

HP

Day 6 - Web Security

OT

網頁應用程式安全 - 翁浩正 (Allen Own)

📄 葉泳志 期待中。

J 我今天要先講一句話！

A 今天不是打站課！！！！！！

HP

資安概論

- [賽門鐵克：去年全球有5.5億筆個資外洩](#)
- [eBay遭黑客入侵1.4億用戶資料外洩](#)
- [AOL坦承系統遭入侵，駭客可能存取大量使用者帳號](#)
- [美國零售商IT系統陷危機 除了Targrt多家零售商也遭殃](#)
- [Home Depot：駭客入侵約造成5600萬筆金融卡資料外洩](#)

A 台灣有最新的攻擊手法！有最新的病毒樣本 XDD

風莫 最新的台灣之光

J 盛產天然資源 – 惡意程式

RL 臺灣學術網路曾有打美國國防部的紀錄

HP 駭客越強，防禦也要與時俱進

J 盛產天然資源 – 惡意程式

RL 正面攻擊，如果對方很弱

側面攻擊，可能性比較高

不安全的人比不安全的系統更可怕

- 被入侵不是因為沒有買XXX設備
- 舊時代的產物，所以密碼無法超過八碼(DES加密)
- 若是看見無法超過八碼，可以預見系統為舊版，要用舊的exploit

📄 秋聲羅 學校行政單位都還用winXP說O_O

王 沒有不安全的系統，只有不安全的人

HP The Strongest Password In The World: 123456

王 穩定的 exploit：不會讓系統or程式當掉，不會讓使用者起疑

HP	123456	CHARLIE	HELLO	FENDER	GOLF	DONALD	MUFFIN	GIANTS	ROSEBUD	CALVIN
	PASSWORD	SUPERMAN	SCOOTER	ANTHONY	BOND007	BIGDADDY	REDSOX	BOOTY	JAGUAR	SHAVED
	12345678	ASSHOLE	PLEASE	BLOWME	BEAR	BRONCO	STAR	BLONDE	GREAT	SURFER
	1234	FUCKYOU	PORSCHE	FERRARI	TIGER	PENIS	TESTING	FUCKED	COOL	SAMSON
	PUSSY	DALLAS	GUITAR	CHICKEN	DOCTOR	VOYAGER	SHANNON	GOLDEN	COOPER	KELLY
	12345	JESSICA	CHELSEA	MAVERICK	GATEWAY	RANGERS	MURPHY	0000	1313	PAUL
	PANTIES	CHelsea	MAVERICK	CHICAGO	GATORS	BIRDIE	FRANK	FIRE	SCORPIO	MINE
	dragon	PEPPER	BLACK	JOSEPH	ANGEL	TROUBLE	HANNAH	SANDRA	MOUNTAIN	KING
	qwerty	IIII	DIAMOND	DIABLO	JUNIOR	WHITE	DAVE	POOKIE	MADISON	RACING
	696969	AUSTIN	NASCAR	SEXSEX	THX1138	TOP GUN	EAGLE1	PACKERS	987654	5555
	mustang	DANIEL	JACKSON	HARDCORE	PORNO	BIG TITS	11111	EINSTEIN	BRAZIL	EAGLE
	letmein	GOLFER	CAMERON	666666	BADBOY	BIG TITS	11111	DOLPHINS	LAUREN	HENTAI
	baseball	WELCOME	654321	WILLIE	DEBBIE	BITCHES	MOTHER	00000	JAPAN	NEWYORK
	master	HEATHER	COMPUTER	CHRIS	SPIDER	GREEN	NATHAN	CHEVY	NAKED	LITTLE
	micHAEL	HAMMER	AMANDA	PANTHER	MELISSA	SUPER	RAIDERS	WINSTON	SQUIRT	REDWINGS
	FOOTBALL	YANKEES	WIZARD	YAMAHA	BOOGER	QA ZWSX	STEVE	WARRIOR	STARS	SMITH
	SHADOW	JOSHUA	XXXXXXXX	JUSTIN	1212	MAGIC	FOREVER	SAMMY	APPLE	STICKY
	MONKEY	MAGGIE	MONEY	BANANA	FLYERS	LAKERS	ANGELA	SLUT	ALEXIS	COCACOLA
	ABC123	BITE ME	PHOENIX	DRIVER	FISH	RACHEL	IPER	8675309	AAAA	animal
	PASS	ENTER	MICKEY	MARINE	PORN	SLAYER	OVI82	ZXCVCBNM	BONNIE	BRONCOS
	fuckme	ASHLEY	BAILEY	ANGELS	MATRIX	SCOTT	JAKE	NIPPLES	PEACHES	PRIVATE
	6969	THUNDER	Knight	FISHING	TEENS	2222	LOVERS	POWER	JASMINE	SKIPPY
	JORDAN	COWBOY	ICE MAN	DAVID	SCOOPY	ASDF	SUCKIT	VICTORIA	KEVIN	MARVIN
	HARLEY	SILVER	TIGERS	MADDOG	JASON	VIDEO	GREGORY	ASDFGH	MATT	BLONDES
	RANGER	RICHARD	PURPLE	HOOTERS	WALTER	LONDON	BUDDY	VAGINA	qwertyui	ENJOY
	Iwantu	FUCKER	ANDREA	WILSON	CUMSHOT	7777	WHATEVER	TOYOTA	DANIELLE	GIRL
	JENNIFER	ORANGE	HORN	BUTTHEAD	BOSTON	MARLBORO	YOUNG	TRAVIS	BEAVER	APOLLO
	HUNTER	MERLIN	DAKOTA	DEVILS	BRVES	SRINIVAS	NICHOLAS	HOTDOG	4321	PARKER
	FUCK	MICHELLE	qaaaaa	FUCKING	YANKEE	INTERNET	LUCKY	PARIS	4128	qwERT
	2000	CORVETTE	PLAYER	CAPTAIN	LOVER	ACTION	HELPME	ROCK	RUNNER	TIME
	TEST	BIGDOG	EDWARD	XAVIER	BARNEY	CARTER	JACKIE	X XXX	SWIMMING	SYDNEY
	BATMAN	CHEESE	CHARLES	STEVEN	VICTOR	JASPER	MONICA	EXTREME	DOLPHIN	WOMEN
	TRUSTNO1	MATTHEW	GIRLS	VIKING	TUCKER	MONSTER	MIDNIGHT	REDSKINS	GORDON	VOODOO
	THOMAS	121212	COFFEE	SNOOPY	PRINCESS	TERESA	COLLEGE	EROTIC	CASPER	MAGNUM
	TIGGER	PATRICK	XXXXXX	BIVE	MERCEDES	JEREMY	BABy	DIRTY	STUPID	JUICE
	ROBERT	MARTIN	bulldog	EAGLES	5150	111111	CUNT	FORD	SHIT	ABGR174
	ACCESS	GINGER	rabbit	WINNER	DOGGIE	BILL	BRIAN	FREDDY	SATURN	77777
	LOVE	BLOWJOB	PEANUT	SAMANTHA	222222	CRYSTAL	MARK	ARSENAL	GEMINI	DREAMS
	buster	NICOLE	JOHN	HOUSE	GUNNER	PETER	STARTREK	ACCESS 14	APPLES	MAXWELL
	1234567	SPARKY	JOHNNY	MILLER	HORNEY	PUSSIES	SIERRA	WOLF	AUGUST	MUSIC
	SECRET	YELLOW	GANDOLF	FLOWER	BUBBA	COCK	LEATHER	NIPPLE	3333	RUSH2112
	SOCCER	CAMARO	SPANKY	JACK	FRED	BEER	232323	ILoveYou	CANADA	RUSSIA
	HOCKEY	WINTER	FIREBIRD	BUTTER	JOHNSON	ROCKET	4444	ALEX	BLAZER	SCORPION
	KILLER	DICK	BRANDY	UNITED	XXXXXX	Theman	BEAVIS	FLORIDA	CUMMING	REBECCA
	GEORGE	FALCON	COMPAG	TURTLE	TITS	OLIVER	BIGCOCK	ERIC	HUNTING	TESTER
	SEXY	TAYLOR	CARLOS	STEELERS	MEMBER	PRINCE	HAPPY	LEGEND	Kitty	MISTRESS
	ANDREW	131313	JAMES	TIFFANY	BOOBS	BEACH	SOPHIE	MOVIE	RAINBOW	PHANTOM
		MIKE	ZXCVCBN			AMATEUR	LADIES	SUCCESS	112233	BILLY
		BRANDON	TOMCAT			777777	NAUGHTY		ARTHUR	ALBERT
									CREAM	6666

500 WORST PASSWORDS
 TAKEN FROM PERFECT PASSWORD SELECTION, PROTECTION, AUTHENTICATION BY MARK BURNETT

<https://iamloud.files.wordpress.com/2010/04/500-worst-passwords1.jpg>

爛密碼：

- 陳 • 長度太短（容易被暴力破解）
- X • 太單純（只有英文或數字，沒有區分大小寫也沒有特殊符號）
- 陳 • 太多都是常見的字串（字典攻擊）
- RL • 已知訊息，如使用者生日

HP 好密碼的長度至少要超過15個字元

Windows 以前的加密 LMHASH 是一種糟糕的加密法，只能 14 個字元，前七碼加密，後七碼加密，拼湊在一起（密碼複雜度降低），NTLM 才改善，所以密碼長

度15個字以上就不會儲存為LM

RL (亦可透過policy停用LM HASH)

HP 這是一場與入侵者的戰爭，不要當個M

王 你該怎麼做防守一個城池？

陳 防守的選擇

- 蓋城牆就對了，蓋得越高越好

HP ◦ 我用投石車，你還在用城牆

陳 ◦ 兩邊的科技不對等，是沒有意義的（？用機器人打城堡

HP ◦ 一定是牆不夠堅固！再加強！

軍師：一定是牆不夠高（Firewall 不夠，你有考慮買 IPS 嗎）

防禦者不懂駭客用的是怎麼樣的科技

王 正確的防禦者思維？

- 不能一昧著防禦，攻擊者的技術往往凌駕於防禦者
- 瞭解了解駭客思維，針對思慮進行防禦

HP • 定期做安全檢測、演練，瞭解自己的弱點

王 駭客的思維跟我們不一樣

RL • 大駭客只看網址就可以知道漏洞

- 讓人想要嘗試的點

- SQL injection

X ◦ Command injection

RL ◦ Path travel

- robots.txt 告訴搜尋引擎不要索引的網址(聽起來很誘人？)

□ Hsieh P <https://www.facebook.com/robots.txt>

RL ◦ 忘記密碼(得到明碼就代表網站不安全)

- 看見403 就代表東西存在，有貓膩；404則無搞頭

- 在那邊演講就試那邊的站

王 • user friendly XD(DDDDDD(hacker friendly!!))

□ 王茂林 <http://www.ntust.edu.tw/robots.txt>

RL • whois(查管理者資料，所屬其它網域)

HP 駭客攻擊流程

- Reconnaissance

RL ◦ 網站誰的、那種系統架設的

BC ◦ 防禦: 盡量讓外洩的資訊少一點 (ex. 不要用個人mail, 用 mailing list)

王 • Scanning

陳 ◦ 查此網站開了什麼服務、哪些漏洞可以利用

BC ◦ 防禦: 不要被scan (裝一些 IDS 啥的)

- 王 • Gaining Access
 - RL ◦ 譬如試用FTP看看版本是否有漏洞
 - BC ◦ 防禦: patch code, 盡量避免有漏洞的 code
- 王 • Maintaining Access
 - RL ◦ 紀錄探查資訊、留下後門
- 王 • Clearing Tracks
 - 陳 ◦ 消滅足跡
 - BC ◦ 防禦: 盡量讓駭客覺得越麻煩越好(ex. 將 log 記錄起來之後傳到另外一台 server)

HP

真實攻擊案例

- 駭客經由網站找到上傳、寫檔等弱點，植入 Webshell
 - 王 ◦ 連入主機後發現帳號權限不足，從主機內搜尋找可以用的資訊
 - 陳 ◦ 查詢系統可用資訊 / var / log
- 王 • 權限：
 - 發現主機 Kernel 版本過舊，有可提權的弱點
 - 陳 ◦ 撰寫 搜尋 Exploit 攻擊，取得 root 權限
- 王 • 放置後門
 - HP ◦ rc.d
- 王 • 消除足跡
 - HP ◦ ~/.histroy
 - ~/.bash_history
 - A ◦ var/log/*

- 王 攻擊者的思維
 - 情報蒐集
 - 黃 ◦ 尋找，分析漏洞
 - PS ◦ 利用漏洞
 - 達成攻擊目標

王

陳 [whois](#)

- 王 • 查詢管理者資訊
- 陳 • E-mail(寄惡意信件、DNS
- RL • 假如管理者的信件domain與網站同，代表網站可能有mail Service
 - 安全的作法，設定一個mail list取代帳號，避免資訊洩漏

王

陳 Reconnaissance 偵查

- 找出目標的相關資訊，以供日後測試需求
- Footprinting

- Whois
- [Http://archive.org](http://archive.org)

王 NMAP

- -sS/sT : TCP SYN/Connect() scans
- 秋羅 • -p <port ranges>: Only scan specified ports
- A • -A: Enable OS detection, version, detection, script scanning, and traceroute
- 王 • -O: Enable OS detection
- 陳 • <http://nmap.org>
- Open Source 的 Port Scanner，可進行掃描、網路探索、安全稽核等

陳 Gaining Access 取得進入權

- 透過掃描到的目標，進行攻擊取得進入權
- 王 • Password Cracking
 - Brute-force Attack
 - Dictionary Attack
 - Hybrid Attack
- RL ◦ Pre-computed Hashes(rainbow table 彩虹表)
- 王 • Malware
- Toosl: pwdump,

Lab

- 使用 Cain 破解本機密碼
- RL • 破解 Hash(md5, sha1 是不安全的)
 - A ◦ 7ac66c0f148de9519b8bd264312c4d64

王 Maintaining Access

- 利用後門等方式

陳

-
-
-

• 事前預防

- 王 ◦ 滲透測試
- RL
 - 只用工具是cost down的做法
 - 使用工具無法透過漏洞進行更深測的檢測
 - 使用工具無法客制化掃描網段(?)
 - 無法大量測試

- 成本不低，人工測試有其價碼
- 誤報表示只用工具，不了解其結果
- 教育訓練(惡意郵件測試,
- 應變計畫(ISMS, IS27001

王 • 事件發生

- HP
- 資安通報
 - 事件演練
 - 緊急應變
 - 事後調查
 - 事件處理
 - 數位鑑識
 - 復原重建

王 你心目中的滲透測試是什麼？

- 陳
- 使用「滲透測試工具」掃描。
 - 五天可以測試 200 個 IP！

- HP
- 應該兩萬塊可以做完吧？
 - 報告一定要有很多誤報

陳 使用自動化工具檢測

- 王
- 無法依據不同網路架構及情境分析
- 黃
- 自動化工具可能癱瘓受檢伺服器
- HP
- 檢測人員名單

陳 資安顧問人工檢測

- RL
- 網站設定不安全(比如說：INC副檔名未鎖、phpmyadmin未設密
- HP
- 透過公開的資源以及駭客知識庫...

木桶理論 (Find Minimum)

- RL
- 看到有洞就補？
 - 駭客會直接攻打最弱的那一點
- HP
- 提升整體水準而非加強特定部份

秋羅 OWASP Top 10

(https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

- HP
- The Ten Most Critical Web
 - A1 - [Injection](#) ()
 - A2 - [Broken Authentication and Session Management](#) ()
 - A3 - [Cross-Site Scripting \(XSS\)](#) ()
 - A4 - [Insecure Direct Object References](#) ()

- A5 - [Security Misconfiguration](#) ()
- A6 - [Sensitive Data Exposure](#) ()
- A7 - [Missing Function Level Access Control](#) ()
- A8 - [Cross-Site Request Forgery \(CSRF\)](#) (跨站匿名請求) 臺灣相當嚴重
- A9 - [Using Components with Known Vulnerabilities](#) (使用已知漏洞的元件)
- A10- [Unvalidated Redirects and Forwards](#) (使用未驗證的轉址)

陳 Insecure Communication(未加密的網路連線)

- X • 網頁傳送敏感資料時並未使用SSL或其他加密方式

陳 •

陳 Man-In-The-Middle Attack (中間人攻擊)

Cain & Abel (今天不會用QQ)

- RL • Arp Spoofing (挾持gateway測錄資料)
- 預防方式，使用加密連線(具第三方憑證者)

🗨 秋馨 羅 可能會跟skype撞到port

陳 Insecure Communication

- 使用第三方憑證
-
-

Information Leakage and Improper Error Handling

- 網頁應用程式
- RL ○ 錯誤訊息會透漏出使用的framework, 套件, path等訊息
- 應該把錯誤訊息關閉
 - 把錯誤頁面替換

陳 Insuffucient Transport Layer Protection

- 盡可能使用加密連線 (HTTPS)
- Cookie 使用 Secure Flag
-
-
-

J

RL Mozilla Firebox 推薦安裝的套件，或是安裝 [OWASP Mantra](#)

- HP • Cookies Manager+
 - <https://addons.mozilla.org/zh-tw/firefox/addon/cookies-manager-plus/developers>
- 劉 • Tamper Data
 - <https://addons.mozilla.org/zh-tw/firefox/addon/tamper-data/?src=ss>
- HP • POST Data修改 或是 header修改
- RL • Live HTTP Headers ((封包擷取
 - <https://addons.mozilla.org/zh-TW/firefox/addon/live-http-headers/?src=userprofile>
- RL • 修改http header (例如神奇的reffer:127.0.0.1
- HP • Web Developer
 - <https://addons.mozilla.org/zh-tw/firefox/addon/web-developer/?src=search>
- RL • Java Disable, cookie edit, 更改視窗大小
- Hack Bar
 - <https://addons.mozilla.org/zh-tw/firefox/addon/hackbar/?src=ss>
- HP • 輔助攻擊用，md5 sha1 base64 decode
- RL • BurpSuite
 - <https://portswigger.net/burp/downloadfree.html>
- RL 好用工具
 - 1passwd(記住各網站的密碼)
 - adblock(擋廣告)
 - 劉 Cookies Manager+ ((修改Cookie)
 - RL firebug(類似Web Developer)
 - 劉 No Script(跳過驗證功能)

王 Lab1

1. 到一個有 HTTPS 的網站
2. 使用 Cookies Manager 看有無 Secure Flag
3. 把 Flag 取消
4. 打開 Live HTTP Headers
5. 強制使用 http 連線網站
6. 看有無傳送 Cookie (應該不會傳)
- 劉 7. 取消 Secure Flag
8. 再看一次會不會傳

陳 Unvalidated Redirects [Day 6 Web Security](#) and Forwards (Cont.)

- JOYNYCHEN 有沒有人有同時開http & https 的範例網站QAQ
- ROCKEY L 聊天室說plurk
- ИССЛЕДО... XD

王 Metasploit

- www.metasploit.com
- github: <https://github.com/rapid7/metasploit-framework>

Cross-Site Request Forgery(CSRF攻擊)

- 黃 1. GET /csrf.htm (.受害者PC->惡意server)
- 陳 2. (惡意server->受害者PC)
- 黃 3. GET/ send.asp?to=XXX (受害者PC->CSRF server)
- 王 4. Your message was sent!! (CSRF server->受害者PC)
- 確保網站沒有任何可以提供XSS攻擊弱點
- X
- 登入時，加上hash token(每次皆不同)，登出、改密碼需有相同token才有辦法執行
 - <input type="hidden" name="login_token" value="19cc227501c16fd00b34a574b658047c@nuahr2">
 - /logout?token=19cc227501c16fd00b34a574b658047c@nuahr2

- 王茂林 共筆不要吵架 XDDDDDDDDDDDD'
- HSIEH P 中文字超會吵架 QQ
- 秋馨 羅 很多企業網管會把公司所有server的密碼存在一個excel(好像拼所)檔中
- ROCKEY L 再把excel加上密碼就好了阿 XDDD
- AWEIMEOW 然後 excel 的密碼也存在另一個 excel 裡面
- 秋馨 羅 確定不是放便條上?
- XIAM9916... 先寫在筆記本上再貼上比較好，才不會衝突
- HSIEH P 好像不管是 Chrome 還是 Safari 中文字都還是會衝突 QQ
- ALICE C 標題怎麼了QQ

HP 下午

- RL
- 數種題目
 - dvwa不太需要工具，瀏覽器可處理大部份
 - allen大大有一個可以打的系統
 - 有一個VM，未知系統，目標拿root
- HP
-

王 Failure to Restrict URL Access

- 網頁沒有權限控管
 - 修改管理介面、修改資料頁面
- RL
- /admin /backup /logs /phpinfo.php /~ /.bak
- 王 HTTP Service 限制 IP

HP Security Misconfiguration

- 密碼沒加密
-

陳 HTTP TRACE Method

- HTTP Server 的設定未將不該開放的 method 關閉，如 TRACE / TRACK / PUT / DELETE 等。建議檢查後直接關閉。
- HP
- TRACE 最為常見，攻擊者可以利用 TRACE 來獲取設定 HTTP Only 屬性 Cookie，進一步搭配 XSS 攻擊竊取使用者帳號。
- P
- 403代表有該目錄但是沒有權限讀取，404代表沒有該目錄

HP Insecure Direct Object References (IDOR) - 不安全的直接存取物件

- 陳
- 攻擊者直接利用網頁應用程式本身的讀取功能，任意存取檔案或重要資料

HP 例如：

- <http://example.com/news.php?lang=en>
 - en 為語系檔案

RL 可能寫法為 `import $_GET[lang]`，所以可以任意讀檔

- HP
- <http://example.com/news.php?lang=../../../../../../etc/passwd>
 - <http://example.com/news.php?lang=/etc/passwd>

BC

- windows路徑不分大小寫

HP

- 想知道其他子網站可以看 `/etc/apache2/apache2.conf`

P 可以將php code灌進log，再去讀取檔案執行

王 防禦措施

Cross-Site Scripting

- RL
- 反射式，一次觸發，直接秀出
 - 儲存式，長久存在，瀏覽時觸發

P filter input

escape output

D `<script>`

```
document.write('')
</script>
```

陳 防禦手法

PS 檢查輸入數值，使用白名單機制過濾，而不單只是黑名單

陳 XSS Prevention Rules

林 ([https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet#XSS_Prevention_Rules](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet#XSS_Prevention_Rules))

陳 Content Security Rules

CSP 類別

CSP 支援

CSP 1.0 作用

載入來源白名單

禁止 (cat ! !

XSS Worst Practice 1

取代字串 遇到 <script> or </script> 就取代成空字串

- 輸入 <sc<script>ript> --> 取代完剩下 <script>

ИССЛЕДО... 古代還有一個例子 把 script 濾掉
所以 <script> 會變成 <>
然後駭客就可以 <scrscrip<script>ript> ==> <script> (done

- 王
- XSS Shell
 - BeEFc

ИССЛЕДО... 沒有下文了!?

HSIEN P 因為機器掛了 (?

ROCKEY L 講師說機器被改IP

ИССЛЕДО... XD

可以改玩 <http://demo.testfire.net/bank/login.aspx>

IBM提供的網站

<http://webgoat.github.io/> 也不錯玩

林 講師提供練習：10.75.3.50

J <http://xss-quizz.int21h.jp>

BC <https://escape.alf.nu>

<http://prompt.ml/0>

陳 Injection (注入)

```
$str = "SELECT * FROM Users WHERE Username='" . $user . "' AND  
Password='" . $Pass . "'";
```

```
SELECT * FROM Users WHERE Username=' ' OR 1=1 --' AND  
Password='oxoxox'
```

```
SELECT * FROM Users WHERE Username='admin' --' AND Password=''
```

攻擊流程

E • 找出未保護變數, 作為注入點

陳 • 猜測完整 SQL 語句並嘗試插入

王 • 猜測欄位數、資料表名稱、SQL版本等資訊

陳 • 搭配 UNION 等方式撈取資料庫資料

```
SELECT ?,? FROM ? WHERE id(?)='3' UNION SELECT user(), version()#'
```

林育慈 <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet> 搭配使用

BC • 可用 order by [column] 來猜測欄位數量

E • 之後再用UNION來撈資料

ОСЛЕДО... [sql injection 好難學. 可以直接用穿山甲嗎!? \(XD](http://resources.infosecinstitute.com/best-free-and-open-source-sql-injection-tools/)
<http://resources.infosecinstitute.com/best-free-and-open-source-sql-injection-tools/>

J VM打法

- fckeditor

林 • 看到 userfiles/ 就有可能, 可以嘗試這個方式

王 • upload web shell

- phpmyadmin

王 • default user/password

林 • into outfile '/var/www/xxx.php'

- wordperss 2.0.2

王 • upload shell

NYNYCHEN 橘語錄:

Q : 好奇 [@orange 8361](#) 是走哪條路線啊?

A : fckeditor 最快，常_所以路徑有背下來

Q : fckeditor 在iis7.5 也可以用嗎?

A : 看版本，2.6.4 以下有機會

dialog/fck_about.html 可以看版本

Q : 想問一下再終端機那邊是怎麼提權成root的?

A : kernel exploit

Q : 所以phpmyadmin 是直接內建功能上傳?

A : PHPMYADMIN , into outfile '/var/www/xxx.php'

mysql 有 root 有 FILE_PRIV 皆可

但是 web root 權限有設

但你可以先寫到 userfiles

一樣可以解

Q : getshell 之後除了找 exploit 之外還有其他變成 root 的方法嗎 XD

A : 看伺服器配置

Q : 橘子是用哪一個 exploit Q_Q

A : udev

不過要自己改 payload

因為他環境怪怪