B04902103 資工四 蔡昀達

**HW1**

1. CIA

* Condentiality: 機密性，是指個人或團體的訊息不為其他不應獲得者獲得。

例如: 避免訊息被竊聽或偷窺。

* Integrity: 真實性、完整性，確保信息或不被未授權的篡改。

例如: 保護訊息在傳輸時被竄改。

* Availability: 可用性，保證合法使用者對資訊和資源的使用不會被不正當地拒絕。

例如: DDOS是癱瘓availability的方式。

1. Hash Function

* one-wayness: 無法以hash value找回原本的x

例如: password hashing需要one-wayness避免被攻擊者還原明碼。

* weak collision resistance: 給定x，無法找到hash value 一樣的x’

例如: checksum 可以利用hash確保下載檔案完整性。

* strong collision resistance: 找到任一兩個(x, x’) ，有同樣的hash value

例如: 不可否認性需要strong collision resistance讓承諾方不可更改承諾。

1. Threshold Signature

Assume a single sinature S is enough to verify k given signatures Si :

e(S, g) = e(∏k si, g) = e(∏k hski, g) = ∏k e(h, g)ski = ∏k e(h, gski) = ∏k e(h, PKi)

Each individuals instead if publish PKi = gski , publish pki = gr \* pki-1

Now thay can claim both signed the messages by S = hr

1. Babe crypto :

Flag : BALSN{CRYPT0\_1S\_3ASY\_XDD}

R1: caesar cipher

R2: 字元相減發現規律

R3: rail fence cipher

R4: base64

1. OTP
2. Flag : BALSN{7ime\_Se3d\_Cr4ck!n9}

random seed 由time.time() 轉成 int，在local同步計算將會得到同樣的結果，因此可以計算key並解密。

1. 略
2. MD5 Collision :

Flag : BALSN{MD5\_Ch3cK5Um\_!5\_Br0k3N}

利用identical prefix attack製造md5 collision，使兩個不同的檔案md5相同。

Hidden : BALSN{Ex3cUTe\_uNtrU5t3d\_C0d3\_15\_V3rY\_d4nG3R0uS}

利用沙盒執行程式碼並輸出結果的方式，讀取執行環境的檔案目錄，找到/home/md5底下的檔案，可以找到hidden flag。

Code1 = ''

Code2 = ''

1. Flag Market :

Flag : BALSN{L3ngTh\_3xeT3n5i0N\_4tTacK\_i5\_34sY\_w1tH\_H4shPump}

利用length extension attack 偽造合法sha256的token，添加重複的&BLASN\_coin可以成功注入錯誤的錢幣數量。

Hidden : BALSN{PyTh0n\_F0rM4t\_5trInG\_C4n\_B3\_daNG3rOuS}

利用python string format的漏洞，可以呼叫str.attributes，並藉此呼叫\_\_doc\_\_，從中拼湊符合的字串。

1. RSA :

Flag : BALSN{Therefore\_We\_5hould\_Not\_Choose\_4\_5mall\_Public\_Key...}

因為是很小的exponent因此利用Håstad's Broadcast Attack，就可以反解得到密文。

1. Backdoor of Diffie Hellman：

Flag : BALSN{black magic number}

根據費馬小定理和提示，goldp-1 mod p ≣ gbackdoor691829 mod p ≣ 1，由此可知gbackdoor是比較小的group，可以暴力搜尋 a, b ∈ [0, 691829) 使得A = gbackdoor^a mod p 且 B = gbackdoor^b mod p。