

Top10 Insufficient Transport Layer Protection (傳輸層保護不足)

對要連結的網站加入 `basename()` 語法，返回內部的網站，不會導到其他網站。

Top8 Unvalidated Redirects and Forwards (未驗證的導向)

導入扣款網站是使用 `Get` 來傳遞價格，簡單就可以改變。基本上用 `Get` 傳資料還是很危險的...

`fgetcsv()` 解析 csv 格式檔案

`file_put_contents(檔名, 內容)` 寫入檔案

解決方法 1

確定是從購買網站進入，且比對 `Session` 才可以完成付費。

`preg_match()`(正規表示條件, 要比對的字串)

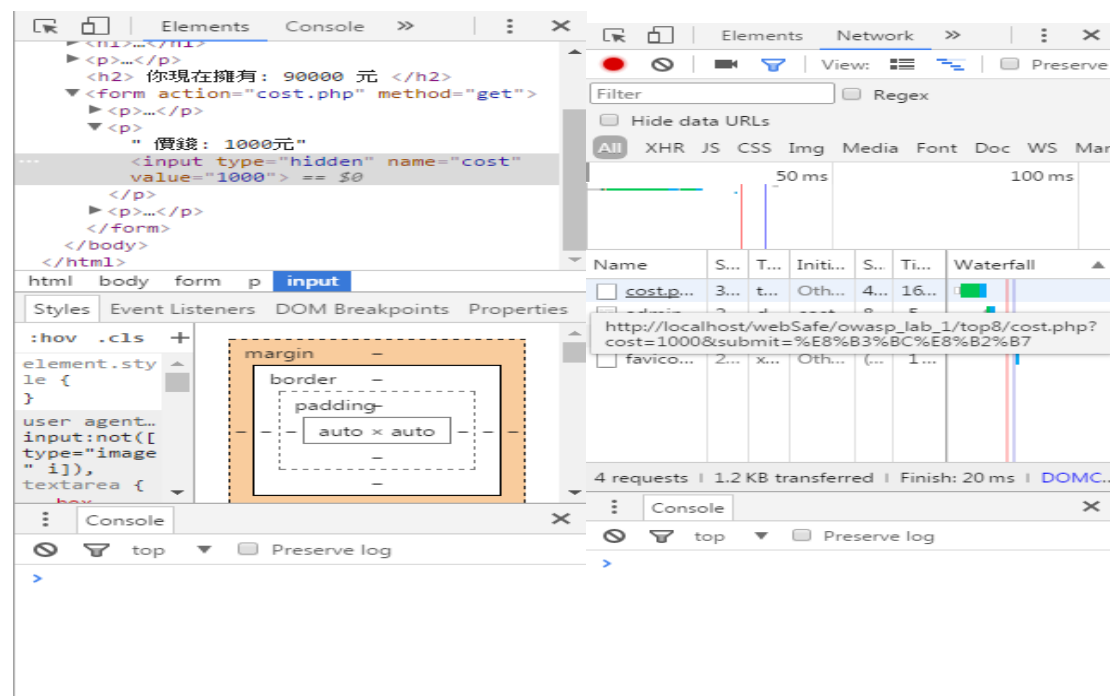
`$_SERVER['HTTP_REFERER']` 前一個網頁的位置

解決方法 2

利用 `sha1(microtime())` 以當前微秒加密後設定 `token` 變數與 `session`，然後進入購買網站後比對我傳入(`get`)的 `token`，與我的 `session` 比對。

`<input type="hidden" name="token" value="<?php print($token);?>` 設定 `token`

`if($_SESSION['login'] != 'admin' || $_SESSION['token'] != $_GET['token']){` 比對



Top7 Failure to Restrict URL Access（限制 URL 存取失敗）

未經過登入畫面進入 admin.php 網頁



解決方法

登入後要設定 session 且要比對 session，若未設定 session 就進入 unsafe.php 網頁。

`$_SESSION[""]` 此值是設定在伺服器上，可以防止權限不足而進入網站問題



Top5

預設密碼一定要改掉，下方網址有產品的預設帳號與密碼

<http://www.defaultpassword.com/>

D-Link	D-Link DIR-300	n/a	Multi	dont need one	admin
d-link	all router		Multi	admin	(blank)
D-Link	Cable/DSL Routers/Switches		Multi	(none)	admin
D-Link	DCS-1000		HTTP	none	none
D-Link	DI-524		Multi	admin	none
D-Link	DI-524		HTTP	admin	none
D-Link	DI-604		HTTP	user	none
D-Link	DI-614+		HTTP	user	(none)
D-Link	DI-614+		HTTP	admin	(none)
D-Link	DI-624		HTTP	Admin	none
D-Link	DI-701	unknown	Multi	admin	year2000
D-link	DI-714P+		Multi	admin	_____BLANK_____
D-Link	DI-804	v2.03	Multi	admin	(none)
D-Link	DIR-300	n/a	Multi	dont need one	admin
D-Link	DIR-655	1.35NA	HTTP	Admin	(none)
D-Link	DSL-300	?	Telnet	none	private
D-Link	DSL-300G+	7.1.0.30	Telnet	(none)	private
D-LINK	DSL-G664T	A1	HTTP	admin	admin
D-Link	DWL 900AP		Multi	admin	public
D-Link	ESL2640RBVMS.B1E		Multi	admin	admin
D-link	hubs/switches		Telnet	D-link	D-link

Top4

直接修改 login 的使用者，即可進入受害者的網頁

owasp_lab2/member.php?login=user

解決方法

登入後要設定 session 且要比對 session，跟上方的 **Top7** 一樣



Top3 Cross-Site Scripting (XSS)

在留言板上傳入可執行的程式

[回首頁](#)

您現在的身分是 user

這是 自我介紹預覽

vdfdfbdsfb
gbfgnfgndfgn1212
456456oihjoljbn j,l

這是 編輯自我介紹

vdfdfbdsfb
gbfgnfgndfgn1212
456456oihjoljbn j,l
<script>alert("A");</script>

確定

localhost 顯示 :
A
☐ 防止此網頁產生其他對話方塊。

確定

解決方法

輸出內容改成 `nl2br(htmlentities(內容))`

`nl2br()` 取代分行字元(`\n`)

`htmlentities()` 將特殊字元轉為 html 實體參照

符號	轉換後	符號	轉換後
&	&	"	"
'	'	<	<
>	>		

Top2 Broken Authentication and Session Management

解決方法

設定 TimeOut 過期時間 `start_session(600);` 600 秒後過期

ID 不要當成 URL 傳遞

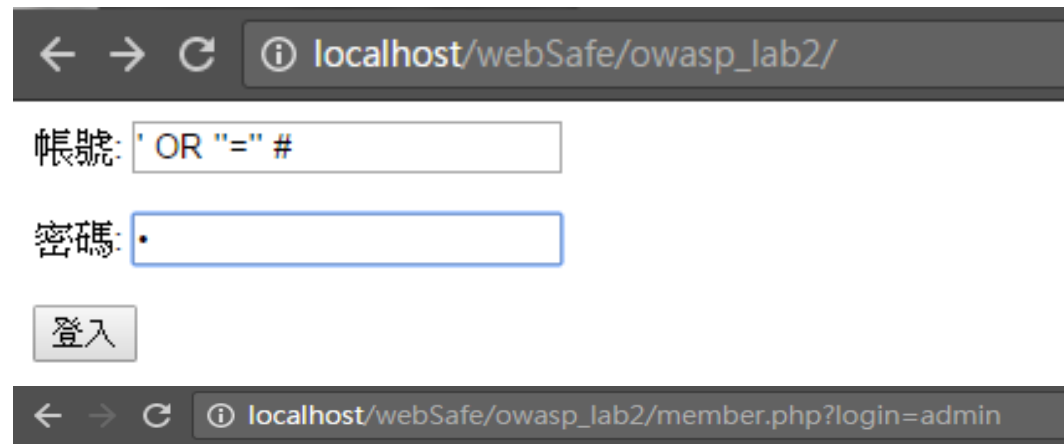
資料加密

Top1 Injection

只要在帳號打上 OR “=” 帳號部分就一定可以成立
而#是 Sql 的註解語法，讓密碼可以不用判斷。所以密碼隨便打都可以進入。

解決方式

使用 PDO (PHP Data Object)



← → ↻ ⓘ localhost/webSafe/owasp_lab2/

帳號: ' OR "=" #

密碼: .

登入

← → ↻ ⓘ localhost/webSafe/owasp_lab2/member.php?login=admin

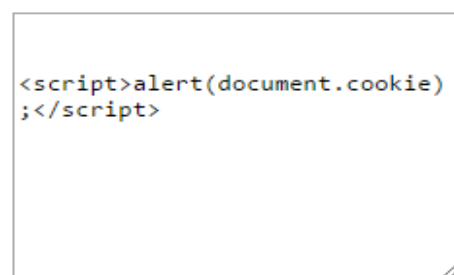
[回首頁](#)

您現在的身分是 **admin**

這是 自我介紹預覽

```
<script>alert(document.cookie);</script>
```

這是 編輯自我介紹



```
<script>alert(document.cookie)
</script>
```

確定

簡略說明，若有更多疑問請看老師的投影片！