jamk.fi

Assignment 1

Web Application Security

Joni Korpihalkola
K1625

Report
01/2018
Information and communication technology
ICT-field

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Contents

Figures

1 Introduction

This document contains answers to Web Application Security course's questions in Assignment 1.

2 Report Template

In my opinion the technical report "Source code audit of Norwegian electronic voting system" was well done. After the title page, the report has an executive summary, where the discovered technical issues are briefly explained and there is a brief list of recommendations. Just reading the executive summary gives the reader a lot of information. The report also makes good use of tables and recommendations are highlighted by small black borders, which helps the reader realize that they are the important part of the report. The only thing about the report that doesn't please my eyes are the unnecessary headers on every page.

A bad report that I read was "Ghost Blogging Platform Web Application Penetration Test Code Review" by VoidSec. The report has a key findings section, but it doesn't provide as much information as the electronic voting system report. A list of recommended actions to improve the system would be helpful. The use of red color in the tables is distracting and makes the text harder to read, a different color should have been used. The layout of the tables is also kind of confusing. The report has headers and footers with a lot of text, which makes the report itself harder to read to me.

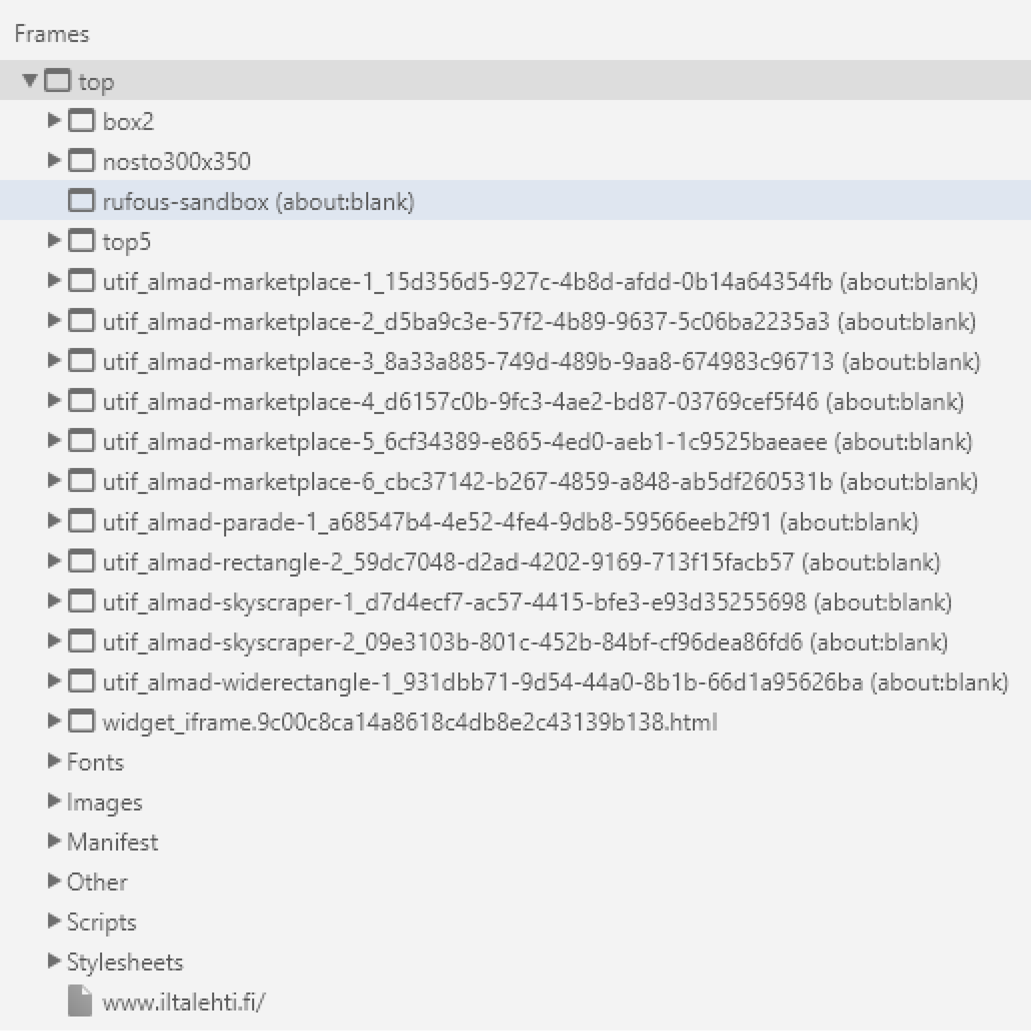
3 The threat landscape

Out of the top 10 security risks, I'm only familiar with SQL injections, because they have been explained in previous courses. Some items on the top 10 list aren't individual vulnerabilities, they are rather bad practices that can be exploited, like security misconfiguration and insufficient logging & monitoring.

It is somewhat interesting, that injections were the greatest security risk in 2013 and they still are. You would think that websites would have more checks today for data sent by users, so they wouldn't run commands by accident. Broken authentication and sensitive data exposure are the things that probably attract the most news headlines, at least I remember many cases where customer information was leaked into the internet or stolen from a company's database.

4 The same-origin Policy

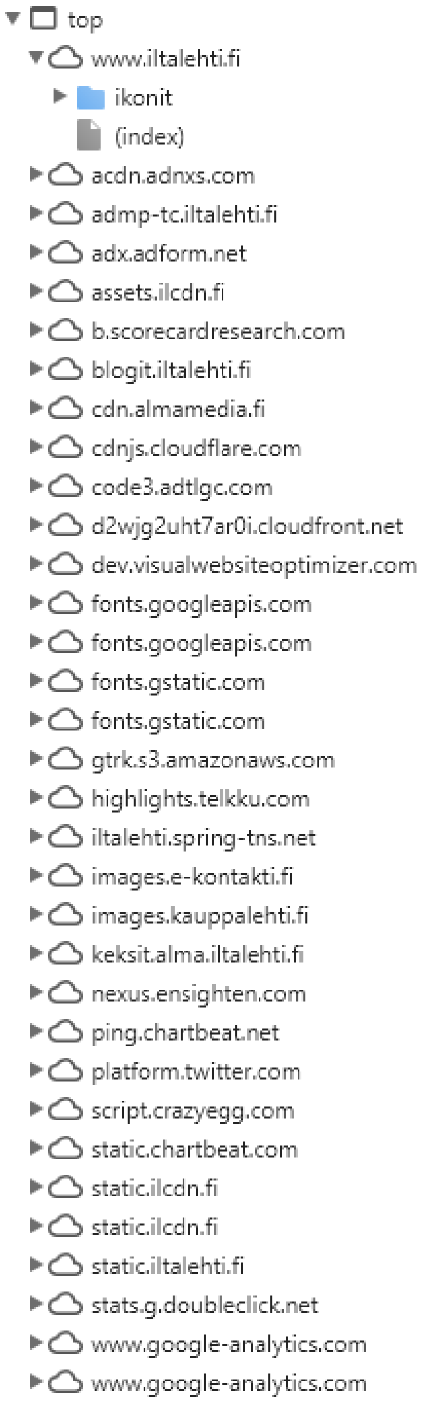
I looked up what happens inside the site https://www.iltalehti.fi. The site has a top frame, which contains many frames that serve as space for ads. (Figure 1)



```
Frames
▼ top
    ▶ box2
    ▶ nosto300x350
      rufous-sandbox (about:blank)
    ▶ top5
    ▶ utif_almad-marketplace-1_15d356d5-927c-4b8d-afdd-0b14a64354fb (about:blank)
    ▶ utif_almad-marketplace-2_d5ba9c3e-57f2-4b89-9637-5c06ba2235a3 (about:blank)
    ▶ utif_almad-marketplace-3_8a33a885-749d-489b-9aa8-674983c96713 (about:blank)
    ▶ utif_almad-marketplace-4_d6157c0b-9fc3-4ae2-bd87-03769cef5f46 (about:blank)
    ▶ utif_almad-marketplace-5_6cf34389-e865-4ed0-aeb1-1c9525baeaee (about:blank)
    ▶ utif_almad-marketplace-6_cbc37142-b267-4859-a848-ab5df260531b (about:blank)
    ▶ utif_almad-parade-1_a68547b4-4e52-4fe4-9db8-59566eeb2f91 (about:blank)
    ▶ utif_almad-rectangle-2_59dc7048-d2ad-4202-9169-713f15facb57 (about:blank)
    ▶ utif_almad-skyscraper-1_d7d4ecf7-ac57-4415-bfe3-e93d35255698 (about:blank)
    ▶ utif_almad-skyscraper-2_09e3103b-801c-452b-84bf-cf96dea86fd6 (about:blank)
    ▶ utif_almad-widerectangle-1_931dbb71-9d54-44a0-8b1b-66d1a95626ba (about:blank)
    ▶ widget_iframe.9c00c8ca14a8618c4db8e2c43139b138.html
    ▶ Fonts
    ▶ Images
    ▶ Manifest
    ▶ Other
    ▶ Scripts
    ▶ Stylesheets
      www.iltalehti.fi/
```

Figure 1. List of frames in iltalehti.fi

Some frames have assets that are loaded from assets.ilcdn.fi, like the font BerninoSans-Web_Bold.woff2 and a small logo of Iltalehti that is a .png picture. The almad-marketplace frames have images and scripts, which seem to handle user clicks. Some small icon images are loaded from static.iltalehti.fi, below is a complete list of sources which iltalehti.fi gets content from. (Figure 2)



```
▼ top
  ▼ www.iltalehti.fi
    ▶ ikonit
      (index)
  ▶ acdn.adnxs.com
  ▶ admp-tc.iltalehti.fi
  ▶ adx.adform.net
  ▶ assets.ilcdn.fi
  ▶ b.scorecardresearch.com
  ▶ blogit.iltalehti.fi
  ▶ cdn.almamedia.fi
  ▶ cdnjs.cloudflare.com
  ▶ code3.adtlgc.com
  ▶ d2wjg2uht7ar0i.cloudfront.net
  ▶ dev.visualwebsiteoptimizer.com
  ▶ fonts.googleapis.com
  ▶ fonts.googleapis.com
  ▶ fonts.gstatic.com
  ▶ fonts.gstatic.com
  ▶ gtrk.s3.amazonaws.com
  ▶ highlights.telkku.com
  ▶ iltalehti.spring-tns.net
  ▶ images.e-kontakti.fi
  ▶ images.kauppalehti.fi
  ▶ keksit.alma.iltalehti.fi
  ▶ nexus.ensighten.com
  ▶ ping.chartbeat.net
  ▶ platform.twitter.com
  ▶ script.crazyegg.com
  ▶ static.chartbeat.com
  ▶ static.ilcdn.fi
  ▶ static.ilcdn.fi
  ▶ static.iltalehti.fi
  ▶ stats.g.doubleclick.net
  ▶ www.google-analytics.com
  ▶ www.google-analytics.com
```

Figure 2. Sources from iltalehti.fi

As can be seen from the sources list, fonts are loaded from Google's font API, a JavaScript file is loaded from twitter and there's at least two sources where ads are loaded from. Google Analytics scripts collect data from visitors and measure their activity on the site.

Below is a simplified image of some of the images, links and ads that iltalehti.fi shows. (Figure 3)

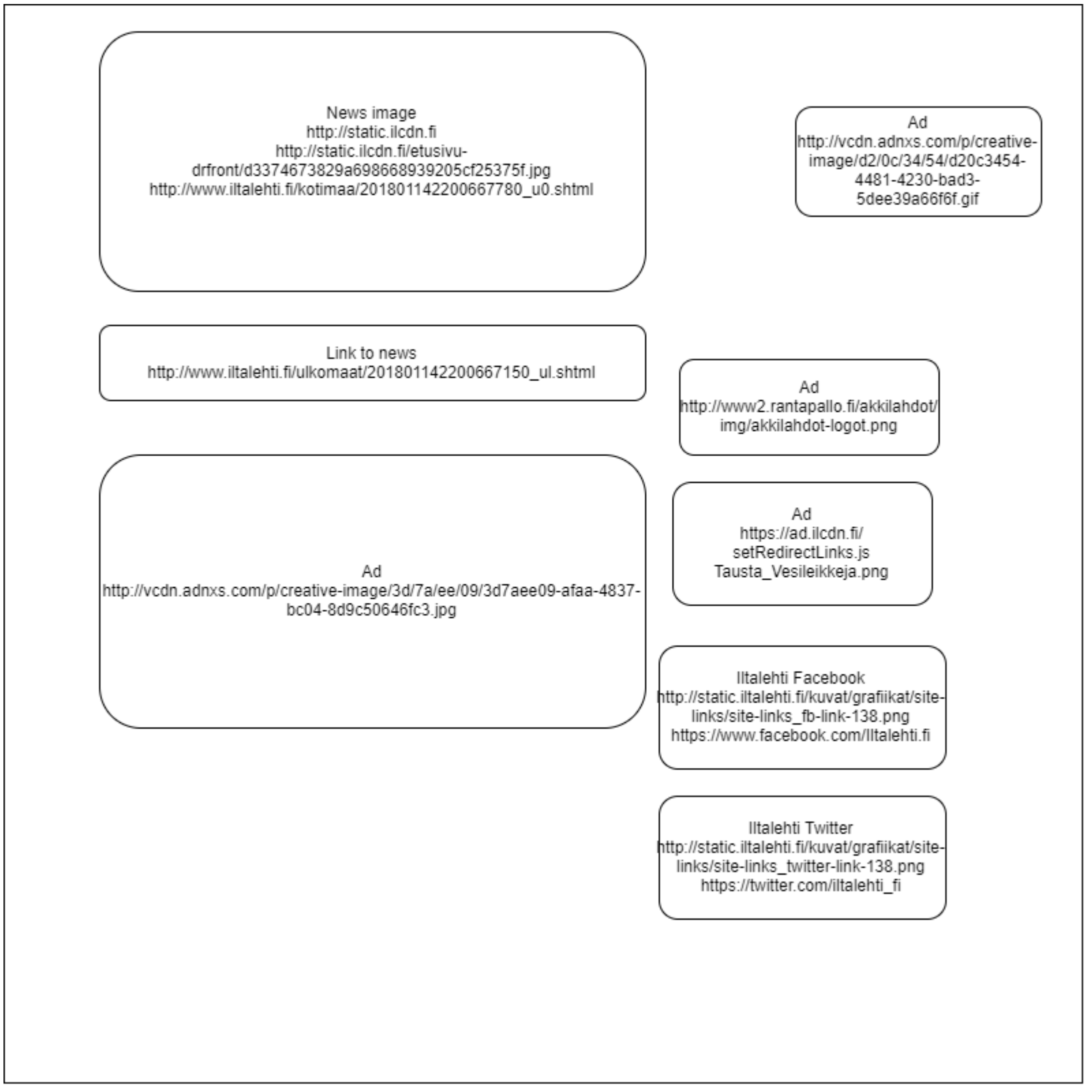

News image
http://static.ilcdn.fi
http://static.ilcdn.fi/etusivu-
drfront/d3374673829a698668939205cf25375f.jpg
http://www.iltalehti.fi/kotimaa/20180114220066778O_u0.shtml
Ad
http://vcdn.adnxs.com/p/creative-
image/d2/0c/34/54/d20c3454-
4481-4230-bad3-
5dee39a66f6f.gif
Link to news
http://www.iltalehti.fi/ulkomaat/20180114220066715O_ul.shtml
Ad
http://www2.rantapallo.fi/akkilahdot/
img/akkilahdot-logot.png
Ad
http://vcdn.adnxs.com/p/creative-image/3d/7a/ee/09/3d7aee09-afaa-4837-
bc04-8d9c50646fc3.jpg
Ad
https://ad.ilcdn.fi/
setRedirectLinks.js
Tausta_Vesileikkeja.png
Iltalehti Facebook
http://static.iltalehti.fi/kuvat/grafiikat/site-
links/site-links_fb-link-138.png
https://www.facebook.com/Iltalehti.fi
Iltalehti Twitter
http://static.iltalehti.fi/kuvat/grafiikat/site-
links/site-links_twitter-link-138.png
https://twitter.com/iltalehti_fi

Figure 3. Simplified image of iltalehti.fi

According to same-origin policy, the ad below the piece of news from vcdn.adnxs.com can access the ad on the right, because they share the same protocol, host and port, they do not have to be in the same directory. The news image from static.ilcdn.fi shouldn't have access to the ad ad.ilcdn.fi, because the hosts are different.