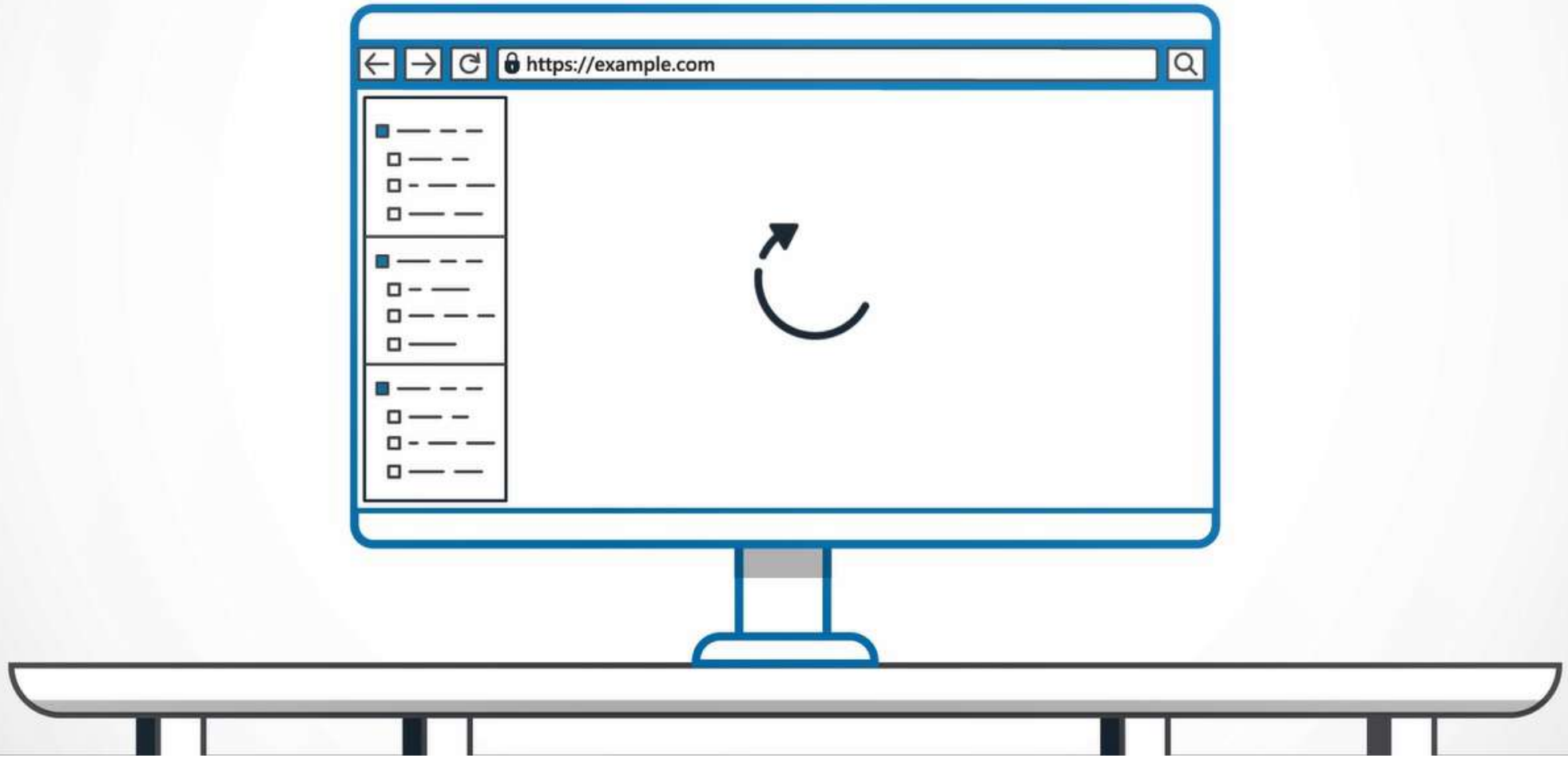
SECURE CODE WARRIOR

ERROR DETAILS

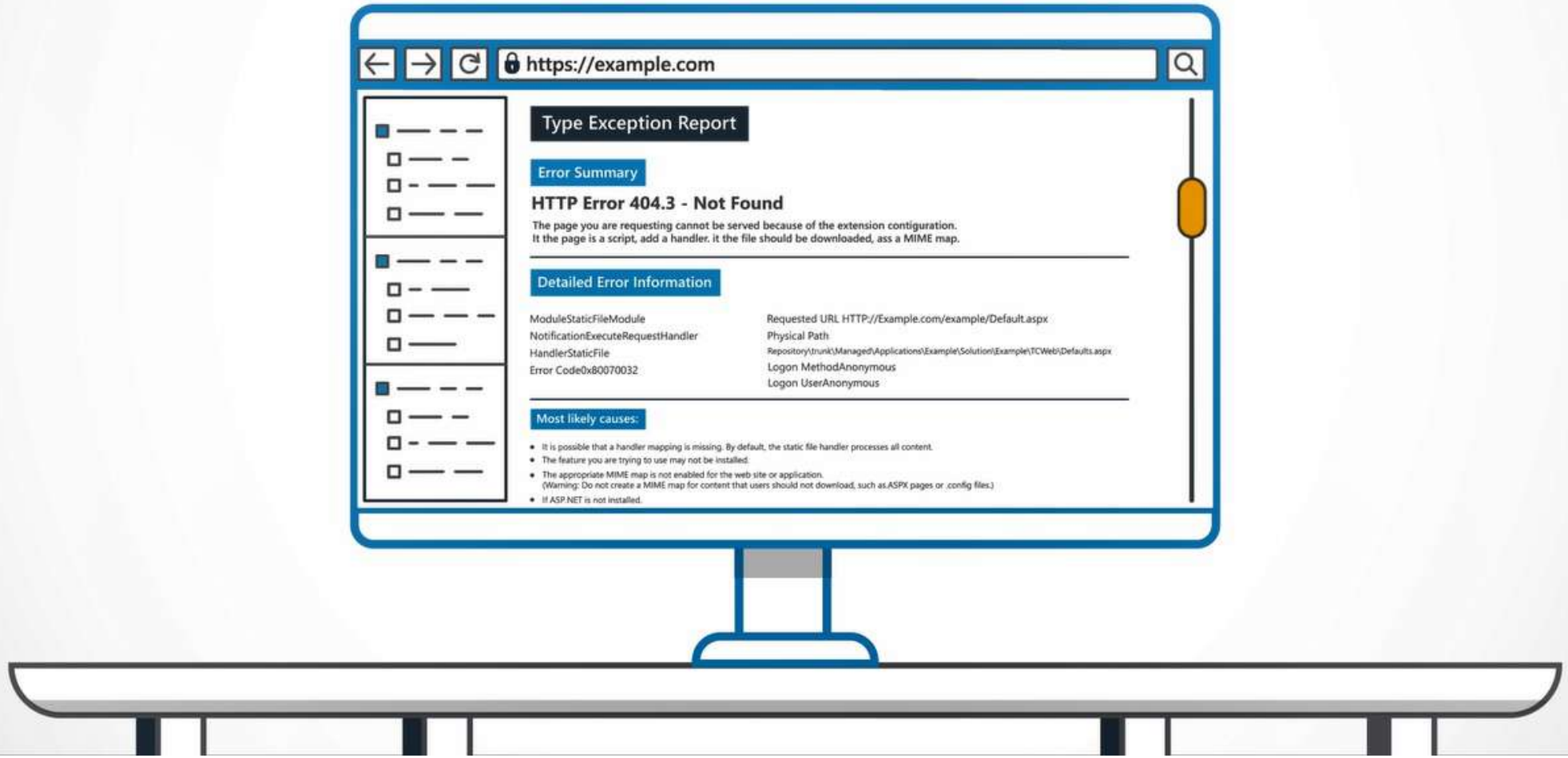
We'll also go through

some causes and preventions of vulnerabilities in this category

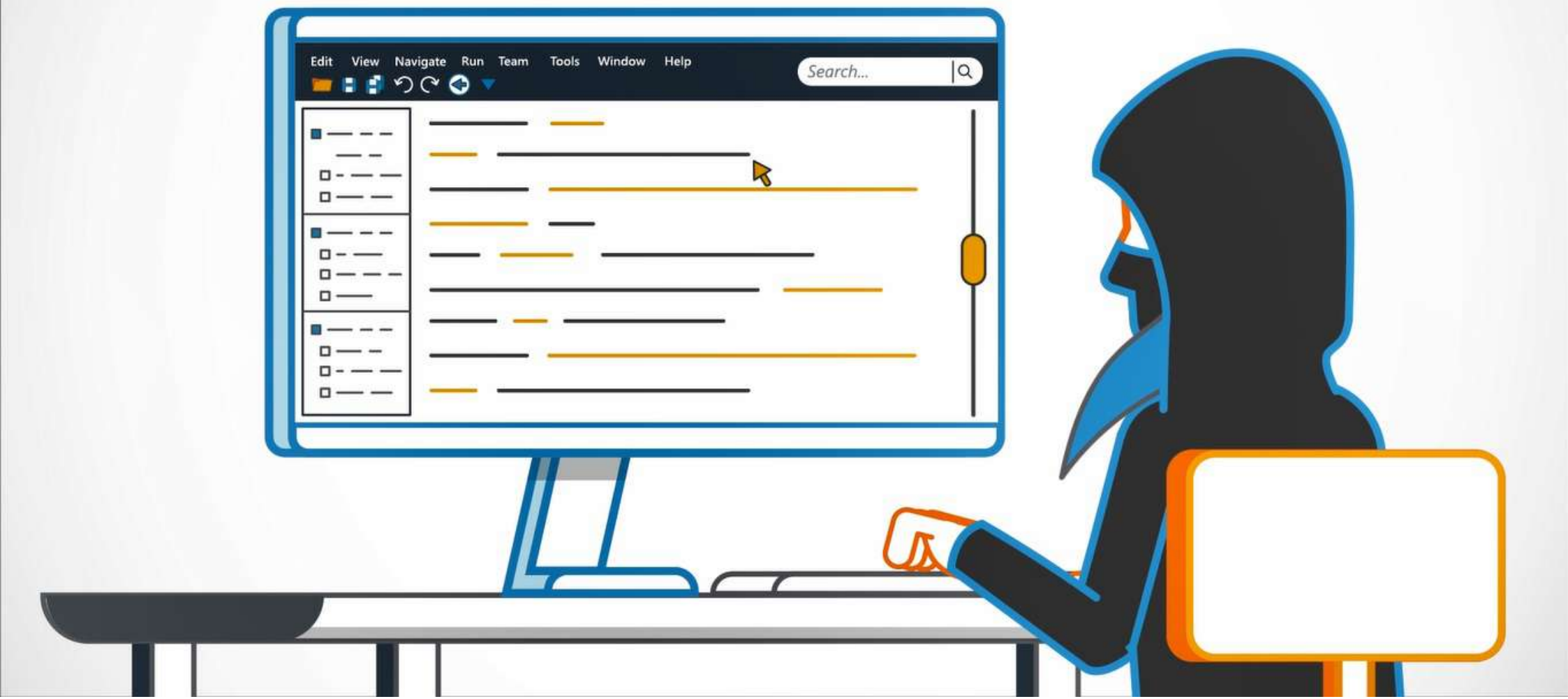
Error Details is a vulnerability that happens when users receive an error in the application,



and too many details are displayed about why that error has occurred.

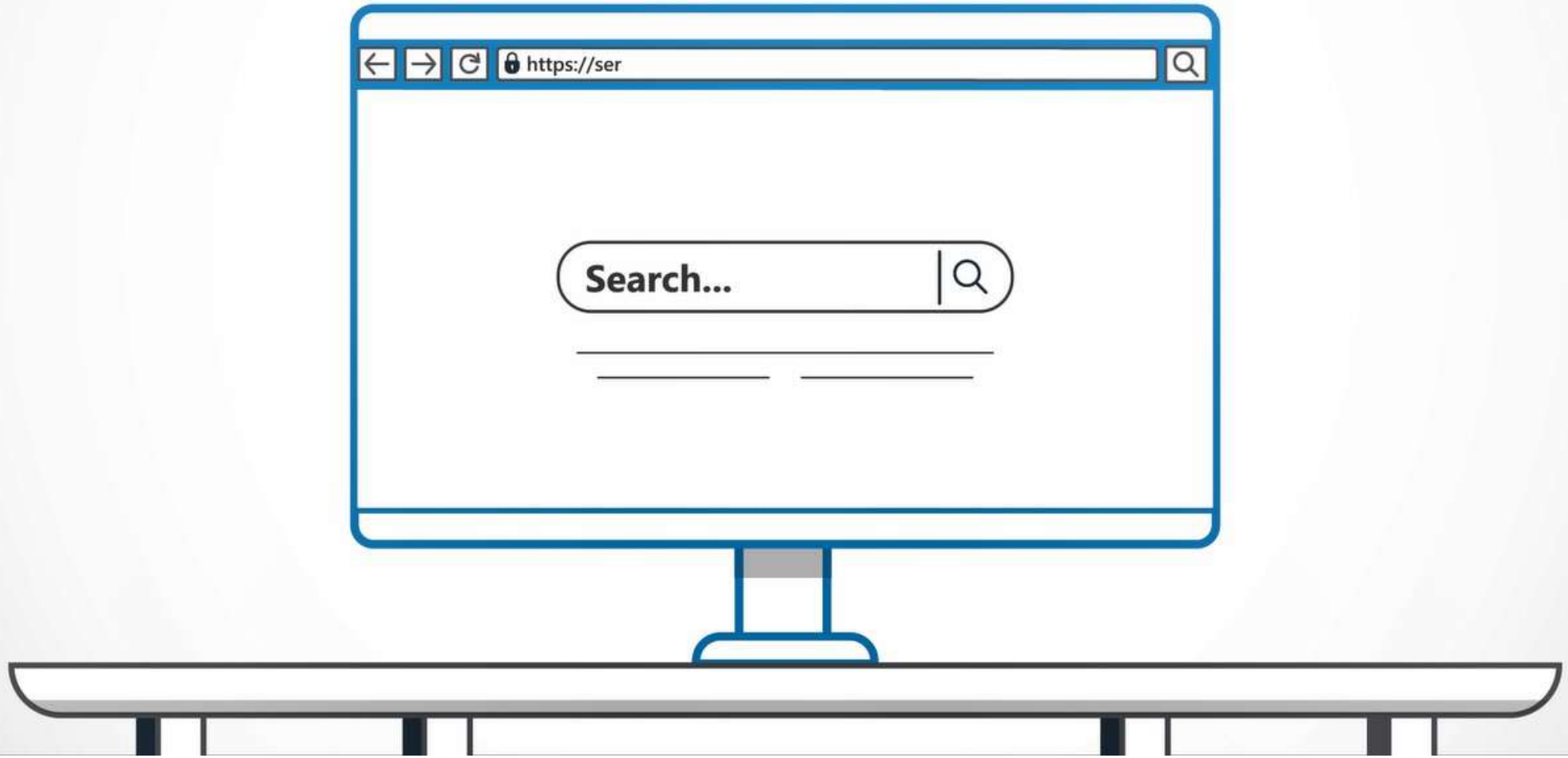


This vulnerability can expose sensitive information or give attackers enough information to exploit a different vulnerability.

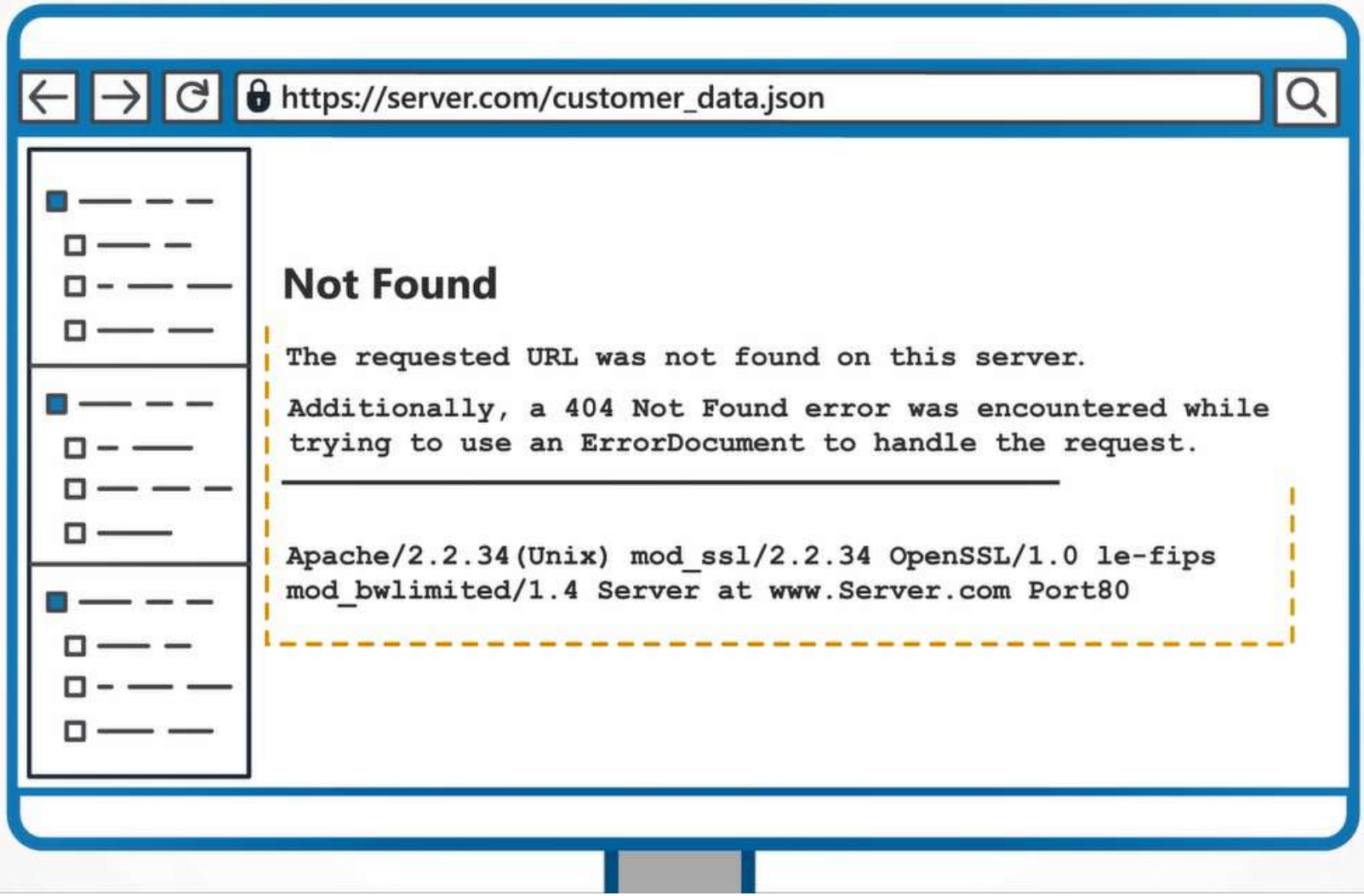


LET'S LOOK AT AN EXAMPLE

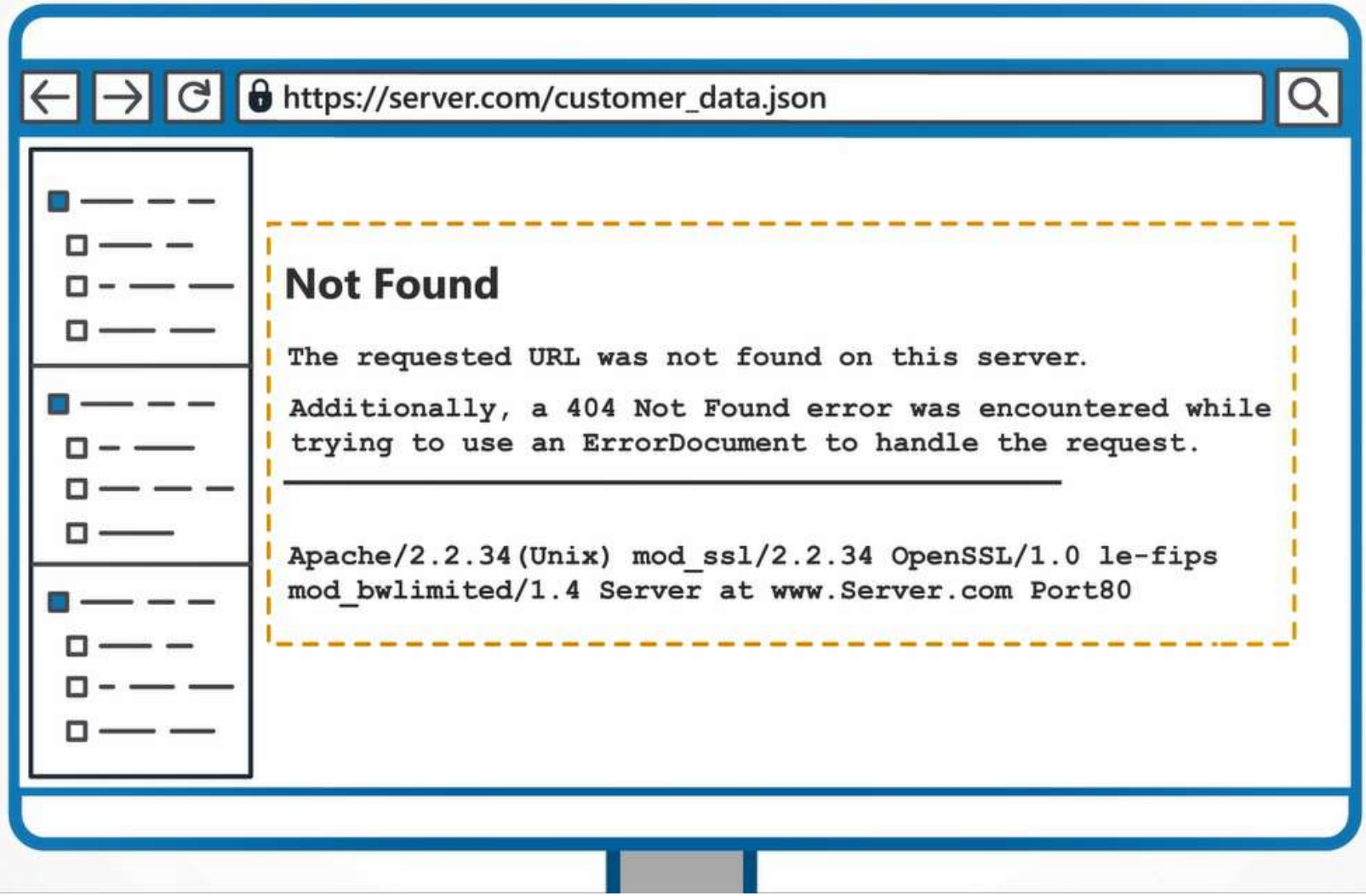
After requesting a URL that doesn't exist,



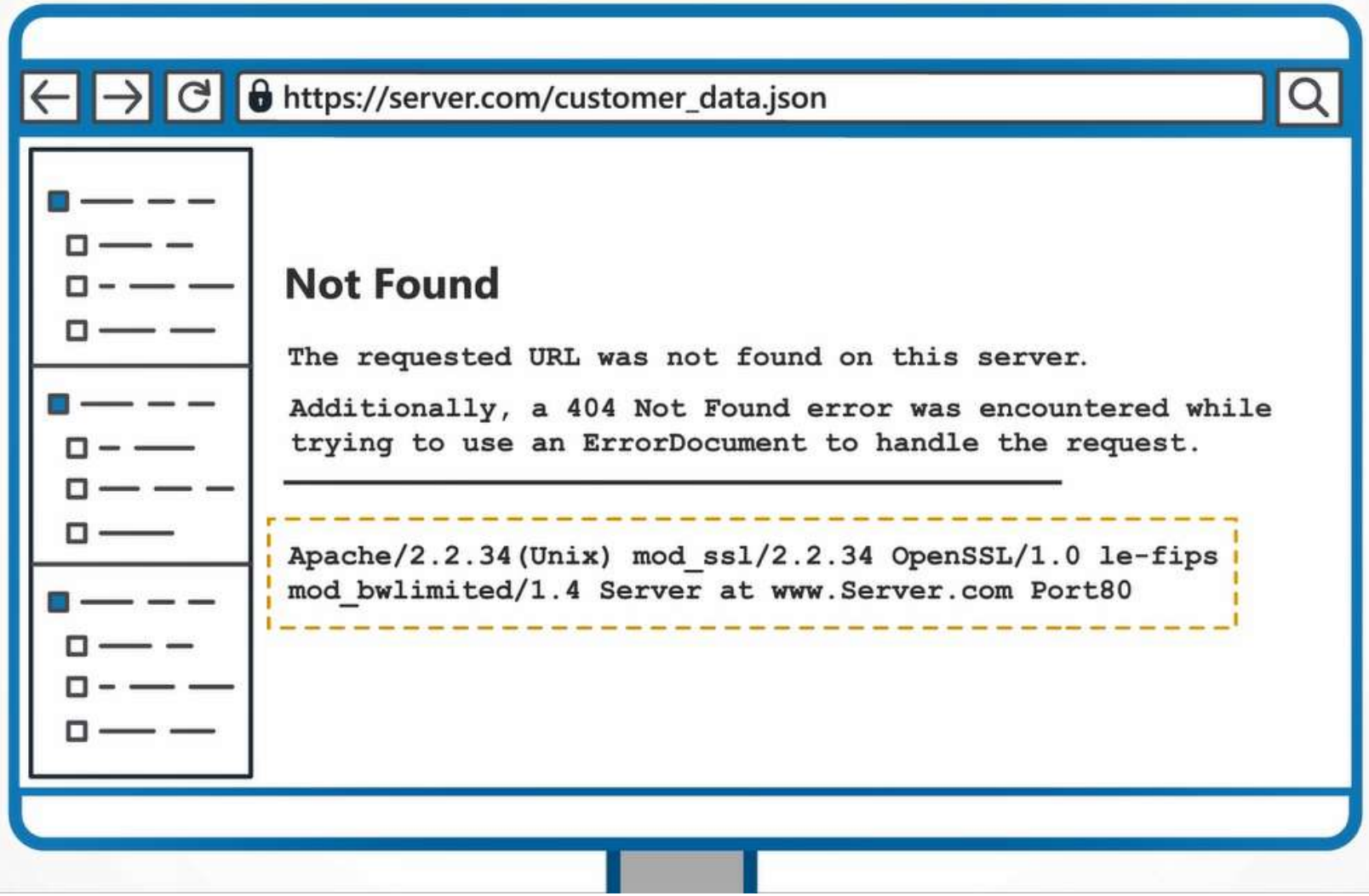
the following error is displayed, informing a user that the file cannot be found.



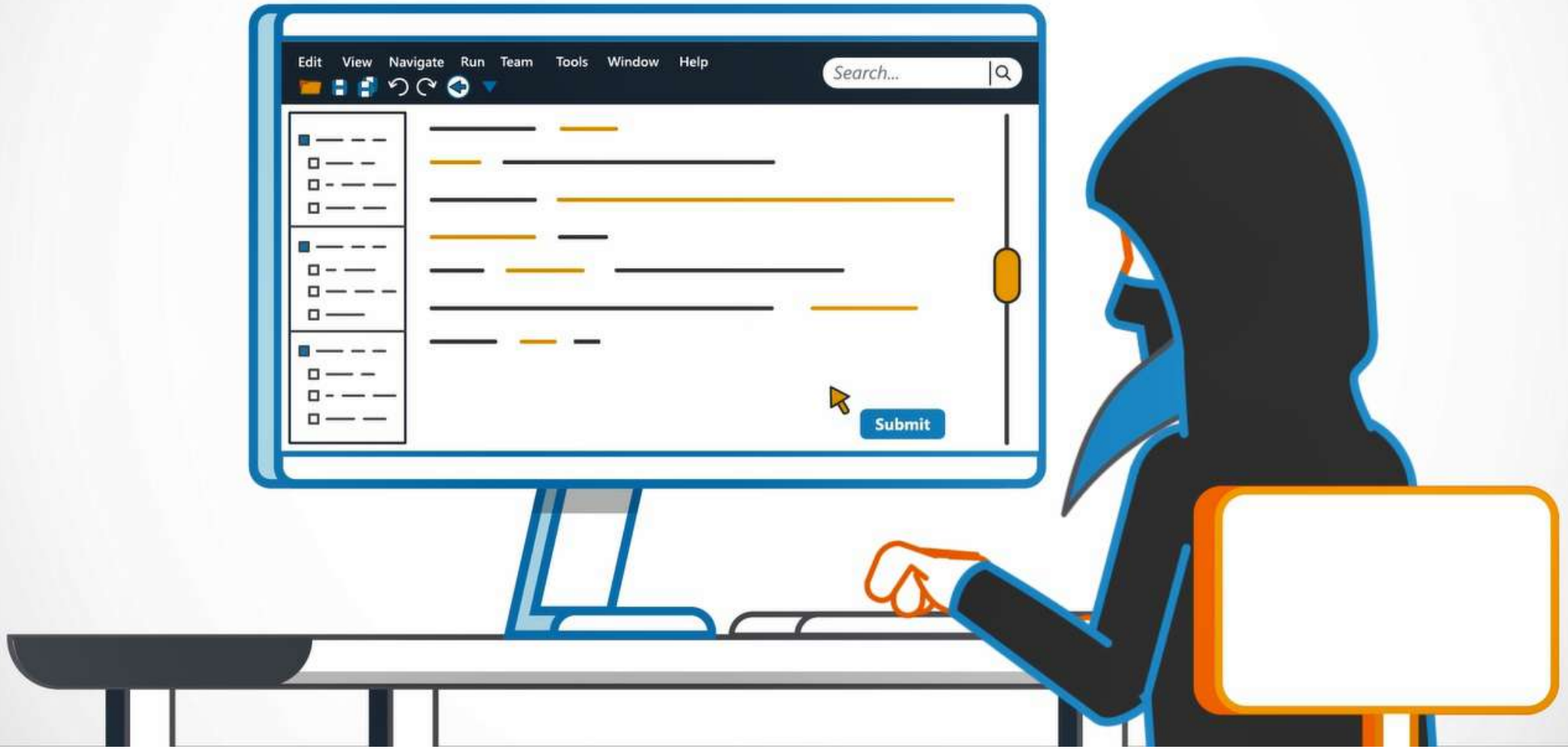
However, this error message also contains some more sensitive data,



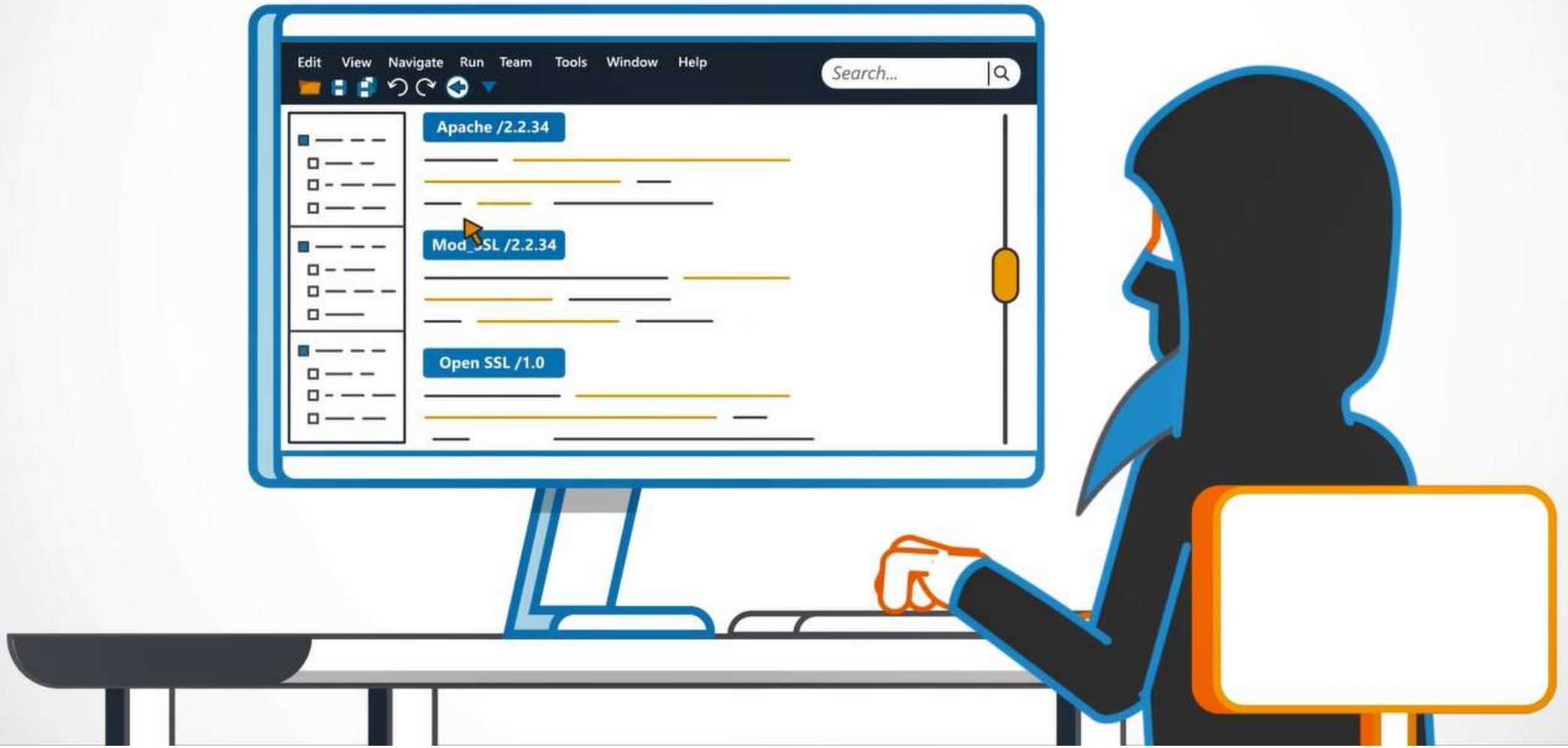
such as the web server version and operating system, as well as the code version in use.



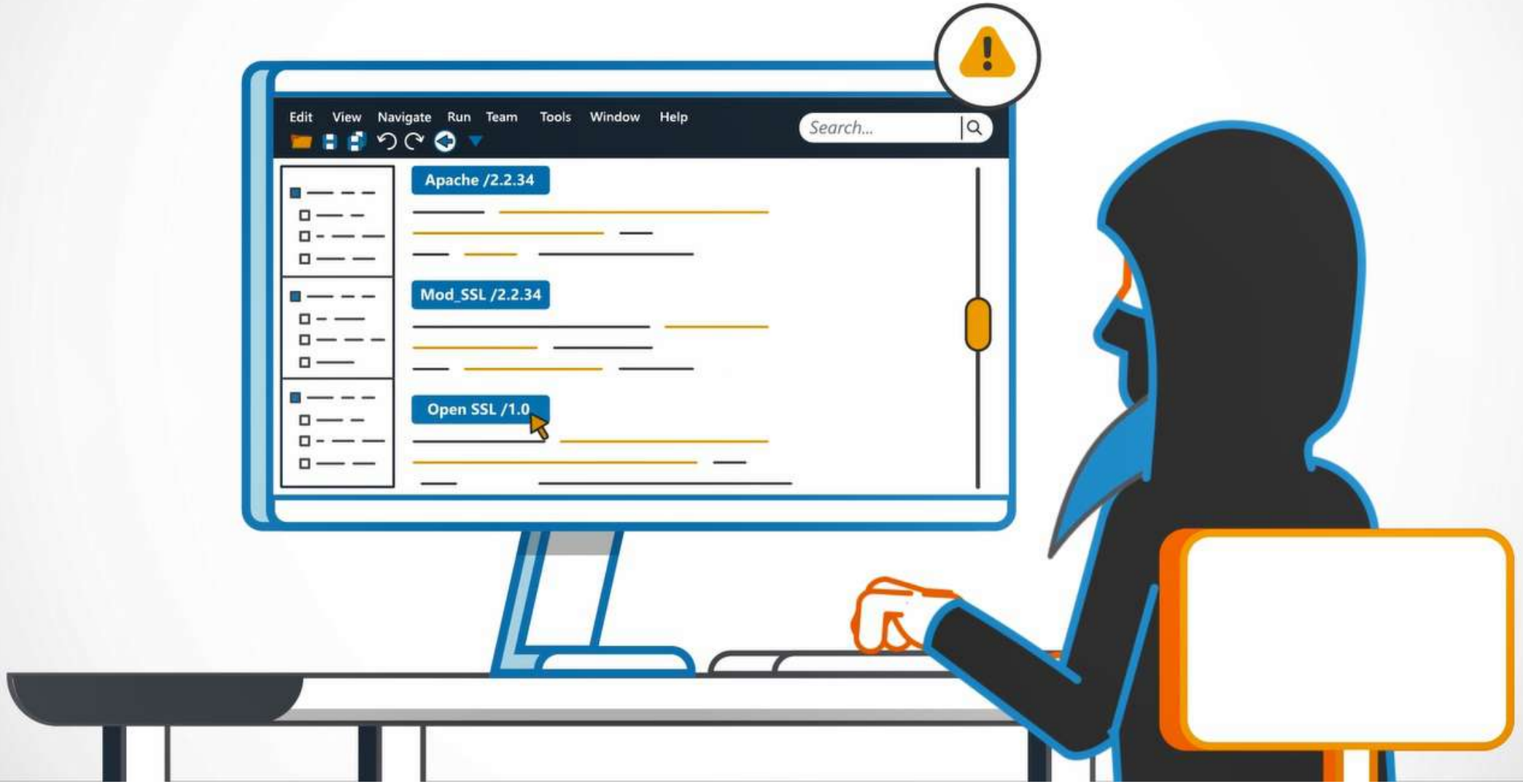
Knowing this, an attacker purposely creates the error. Now, she knows the software versions in use by the web app.



With this information, the attacker is able to look up known vulnerabilities in these software versions,



and gain enough insight to plan and execute an attack.



To prevent Error Details vulnerabilities, developers should:

- Exclude system specific information from errors when they are sent to the user
- Avoid relying on default error message generation settings
- Analyze error handling to ensure that errors do not reveal inessential app or system details

To prevent Error Details vulnerabilities, developers should:

- Ensure robust testing is in place, to check for unexpected errors and exceptions
- Log errors for regular analysis and look for possible hacking attempts

Congratulations, you have now completed this module!

www.securecodewarrior.com