

9.其他發現事項(8/14)

系統名稱 (子系統)	校安反應平台
風險位置	https://m.tnua.edu.tw/filemanager/filemanager/dialog.php?editor=0&type=0&lang=en_EN&popup=0&crossdomain=0&field_id=&relative_url=0&akey=key&fldr=&6a997a376c04c&1788443208358
風險等級 (CVSS)	中
網路存取控制 (內/外網)	內外網皆可存取
檢測發現 (OWASP/防護基準)	A05:2025 - 注入式攻擊
發現說明	網站使用之Responsive FileManager套件版本v.9.9.6存在CVE-2022-44276弱點。無需認證，可繞過上傳副檔名限制，上傳如php,html檔案至網站中，上傳目錄無法執行PHP，但可成功執行XSS語法。

CVE-2022-44276 弱點



Description

In Responsive Filemanager < 9.12.0, an attacker can bypass upload restrictions resulting in RCE.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0 SSVC

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score:

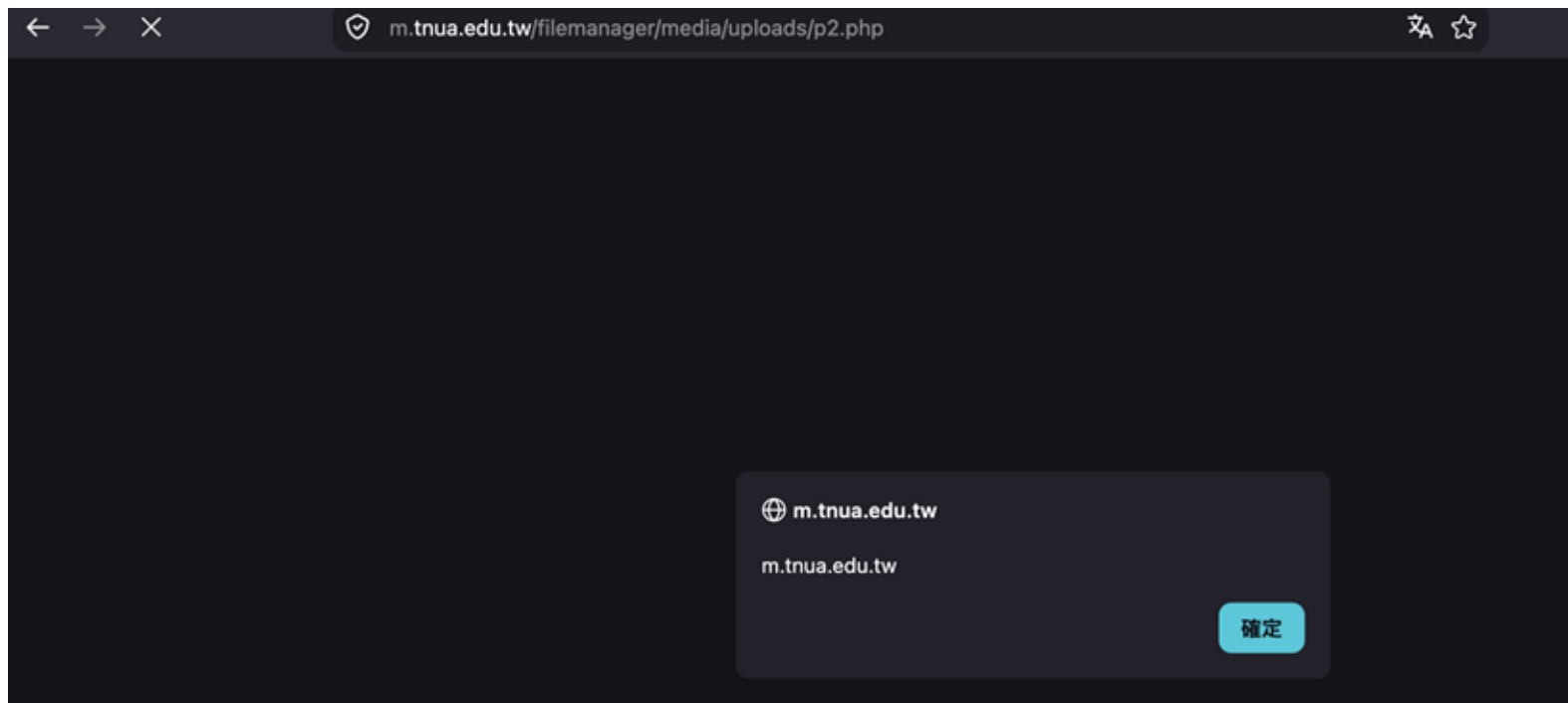
9.8 CRITICAL

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



可上傳PHP檔案執行XSS語法



9.其他發現事項(9/14)

系統名稱 (子系統)	全校課程查詢
風險位置	https://m.tnua.edu.tw/course/view?year=&sem=&teacher_id=%22%3E%3Cscript%3Ealert(document.domain)%3C%2fsript%3E&course=
風險等級 (CVSS)	低
網路存取控制 (內/外網)	內外網皆可存取
檢測發現 (OWASP/防護基準)	A05:2025 - 注入式攻擊
發現說明	全校課程查詢功能之教師代碼參數(teacher_id)存在XSS弱點, 可執行XSS語法。

反射性XSS弱點

