**Security in Web Development Elective, KEA**

1. **Mandatory**

**Alexander B. T. Christensen**

Github repo: <https://github.com/realkoder/soft-dev-02-web-sec>

Table of Contents

[1.0 Finding Subdomains 2](#_Toc210993244)

[1.1 Google approach 2](#_Toc210993245)

[1.2 Ruby script fetching ctr.sh 2](#_Toc210993246)

[2.0 API analysis 2](#_Toc210993247)

[3.0 Third party dependencies 2](#_Toc210993248)

[4.0 Appendixes 2](#_Toc210993249)

[4.1 Subdomains for \*kea.dk 2](#_Toc210993250)

[4.2 Subdomains for \*ek.dk 6](#_Toc210993251)

# 1.0 Finding Subdomains

Assignment: Find as many subdomains as possible for \*.kea.dk (or \*.ek.dk)

## 1.1 Google approach

For a quick simple approach, I went to google and did the following two searches for indexed subdomains and public pages:

*site:\*.kea.dk  
site:\*.ek.dk*

It’s fast and useful for a first pass, but it’s not as strong as using scripting or subfinder tools such as *amass*, subfinder or gobuster.

## 1.2 Ruby script fetching ctr.sh

I wrote a [Ruby script](https://github.com/realkoder/soft-dev-02-web-sec/blob/main/assignments/mandatory-1/finding_subdomains_on_crt_sh_script.rb) that queries *Certificate Transparency* via crt.sh - "https://crt.sh/?q=%25.#{domain}&output=json" to retrieve public TLS certificates and extract registered subdomains for a given domain.  
With the script I save the raw JSON and produces a normalized list of unique subdomains.

For the subdomains either checkout **appendix 4.1 & 4.2** or click this link: [websecdev-repo-man1-assets](https://github.com/realkoder/soft-dev-02-web-sec/tree/main/assignments/mandatory-1/assets)  
This is a passive, non-intrusive method suitable for asset discovery and reconnaissance.

## 1.3 Subdomain discovery tools

Subdomain discovery tools as Amass and Subfinder sems to be more effective as they aggregate results from multiple sources, APIs, and DNS records, they do this enumeration at scale which should discover far more subdomains compared to single-source queries such as my google and scripting approach.  
Checkout **appendix 4.3.**

# 2.0 API analysis

# 3.0 Third party dependencies

# 4.0 Appendixes

## 4.1 Subdomains for \*.kea.dk

\*.kea.dk  
\*.library.kea.dk  
alumne.kea.dk  
alumne.kea.dk.buchs.dk  
bestyrelse.kea.dk  
bestyrelse.kea.dk.buchs.dk  
bibliotek.kea.dk  
bibliotek.kea.dk.buchs.dk  
buchstest.kea.dk  
chatgpt.kea.dk  
cloudvpsserver1.kea.dk  
cpanel.alumne.kea.dk  
cpanel.bestyrelse.kea.dk  
cpanel.bibliotek.kea.dk  
cpanel.buchstest.kea.dk  
cpanel.cloudvpsserver1.kea.dk  
cpanel.global.kea.dk  
cpanel.it.kea.dk  
cpanel.karriere.legacy.kea.dk  
cpanel.kea.dk  
cpanel.kompetence.kea.dk  
cpanel.materialdesignlab.kea.dk  
cpanel.mdl-temp.kea.dk  
cpanel.mit.kea.dk  
cpanel.mitkea.legacy.kea.dk  
cpanel.neh.kea.dk  
cpanel.optometri.kea.dk  
cpanel.projekter.kea.dk  
cpcalendars.alumne.kea.dk  
cpcalendars.bestyrelse.kea.dk  
cpcalendars.bibliotek.kea.dk  
cpcalendars.buchstest.kea.dk  
cpcalendars.cloudvpsserver1.kea.dk  
cpcalendars.global.kea.dk  
cpcalendars.it.kea.dk  
cpcalendars.karriere.legacy.kea.dk  
cpcalendars.kea.dk  
cpcalendars.kompetence.kea.dk  
cpcalendars.materialdesignlab.kea.dk  
cpcalendars.mdl-temp.kea.dk  
cpcalendars.mit.kea.dk  
cpcalendars.mitkea.legacy.kea.dk  
cpcalendars.neh.kea.dk  
cpcalendars.optometri.kea.dk  
cpcalendars.projekter.kea.dk  
cpcontacts.alumne.kea.dk  
cpcontacts.bestyrelse.kea.dk  
cpcontacts.bibliotek.kea.dk  
cpcontacts.buchstest.kea.dk  
cpcontacts.cloudvpsserver1.kea.dk  
cpcontacts.global.kea.dk  
cpcontacts.it.kea.dk  
cpcontacts.karriere.legacy.kea.dk  
cpcontacts.kea.dk  
cpcontacts.kompetence.kea.dk  
cpcontacts.materialdesignlab.kea.dk  
cpcontacts.mdl-temp.kea.dk  
cpcontacts.mit.kea.dk  
cpcontacts.mitkea.legacy.kea.dk  
cpcontacts.neh.kea.dk  
cpcontacts.optometri.kea.dk  
cpcontacts.projekter.kea.dk  
diy.projekter.kea.dk  
evaluering.kea.dk  
glitteringunicorn.kea.dk  
global.kea.dk  
help.dreakspark.kea.dk  
help.dreamspark.kea.dk  
help.imagine.kea.dk  
help.vmap.kea.dk  
intra.kea.dk.buchs.dk  
ipv6.it.kea.dk  
ipv6.kea.dk  
ipv6.projekter.kea.dk  
it.kea.dk  
it.kea.dk.buchs.dk  
jobportal.kea.dk  
jobportal.original.kea.dk  
karriere.kea.dk  
karriere.legacy.kea.dk  
katalog.kea.dk  
kea.dk  
kea@kea.dk  
keanet.dk.kea.dk  
kompetence.kea.dk  
kompetence.kea.dk.buchs.dk  
ldaps.kea.dk  
legacy.bibliotek.kea.dk  
legacy.kea.dk  
legacy.kompetence.kea.dk  
library.kea.dk  
mail.alumne.kea.dk  
mail.bestyrelse.kea.dk  
mail.bibliotek.kea.dk  
mail.buchstest.kea.dk  
mail.cloudvpsserver1.kea.dk  
mail.global.kea.dk  
mail.it.kea.dk  
mail.karriere.kea.dk  
mail.karriere.legacy.kea.dk  
mail.kea.dk  
mail.kompetence.kea.dk  
mail.materialdesignlab.kea.dk  
mail.materialdesignlab.kea.dk.buchs.dk  
mail.mdl-temp.kea.dk  
mail.mit.kea.dk  
mail.mitkea.legacy.kea.dk  
mail.my.kea.dk  
mail.neh.kea.dk  
mail.opgaver.kea.dk  
mail.optometri.kea.dk  
mail.projekter.kea.dk  
materialdesignlab.kea.dk  
materialdesignlab.kea.dk.buchs.dk  
mda@kea.dk  
mdl-temp.kea.dk  
mit.kea.dk  
mitkea.legacy.kea.dk  
mpk@kea.dk  
my.kea.dk  
neh.kea.dk  
nyheder.kea.dk  
old.global.kea.dk  
old.kea.dk  
opgaver.kea.dk  
optometri.kea.dk  
parkering.kea.dk  
portal.kea.dk  
projekter.kea.dk  
psrad.kea.dk  
psrodc-01.kea.dk  
publish.kea.dk  
resourcebooker.kea.dk  
selvstudie.projekter.kea.dk  
service.kea.dk  
servicedesk.kea.dk  
servicedesk.kea.dk.it.kea.dk  
serviceportal.kea.dk  
ssp.kea.dk  
studieordninger.kea.dk  
studietest.projekter.kea.dk  
survey.kea.dk  
temp.kea.dk  
test.projekter.kea.dk  
webdisk.alumne.kea.dk  
webdisk.bestyrelse.kea.dk  
webdisk.bibliotek.kea.dk  
webdisk.buchstest.kea.dk  
webdisk.global.kea.dk  
webdisk.it.kea.dk  
webdisk.karriere.legacy.kea.dk  
webdisk.kea.dk  
webdisk.kompetence.kea.dk  
webdisk.materialdesignlab.kea.dk  
webdisk.mdl-temp.kea.dk  
webdisk.mit.kea.dk  
webdisk.mitkea.legacy.kea.dk  
webdisk.neh.kea.dk  
webdisk.optometri.kea.dk  
webdisk.projekter.kea.dk  
webmail.alumne.kea.dk  
webmail.bestyrelse.kea.dk  
webmail.bibliotek.kea.dk  
webmail.buchstest.kea.dk  
webmail.cloudvpsserver1.kea.dk  
webmail.global.kea.dk  
webmail.it.kea.dk  
webmail.karriere.legacy.kea.dk  
webmail.kea.dk  
webmail.kompetence.kea.dk  
webmail.materialdesignlab.kea.dk  
webmail.mdl-temp.kea.dk  
webmail.mit.kea.dk  
webmail.mitkea.legacy.kea.dk  
webmail.neh.kea.dk  
webmail.optometri.kea.dk  
webmail.projekter.kea.dk  
whm.cloudvpsserver1.kea.dk  
whm.kea.dk  
www.alumne.kea.dk  
www.alumne.kea.dk.buchs.dk  
www.bestyrelse.kea.dk  
www.bestyrelse.kea.dk.buchs.dk  
www.bibliotek.kea.dk  
www.bibliotek.kea.dk.buchs.dk  
www.buchstest.kea.dk  
www.cloudvpsserver1.kea.dk  
www.diy.projekter.kea.dk  
www.glitteringunicorn.kea.dk  
www.global.kea.dk  
www.intra.kea.dk.buchs.dk  
www.it.kea.dk  
www.it.kea.dk.buchs.dk  
www.jobportal.kea.dk  
www.jobportal.original.kea.dk  
www.karriere.kea.dk  
www.karriere.legacy.kea.dk  
www.kea.dk  
www.keanet.dk.kea.dk  
www.kompetence.kea.dk  
www.materialdesignlab.kea.dk  
www.materialdesignlab.kea.dk.buchs.dk  
www.mdl-temp.kea.dk  
www.mit.kea.dk  
www.mitkea.legacy.kea.dk  
www.my.kea.dk  
www.neh.kea.dk  
www.opgaver.kea.dk  
www.optometri.kea.dk  
www.projekter.kea.dk  
www.selvstudie.projekter.kea.dk  
www.service.kea.dk  
www.servicedesk.kea.dk  
www.servicedesk.kea.dk.it.kea.dk  
www.studieordninger.kea.dk  
www.studietest.projekter.kea.dk  
www.temp.kea.dk  
www.test.projekter.kea.dk

## 4.2 Subdomains for \*.ek.dk

\*.ek.dk  
cpanel.jas.ek.dk  
cphbusinessintra.ek.dk  
ek.dk  
ek.dk aps  
filemakerdev.ek.dk  
filemakerserver.ek.dk  
intra.ek.dk  
jas.ek.dk  
ldaps.ek.dk  
staging.ek.dk  
www.ek.dk

## 4.3 Subdomain discovery tools

Only discovering subdomains for: \*.kea.dk

### 4.3.1 Using amass

### 4.3.1 Using subfinder