Binary:

1. Soeasy: 直接對程式進行strings 即可找到flag
2. MyFirstObfuscatedCode: 拿去顏文字javascript 上面翻譯

Misc:

1. Ascii: 將 Ascii 轉成strings
2. Secrets in pdf: PDF 中有一行白色文字是flag
3. Secret of Metadata : 將檔案下載下來 檔案註解裡面有flag
4. Secret images in pictures:用files 發現他是兩張圖片合起來的,用binwalk將它拆解，其中一張圖片為flag
5. Linux-hidden file:用ssh連線進去之後ls發現沒有檔案，用ll發現檔案為隱藏檔將其cat出來
6. Linux-find file:同一個連線裡面用find / -name secret -type f 即可找到檔案

Web:

1. Developer Tools:Flag按下F12即在註解裡面，將其base64轉換後得到
2. Robots.txt :robots 中有個檔案不給爬蟲爬，連到後顯示flag
3. SQL injection:基本的SQLinjection 用 ‘ OR“=”—即可
4. Command Injection :發現在輸入加個;即可執行linux指令，因為不知道檔案所在地，先執行一次find / -name flag -type f 後得知路徑在/var/www/flag顧cat即可得到
5. Flashing\_Redirect:因為一跳進去就會被跳轉，所以用curl 即可固定住畫面
6. New HTTP method:點進去題目發現他不支援GET，POST等Method 所以看一下其header 發現可以用一個他們自創的method叫做Give Me flag 然後curl –X GiveMeFlag 網址 即可得到
7. GuessingAdminSession- 用burpsuite 攔截barry跟clare的sessionID 發現其設計簡單，用admin代換掉sessionID後重送即可進admin帳號得到flag
8. To serialize or Not to serialize:本題用的是PHP serialize 的bug程式如下<?php  
   class MyFirstCTF {  
       protected $test = "CTF";  
       function \_\_wakeup()  
       {  
           print "Wake up yo!<br>";  
           system("echo ".$this->test);  
       }  
   }  
   $input = $\_GET['str'];

$kb = unserialize($input);  
highlight\_file(\_\_FILE\_\_);

我們可以發現中間有一個system的call，所以我們可以仿照一個序列化的call，送進str裡面來讓他執行，因為序列化的格式不好寫，所以抄其程式後再本機端試跑得出O:10:"MyFirstCTF":1:{s:7:"%00\*%00test";s:7:";ls -al";}即可讓他跑ls –al然後得知裡面有一個檔Th1s\_1S\_f1ag\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_y0

因為不好計算他幾個字元，所以用O:10:"MyFirstCTF":1:{s:7:"%00\*%00test";s:7:";cat%20T\*";}

就可以得到flag

Crypto:

1. 我愛凱薩:用第一個比對M發現rot21 拿去網路解凱薩用的解完得知答案。
2. Hashing Service:nc到題目給的網址後發現題目要你sha1一段明文，sha1後餵給server得到flag
3. Md5 Collinsion: 用php的弱比對漏洞，0e後面他都省略，而題目要求的密碼剛好是0e開頭，故找一個0e開頭的明文即可登入
4. Sha1 Collinsion: 跟上題一樣找個開頭是0e的sha1即可過
5. Transposition Cipher:題目bcvqMeqacytqazFigwiiobxrrrtuiszahftreqcCreqcTreqcFkgd4{bnjrWwgk8egbcelrwqrcfvbmotewsmjkloehmkotooyfovbnkMii87yrfghFnakiiutfbrghk9so987t5tfbChjioTo087Ftfcv} 發現他每四個就會有一個關鍵字，刪掉即可得到flag
6. My First Rsa:簡單RSA解密 ，N先拿去質因數分解後發現有三個因數而隨機刪掉一個短的，即發現得到答案，程式如下。

import libnum

p=2262150367

q=12218233223644524650141958853163065112163255395621655741865064529020634406575730714768264558014607893896434523845321502371618344594488810317052606914954669

e=11

c=52647343688614059600786250163473723502435567148944634413225109321763985726312135145964712577508657083981623768580181565681763009751782302903251421007306111622629067075415325

n=p\*q

phi=(p-1)\*(q-1)

d = libnum.modular.invmod(e, phi)

print libnum.n2s(pow(c, d, n))

print p\*q



參加人數約略150人左右