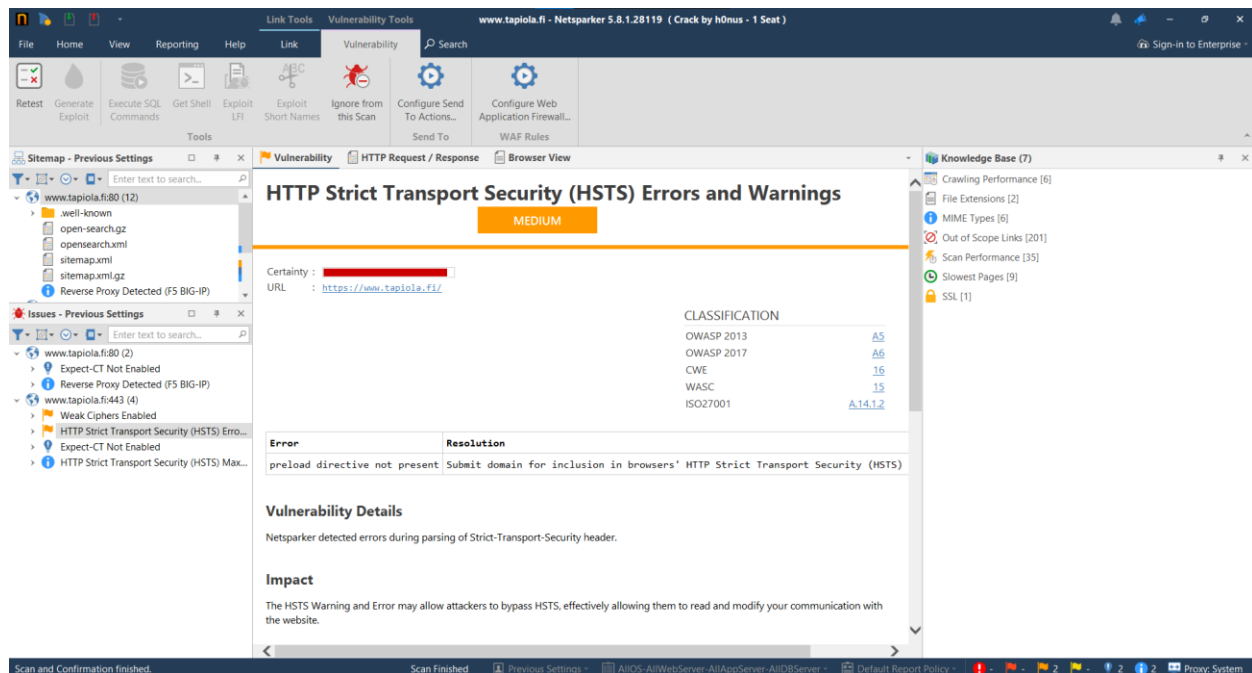
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

- **Remedy**

Configure your web server to disallow using weak ciphers.

## 2) HTTP Strict Transport Security (HSTS) Errors and Warnings



Risk type : Medium

URL : https://www.tapiola.fi/

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

### • Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header.

### • Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

### • Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages.

Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate

- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

- Serve an HSTS header on the base domain for HTTPS requests:

  - The max-age must be at least 31536000 seconds (1 year)

  - The includeSubDomains directive must be specified

  - The preload directive must be specified

  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)