eLEARNING CONSORTIUM
電子學習聯盟

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

eLEARNING CONSORTIUM
電子學習聯盟

Objective

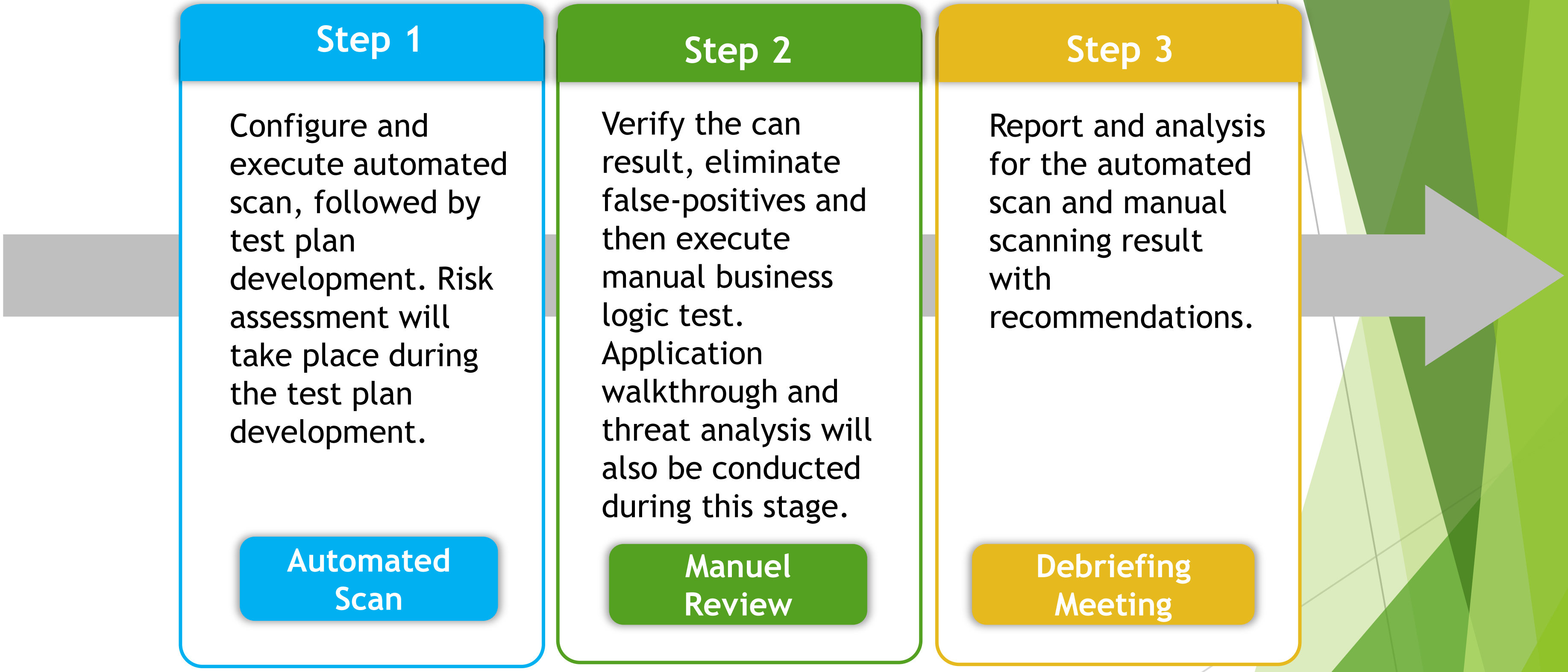
As an independent consultant in providing a series of vulnerabilities scanning, penetration tests and reviews for more then thirty K12 schools' website security.

Identifying potential areas for further improvement to protect school's sensitive data and good will.

HKT
30+ Schools

eLEARNING
CONSORTIUM
電子學習聯盟

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.

Automated Scan

Step 2

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

Manuel Review

Step 3

Report and analysis for the automated scan and manual scanning result with recommendations.

Debriefing Meeting

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

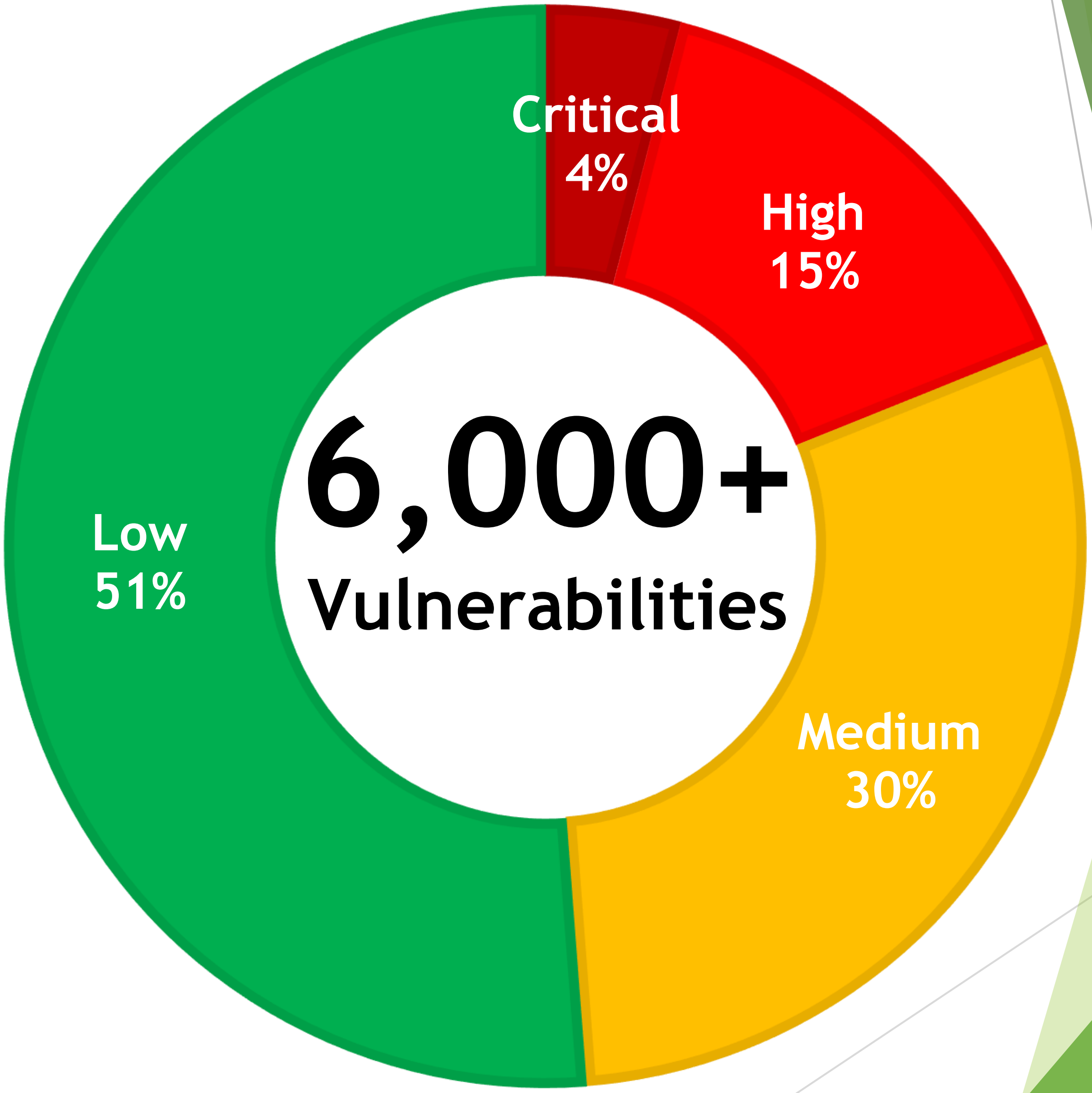
20,000+

PERSONAL DATA RECORD

Including email, name, HKID etc

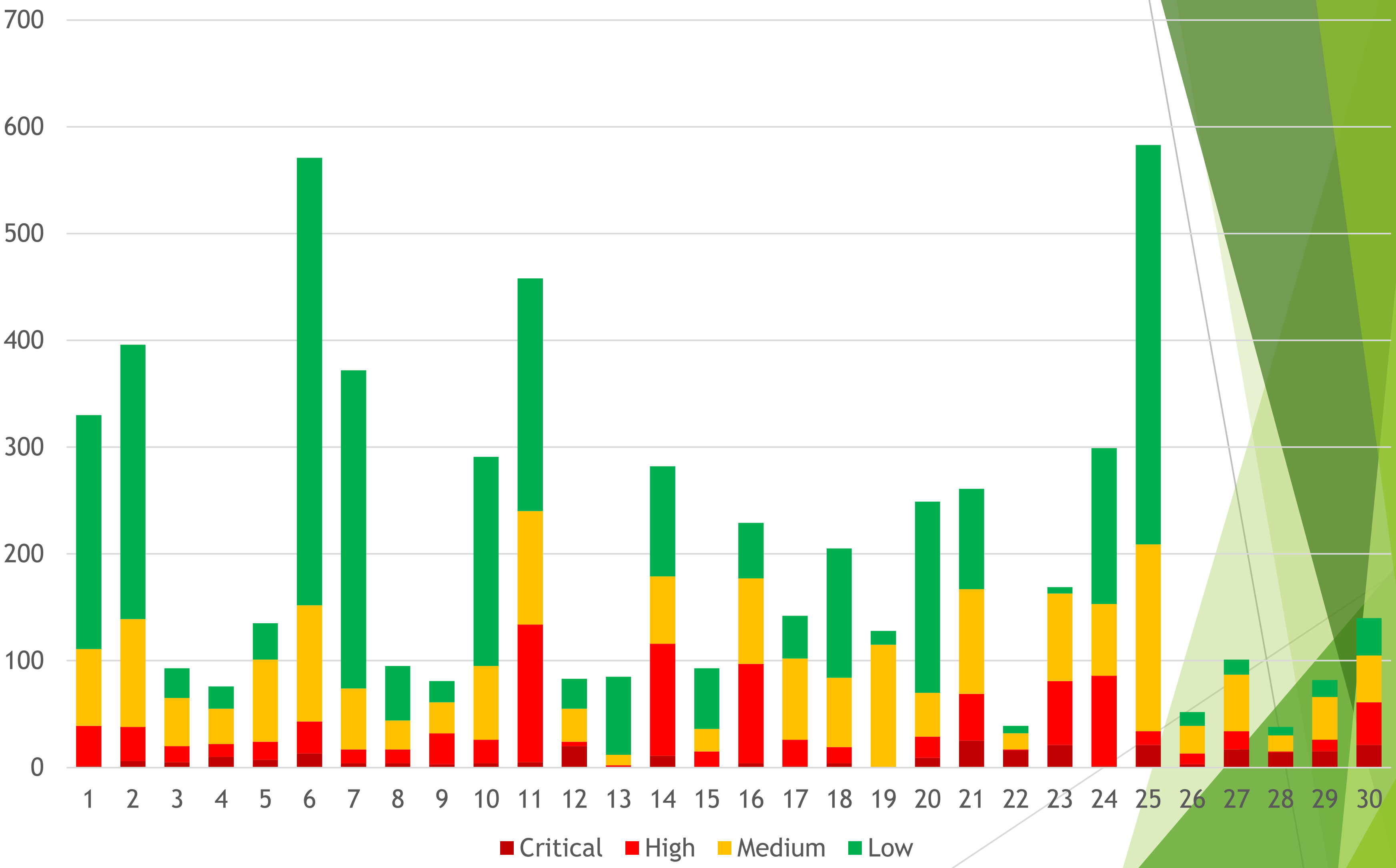
eLEARNING
CONSORTIUM
電子學習聯盟

Vulnerability

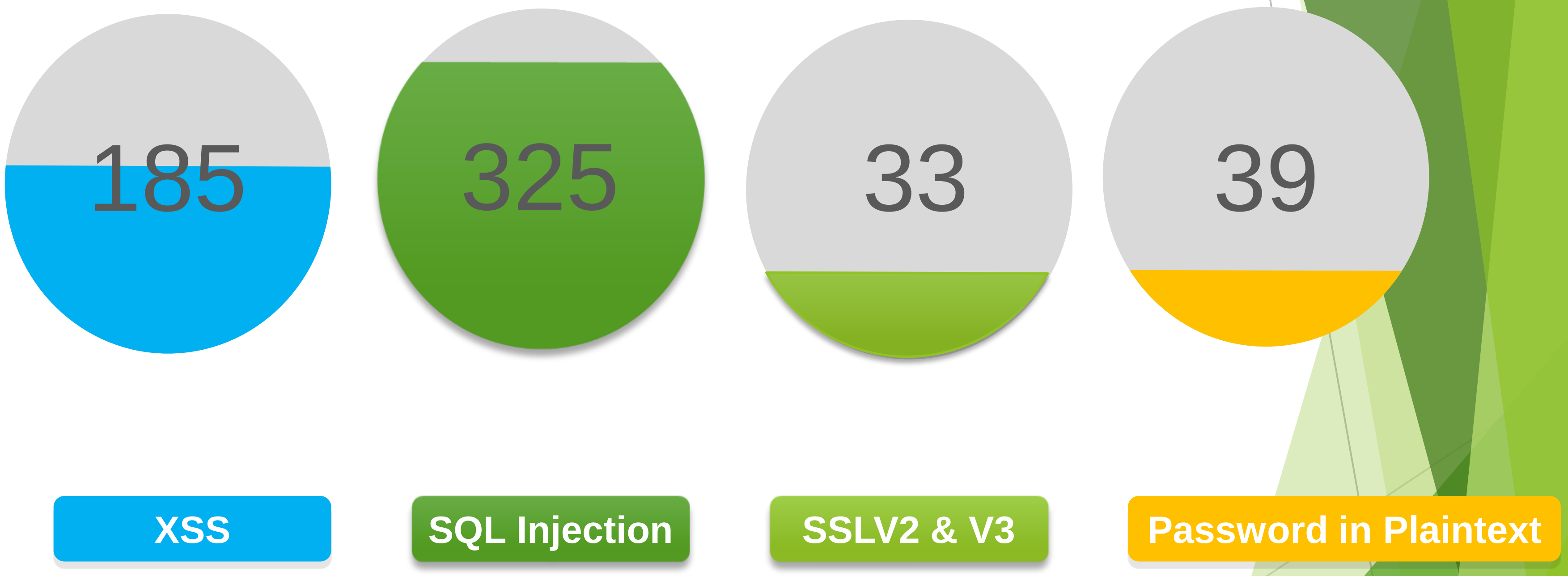


eLEARNING CONSORTIUM
電子學習聯盟

Overall Findings



Critical Vulnerabilities



185

325

33

39

XSS

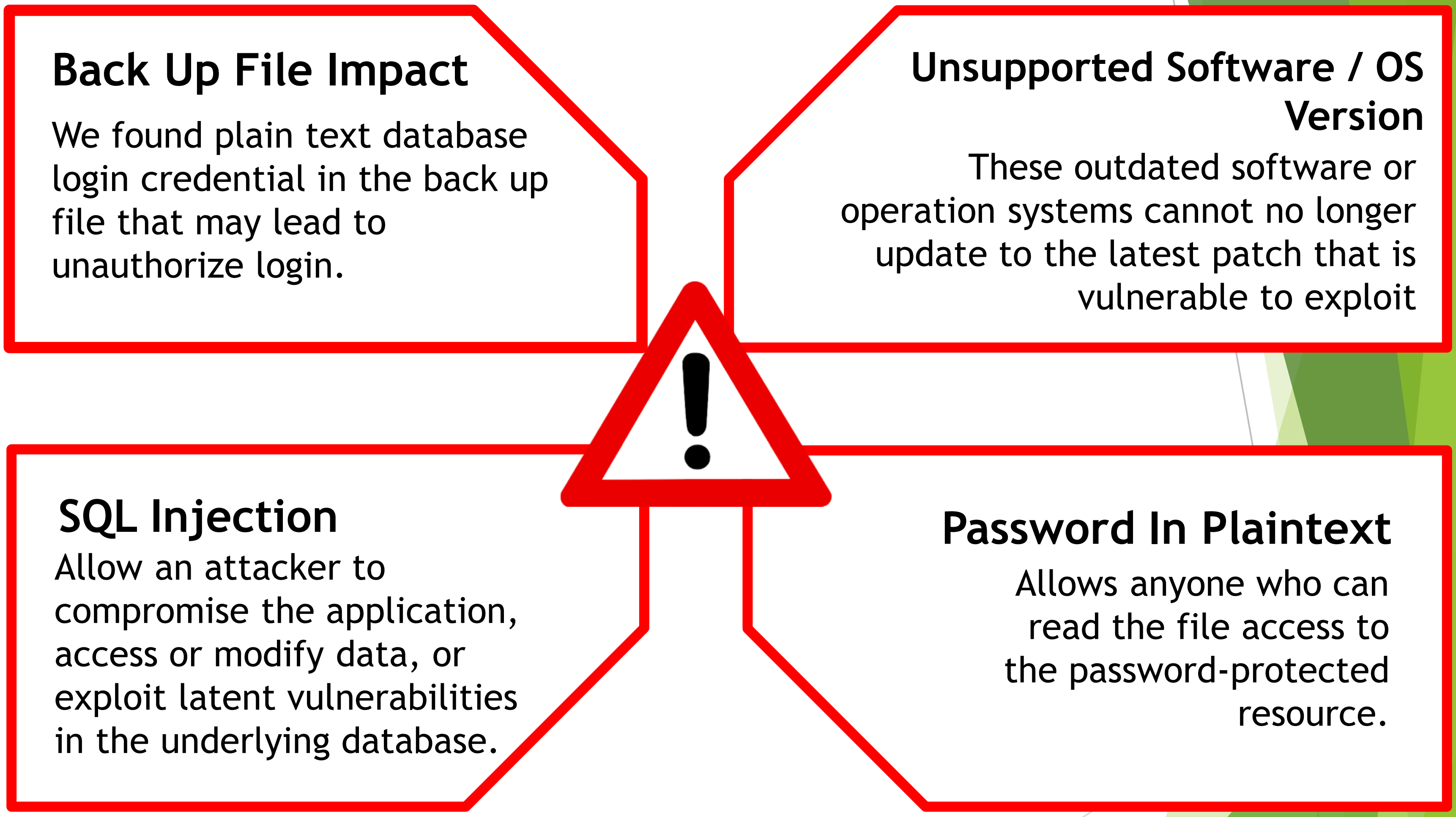
SQL Injection

SSLV2 & V3

Password in Plaintext

eLEARNING CONSORTIUM 電子學習聯盟

Top Security Impact Vulnerabilities



Back Up File Impact

We found plain text database login credential in the back up file that may lead to unauthorize login.

Unsupported Software / OS Version

These outdated software or operation systems cannot no longer update to the latest patch that is vulnerable to exploit

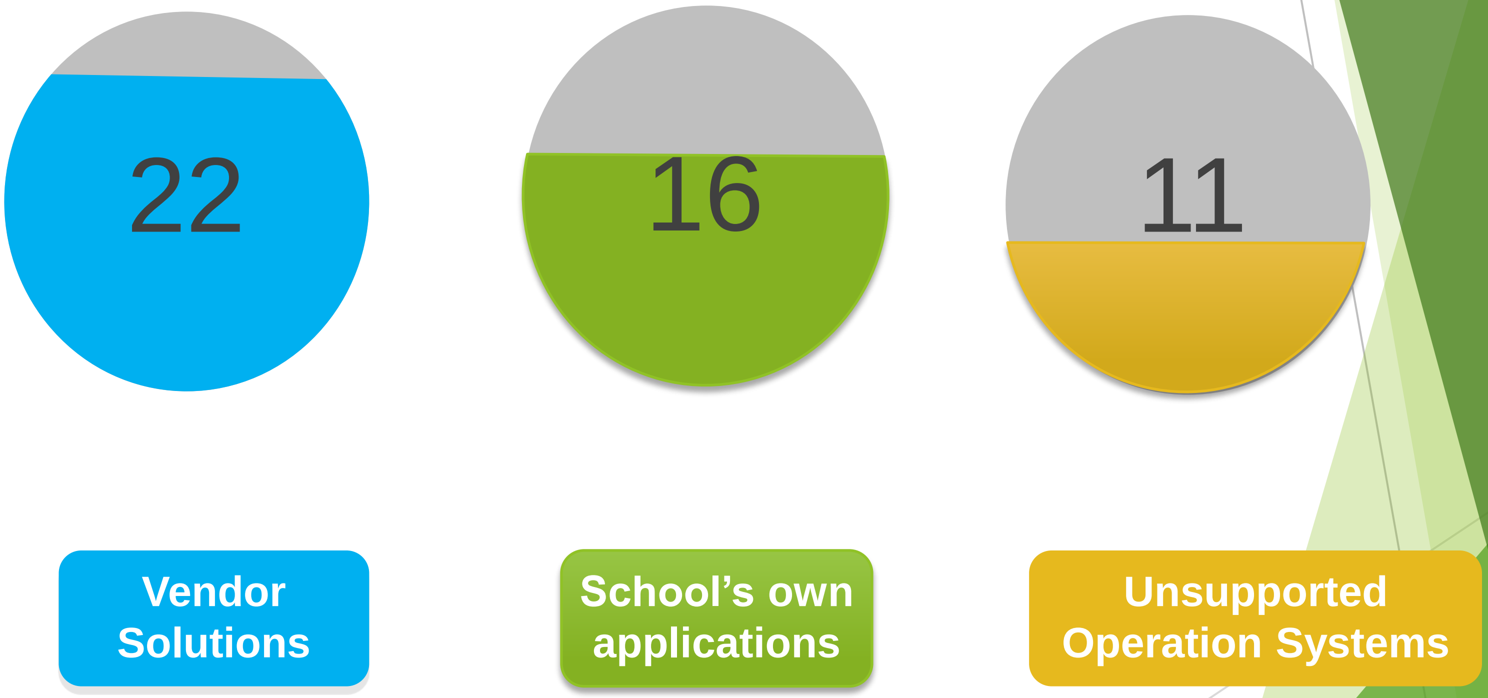
SQL Injection

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

Password In Plaintext

Allows anyone who can read the file access to the password-protected resource.

SQL Injection

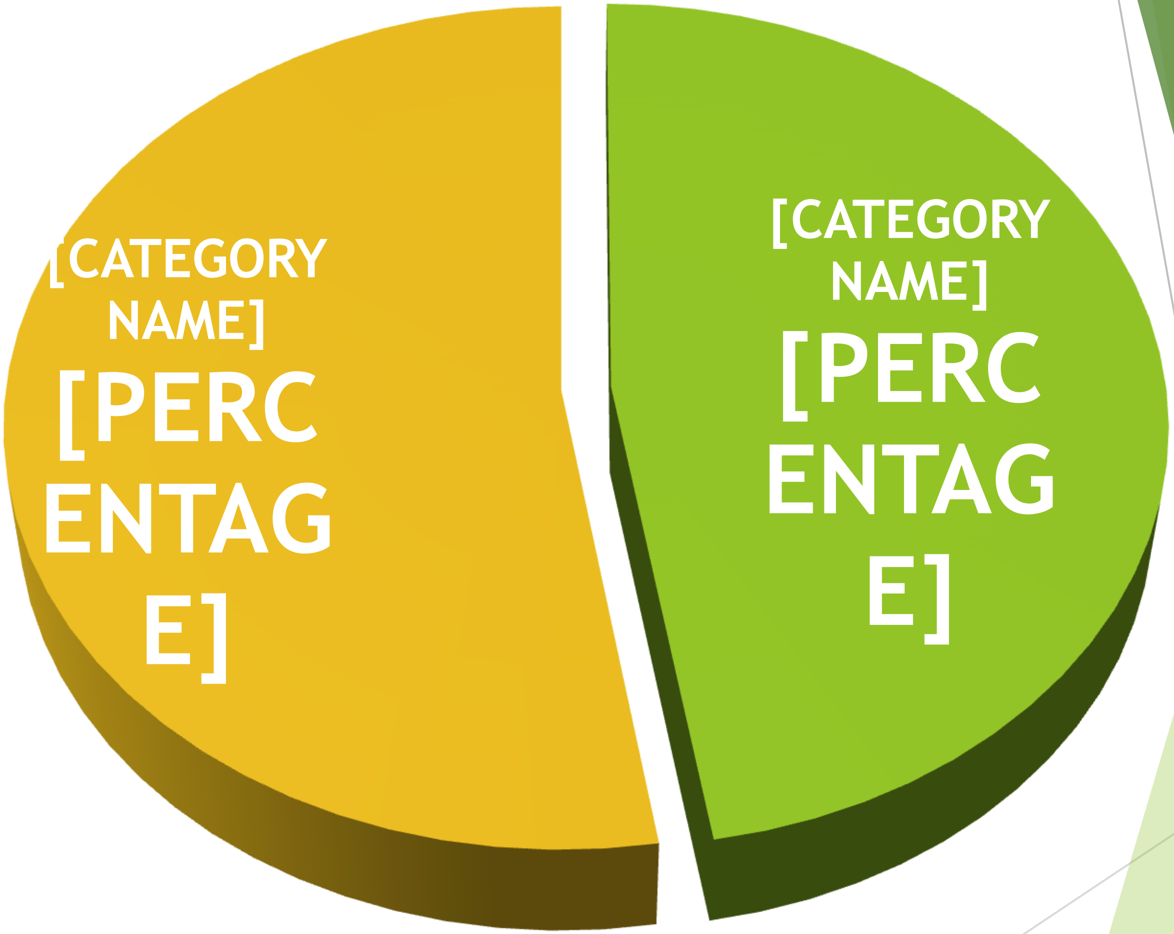


Vendor Solutions

School’s own applications

Unsupported Operation Systems

SSL Cert



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.

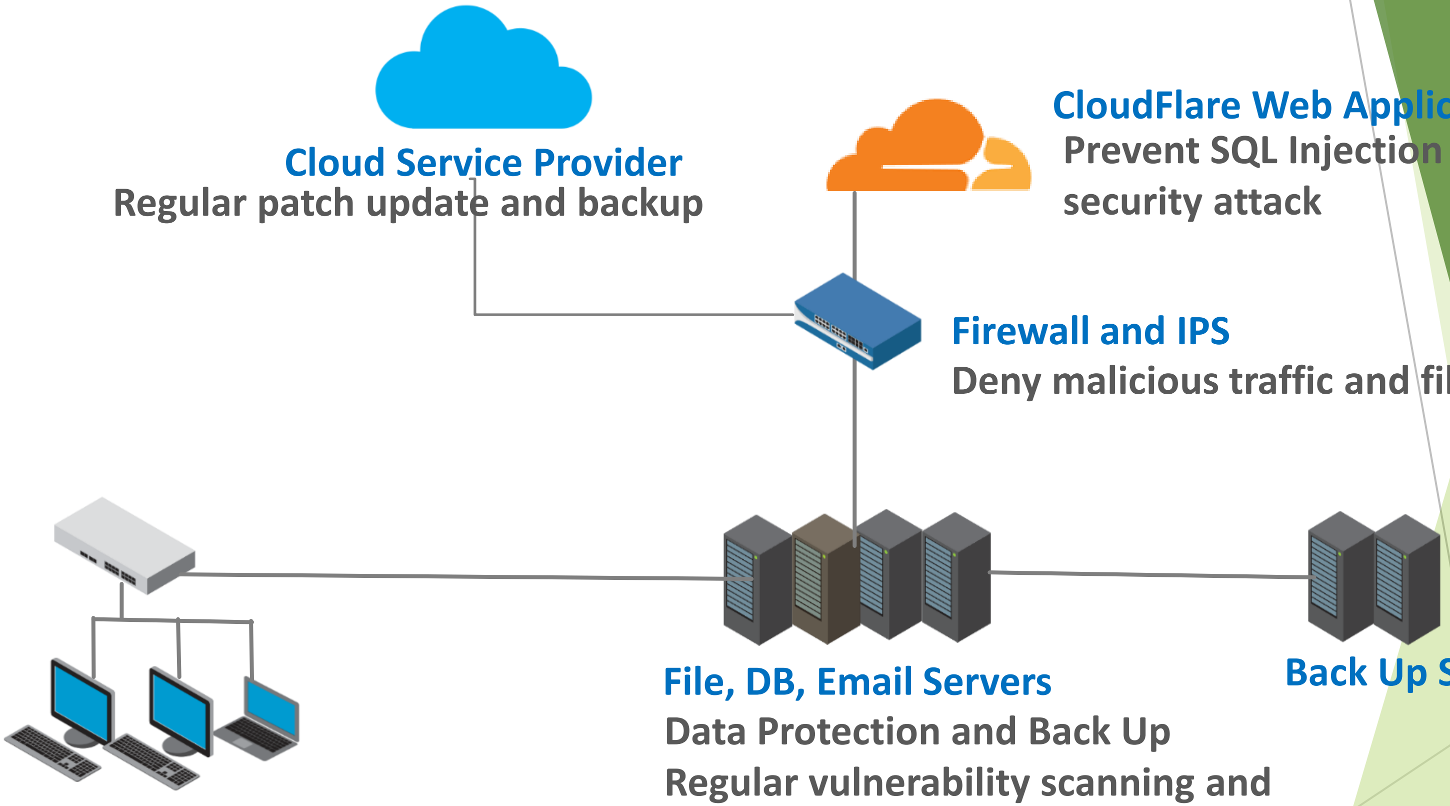
Regular Scanning

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

eLEARNING CONSORTIUM 電子學習聯盟

More info: Information Security in Schools - Recommended Practice (Jan 2019) https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/Information-Security/information-security-in-school.html

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

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

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

Back Up Storage

More info: Information Security in Schools - Recommended Practice (Jan 2019)
https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/Information-Security/information-security-in-school.html

eLEARNING CONSORTIUM 電子學習聯盟

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 cybersecurtiy

BEST PRACTICE

Regular update on education specific security incident and best practice

Thank you!