Security Strategies in Web Applications and Social Networking

Lesson 11

Testing and Quality Assurance for Production Web Sites

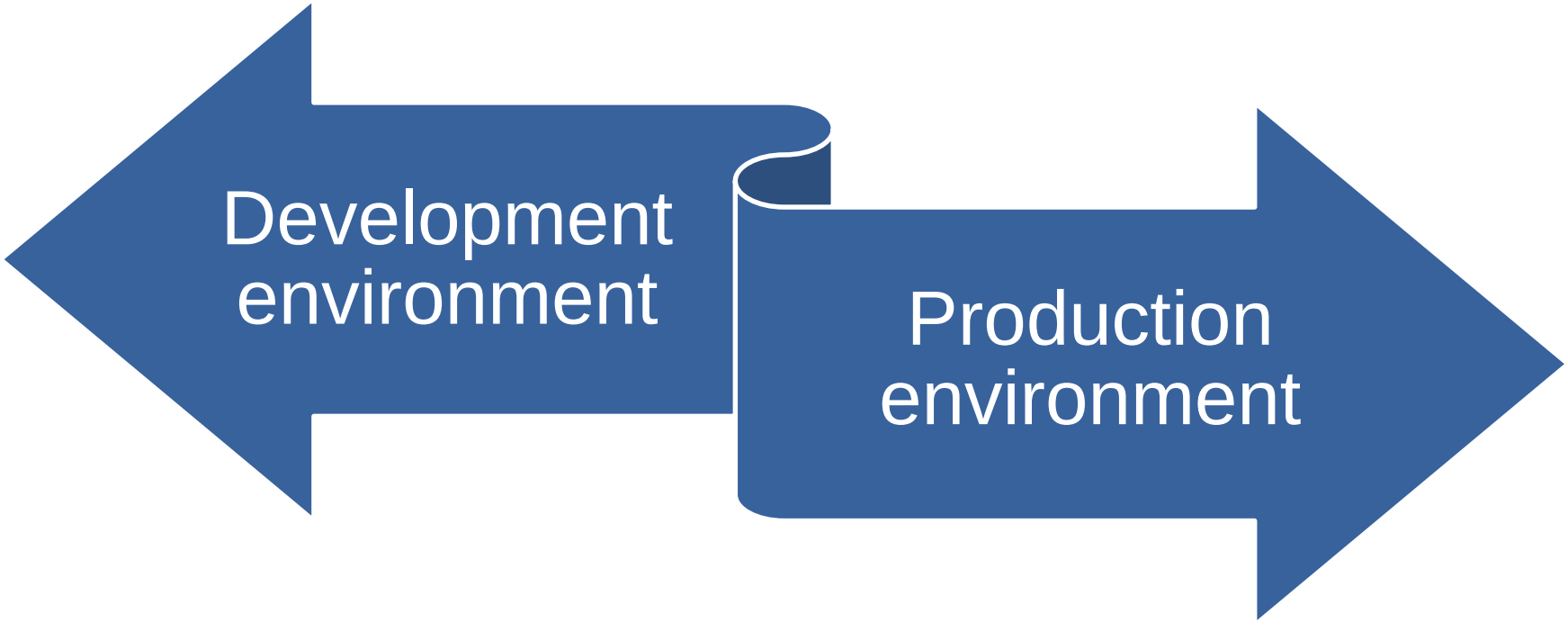
Learning Objective

- Analyze the role and importance of quality assurance (QA) testing for Web applications.

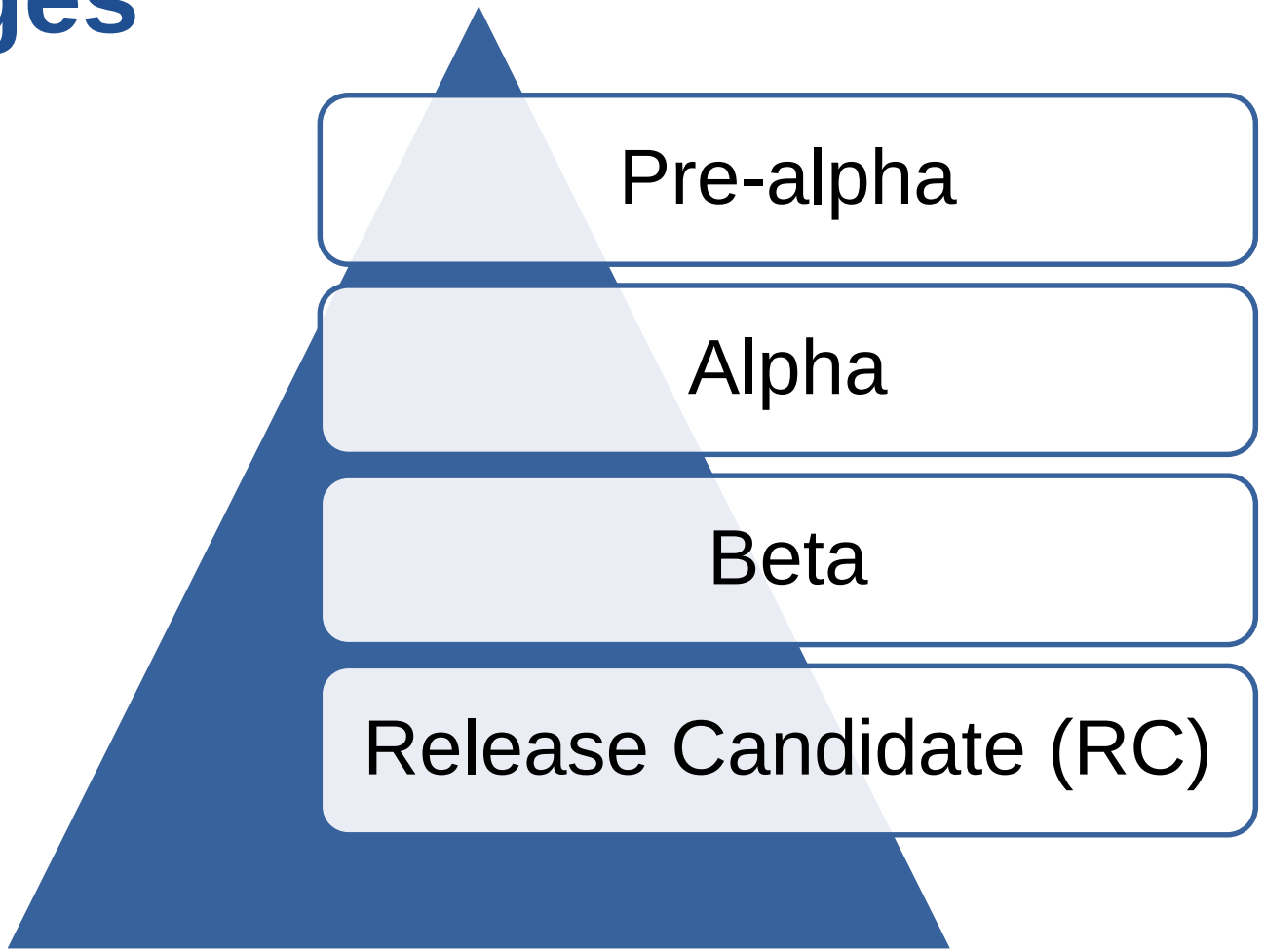
Key Concepts

- Configuration and change management
- Quality assurance testing and gap analysis
- Metrics and measurement programs
- Monitoring production applications
- Strategies and best practices

Development vs. Production Environments



Software Development Life Cycle Stages



Formalizing Software and System Changes

- Change management
  - Provides all stakeholders in the application the knowledge of *what* will be changed and *when* it will be changed
- A formal deployment plan is a best practice for separation of duties from developers, QA analysts, and system administrators.

Formalizing Software and System Changes (Continued)

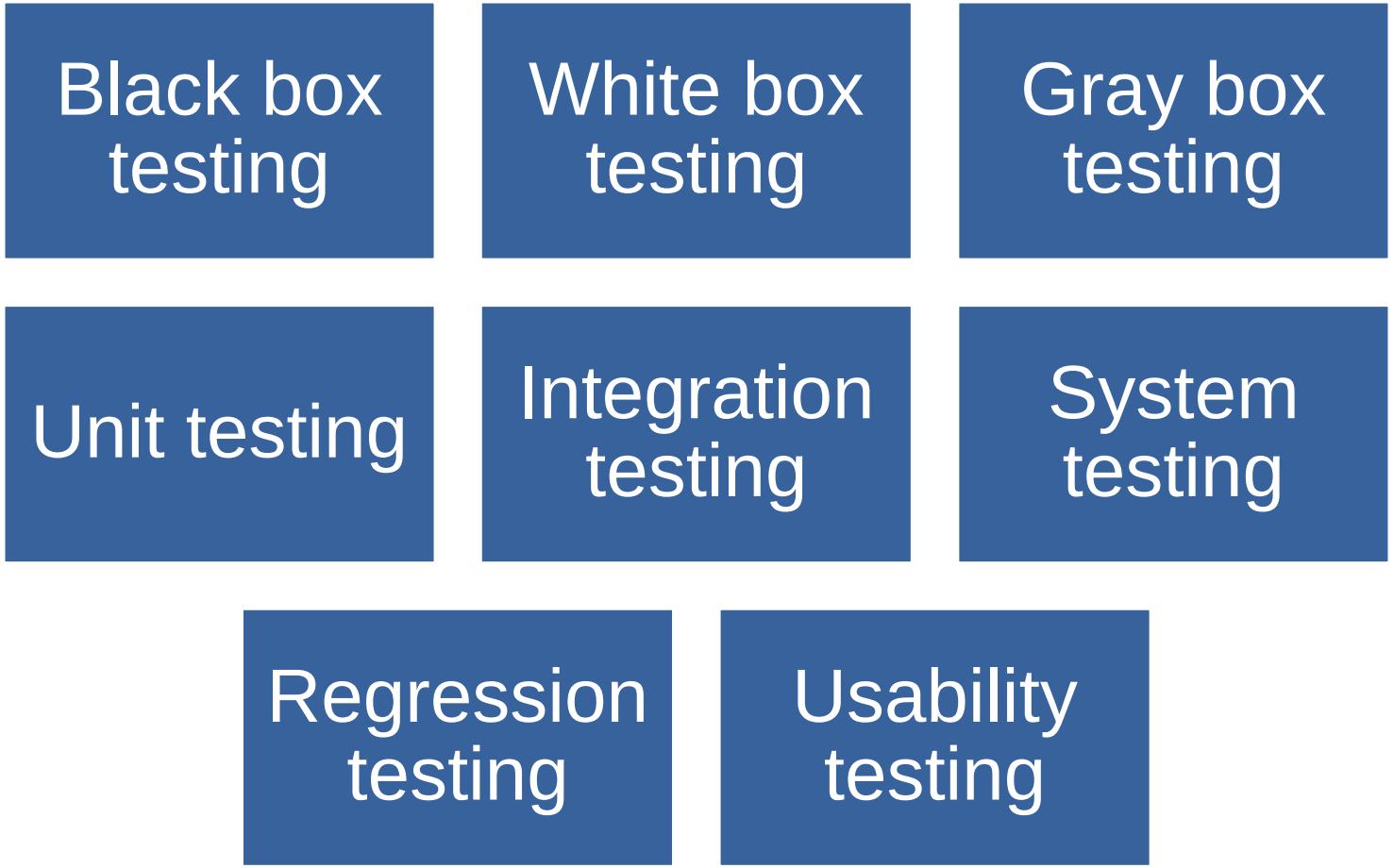
- Configuration management
  - Provides system administrators and developers with documented history of changes in case a rollback to a previous version or full restore of an application is necessary

Network Documentation

Web Site Deployment Checklist

- Verify links
- Test browser compatibility
- Test all downloads
- Verify digital certificates and Secure Sockets Layer (SSL) URLs work correctly
- Test forms and form controls
- Verify path traversal
- Review navigational structure
- Verify shopping features
- Web page load times

Software Testing Techniques



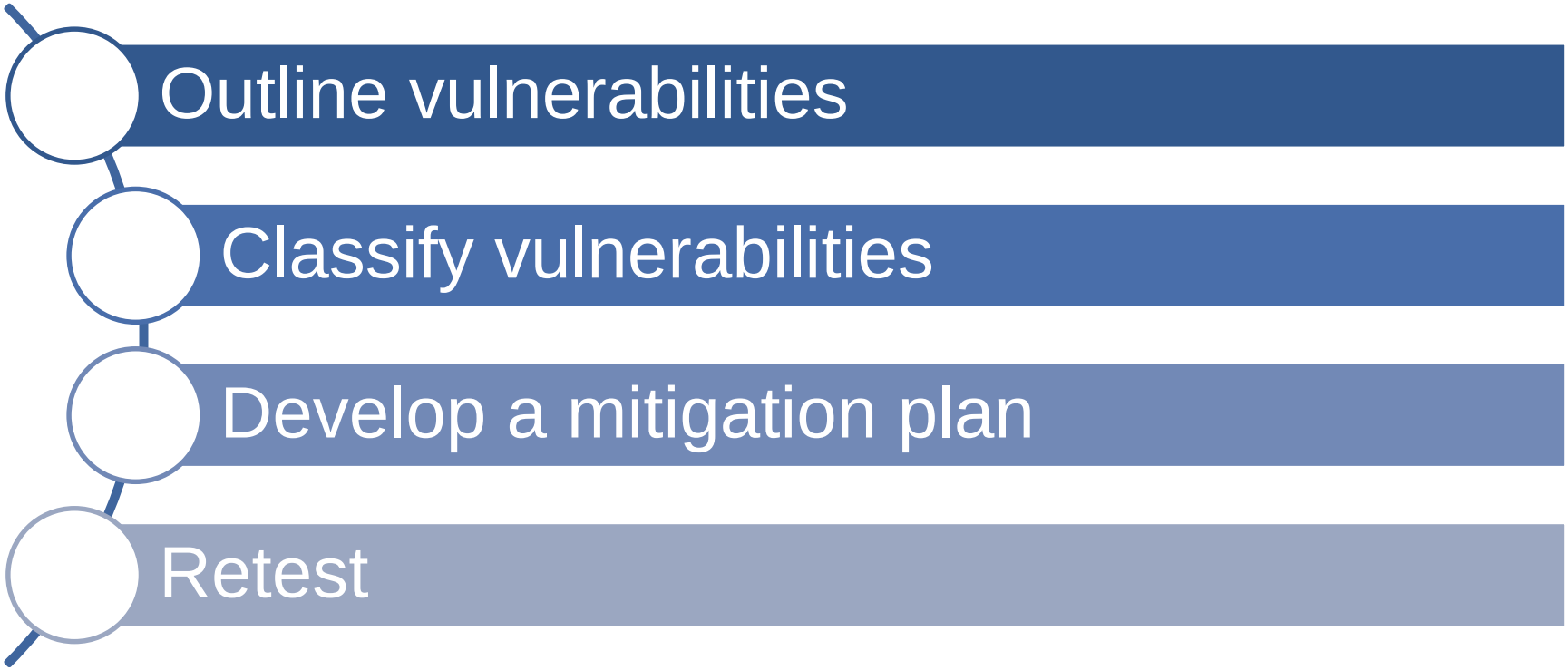
Software Testing Techniques

Performance testing	Software stress testing	Recovery testing
Security testing	Compatibility testing	Regulatory compliance testing

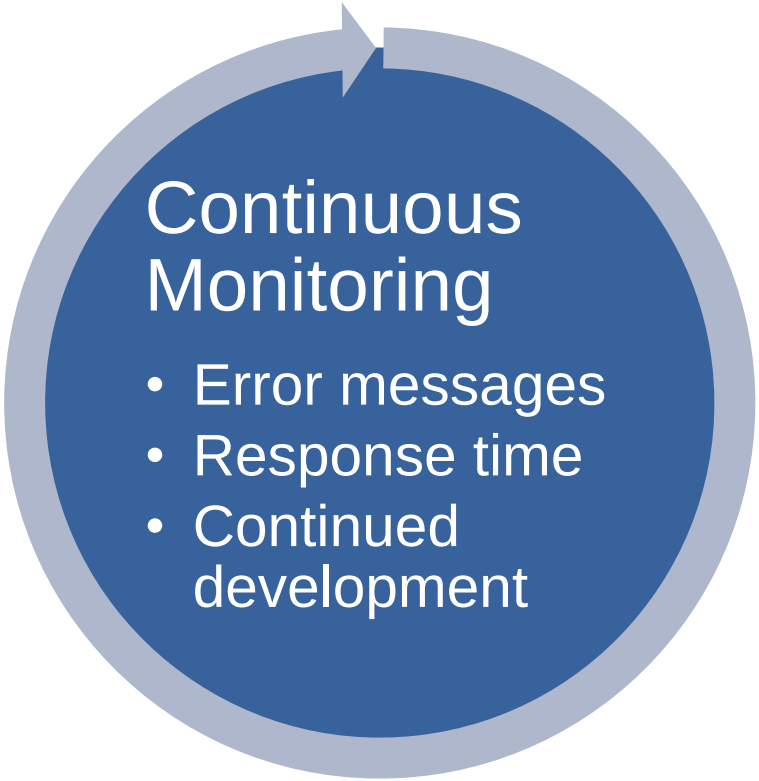
Key Areas of Security Vulnerability Testing

- Application design
- Default security measures
- Mass deployment security
- Information and response abilities

Mitigating Security Holes



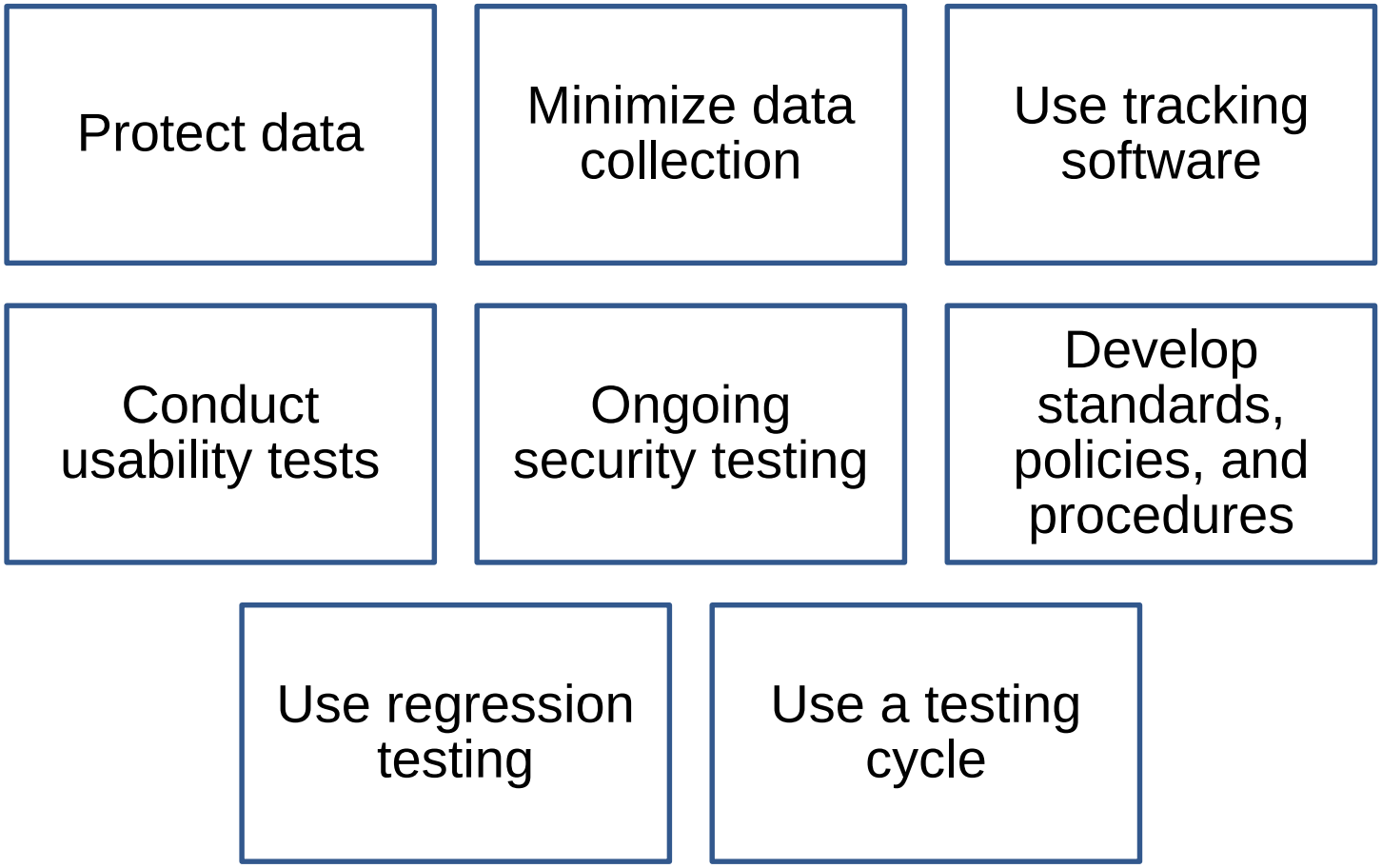
Production Deployment



Analyzing Web Page Statistics

Analytics	Browser statistics
	Bounce rate
	Network performance
	Visitor paths
	Shopping cart abandonment
	Visitor location

Best Practices



Summary

- Configuration and change management
- QA test plans
- Metrics and measurement programs
- Monitoring production applications
- Formalizing software and system changes

Virtual Lab

- Performing Dynamic and Static Quality Control Testing

If your educational institution included the Jones & Bartlett labs as part of the course curriculum, use this script to introduce the lab:

“In this lesson, you learned about quality assurance testing for Web applications. You explored configuration and change management, gap analysis, metrics and measurement programs, monitoring production applications, and strategies and best practices.

In the lab for this lesson, you will use skipfish, a dynamic testing tool, to identify vulnerabilities in the Damn Vulnerable Web Application (DVWA). The DVWA is a Web application that is made purposefully vulnerable. It is installed on a local Web server to allow security analysts a safe place to test the security of their applications. You also will use RATS (Rough Auditing Tool for Security) to perform static analysis testing on the DVWA. You will use the vi Editor to review the source code for a part of the DVWA to identify exactly where the software code is most vulnerable. Finally, you will compare the results of both skipfish and RATS reports.”