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

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 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.
This script save the raw JSON and produces a normalized list of unique subdomains.
For the subdomains either checkout **appendix 4.1** - **4.2** or see the actual files: websecdev-repo-man1-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

The discovered subdomains will be used for the next step for both *.kea.dk and *.ek.dk.

2.1 Make a list of endpoints / pages

I have used gobuster which is a strong tool to brute-force endpoints and pages across the target domains and subdomains. I created a simple bash script for *.ek.dk and *.kea.dk iteration through the discovered subdomains to systematically execute gobuster command with each subdomain route as the URL argument the flag -u.

```
┌──(alex㉿kali)-[~/Documents]
└─$ gobuster dir -u "$url" -w /usr/share/seclists/Discovery/Web-Content/common-api-endpoints-mazen160.txt -o ...
```

Checkout script or appendix 4.4 for collected subdomains

While the current scan revealed limited interesting endpoints, expanding the wordlist with a larger collection would maybe have given more results through a more comprehensive brute-forcing.

2.2 Find authentication login endpoints

Discovered login endpoints from gobuster enumeration:

https://mit.kea.dk/login

- Homemade login flow - taking classic username and password credentials

Manually found these login pages:

webdisk.projekter.kea.dk

- Homemade login flow - taking classic username and password credentials

https://bestyrelse.kea.dk/log-ind

- Homemade login flow - taking classic username and password credentials

3.0 Third party dependencies

Based on the gobuster endpoints discovery I will include the following targets:
ek.dk cphbusinessintra.ek.dk/ bestyrelse.kea.dk evaluering.kea.dk
I will be using combination of whatweb which will detect client side frameworks, JS libraries server side frameworks, databases, headers, errors and more. I will also manually check the sites and inspect them with chrome developer tools and looking for network requests in terms of JS files, errors etc.

Whatweb command used: `whatweb -a 3 <target_url>`

3.1 ek.dk

Microsoft Azure Application Insights based on a comment I found in a fetched js file:
/*! * Application Insights JavaScript SDK - Web, 3.3.10 * Copyright (c)Microsoft and contributors. All rights reserved. */

Frontend: HTML5

Backend: ASP.NET, **Microsoft Azure Application Insights**

3.2 cphbusinessintra.ek.dk

Just accessing https://cphbusinessintra.ek.dk/ displays an error revealing the use of Umbraco as CMS: **Version Information:** Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4770.0

3.3 bestyrelse.kea.dk

Frontend: JQuery, MetaGenerator[Joomla! - Open Source Content Management], Bootstrap[3.3.7]

Backend: HTTPServer[Apache]

3.4 https://evaluering.kea.dk

Frontend: JQuery, TypeScript, Bootstrap, Knockout JavaScript library v3.5.1

Backend: ASP.NET

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

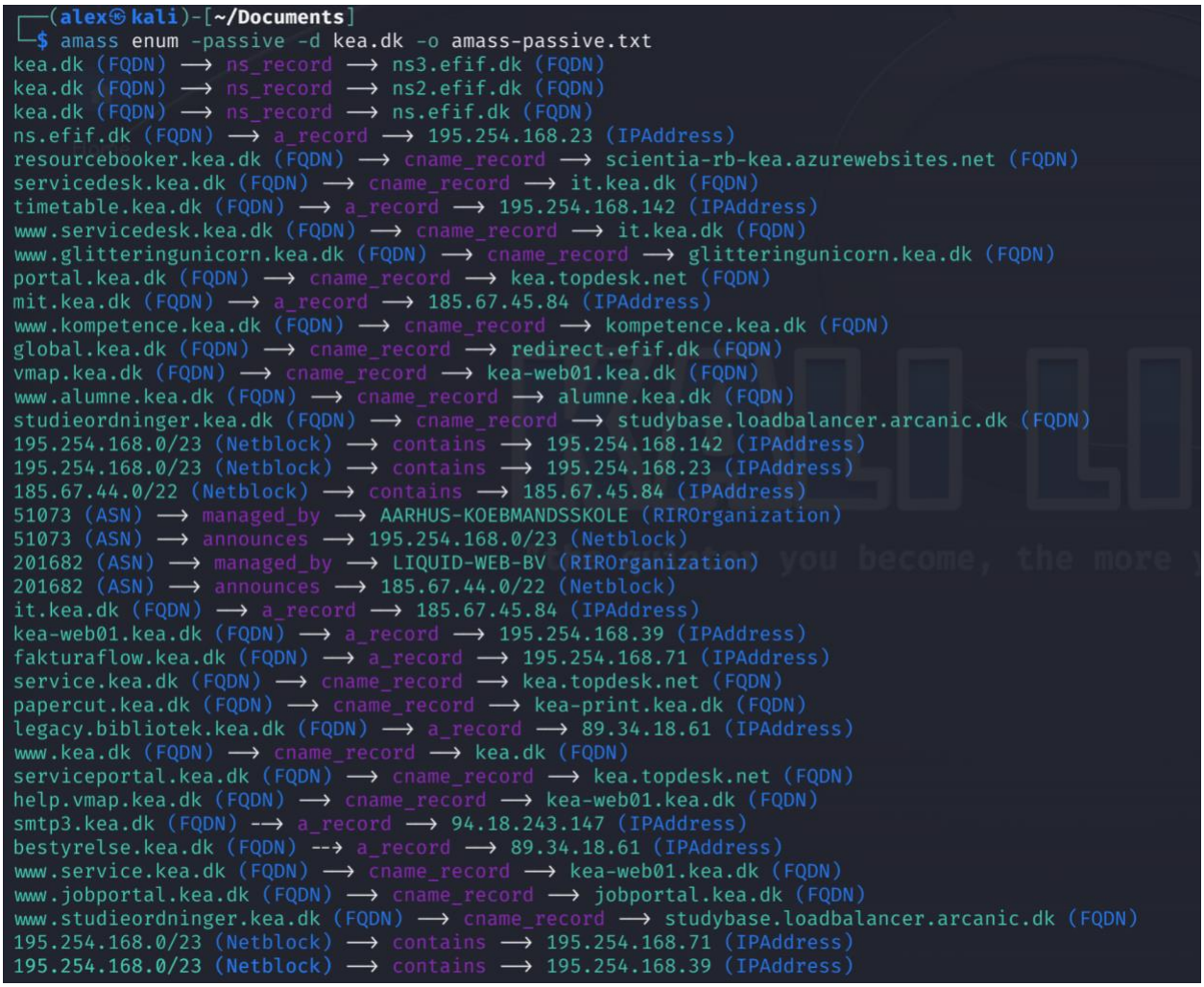
ldaps.ek.dk

staging.ek.dk

www.ek.dk

4.3 Subdomain discovery tool Amass

Only discovering subdomains for: *.kea.dk



Click here to checkout generated amass-passive.txt

4.4 Gobuster endpoint discovery

Discovered endpoints for *.ek.dk:

https://jas.ek.dk/pages

https://jas.ek.dk/docs

Discovered endpoints for *.Kea.dk

target url: https://bestyrelse.kea.dk

/log

target url: https://evaluering.kea.dk

/help /mail /photo /report /Search /search

target url: https://katalog.kea.dk

/admin /Search /search

target url: https://legacy.kea.dk

/3 /connect /contact /log

target url: https://legacy.kompetence.kea.dk

/log

target url: https://mit.kea.dk

/api /log /login

target url: https://neh.kea.dk

/log /contact

target url: https://old.global.kea.dk

/log /Search /search

target url: https://old.kea.dk

/api /connect /log

target url: https://studieordninger.kea.dk

/1 /2 /3 /6 /0 /4 /5 /8 /7 /9 /preview /admin

target url: https://survey.kea.dk

/api /help /results /support /users