Experience Sharing on School Pentest Project

Eric Fan
Chairman, eLearning Consortium
Agenda

- School Pentest Project
- Our Findings
- Recommendation
- Best Practice for School
- Look Forward in Year 2020
Objective

As an independent consultant in providing a series of vulnerabilities scanning, penetration tests and reviews for more than thirty K12 schools’ website security. Identifying potential areas for further improvement to protect school’s sensitive data and good will.
What we do?

**Step 1**
Configure and execute automated scan, followed by test plan development. Risk assessment will take place during the test plan development.

**Step 2**
Verify the scan result, eliminate false-positives and then execute manual business logic test. Application walkthrough and threat analysis will also be conducted during this stage.

**Step 3**
Report and analysis for the automated scan and manual scanning result with recommendations.
School Project Findings

- **78 APPLICATIONS**
  - Including public, intranet, internal applications of 30 schools

- **240+ CRITICAL VULNERABILITIES**

- **30 SCHOOLS**
  - Including public, private, primary and secondary schools

- **20,000+ PERSONAL DATA RECORD**
  - Including email, name, HKID etc
Vulnerability

6,000+ Vulnerabilities

- Critical: 4%
- High: 15%
- Medium: 30%
- Low: 51%
Critical Vulnerabilities

185 | XSS
325 | SQL Injection
33  | SSLV2 & V3
39  | Password in Plaintext
Top Security Impact Vulnerabilities

**Back Up File Impact**
We found plain text database login credential in the back up file that may lead to unauthorized login.

**Unsupported Software / OS Version**
These outdated software or operation systems cannot no longer update to the latest patch that is vulnerable to exploit.

**SQL Injection**
Allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

**Password In Plain Text**
Allows anyone who can read the file access to the password-protected resource.
SQL Injection

- **Vendor Solutions**: 22
- **School’s own applications**: 16
- **Unsupported Operation Systems**: 11
Recommendations

**Regular Patch Operation Systems**

Regular review and update the hardware and application operation systems to the latest patch, in order to avoid vulnerable malware and exploits.

**Reliable Vendor Solutions**

Software and application vendors should offer OS or patch update for use to fix their software and application vulnerabilities.

**Regular Scanning**

Yearly or half-year vulnerability scanning and penetration test is recommended.

More info: Information Security in Schools - Recommended Practice (Jan 2019)
Best Practice for Information Security in School

- Cloud Service Provider
  - Regular patch update and backup

- CloudFlare Web Application Firewall
  - Prevent SQL Injection and web security attack

- Firewall and IPS
  - Deny malicious traffic and file download

- File, DB, Email Servers
  - Data Protection and Back Up
  - Regular vulnerability scanning and penetration test

- End Point Computer and Tablets
  - Anti-Virus and Anti-Ransomware

- Back Up Storage

More info: Information Security in Schools - Recommended Practice (Jan 2019)
Look Forward in Year 2020

MEET WITH THE STAKEHOLDERS
To seek resources for the education sector on CyberSecurity

TRAINING TO PRACTITIONER
Provide training to the education practitioner on cybersecurity

BEST PRACTICE
Regular update on education specific security incident and best practice
Thank you!