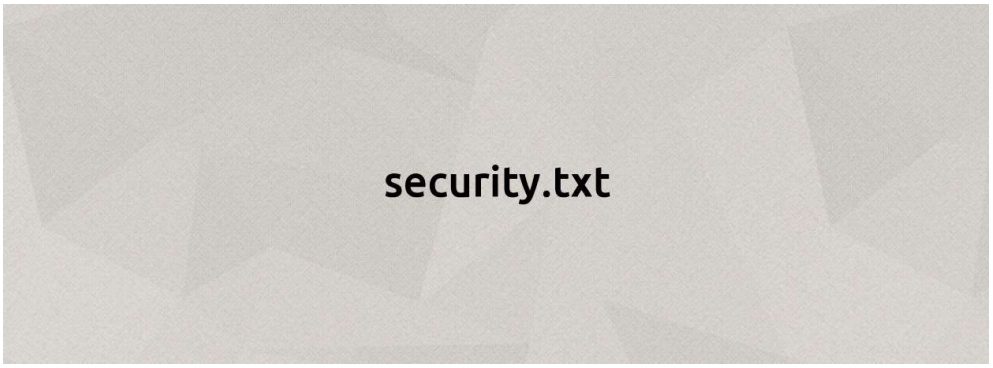
Security.txt Standard Proposed, Similar to Robots.txt

By **Catalin Cimpanu (https://www.bleepingcomputer.com/author/catalin-cimpanu/)** September 15, 2017 11:10 AM 7



Ed Foudil (https://edoverflow.com/), a web developer and security researcher, has submitted a draft (https://www.ietf.org/id/draft-foudil-securitytxt-00.txt) to the IETF — Internet Engineering Task Force — seeking the standardization of security.txt, a file that webmasters can host on their domain root and describe the site's security policies.

The file is akin to robots.txt, a standard used by websites to communicate and define policies for web and search engine crawlers.

Security.txt is for security-related problems

The distinction between security.txt and robots.txt is that security.txt will be used to communicate a company's security practices only, and is likely to be read by humans, rather than automated scanners.

For example, if a security researcher finds a security vulnerability on a website, he can access the site's security.txt file for information on how to contact the company and securely report the issue.

According to the current IETF draft, website owners would be able to create security.txt files that look like this:

```
#This is a comment
Contact: security@example.com
Contact: +1-201-555-0123
Contact: https://example.com/security
Encryption: https://example.com/pgp-key.txt
Acknowledgement: https://example.com/acknowledgements.ht
ml
Disclosure: Full
```

Infosec community welcomed the idea

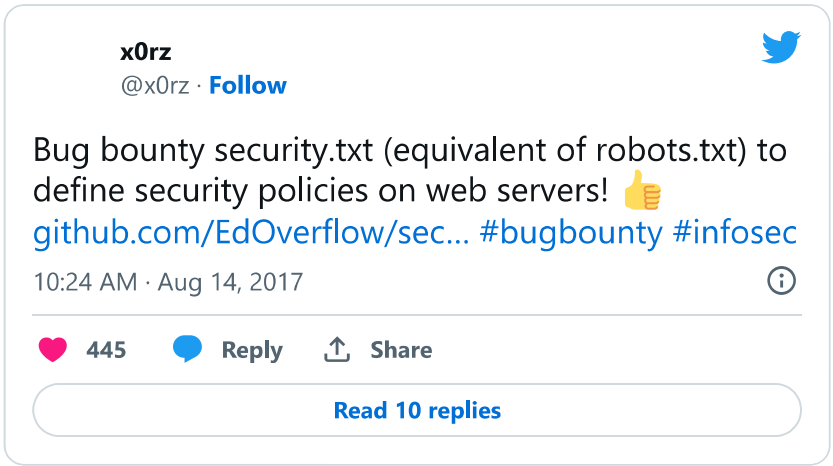
Speaking to *Bleeping Computer*, Foudil says he came up with the idea after attending the DEF CON security conference and the H1702 CTF event in the US at the start of August.

"During that time I was reflecting on the amazing contributions some of the people from the events in [Las] Vegas make to the security industry and our society as a whole," Foudil told *Bleeping*. "This motivated me to stop keeping my ideas to myself and start working on projects and sharing my ideas."

Projects like SECURITY.md (https://github.com/electron/electron/blob/master/SECURITY.md) and BUG-BOUNTY.md (https://github.com/square/wire/blob/master/BUG-BOUNTY.md) — files added to GitHub repositories to describe security policies — were also a major inspiration.

This is when Foudil put together a first version of the security.txt specification that he later published on GitHub. Early feedback from the IT security industry convinced the researcher to go on.

"When x0rz [well-known security researcher] tweeted about my proposal I realized that this was something people really wanted and that it was time to start writing up an RFC draft," Foudil said.



The researcher had lots of help from people in the infosec industry. Foudil says feedback from HackerOne, Bugcrowd, Google, and others helped him shape his IETF proposal.

Start small now. Improve and get better later.

The current IETF draft of security.txt only includes support for four directives (Contact, Encryption, Disclosure, and Acknowledgement). The security.txt GitHub repo (https://github.com/EdOverflow/security-txt) lists many more directives, such as In-scope, Out-of-scope-vuln, Rate-limit, Platform, Reward, Payment-method, Currency, Donate, and Disallow.

Foudil explained to *Bleeping Computer* why he axed most of the directives, which in hindsight, were quite helpful and would have given security.txt more depth.

"A major tech company told me that I am better off starting slow and seeing how companies start using security.txt, then with the help of those companies' feedback, security.txt can be adapted with new directives," Foudil said.

"Casey Ellis (https://twitter.com/caseyjohnellis) used the expression 'axe first, then sandpaper', implying that now that I have all these ideas, I should start chiseling away at them one by one ending up with a well-thought through draft," the researcher added.

"Now that I have published the Internet draft I get emails on a regular basis with valuable input that allows me to see where possible changes could be made in the future," Foudil said.

Bug bounty platforms have offered to help

Right now, security.txt is at the status of Internet Draft, which is the first IETF regulatory step in a three-stage process that also includes RFC (Request For Comment) (https://en.wikipedia.org/wiki/Request_for_Comments) and official Internet Standards (https://en.wikipedia.org/wiki/Internet_Standard).

"Once security.txt becomes an RFC the focus will shift to spreading the word and encouraging companies to setup a security.txt file," Foudil told *Bleeping Computer*.

"Several bug bounty platforms have already offered to help out with this step and hopefully if some of the big companies have a security.txt this will set a good example that could convince others to follow suit."

UPDATE [October 4, 2017, 19:35 ET]: Security.txt now has a dedicated website (https://securitytxt.io/).

INFOSEC (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/INFOSEC/)

(https://www.bleepingcomputer.com/author/catalin-cimpanu/)

CATALIN CIMPANU (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/CATALIN-CIMPANU/)

(HTTPS://TWITTER.COM/CAMPUSCODI)

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

PREVIOUS ARTICLE NEXT ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/NEW-LLS-INFOSTEALER-TROJAN-THAT-IT-LOADS-VIA-CHROME-DLL-HIJACKING/) (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/OUR-HACKS-VEVO-AFTER-EMPLOYEE-WAS-DISRESPECTFUL-TO-HACKERS-ON-LINKEDIN/)

Comments

Sloth
(https://www.bleepingcomputer.com/forums/u/1045018/sloth/)
- 5 years ago

Ill bet those contact details will make a very nice spam target. I don't envy the poor sap that has to search through thousands of spams every day in case a security issue has been reported....

Demonslay335
(https://www.bleepingcomputer.com/forums/u/726225/demonslay335/)
- 5 years ago

Agreed, that was my first thought. If it wasn't for it being just a text file, maybe someone could think of a clever way of hiding it behind a CAPTCHA or something.

Occasional
(https://www.bleepingcomputer.com/forums/u/1059255/occasional/)
- 5 years ago

GT500
(https://www.bleepingcomputer.com/forums/u/377072/gt500/)
- 5 years ago

Blast away at every opportunity spam will always be (https://www.bleepingcomputer.com/forums/u/377072/gt500/) to "target" the security feedback contact information? Are security teams likely to fall for work-at-home schemes, or buy diet pills? Wouldn't they be more likely to have the skills to trace the spam, or just filter it?

Besides, isn't most of that contact information already on responsible websites (those that would comply with security.txt)? it's just not organized in a reference file.

As for the usefulness, some websites don't include publicly viewable contact information (mine for instance), however they would respond to vulnerability reports if they received them. WHOIS doesn't always have this information either, as many websites pay extra for domain protection services that essentially submit the registrar's contact information instead of the customer's for the WHOIS records.

I get spam on my domain and website regardless of how obvious it might be that I wouldn't fall for it. Spam bots don't care. They just flood mail servers. Every now and then you get one that for all appearances looks legit, and you have to actually do some research to make sure that it really is spam.

SpoonOfDoom
(https://www.bleepingcomputer.com/forums/u/1067602/spoonofdoom/)
- 5 years ago

Tell me about it. In Germany, you're required by law to include contact information on your site if it's anywhere remotely commercial. And even if it isn't, it's often the safer option to do if you think that a lawyer might be able to construe it in some way as being commercial. There's shady lawyer companies who basically survive on hunting down such minor errors and send expensive letters to the responsible people.
The result is a mountain of spam and the nice knowledge in the back of your mind that your full name, postal address and possibly phone number are publicly available for spammers, stalkers or internet hate mobs, should you ever become a target of one of those.

Occasional (https://www.bleepingcomputer.com/forums/u/1059255/occasional/)
- 5 years ago

Anything beyond contact information could be problematic (and even that, if it changes).

Once you declare a policy (encryption, disclosure...), what happens if you fail to stick to it (either a deliberate change, or inadvertently, if underlying software is changed by an update, etc.)? Where's the mechanism to sync what's in security.txt with actual data and policy?

If security.txt is intended to be read by human eyes, are you expecting the user to read it (incase it's been updated), each time they visit the site?

Wouldn't it be better to have the browser check the file, and notify the user if/when there has been a change, when it was last verified... - as well as if the site complies with the standard, and a menu item/button to view the file?

Aventura5 (https://www.bleepingcomputer.com/forums/u/1068168/aventura5/)
- 5 years ago

I think this is not meant for people visiting the site, but for researchers who have found security flaws in the site and need to contact someone at the company about it. I'm not in security but I've read many stories about how it's near impossible to contact a tech person rather than a PR person at some companies and that's what this tries to solve. Of course, no one is forced to include a security.txt.

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

You may also like:

POPULAR STORIES

Slack's private GitHub code repositories stolen over holidays

(https://www.bleepingcomputer.com/news/security/slacks-private-github-code-repositories-stolen-over-holidays/)

Amazon S3 will now encrypt all new data with AES-256 by default

(https://www.bleepingcomputer.com/news/security/amazon-s3-will-now-encrypt-all-new-data-with-aes-256-by-default/)

LATEST DOWNLOADS

Malwarebytes Anti-Malware (https://www.bleepingcomputer.com/download/malwarebytes-anti-malware/)
Version: 4.5.19
4M+
DOWNLOADS

Windows Repair (All In One) (https://www.bleepingcomputer.com/download/windows-repair-all-in-one/)
Version: 4.13.1
2M+
DOWNLOADS

Everything Desktop Search (https://www.bleepingcomputer.com/download/everything-desktop-search/)
Version: 1.4.1.1017
21,940
DOWNLOADS

Zemana AntiLogger Free (https://www.bleepingcomputer.com/download/zemana-antilogger-free/)
Version: 1.8.2.320
52,345
DOWNLOADS

Zemana AntiMalware (https://www.bleepingcomputer.com/download/zemana-antimalware/)
Version: NA
304,341
DOWNLOADS

FOLLOW US:

(https://www.bleepingcomputer)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)
Downloads (https://www.bleepingcomputer.com/download/)
Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)
Tutorials (https://www.bleepingcomputer.com/tutorials/)
Startup Database (https://www.bleepingcomputer.com/startups/)
Uninstall Database (https://www.bleepingcomputer.com/uninstall/)
Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)
Forum Rules (https://www.bleepingcomputer.com/forum-rules/)
Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)
Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)
Contact Us (https://www.bleepingcomputer.com/contact/)
Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)
Advertising (https://www.bleepingcomputer.com/advertise/)
Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)
Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)
Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/)