ARTIFACT EVALUATED
usenix ASSOCIATION
AVAILABLE

USENIX Security ’24 Artifact Appendix: Trust Me *If You Can* – How Usable Is Trusted Types In Practice?

Sebastian Roth
sebastian.roth@tuwien.ac.at
TU Wien

Lea Gröber
lea.groeber@cispa.de
CISPA Helmholtz Center for Information Security

Philipp Baus
s8phbaus@stud.uni-saarland.de
Saarland University

Katharina Krombholz
krombholz@cispa.de
CISPA Helmholtz Center for Information Security

Ben Stock
stock@cispa.de
CISPA Helmholtz Center for Information Security

A Artifact Appendix

A.1 Abstract

Our replication package includes the following artifacts:

- `analytics/`: A folder that contains our results and the analysis script for identifying the most commonly used third-party script inclusions in the Web.
- `survey/`: A folder that contains the python Django application that hosts our presurvey.
- `webapp/`: A folder that contains the python Django Web application that was used during the coding interview for implementing Trusted Types.
- `assets/`: A folder that contains the python Django application that was used as a custom advertisement provider by the coding interview application.
- `roadmap/`: A folder that contains the HTML / JS / CSS files for the interactive roadmap mentioned in section 5.4 of the paper.
- `Codebook.json`: A JSON file that contains the saturated final version of the code book for the study.

Notably, we can neither share the recorded interviews nor their transcripts as they might contain PII and we promised our participants to keep them confidential. We have however added the saturated final version of the code book as a comparison point for replication studies.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

Although we are not performing any critical actions, we can understand that running (untrusted) applications as root/admin is something that most people do not like. However, the `assets` need to be served from port 80 in order to work. Notably, **if you do not want to run the asset app as root**, you can also use a proxy like nginx or apache to pass the request from port 80 of your machine to another (unprivileged) port such that you can run the app with lower permissions.

Given that we have used real-world third parties in our study application (`webapp`), those third parties collect information about your browsing session. We recommend using the incognito mode or a fresh browser profile to minimize the information that they can gather. Still, information like the IP you are using will be leaked to third parties. The third parties used are: Facebook, X (Twitter at the time of conducting the study), Google (Google Tag Manager / Analytics), as well as CDNs (jquery.com, jsdelivr.net, bootstrapcdn.com).

A.2.2 How to access

GitHub:
https://github.com/cispa/trust-me-if-you-can/tree/618e02a220843db03dce4fd19220d9a796de9c04

A.2.3 Hardware dependencies

None. Anything that can run `python3` and a browser works.

A.2.4 Software dependencies

For all artifacts, you will need a Chromium-based browser as only those currently support Trusted Types. Additionally, depending on which part of the artifact is evaluated, you’ll need:

- `analytics/`: *python3* as well as the python packages *tldextract* and *psycopg2*.
- `survey/`: *python3* as well as the python package *Django*.
- `webapp/`: Docker, or *python3* and the python package *Django*.

- `assets/`: *python3* as well as the python package *Django*.
- `roadmap/`: A Browser

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation

Depending on which part of the artifact is evaluated, you'll need to follow different installation instructions:

Analysis of the third-party usage in the wild (analytics/): After you have installed `python3` as well as the python `tldextract` and *psycopg2* package (see Appendix A.2.4) you can execute the script. Notably, we are not able to give external access to our database nor to add the entire database to the repository so this script needs to be analyzed via manual code review. Still, we also added the resulting JSON file.

Presurvey WebApp (survey/): After you have installed `python3` as well as the python `Django` package (see Appendix A.2.4) you need to use the commands below to setup the application. The first three are setting up the database for the application (sqlite) the *createsuperuser* command shows you a dialog to create a superuser that can access the database via `/admin` in your web browser, and *runserver* starts the application at port 8000.

```
python3 manage.py makemigrations
python3 manage.py makemigrations website
python3 manage.py migrate
python3 manage.py createsuperuser
python3 manage.py runserver
```

Assets for the study WebApp (assets/): First add the following three lines to your `/etc/hosts` file, such that the domains for the assets are pointing to your device.

```
127.0.0.1 tt-study.local
127.0.0.1 ads.tt-study.local
127.0.0.1 mensa.tt-study.local
127.0.0.1 hireing-ads.tt-study.local
```

Then, assuming you have installed `python3` as well as the python `Django` package (see Appendix A.2.4), you need to use the commands below to setup and run the application. Notably, as this part is required to use port 80 you need to start the django app as root/admin user. See Appendix A.2.1 if you do **not** want to run the asset app as a privileged user.

```
python3 manage.py migrate
sudo python3 manage.py runserver 80
```

WebApp for the coding interviews (webapp/): The easiest way to start the application is to start it as a docker container with `docker-compose up`. If you do not have docker installed or do not want to use the docker you can also execute the commands from the `install.sh` file and manually start the application with `python3 manage.py runserver`. Notably, for the assets to work you **must** have the application of the assets up & running.

Interactive roadmap for TT deployment (roadmap/): None. Just open the `index.html` with your web browser.

A.3.2 Basic Test

Use a browser to interact with the pages to see in the terminal output of the runserver or docker command if something breaks. The pages that will be best for testing those are:

- `survey`: `http://127.0.0.1:8000/`
- `webapp`: `http://127.0.0.1:8000/`
- `assets`: `http://ads.tt-study.local/get-ad`

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at `https://secartifacts.github.io/usenixsec2024/`.