1-Week Vulnerability Assessment

eCloudvalley x Microsoft Azure

Vulnerability Assessment: 1-Wk Assessment

A vulnerability assessment is a way to identify security weaknesses of an organization's digital assets such as cloud computing instances or web applications on Azure cloud .

This assessment methodology inspect application's vulnerabilities from outside, use a systematic automated scanning tool to find out the vulnerabilities exposed on the Internet which might be exploited by attackers. After the scan, assess the severity level of the vulnerabilities and provide appropriate recommendations for remediation to the organization.

Vulnerability Assessment: 1-Wk Assessment

Why perform vulnerability assessment?

- ✓ Understand where the digital assets are most vulnerable.
- ✓ Improve enterprise security by patching systems based on the assessment report.

Deliverables:

- ✓ A report will be delivered that include:
  - Executive summary
  - Assessment overview
  - Risk severity
  - Vulnerability description
  - Initial remediation
- ✓ (Optional) An 1-hr consultation include:
  - Vulnerability consulting
  - Remediation consulting

Notes:

Pricing and duration may be varied based on the scope of assessment.

Vulnerability Assessment Process

Communication

Confirm the client's system architecture and the scope before assessment.

Preparation

Connection confirmation and assessment environment setup.

Execution

Scanning

Assessment

Analysis

Reporting

Generate and provide the vulnerability assessment report.

Consultation

Provide consultation to customer based on the assessment results

Vulnerability Assessment Report Content

- 專案說明 (Project Description)
- 作業資訊 (Assessment Information)
- 更版資訊 (Version Information)
- **風險摘要 (Vulnerability Summary)**
- 漏洞清單 (Vulnerability List)
- 漏洞說明與修補建議 (Vulnerability Description Remediation)

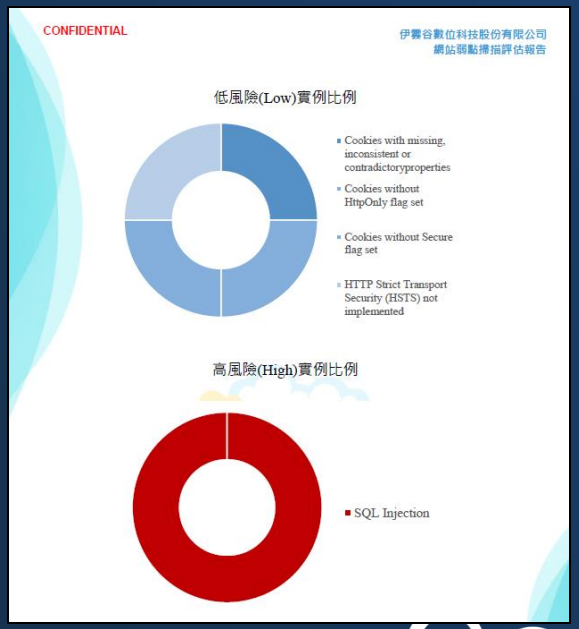
Example:

風險數量

高風險 HIGH	中風險 MEDIUM	低風險 LOW
4	0	4

風險與實例數量分級

嚴重性 Severity	弱點數量 Vulnerabilities	實例數量 Instances
High	1	4
Medium	0	0
Low	4	4
Total	5	8



Vulnerability Assessment Report Content

- 專案說明 (Project Description)
- 作業資訊 (Assessment Information)
- 更版資訊 (Version Information)
- 風險摘要 (Vulnerability Summary)
- **漏洞清單 (Vulnerability List)**
- 漏洞說明與修補建議 (Vulnerability Description Remediation)

Example:

CONFIDENTIAL

伊雲谷數位科技股份有限公司
網站弱點掃描評估報告

五、漏洞清單

本次作業發現漏洞列表

編號	風險等級	漏洞類別	事件
1	高	SQL injection	4
2	低	Cookies with missing, inconsistent or contradictory properties	1
3	低	Cookies without HttpOnly flag set	1
4	低	Cookies without Secure flag set	1
5	低	HTTP Strict Transport Security (HSTS) not implemented	1

Vulnerability Assessment Report Content

- 專案說明 (Project Description)
- 作業資訊 (Assessment Information)
- 更版資訊 (Version Information)
- 風險摘要 (Vulnerability Summary)
- 漏洞清單 (Vulnerability List)
- **漏洞說明與修補建議 (Vulnerability Description Remediation)**

Example:

HIGH SQL injection

造成漏洞的網頁請求回應資訊

下列網頁請求的HTTP標頭X-Forwarded-For可能遭受SQL injection攻擊:

- https://xxx.com/frontend/login.php

Request

GET /frontend/login.php / HTTP/1.1
Referer: https://xxx.com/frontend
User-Agent: ...

造成原因

SQL injection讓攻擊者可以透過網頁應用程式執行惡意的SQL查詢....影響資料庫...

建議作法

在處理包含用戶輸入的 SQL 查詢時使用...

Facebook (TW)

LinkedIn (TW)

Website (TW)

Line@

Instagram

Redefine IT with Cloud