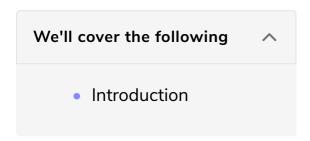# Security.txt

In this lesson, we'll learn about security.txt.

Introduction

The `security.txt` is a proposed standard to advertise the security policies of a website. In other words, it allows us to publish a file that informs researchers about the existence and terms of your BBP.

A valid example of `security.txt` file could look like this:

```
Contact: mailto:security@example.com
Preferred-Languages: en
Canonical: https://example.com/security.txt
Policy: https://example.com/bug-bounty-program.html
Hiring: https://example.com/careers.html
Acknowledgments: https://example.com/hall-of-fame.html
```

It's a simple, plaintext file listing information for security researchers:

- The contact section will state how a researcher should get in touch with the organization.
- The preferred languages section will state what language to use.
- The policy section will lead to the full-blown version of the BBP, where the researcher can better understand what the rules of engagement are.

Additional sections, such as a link to security-related job openings at your company and acknowledgements to ethical hackers who have helped the organization in the past, make for additional, complementary pieces of information that researchers might find useful.

You can read more about the standard at securitytxt.org; for an example file, visit

facebook.com/security.txt

Having a `security.txt` allows researchers to find more about your BBP with a standardized process, something that saves them precious time. Remember, ethical hackers are on the hunt for security programs with limited time on their hands and, for many of them, bounties are a significant source of income. Making sure they can easily understand how your program works is an effective incentive to attract them towards your web applications.

We'll learn about HackerOne in the next lesson.