QUALYSEC
BEYOND CYBERSECURITY

Case Study

Web application penetration testing

E-Commerce

INDUSTRY

Challenges and Objectives

Challenges

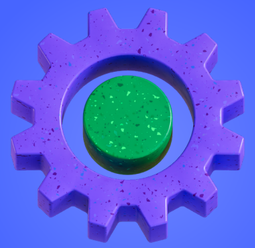
- Protect sensitive customer data, such as credit card numbers and personal identification information
- Comply with industry regulations and standards, such as PCI DSS, by addressing vulnerabilities
- Ensure the availability and reliability of the website for customers

Objectives

- Their development team said some bots are trying to hack their application, previously.
- Website assessment is required to identify vulnerabilities
- The development team seeks guidance on remedying vulnerabilities
- Ensure website security and integrity for customer trust

Project Overview

Target



Web Application

Technology

PHP, Mysql, Payment gateway

Team

2 Certified Pentester

Reason

Fulfil corporate client requirement to have a pentest

METHODOLOGIES USED FOR PENETRATION TESTING

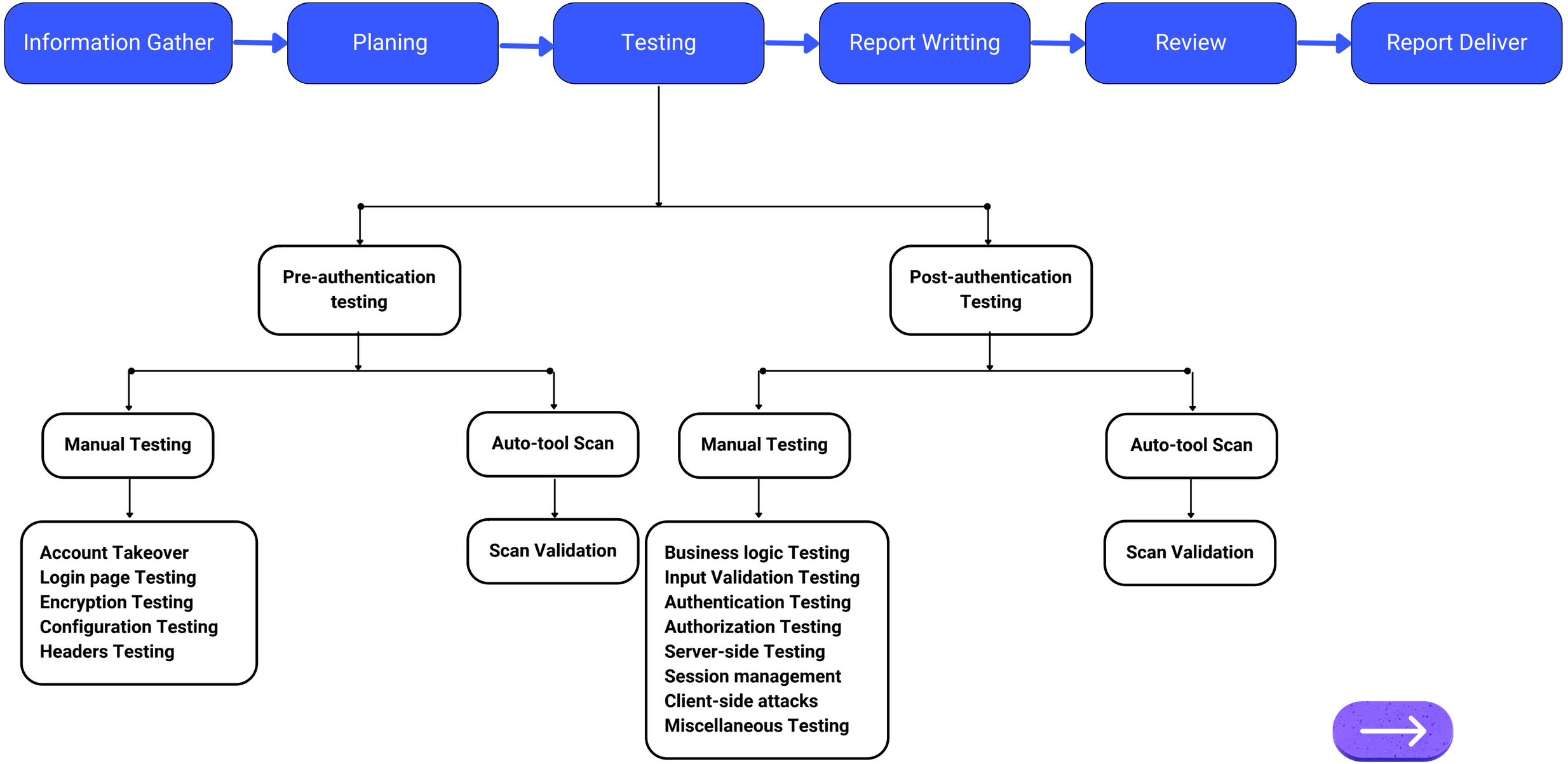
Penetration Testing Execution Standard

Open-source Security Testing Methodology Manual

OWSAP Testing Guide

SANS 25 security Threats

PENETRATION TESTING PROCESS



VULNERABILITIES FOUND

Minimal

- Missing X-XSS-Protection Header
- Missing Content-Security-Policy Header

Low

- Password Reset Username Enumeration
- Database Error Pattern Found
- Arbitrary Host Header acceptance
- TLSv1.0 Supported
- Insecure HTML5 Local Storage
- HTTP Strict Transport Security (HSTS) Not Implemented
- Verbose Server Version

Critical

- Web Shell Uploading
- Stored Cross-Site Scripting (S-XSS)
- Payment Manipulation

High

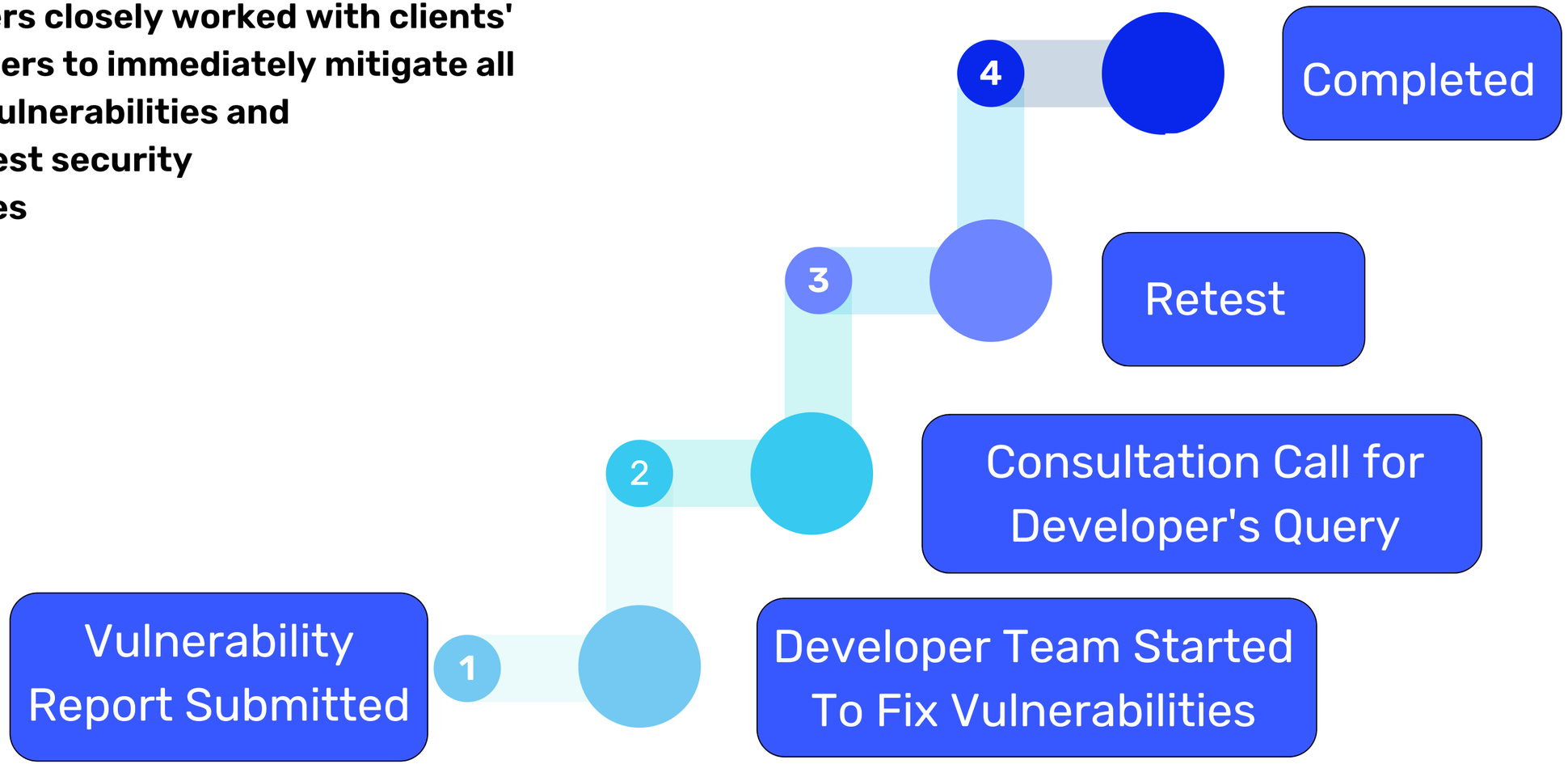
- Reflect Cross-Site Scripting (XSS)
- Html Injection
- Withdraw any amount from wallet without having any balance (Business Logic issue)

Medium

- Cross-Site Request Forgery (CSRF)
- Improper Restriction of Excessive Authentication Attempts
- Clickjacking
- Admin Login Page accessible to Unauthorized Users

RECOMMENDATION PHASE

At this phase, Qualysec security engineers closely worked with clients' developers to immediately mitigate all found vulnerabilities and apply best security practices



Roadmap

Tasks	Week1	Week2	Weak3	Week4	Week5	Week6
Application Profiling and Planning	Planning					
Autoscan Testing	Auto scan					
Manual Testing	Manual Testing					
Report Writing		Reporting				
Internal Review & Final report submit			Review			
Retest					Retest	
Letter of Attestation and Certificate						Complete

PROJECT RESULTS

Before

- Excellent
- Good
- Fair
- **Unsatisfactory**
- Inadequate

Qualysec has delivered a comprehensive report covering all found vulnerabilities and providing recommendations on the best ways of mitigation

At the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and get a Qualysec verified certificate assuring board of directors in good security posture.

After

- **Excellent**
- Good
- Fair
- Unsatisfactory
- Inadequate

Client Testimonial

"We were impressed by the thoroughness and professionalism of the Qualysec team during our penetration testing engagement. Their findings and recommendations have helped us identify and address potential vulnerabilities, ensuring the security of our ecommerce platform and our customers' data."

CTO

QUALYSEC
BEYOND CYBERSECURITY

Get In Touch

Let's make your application secure.

Email
contact@qualysec.com

Website
https://www.qualysec.com

Call us
+91 8658663664