How to report a security issue in a standardized manner with Security.txt

May 18, 2021

Share

The sushi syntax is incorrect

Our story begins on a Friday evening. An InfoSec guy passes an order on an only sushi shop to take a romantic break with his sweetheart. He selects dishes and clicks on the "*Checkout*" button, however, instead of receiving the expected checkout page, he gets an SQL error page:

> *"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "**Sushi**"."*

He says to himself: "*This may be a security issue. I am going to send an e-mail to the security contact point to inform them of this bug…*" But, it is impossible to find a security contact point, only a general contact form is available. So, he fills the contact form and finally manages to place the order. However, he never got any feedback from the shop for his report. What will happen if a less ethical hacker passes by and discover this issue?

Why can't a generic contact form fulfill the job?

A generic contact form[1], most of the time, is designed to transfer public/non-sensitive information from a prospect to the marketing or sales department of a company. On the contrary, when a person notifies a company about a security vulnerability, they want to fulfill the following objectives:

- Preserve the confidentiality of the information during its transmission in order to only disclose the vulnerability to people that are in charge of the security. The goal is to give the information to people in a position to take the effective decision regarding vulnerability analysis and remediation.
- Ensure responsiveness from the company regarding the fact that they received the report and they understood the problem. Sometimes, the vulnerability is already actively exploited by an attacker, so it becomes a race against time to close the hole…

A generic contact form does not fulfill these because it does not ensure the confidentiality of the information (and its transfer) and it may start an "internal ping-pong" game at the target company between the recipient behind the contact form and the team expected to handle security incidents.

Moreover, since a contact form may not be able to receive attachments (at all or only specific types), it could be tricky to communicate securely with the company. Here is the kind of response our CSIRT got from a software provider following an email notifying them of a critical vulnerability:

"As *you sent us a protected archive alongside your mail, we thought it was spam and therefore your email was permanently deleted.*"

For these reasons, a visible direct contact point to the team handling security incidents is important.

Security.txt file to rescue

As this situation occurs often, a group of people decided to launch an initiative in order to address this issue. The objective was to define a way to indicate how to report a security issue in a standardized and simple manner.

The security.txt Internet draft was born[2].

What is this security.txt file?

As described on its homepage [3], it is a text file (text/plain Internet media type) located in one of the following locations:

1. Recommended location: /.well-known/security.txt
2. Fallback: /security.txt

It contains the following information[4] :

Field	Required	Description
Contact	Yes	A link or e-mail address for people to contact you about security issues.
Expires	Yes	The date and time when the content of the security.txt file should be considered stale.
Encryption	No	A link to a key which security researchers should use to securely talk to you.
Acknowledgments	No	A link to a web page where you say thank you to security researchers who have helped you.
Preferred-Languages	No	A comma-separated list of language codes that your security team speaks.
Canoical	No	The URLs for accessing your security.txt file.
Policy	No	A link to a policy detailing what security researchers should do when searching for or reporting security issues.
Hiring	No	A link to any security-related job openings in your organization.

A sample of security.txt file containing required and optional fields:

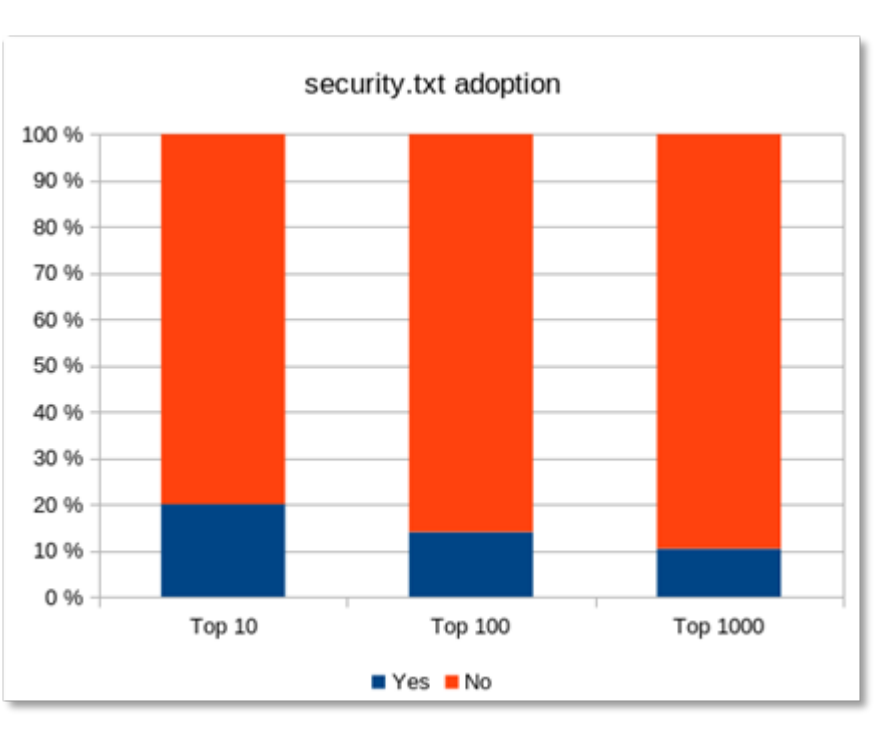
```
Contact: mailto:emergency@excellium-services.com

Expires: Sun, 1 Jan 2025 00:00 +0100

Encryption: https://excellium-services.com/assets/EMERGENCY_PKEY.asc

Preferred-Languages: en,fr

Canonical: https://excellium-services.com/.well-known/security.txt

Policy: https://excellium-services.com/emergency-service/

Hiring: https://excellium-services.com/career-opportunities/
```

Security.txt adoption

Worldwide

In April 2020[5], someone analyzed the usage of the security.txt file against the Top Alexa 1 million most visited sites[6]. Note: This data, as shown by the chart below, reveals that adoption of this feature, at the Internet level, is very low, with only 10% to 20% of sites having such file.

While created in 2017, this initiative seems to suffer from a lack of awareness.



[7]

Although statistics at the Internet level are interesting, what is the situation in our small and beloved country?

Luxembourg (raw results)

Based on the study mentioned in the previous section, we decided to look at the adoption of the security.txt file on the LU domains.

In this evaluation round, no filtering was applied on the gathered domains regarding the type of entity to which a domain belongs (government, bank, insurance, personal, association, etc.). The goal was to obtain a global overview of a maximum of LU domains.

To achieve that, we leveraged the *Certificate Transparency* log, as a data source, in order to extract a list of ".lu" domains.

A shell script was created to perform the extraction[8]:

```
$ generate-source-ct.sh

[+] Call: https://crt.sh/?dNSName=.lu&match=LIKE&output=json

9655 source.txt

[+] Let the server cool down to prevent to receive a HTTP 504.

[+] Call: https://crt.sh/?CN=.lu&match=LIKE&output=json

19510 source.txt

[+] Let the server cool down to prevent to receive a HTTP 504.

[+] Extraction finished.

8143 source-ct.txt
```

Once the list of LU domains was generated, we created a script[9] in order to verify the presence of the security.txt file on the domains extracted.

```
$ python generate-stats.py source-ct.txt

[+] Prepare the list of domains…

7975 domains selected.

[+] Initialize DB…

[+] Process the list…

Testing domain: zwiki.lu

[+] 7975 domains tested – Results:

ABSENT  : 7938 (99.54%)

PRESENT : 37    (0.46%)
```

0.46%, so, less than 1% of the Luxembourgish domains have a security.txt file…

Following the results from the study at the Internet level; Luxembourgish domains are not better informed about this initiative…Therefore, this blog post seemed to be a good idea to spread the word. 🙂

Luxembourg (pre-filtered domains)

In this evaluation round, a filter was applied to match one applied for the evaluation at the Internet level and then, made results against LU domains similar.

If we want to apply the same type of comparison like the one used for the Top Alexa 1 million most visited sites, we need to perform the analysis against the most visited LU domains. Indeed, our previous results include websites for which the usage of security.txt may be questionable.

The list was obtained from the Majestic Top 1 million most visited sites[10], which is similar to Alexa's Top but is free. Once again, we extracted the LU domains.

A shell script was created to perform the extraction[11]:

```
$ generate-source-majestic.sh

[+] Download Majestic CSV file and extract the data.

[+] Extraction finished.

177 source-majestic.txt
```

The analysis script[12] gave the following result:

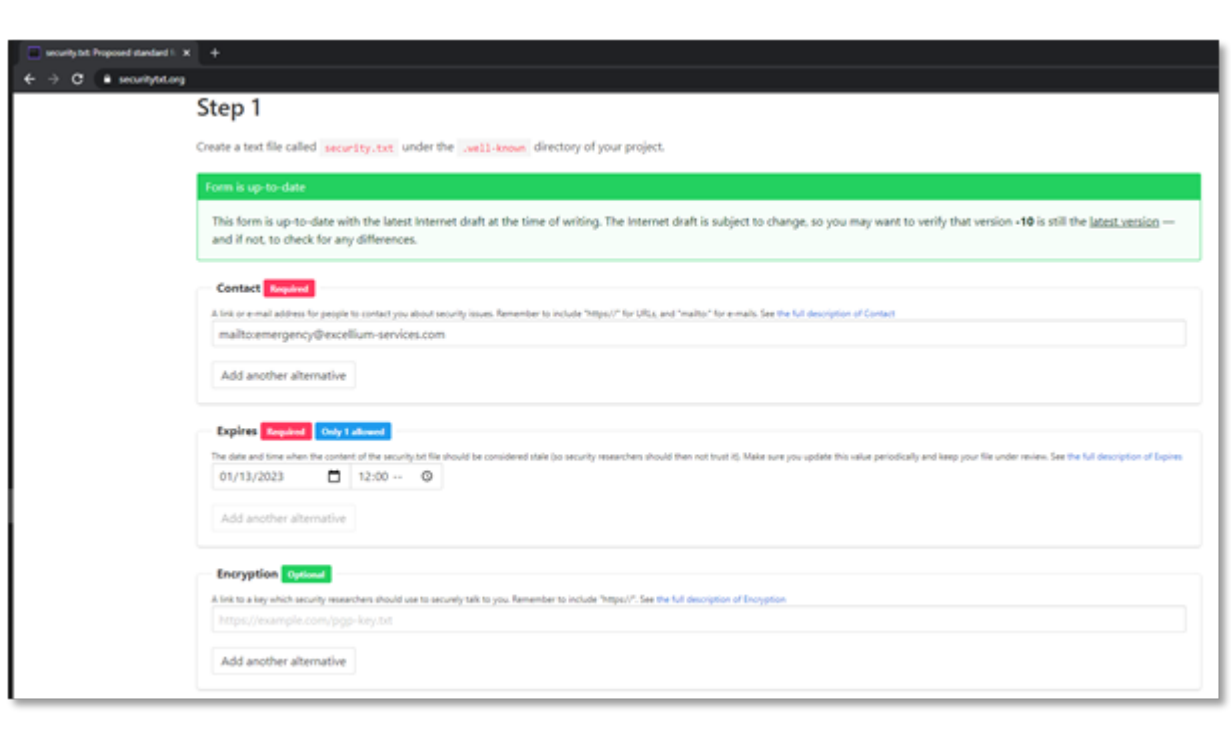
```
$ python generate-stats.py source-majestic.txt

[+] Prepare the list of domains…

177 domains selected.

[+] Initialize DB…

[+] Process the list…

Testing domain: itm.lu

[+] 177 domains tested – Results:

ABSENT  : 172   (97.18%)

PRESENT : 5     (2.82%)
```

2.82%, so, less than 3% of the most visited Luxembourgish domains have a security.txt file…

Results from this round follow the previously observed trend and confirm the awareness issue regarding this initiative.

It is never too late to add a security.txt file

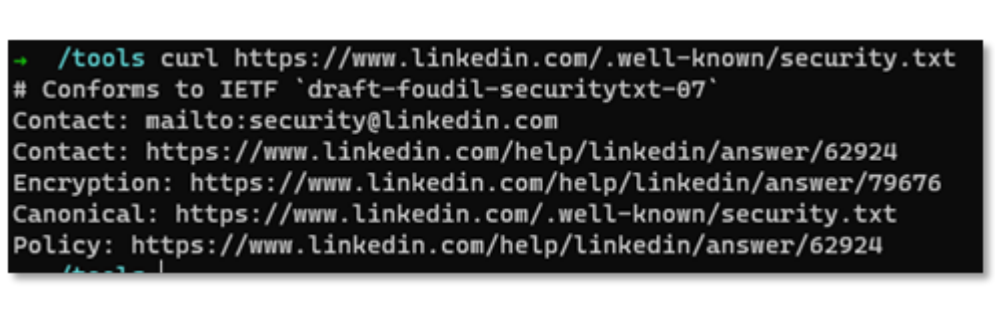
The team behind the project has anticipated this point and they have created an online tool (https://securitytxt.org/) to generate such file:



The creation procedure is simple:

1. Fill the form for the fields that you want to specify.
2. Click on the button "*Generate security.txt file*".
3. Copy the content into a file named txt (thank you captain obvious J).
4. Place the file in the location "/.well-known/security.txt" on your main domain website.
5. Check that the file is reachable using an anonymous point of view (see below).

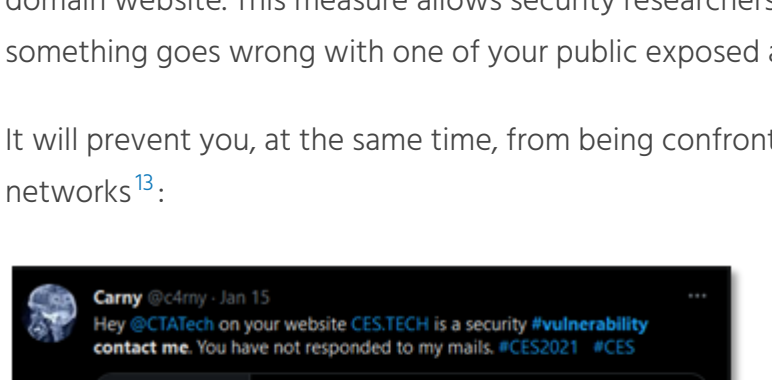
```
$ curl https://[YOUR_DOMAIN]/.well-known/security.txt
```

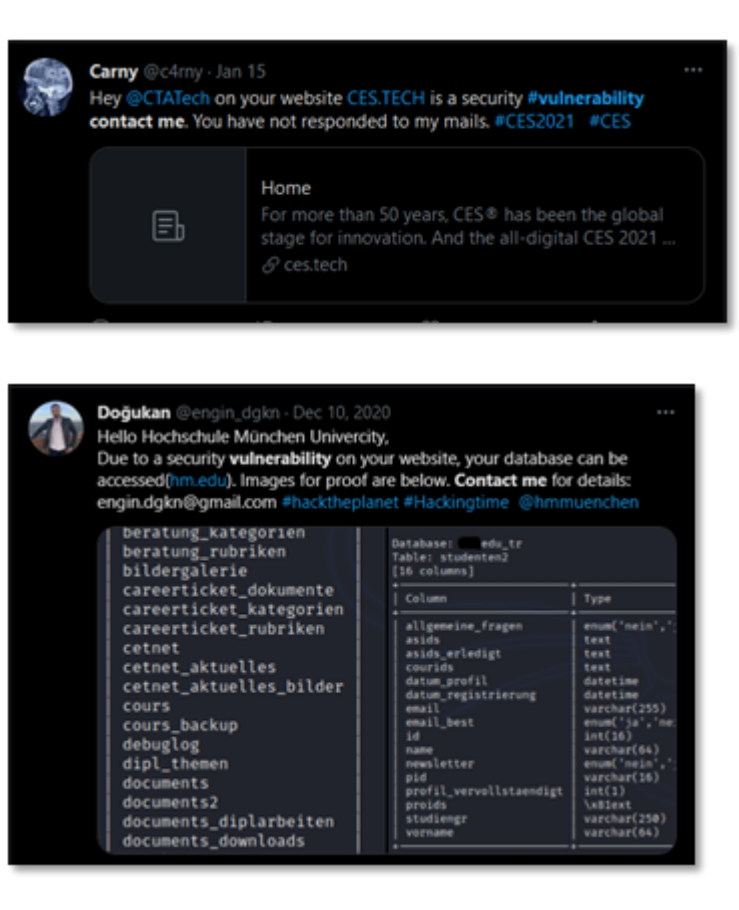


The final word

Even if the current usage of the security.txt file is not widespread, it is important to deploy such a file on your main domain website. This measure allows security researchers and other people to contact you discretely and securely if something goes wrong with one of your public exposed assets.

It will prevent you, at the same time, from being confronted with the following kind of advertising on social networks[13]:





All elements used/created for this study are stored on the following GitHub repository:

https://github.com/ExcelliumSA/SecurityTXT-Study

Credits

Dominique Righetto

Valentin Giannini

More about our Intrusion Test Services

Advice, General

Let's deliver the right solution for your business

CONTACT US