VULNERABILITY DECODER

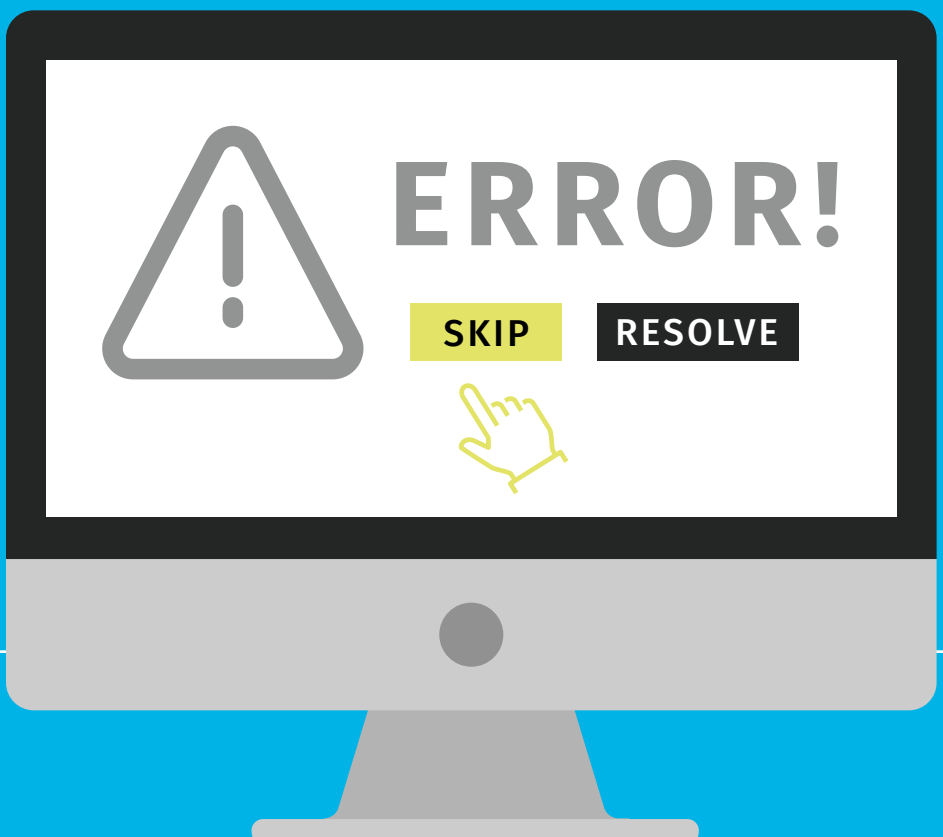
Improper Error Handling

The Vulnerability

Error messages are a normal part of operations, but improperly handling error messages introduces significant security risks.

The Risks

Attackers can use improperly handled error messages to exploit flaws, break into systems, and access sensitive data and information, including passwords.



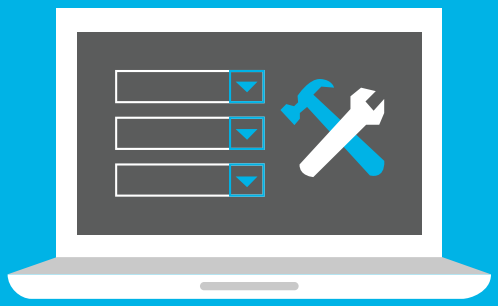
5.5%

of applications have an error handling vulnerability on initial scan.

Source: SOSS v11

Prevention & Remediation

It's important to provide error messages that deliver useful information without revealing unnecessary system or application details. This requires security teams to test sites and other resources for various types of errors and understand how they respond.



Here's an OWASP example of an HTTP 404 Not Found error that reveals sensitive information:

```
Not Found
The requested URL /page.html was not found on this server.
Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g  DAV/2 PHP/5.1.2 Server at localhost Port 80
```

The above message is generated when the user requests a non-existent URL. In addition to informing the user that an error has occurred and the file can't be found, the code delivers valuable information about the web server version, OS, modules, and code used. An attacker can use this information to design an attack.

Recommendations

Nobody writes perfect code the first time around.
You can avoid vulnerabilities and prevent breaches when you:

- ☑ Get training in secure coding best practices through on-demand eLearning courses, in-person security consultations, and professional development certifications and conferences.
- ☑ Scan early and often to detect flaws while you code. Use application security tools that allow you to scan small batches of code instantaneously, and provide remediation guidance within your development workflow.

Download the Secure Coding Best Practices Handbook

Join the Veracode Community
community.veracode.com

VERACODE