Practicum of Attack and Defense of Network Security (2024)

期中個人網站攻防說明書

一、簡介

本次期中考試為進行個人網站攻防，每位同學需建立自己的個人網站(須滿足第二項個人網站設計需求)，並於提交個人網址於下方表格連結，之後於網站相互攻打的開放期間，對其他同學進行攻擊(詳細的攻防判定說明餘第三項目)，如果攻擊成功，需撰寫如附件一的攻擊報告，包含攻擊成功的截圖。每位具有完整網站功能的同學皆會有 80 分的期中基本分，成功攻擊別人網站的同學將會+4 分，而被攻擊的同學會被-4 分。

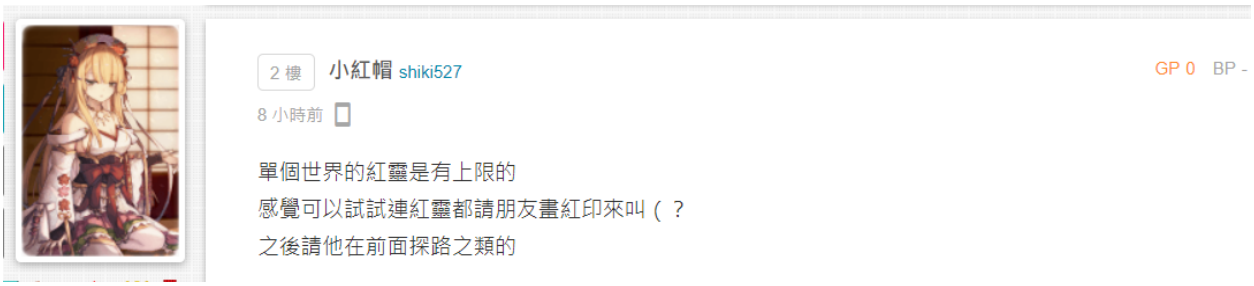
二、個人網站設計要求

1. 網站頁面設計須包含

   (1). 網站主人個人頭貼（10 分）
   (2). 網站主人自我介紹（10 分）

2. 網站功能需包含

   (1). 供訪客註冊以及登入的功能(以資料庫儲存帳號、密碼以及訪客的頭貼)（40 分）
   (2). 可以讓訪客上傳圖片作為頭貼（僅限 jpg、png 格式）(20 分)
   (3). 網站留言板功能（註冊的訪客可以進行留言，並且左側會包含留言者頭貼，留言者可刪除自己的留言)，如下圖所示（20 分）



3. 個人網站上傳連結

   請至以下網站填上個人網站網址

   https://www.dropbox.com/scl/fi/qcspk3n5ntxjqwop7p99a/DOMAIN.xlsx?rlkey=b21n10z1b1m6w0bbqfm306ooa&dl=0

4. 導入 AI 功能（加分項目+20）

現在 AI 火紅，同學們可以串接其他 AI 網站提供的 API 來提供給網站的訪客使用，如以下範例:

(1) 訪客可以透過輸入一串文字敘述，生成一張圖片

(2) 訪客可以透過輸入一串文字敘述，生成一段音樂

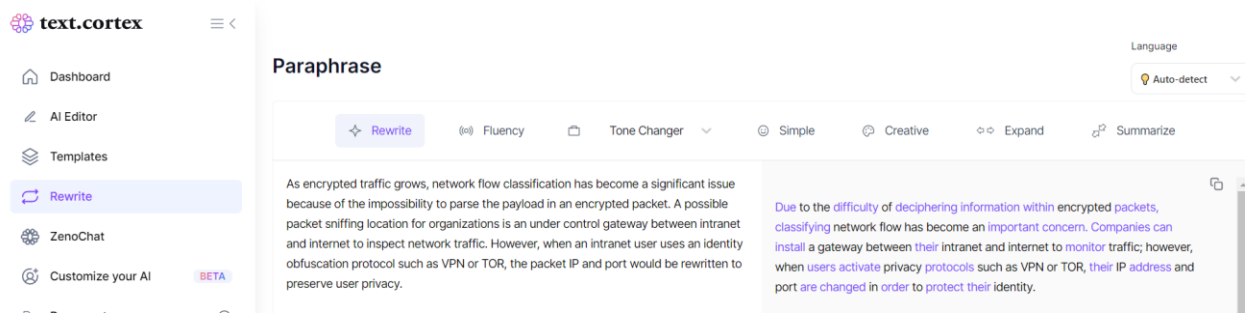
(3) 訪客可以透過輸入個人資訊和近期發生的事，生成一段占卜文字

(4) 訪客可以透過輸入文字功能敘述，生成對應程式碼

(5) 訪客可以輸入一串文字，生成改寫後的文字（如下圖範例）

(6) 網站的前後端是利用 AI 生成的(需要描述如何利用 AI 協助生成前後端)

(7)其他



三、攻防判定說明

1. 攻防期間: 4/17（三）中午 12:00 到 4/24(三)中午 12:00
2. 攻擊成功範圍如下:
   (1). 竊取獲得網站主人資料庫內容(如 SQL Injection)。
   (2). 修改網站主人頁面內容(如 XSS)，在自身瀏覽器上修改不算。
   (3). 取得網站的後端控制權（如上傳 webshell，漏洞利用)。
   (4). 取得網站主人後端檔案。
3. 以下不屬於攻擊成功範圍
   (1).撰寫腳本程式塞爆他人網站資料庫
   (2).DDoS 他人網站
   (3).取得他人伺服器上開的非網站服務資訊
   (4).通靈取得別人帳密
   (5).社交工程

4. 注意事項

(1).請勿分享漏洞給他人知道

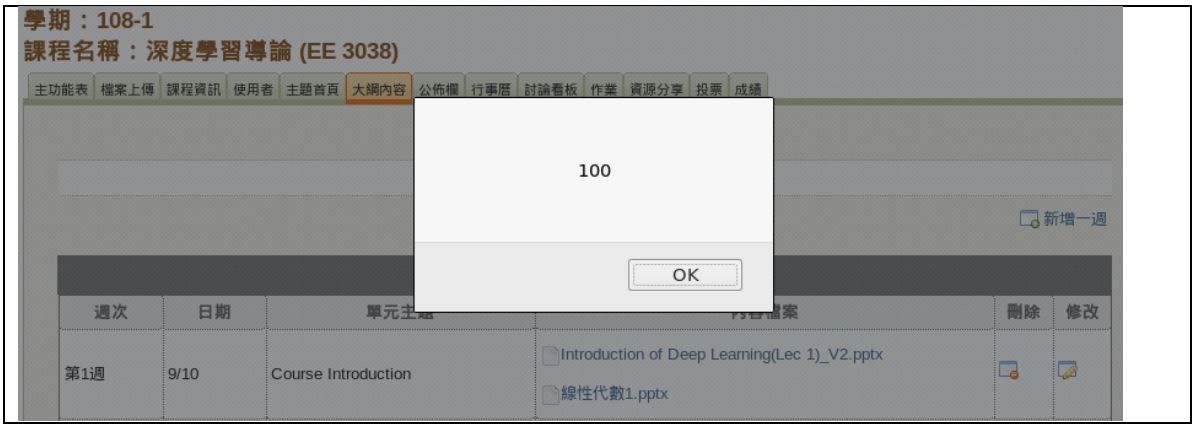
(2).請勿對他人網站進行侵入式破壞，如 DDoS、破壞資料庫、關閉伺服器等

四、攻擊成功寄件注意事項

於攻擊成功後，需撰寫郵件通知助教(F08942066@ntu.edu.tw)並附件給受害者，如果不想讓受害者知道自己的身分，則可在信中標註，並在報告中填寫匿名，由助教代為轉送信件。

附件一:期中報告

攻擊者學號	EX:R08942066
受害者學號	EX:R12345678
受害者網站	https://ceiba.ntu.edu.tw/ta/
攻擊手段	EX: SQL injection、XSS、upload webshell 等
漏洞位置	EX:留言板、登入帳號的地方
攻擊指令	EX:<script>alert(100) </script>
成功攻擊截圖	


學期：108-1
課程名稱：深度學習導論 (EE 3038)
主功能表
檔案上傳
課程資訊
使用者
主題首頁
大綱內容
公佈欄
行事曆
討論看板
作業
資源分享
投票
成績
100
OK
新增一週
週次
日期
單元主題
刪除
修改
第1週
9/10
Course Introduction
Introduction of Deep Learning(Lec 1)_V2.pptx
線性代數1.pptx