Lab name: [Information disclosure in error messages](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages)

Severity: High

Lab description:

* Information disclosure is data leakage. This can happen in various ways, some of them are:
* Revealing hidden directories
* Revealing hidden data
* Revealing data about users like card information or any PII
* Revealing source code
* Revealing API keys
* Revealing sensitive data to unauthorized parties
* This lab expects us to gather information from the verbose error messages that have potential of revealing unwanted information about the applications.

Impact:

* The error message is revealing unwanted information like the version of web application framework.
* The error message also reveals the errors in the java file (Stack traces). All these leads to unwantedly revealing error messages.
* This can lead to gaining unauthorized access, exploiting known CVEs.

Recommendations:

* Use custom error handlers which outputs only generic errors.
* Regular code reviews would help in avoiding information leakage.
* The application should never expose raw stack traces which can probably expose file structures, used libraries.
* Log all the errors so that only the developers can see the complete details of the error message.

Steps to reproduce:

This lab can be solved with or without burp.

Using burp,

1. In the lab, access any product on the website. Capture the requests in Burp suite.
2. In the Proxy tab -> HTTP history tab, notice that there is GET method with URL ‘*/product?productId=1’*
3. Send this request to the repeater tab.
4. Modify the */product?productId=1* to */product?productId=xyz* and send the request.
5. Now we can see all the response with stack error messages and the version of Apache struts.

Without using burp,

1. We can just change the URL in the browser. That is, changing

*Websecurity-academy.net/product?productId=1* to *Websecurity-academy.net/product? productId=abc*

1. This also reveals the same error in the webpage.
2. 