Penetration Testing Plan for the Redesign and Development of 21st Century Technologies Ltd Website

Overview:

This penetration testing plan is designed to ensure the security of the redesigned website for 21st Century Technologies Ltd. The website will feature a pentagonal layout with various sections such as Data Center, Konet, Payment (KonetPay), Power, Academy, and an overview of core services. This plan will cover a comprehensive set of tests aimed at identifying vulnerabilities across the landing page and its associated pages.

This penetration test will focus on identifying common vulnerabilities, including Cross-Site Scripting (XSS), HTML Injection, SQL Injection, Open Redirects, and other critical security concerns that may affect the website's functionality, user experience, and data integrity.

Objective:

The objective of this penetration test is to:

- Identify security vulnerabilities within the website infrastructure.
- Ensure that critical data (user information, payment details, and documents) is protected.
- Provide actionable recommendations to improve security.
- Test how well the website withstands common cyber-attacks and malicious exploitation attempts.

Scope of the Penetration Test:

The objective of this penetration test is to:

- **Landing Page Security:**
  - Validate the security of the navigation elements (Pentagon sections).
  - Test for vulnerabilities like Cross-Site Scripting (XSS) and HTML injection.
- **Pentagon Sections:**
  - Each pentagon represents a service. We will test the security of each section, including Data Center, Konet, Payment (KonetPay), Power, and Academy.

- **Input Validation:**
  - Test all user input areas such as forms (e.g., contact forms, registration, payment).
  - Ensure that inputs are correctly validated and sanitized to prevent XSS and SQL injection attacks.
- **API Security:**
  - Test for any vulnerabilities in API calls and data processing.
- **Sensitive Data Exposure:**
  - Test for leaks of sensitive information such as payment details, personal user data, or server configurations.

Timeline and Milestones

Phase	***Activities***	***Duration***	***Milestone Date***
Planning	Define scope, gather technical details, and schedule testing activities.	1 day	1 day
Reconnaissance	Conduct passive and active reconnaissance to gather intelligence on the website.	4 days	5 days
Vulnerability Assessment	Perform vulnerability scans and manual testing for input validation and API security.	1 week	12 days
Exploitation	Attempt to exploit the identified vulnerabilities.	1 week	19 days
Reporting	Compile findings, provide detailed recommendations, and deliver the final report.	2 days	21 days
Retesting	Conduct a retest to ensure vulnerabilities have been fixed.	3 days	24 days

Total Duration: 24 days (3 weeks 3 days)

Deliverables

- **Initial Findings Report:** Summary of vulnerabilities discovered during testing.
- **Final Penetration Testing Report:** Detailed document outlining findings, risk, levels, and recommendations.
- **Retesting Results:** Report confirming remediation of identified vulnerabilities

Budget

Activity	***Cost***
Planning and scoping	N….
Reconnaissance	N….
Vulnerability Assessment	N….
Exploitation Testing	N….
Reporting and Documentation	N….
Retesting and Verification	N….
Total Estimate cost	N….

Conclusion

In conclusion, this penetration test will identify any potential vulnerabilities in the redesigned website of 21st Century Technologies Ltd. It will help in ensuring that the website is secure, performs optimally, and provides a safe experience for your users. Our team is committed to providing you with actionable insights tht enhance the overall security of your digital assets.