「政府資通安全防護巡迴研討會」

網路應用服務資訊安全

*Web AP*安全建議

行政院國家資通安全會報
技術服務中心
鍾榮翰顧問
barbet@icst.org.tw

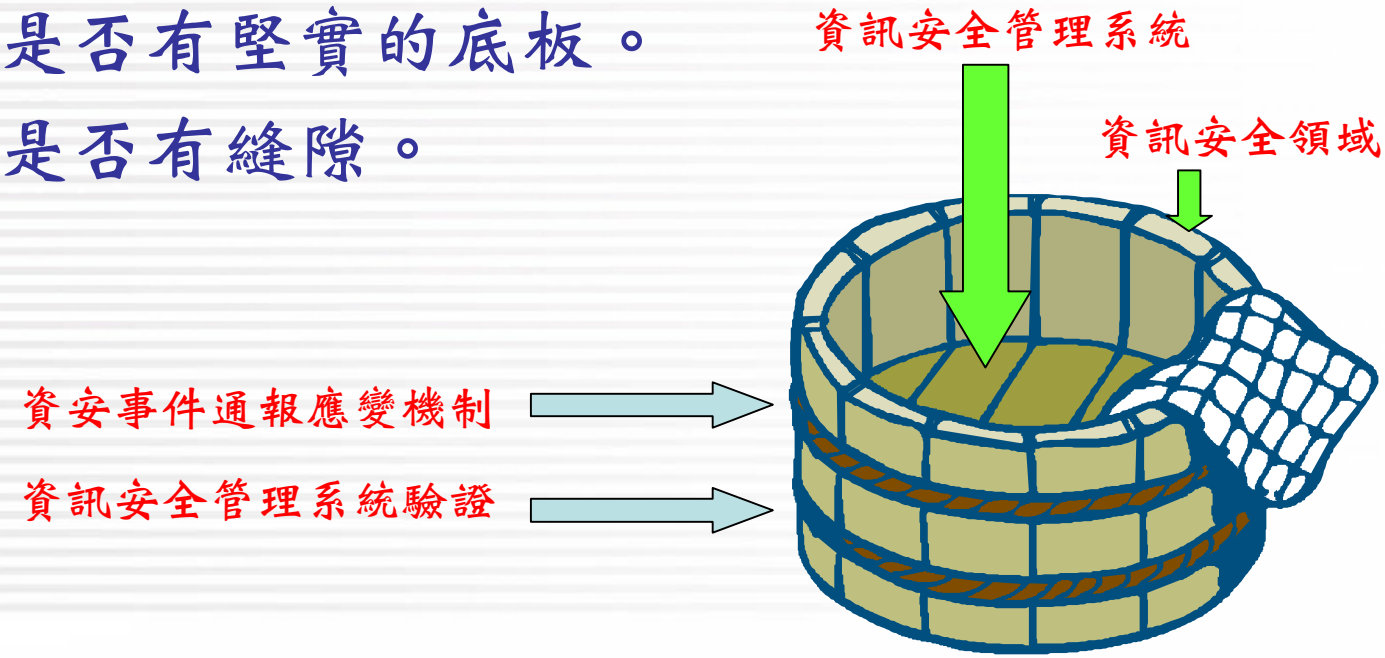
96年3月27日

大　　綱

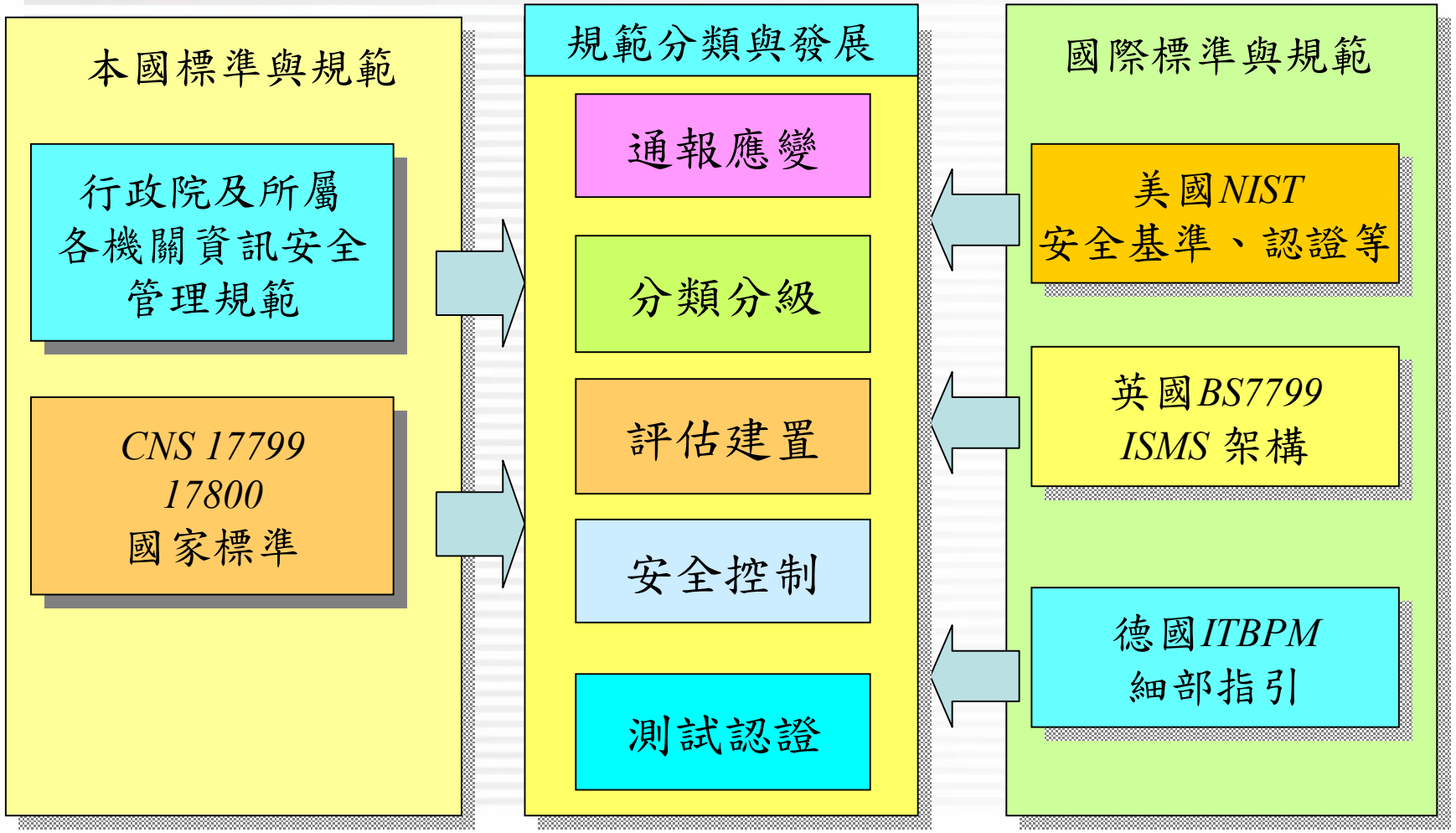
- 政府資安作業共通規範發展概況
- Web 應用程式安全
- 實務案例分享

資訊安全管理—木桶理論新解

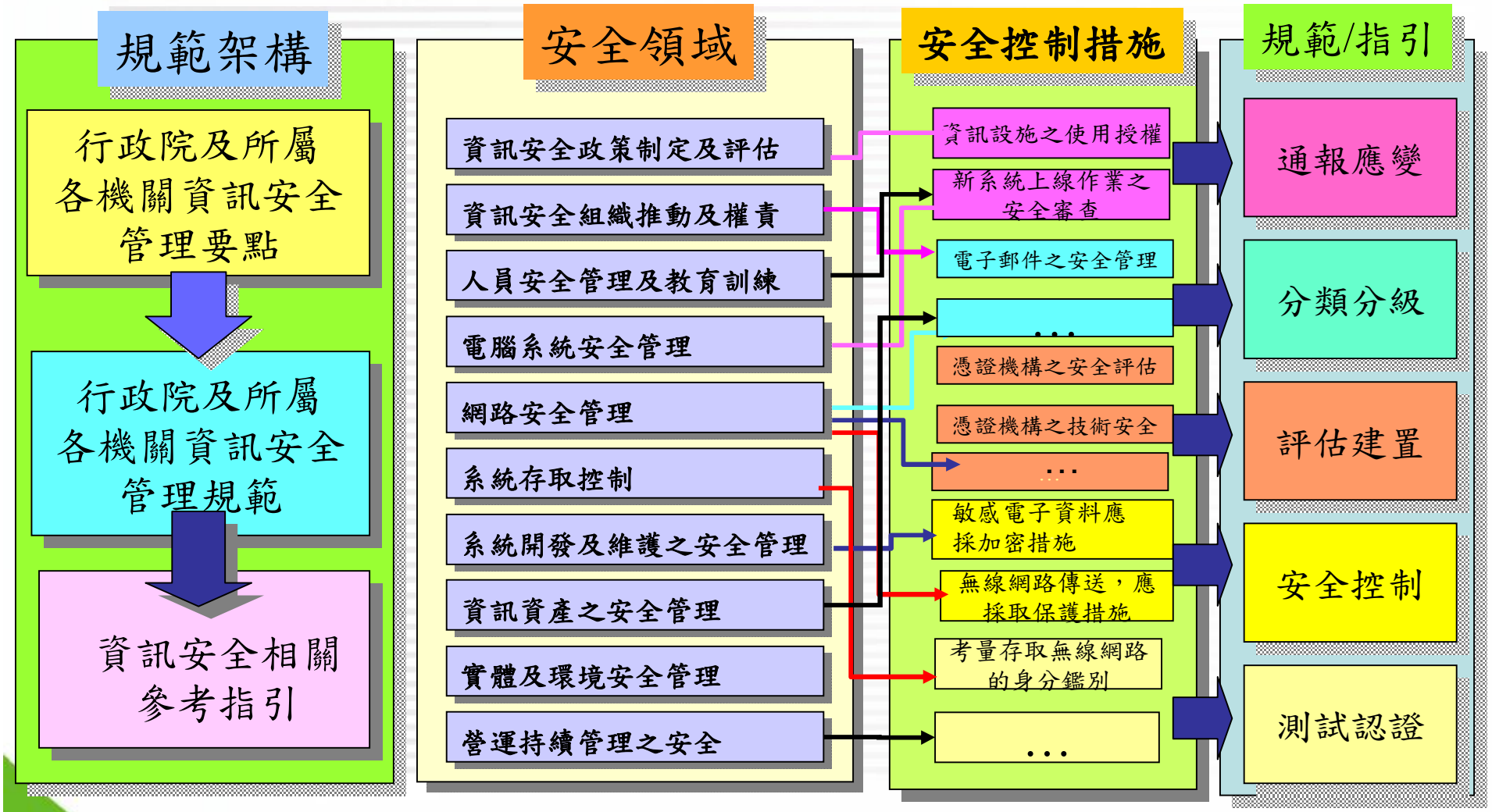
- 一個由許多塊長短不同的木板箍成的木桶，決定其容水量大小的並非是其中最長的那塊木板或全部木板長度的平均值，而是取決於其中最短的那塊木板。
- 這個木桶是否有堅實的底板。
- 木板之間是否有縫隙。



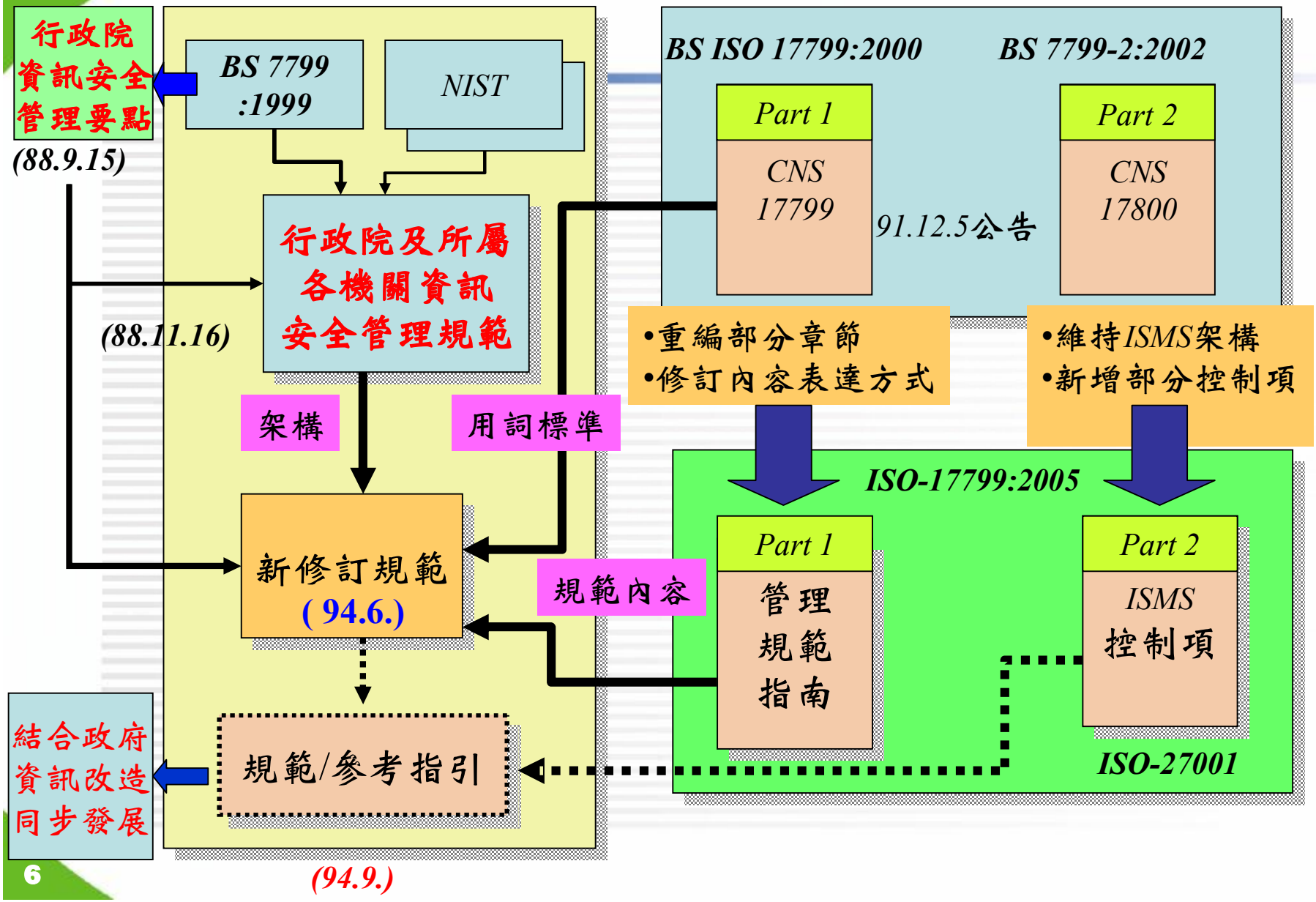
資安規範藍圖發展架構


本國標準與規範
行政院及所屬
各機關資訊安全
管理規範
CNS 17799
17800
國家標準
規範分類與發展
通報應變
分類分級
評估建置
安全控制
測試認證
國際標準與規範
美國NIST
安全基準、認證等
英國BS7799
ISMS 架構
德國ITBPM
細部指引

資安規範藍圖發展程序


規範架構
行政院及所屬各機關資訊安全管理要點
行政院及所屬各機關資訊安全管理規範
資訊安全相關參考指引
安全領域
資訊安全政策制定及評估
資訊安全組織推動及權責
人員安全管理及教育訓練
電腦系統安全管理
網路安全管理
系統存取控制
系統開發及維護之安全管理
資訊資產之安全管理
實體及環境安全管理
營運持續管理之安全
安全控制措施
資訊設施之使用授權
新系統上線作業之安全審查
電子郵件之安全管理
...
憑證機構之安全評估
憑證機構之技術安全
...
敏感電子資料應採加密措施
無線網路傳送，應採取保護措施
考量存取無線網路的身分鑑別
...
規範/指引
通報應變
分類分級
評估建置
安全控制
測試認證

行政院資安管理規範修訂背景與構想



機密等級： C

訂定資安作業共通規範指引

FY94

- 資安事件通報應變作業規範
- 資訊安全責任等級分級作業辦法
- 資訊安全產品選擇參考指引
- 電子資料保護參考指引
- 政府資訊作業委外安全參考指引

FY95

- 資安事件應變作業參考指引
- 資訊系統風險評鑑參考指引
- 無線網路安全參考指引
- 電子身份認證參考指引
- Web應用程式安全參考指引
- VPN安全參考指引
- 實體隔離作業安全參考指引
- 作業系統安全參考指引
- 防火牆安全參考指引
- 電子郵件安全參考指引
- 入侵偵測/預防系統安全參考指引

FY96

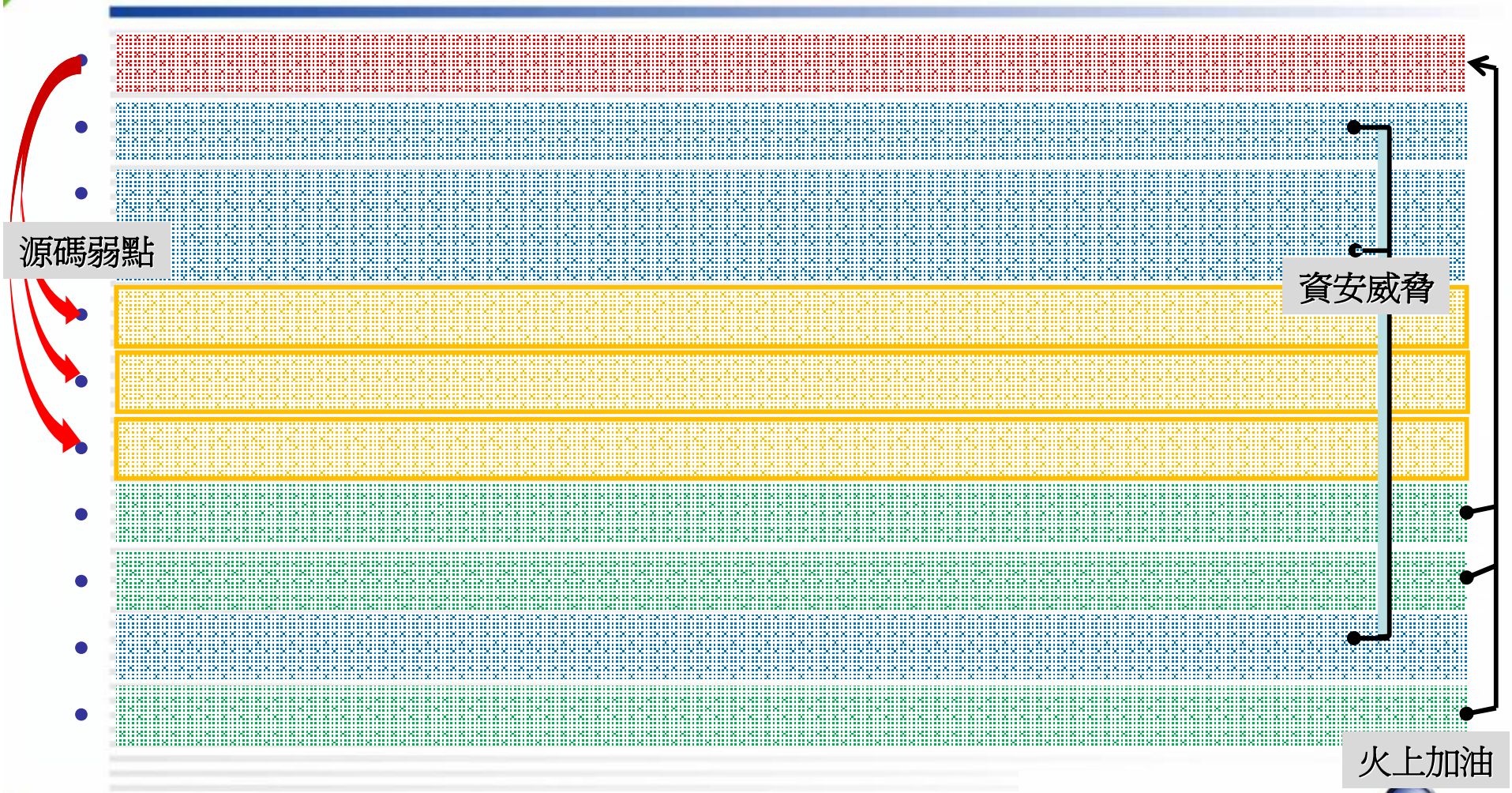
- 資訊系統持續運作參考指引
- 電腦鑑識參考指引
- 資訊與資訊系統分類參考指引
- 安全衝擊分級參考指引
- 資訊系統發展生命週期安全參考指引
- 資訊安全管理稽核作業規範
- 資訊安全管理系統建置參考指引
- 可攜式媒體安全參考指引
- 惡意程式防護安全參考指引
- 網站服務安全參考指引
- 系統弱點修補參考指引

FY97

- 電腦稽核作業參考指引
- 資訊系統互連安全參考指引
- 資安稽核評量作業參考指引
- 資訊安全教育訓練參考指引
- VOIP系統安全參考指引
- 公開金鑰基礎建設使用安全指引
- 金鑰管理安全參考指引
- 資訊系統安全測試參考指引
- 網路安全測試參考指引
- 資訊系統認證授權作業規範

Web應用程式安全參考指引(草案)

OWASP 2004 TOP10資安漏洞列表



資料來源：

OWASP Taiwan
http://www.owasp.org.tw

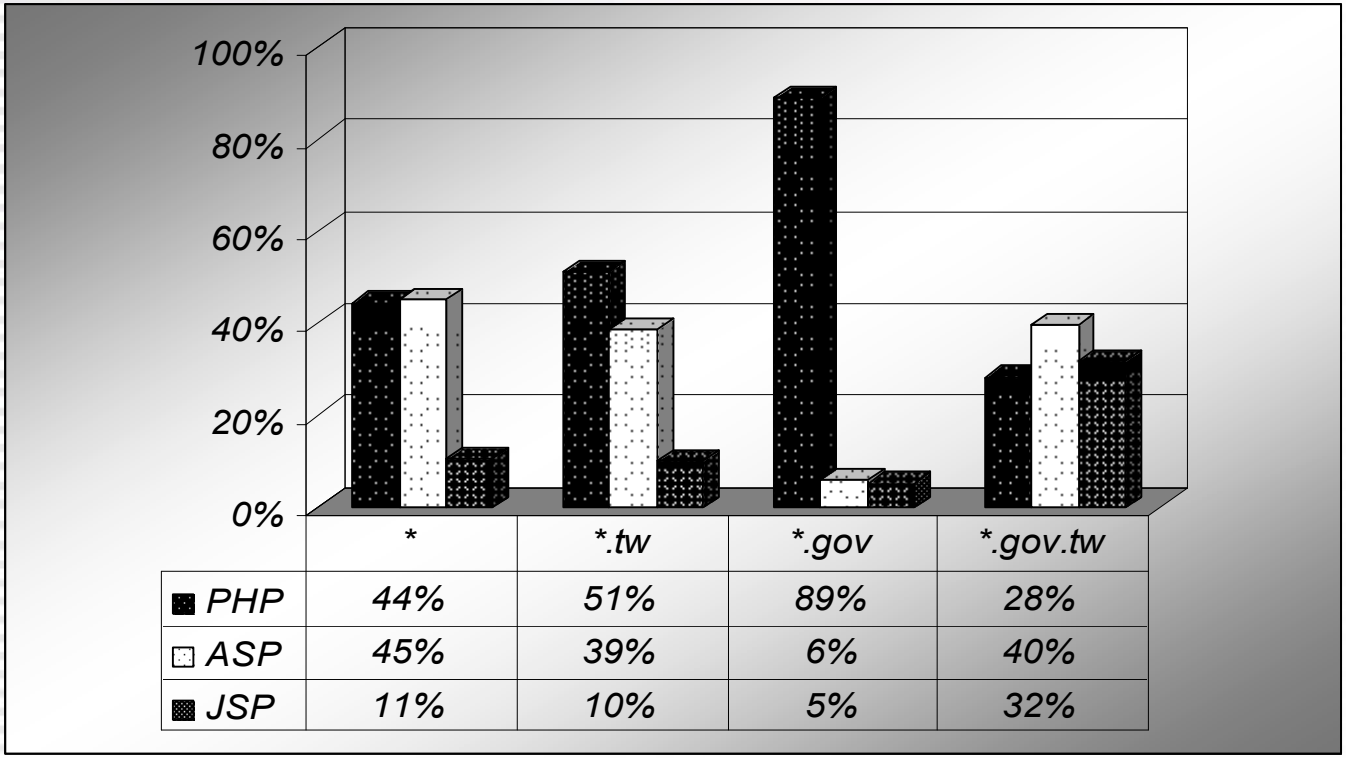
OWASP 2007 TOP 10最新修訂

源碼弱點

火上加油

各種Web開發語言使用比例

- 全球*PHP*與*ASP*之比例差不多
- 在政府機關(構)之網站，美國廣泛採用*PHP*，而台灣則是*ASP*高於其他語言



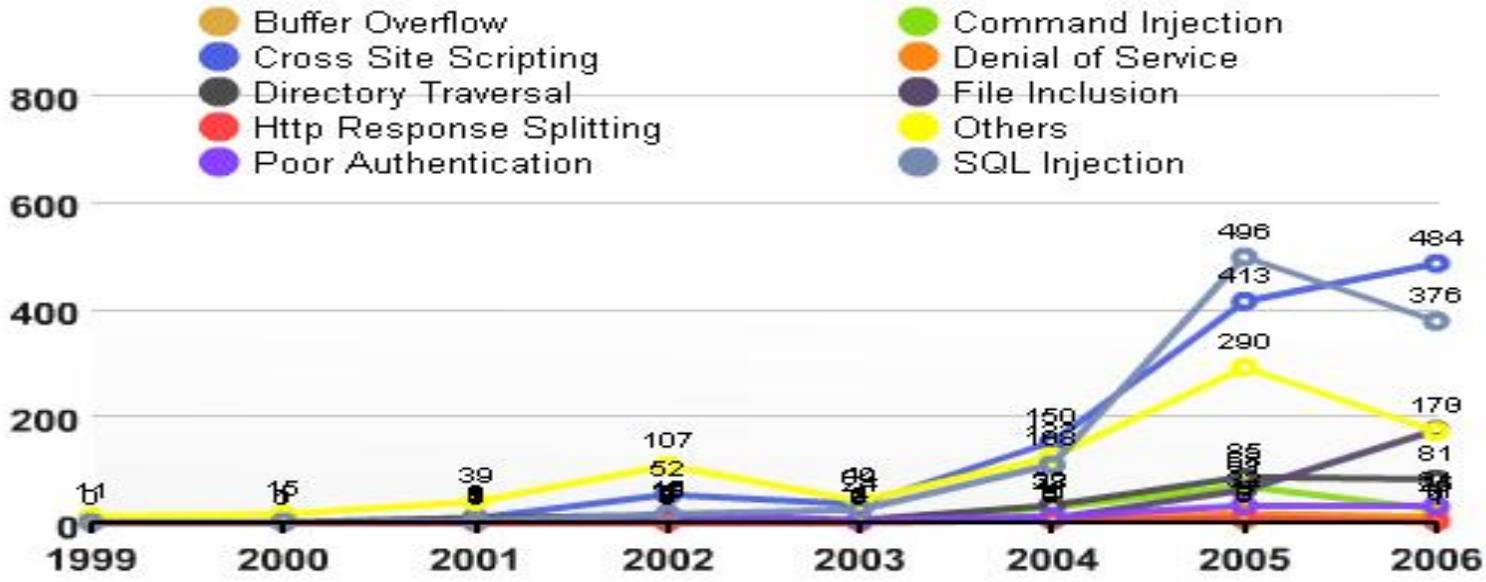
	*	*.tw	*.gov	*.gov.tw
PHP	44%	51%	89%	28%
ASP	45%	39%	6%	40%
JSP	11%	10%	5%	32%

資料來源：Google,Dec.2006

歷年CVE脆弱性暴露數量與分類

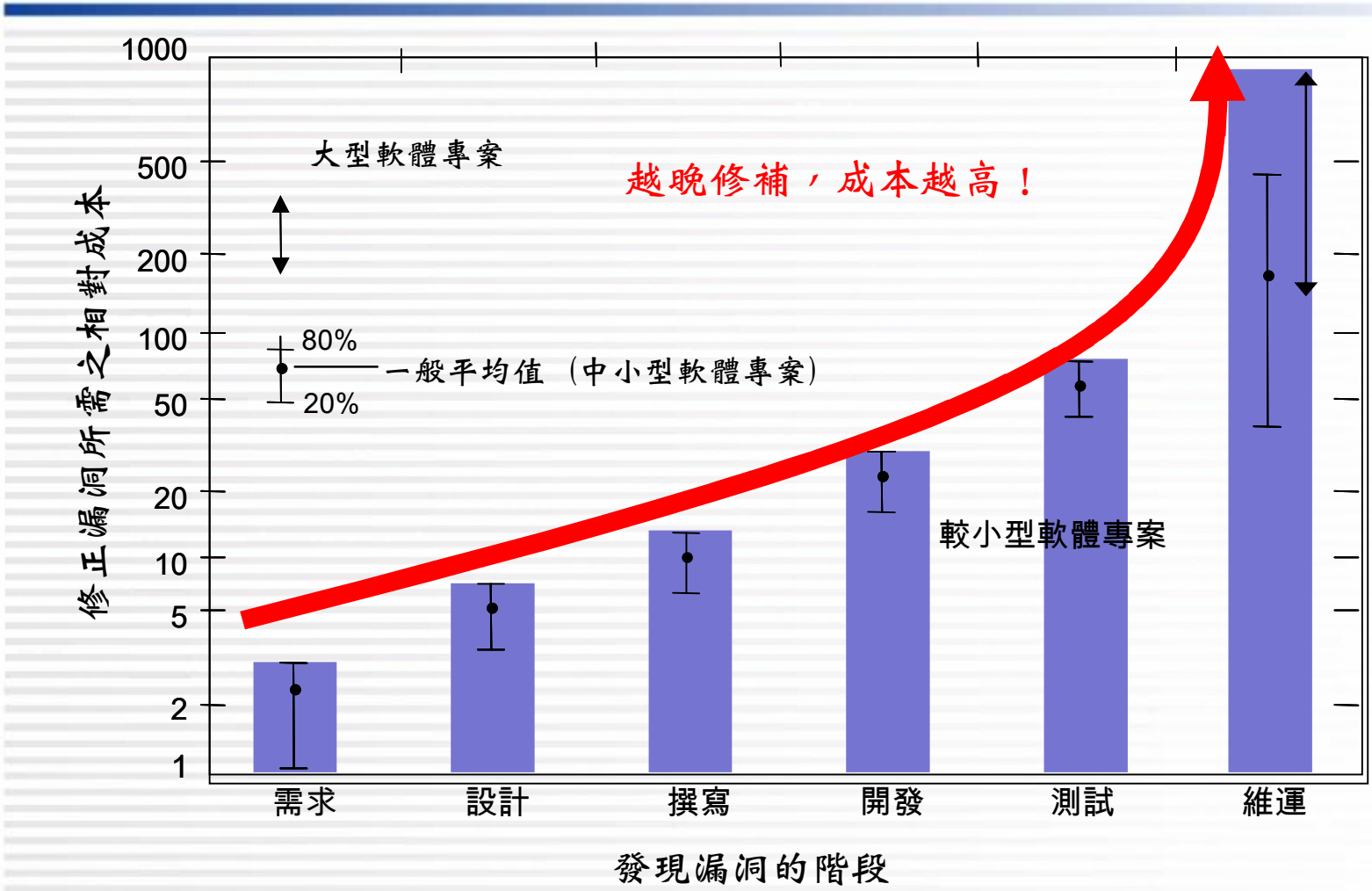
Vulnerability Database

Armorize Vulnerability Database is a comprehensive library that allows you to effectively search web application vulnerability and automatically illustrates your search result in real time.

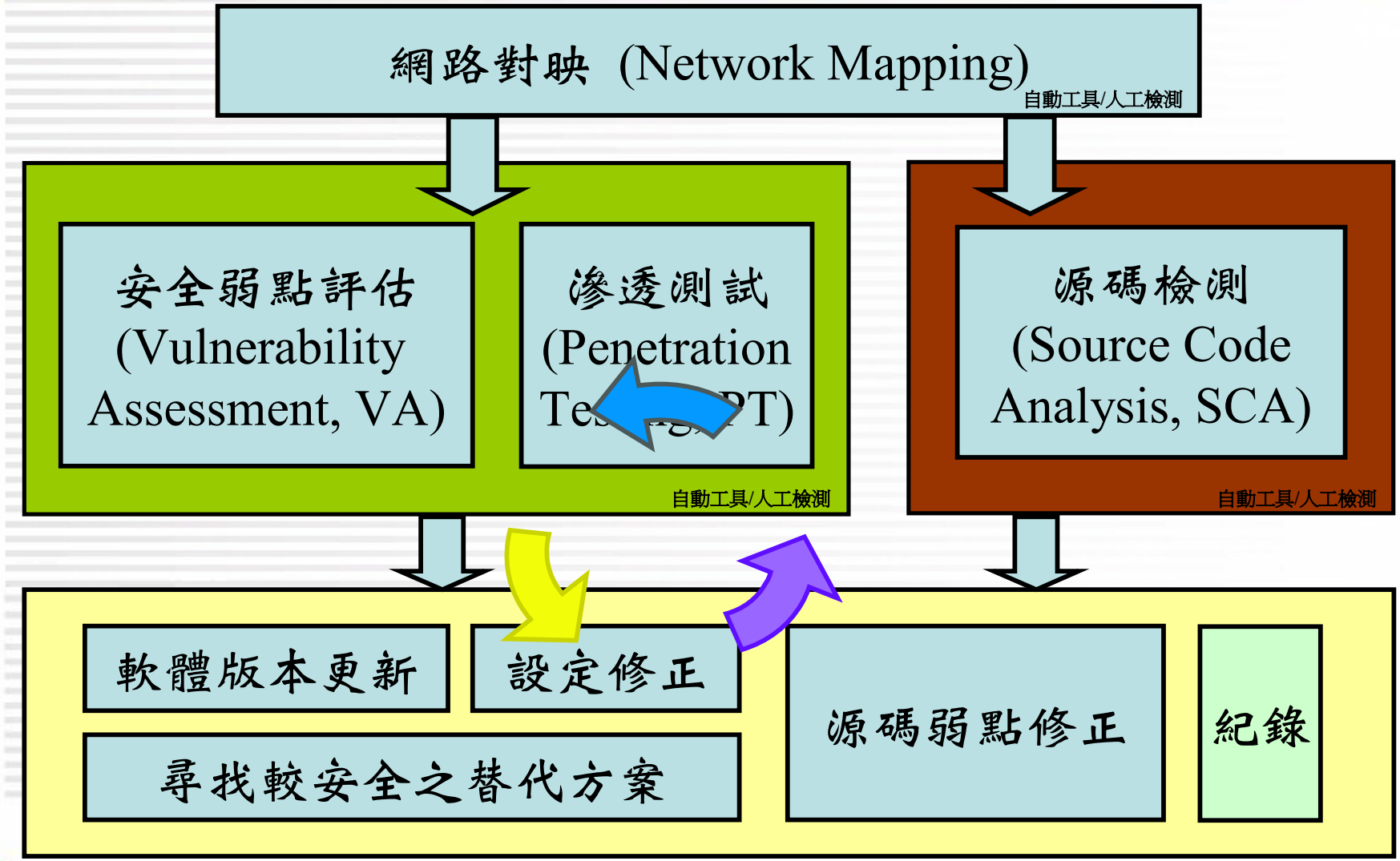


資料來源：

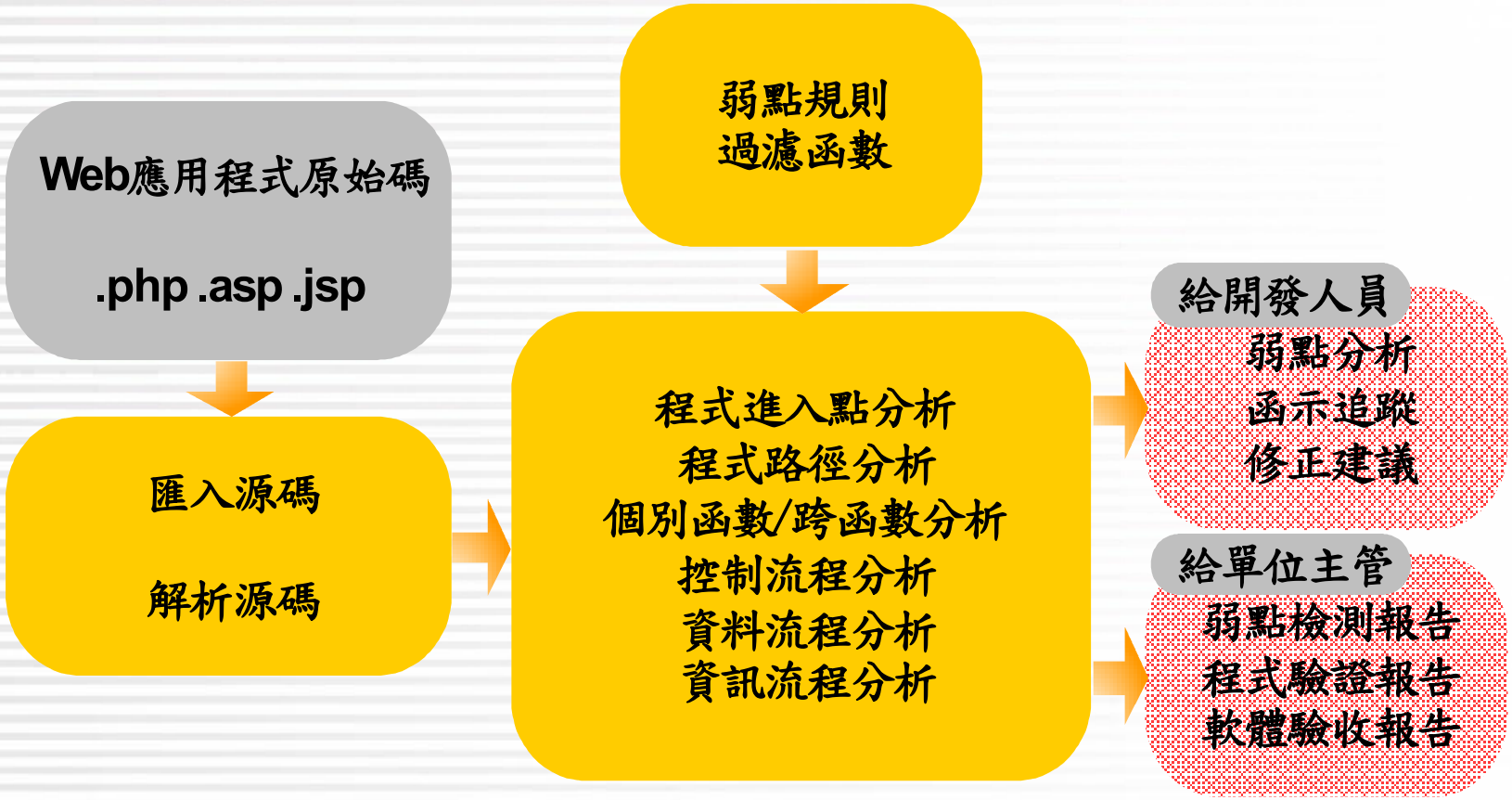
修正漏洞之相對成本


1000
500
200
100
50
20
10
5
2
1
修正漏洞所需之相對成本
大型軟體專案
80%
一般平均值（中小型軟體專案）
20%
越晚修補，成本越高！
較小型軟體專案
需求
設計
撰寫
開發
測試
維運
發現漏洞的階段

如何實現Web安全

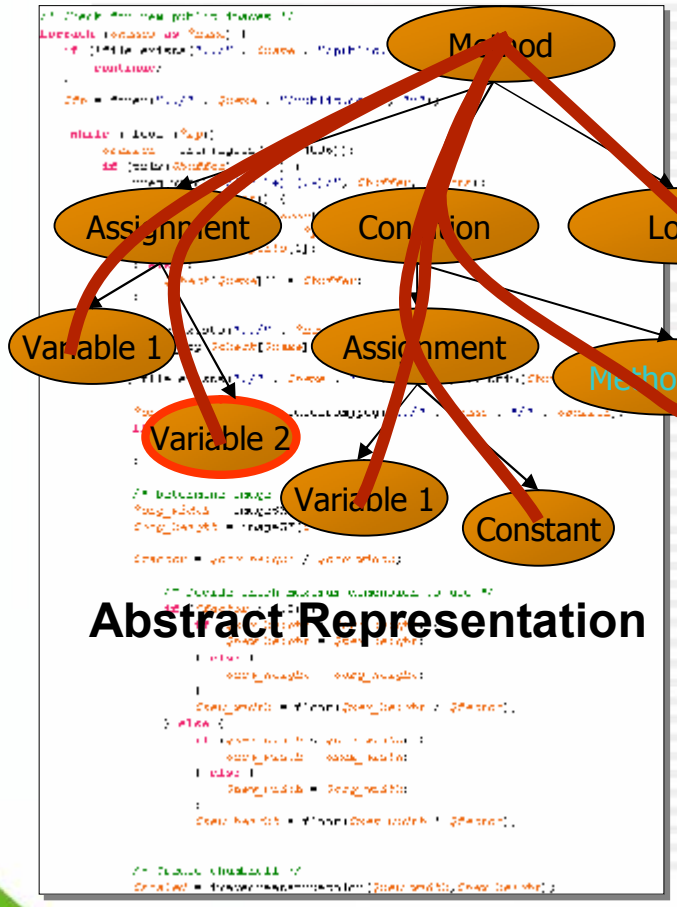

網路對映 (Network Mapping)
自動工具/人工檢測
安全弱點評估 (Vulnerability Assessment, VA)
滲透測試 (Penetration Test, PT)
自動工具/人工檢測
源碼檢測 (Source Code Analysis, SCA)
自動工具/人工檢測
軟體版本更新
設定修正
尋找較安全之替代方案
源碼弱點修正
紀錄

軟體驗證與自動靜態分析技術

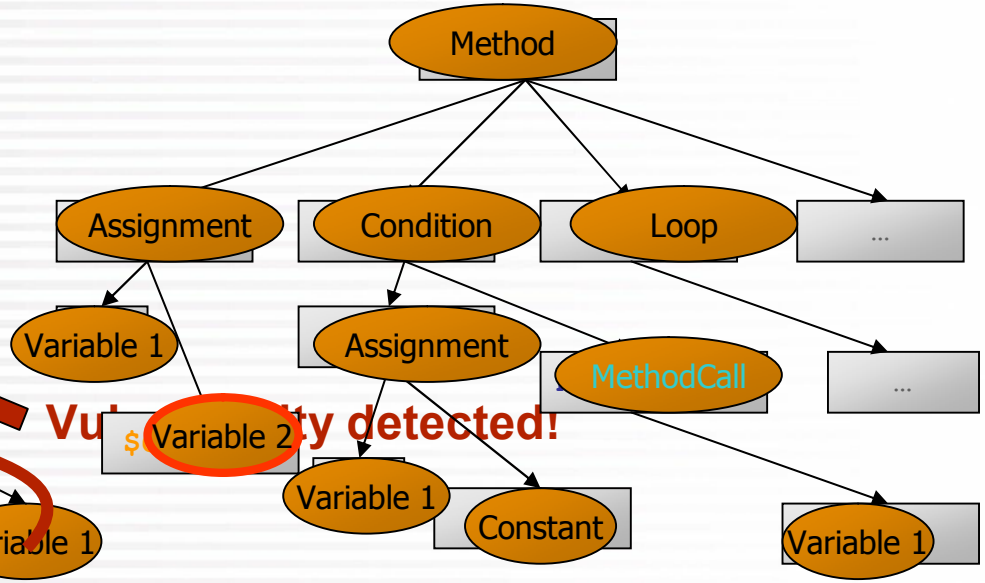


技術概觀

Source Code



Abstract Syntax Tree



資料來源：

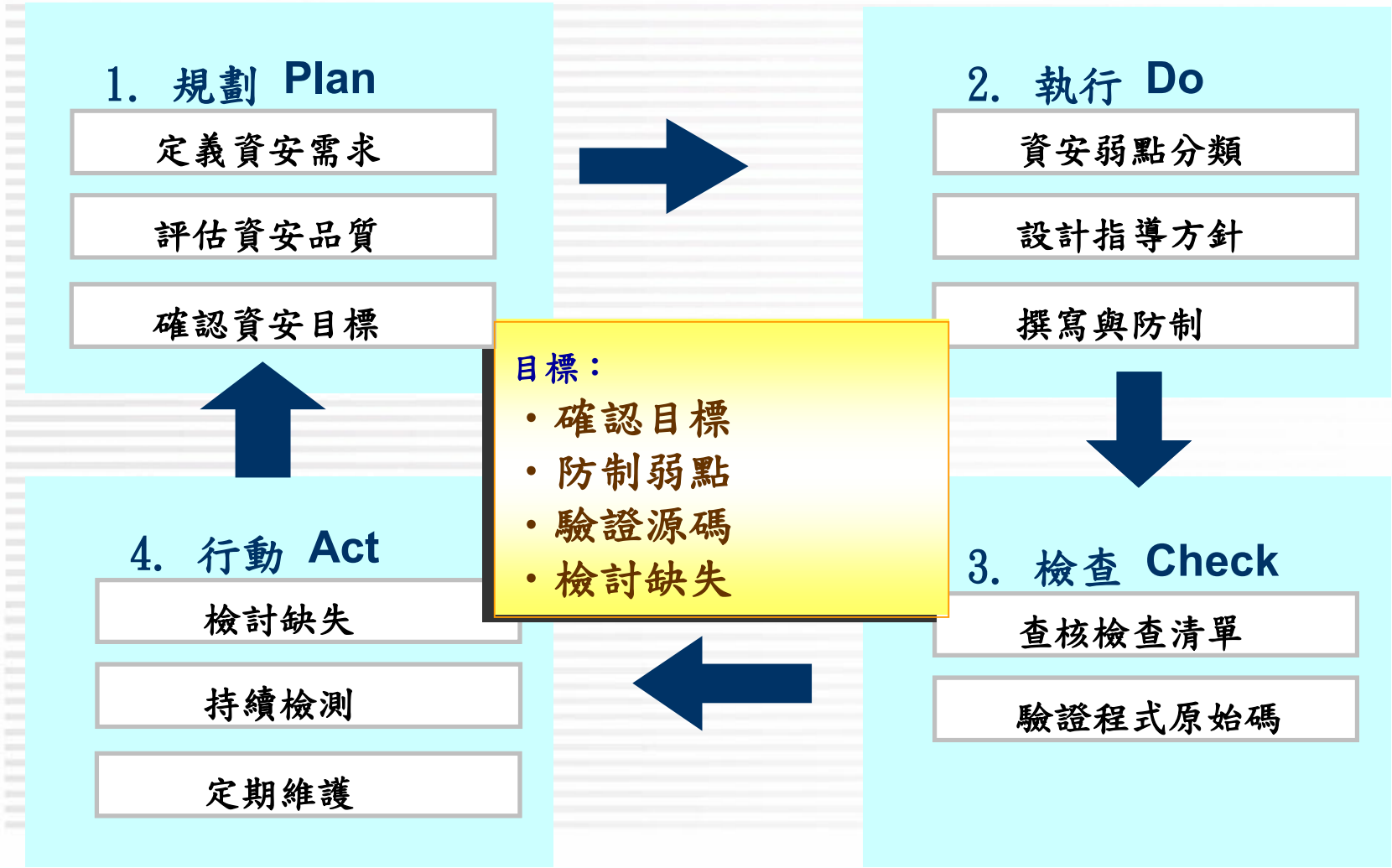
Web應用程式安全解決方案部署原則

- 保護最薄弱的環節
  - Web服務必須對外開放，無法躲在防火牆之後
  - 應該首先消除最嚴重的威脅，而不是最容易減輕的威脅
  - 掌握未知漏洞之先機
- 採用縱深防禦
  - 防禦機制需具不重疊的安全性功能
  - 目前普遍缺乏Web應用程式源碼之防護
- 釐清因果關係
  - 成本導向的委外專案無法確保軟體安全品質
  - 明瞭執行操作所必需的最少存取權，並且掌握執行結果
  - 安全性驗收之落實
- 遵循簡單性
  - 勉強實作複雜而花俏的專案，往往會違反簡單性原則
  - 委外案之驗收

實體隔離技術架構示意圖

存取控制(Access Control)

管理程序流程架構

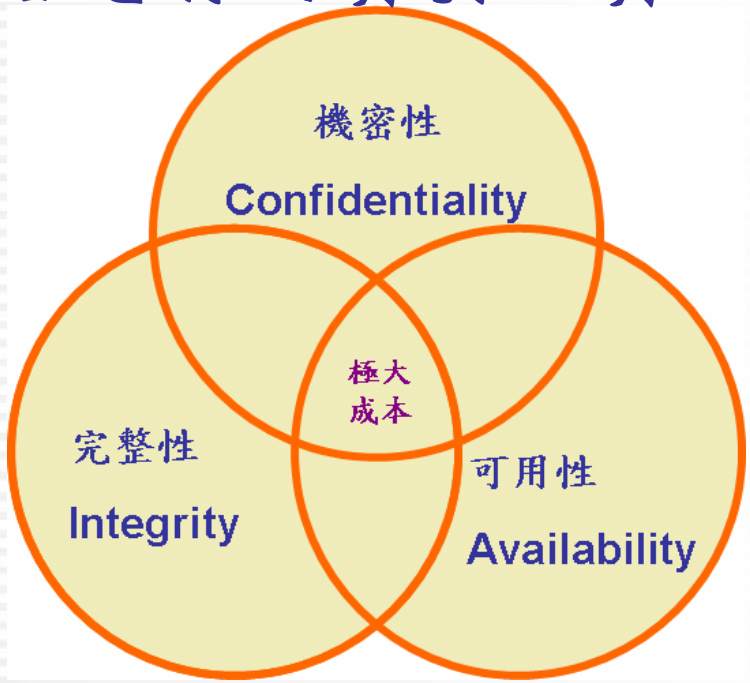

1. 規劃 Plan
定義資安需求
評估資安品質
確認資安目標
2. 執行 Do
資安弱點分類
設計指導方針
撰寫與防制
3. 檢查 Check
查核檢查清單
驗證程式原始碼
4. 行動 Act
檢討缺失
持續檢測
定期維護
目標：
• 確認目標
• 防制弱點
• 驗證源碼
• 檢討缺失

3.1 規劃

- 3.1.1定義資安需求
- 3.1.2評估資安品質
- 3.1.3確認資安目標

評估資安品質

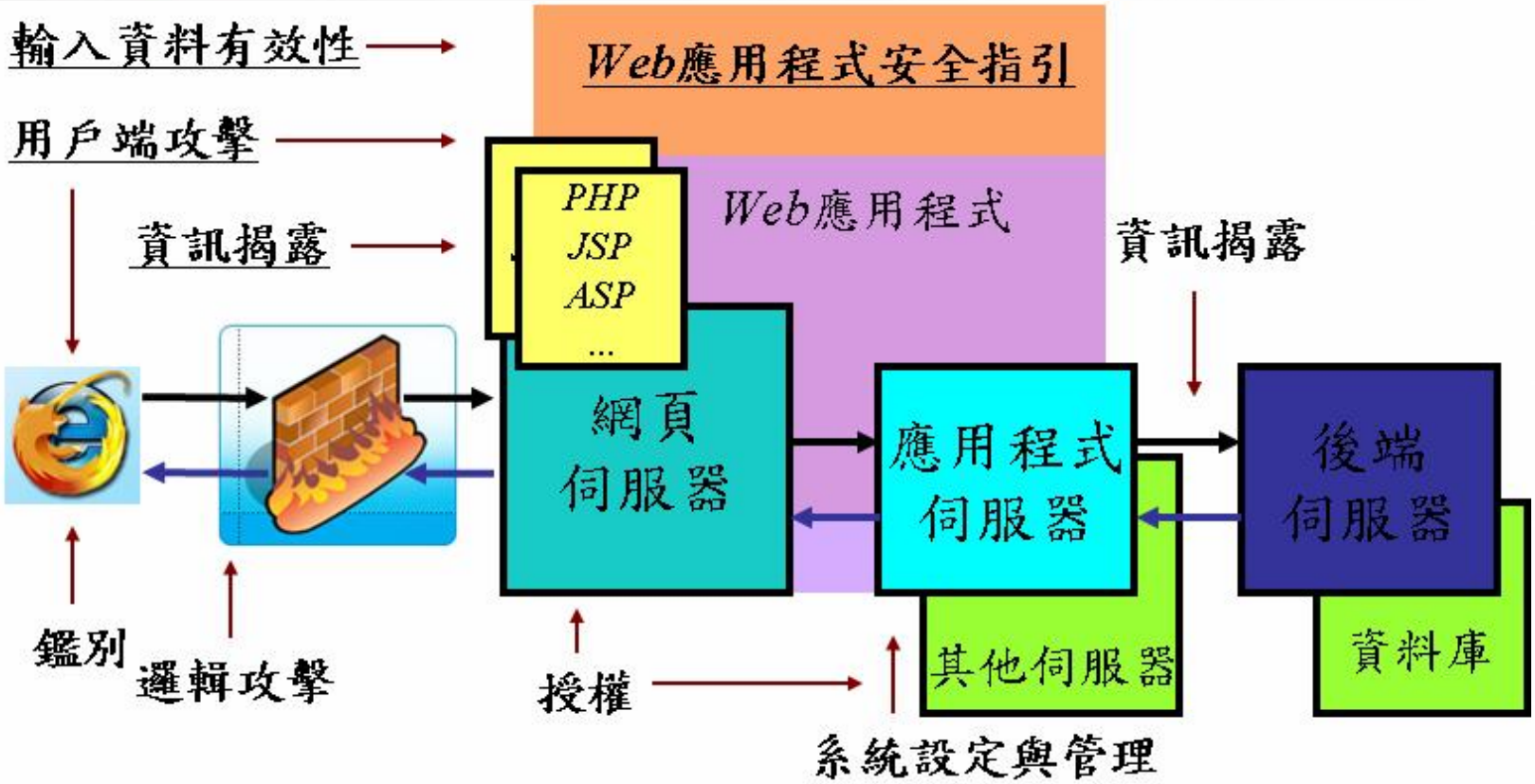
- 當被操作的程式或系統在面對來自周遭環境的資安威脅時，必需具有的安全性有哪些，同時又需要符合怎樣的資安品質



3.2 執行

- 3.2.1 資安弱點分類
- 3.2.2 設計指導方針
- 3.2.3 撰寫與防制

設計指導方針


輸入資料有效性
用戶端攻擊
資訊揭露
Web應用程式安全指引
PHP
JSP
ASP
...
Web應用程式
資訊揭露
網頁
伺服器
應用程式
伺服器
後端
伺服器
其他伺服器
資料庫
鑑別
邏輯攻擊
授權
系統設定與管理

撰寫與防制

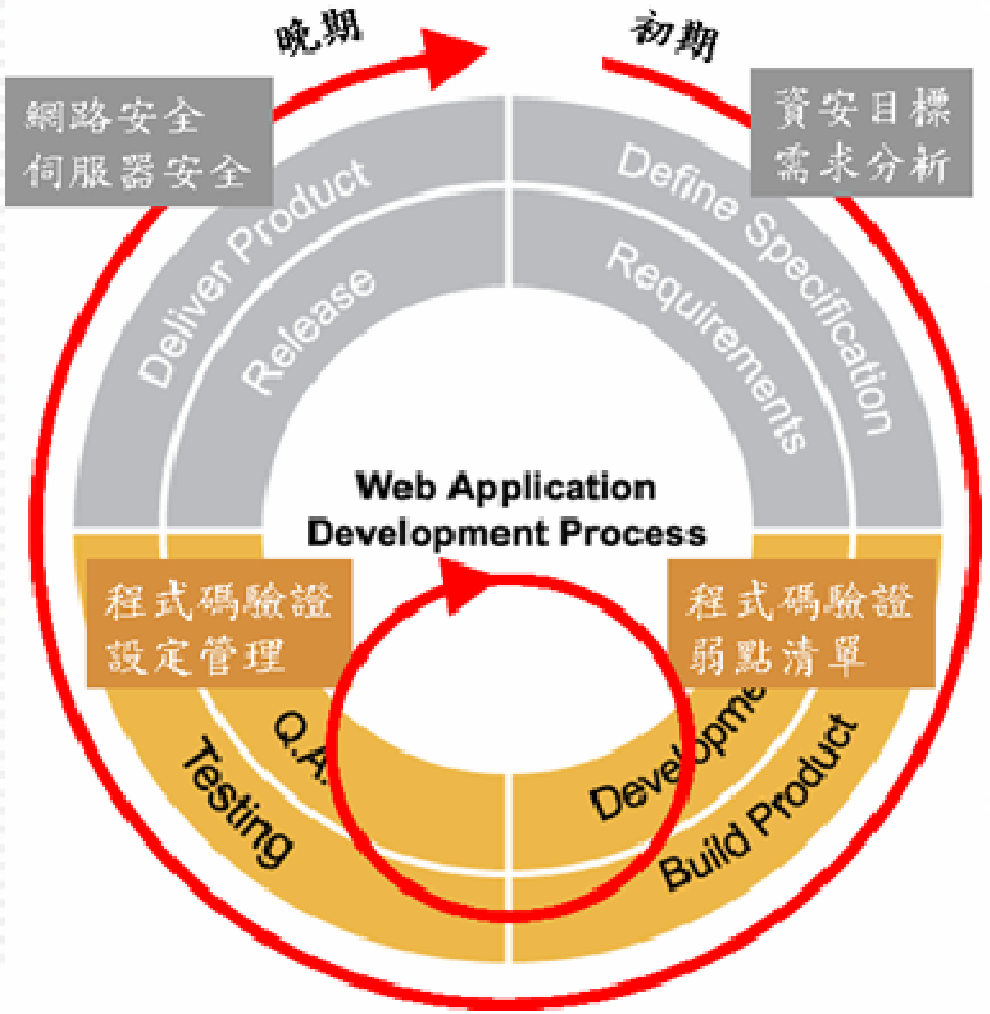
- 未經驗證的輸入資料
  - 資料形式(字串、整數...等)
  - 允許使用的字元集
  - 最短與最長的字串長度
  - 是否允許空字串(*NULL*)
  - 使否允許資料複製
  - 數字範圍
  - 特定的合法數值
  - 特定的模式(規則表示法)

3.3 檢查

- 3.3.1 查核檢查清單
- 3.3.2 檢測程式原始碼

檢測程式原始碼

- 步驟1
  - 資安目標、需求分析
- 步驟2
  - 程式碼驗證搭配弱點清單
- 步驟3
  - 程式碼驗證搭配設定管理
- 步驟4
  - 網路安全、伺服器安全



3.4 行動

- 3.4.1 發現並修正缺失
- 3.4.2 持續的檢測
- 3.4.3 定期的維護

Web安全網路資源

- OWASP (開放Web軟體安全計畫)
  - http://www.owasp.org
- OWASP Taiwan 台灣分會
  - http://www.owasp.org.tw
- WASC (Web軟體安全協會)
  - http://www.webappsec.org/
- 政府資安作業共通規範網站
  - http://www.giscc.org.tw

OWASP（開放Web軟體安全計畫）

OWASP (開放Web軟體安全計畫)

有關OWASP

OWASP (開放Web軟體安全計畫 - Open Web Application Security Project - http://www.owasp.org/) 是一個開放社群、非營利性組織，目前全球有82個分會近萬名會員，其主要目標是研議協助解決Web軟體安全之標準、工具與技術文件。美國聯邦貿易委員會(FTC)強烈建議所有企業需遵循OWASP所發佈的十大Web弱點防護守則，美國國防部亦列爲最佳實務，國際信用卡資料安全技術PCI標準更其列爲必要元件。目前OWASP有30多個進行中的計畫，包括最知名的 OWASP Top 10 (十大Web弱點)、WebGoat(代罪羔羊練習平台、安全PHP/Java/ASP.Net等計畫，針對不同的軟體安全問題在進行討論與研究。

OWASP 為非營利機構，致力於提升全球Web軟體安全品質。

OWASP Taiwan 台灣分會正進行OWASP Top 10中文化，
現免費招募會員，贈自由軟體光碟

http://www.owasp.org/index.php/Taiwan
http://www.owasp.org.tw

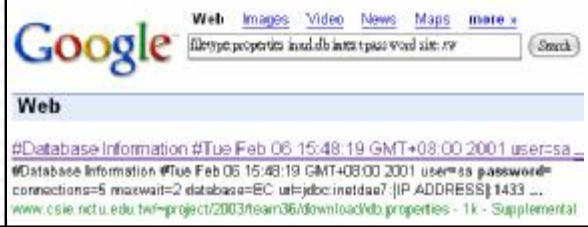
推薦的Web安全工具(一)

項目 \ 工具	種類	用法與效果	下載
Nmap	Network Mapping	Linux工具,可偵測作業系統版本,網路服務, 防火牆等設定	http://www.insecure.org/nmap
Nessus	VA	Linux工具,可執行作業系統弱點偵測,模擬攻擊	http://www.nessus.org/
Nikto	VA, PT	Perl程式,可執行弱點偵測與滲透測試	http://www.cirt.net/code/nikto.shtml
Wikto	VA, PT	整合Nikto與Google搜尋等功能	http://www.sensepost.com/research/wikto
N-Stalker (free edition)	PT	Win32滲透測試工具(免費下載)	http://www.nstalker.com/
Syhunt Sandcat	PT	Win32滲透測試工具(免費下載)	http://www.syhunt.com/section.php?id=sandcat

推薦的Web安全工具(二)

項目 \ 工具	種類	用法與效果	下載
LiveHTTP Headers	PT輔助工具	HTTP Proxy Firebox 外掛工具	http://Livehttpheaders.mozdev.org
Tamper Data	PT輔助工具	HTTP Proxy Firebox外掛工具	http://tamperdata.mozdev.org
TamperIE	PT輔助工具	HTTP Proxy IE外掛工具	http://www.bayden.com
IEWatch	PT輔助工具	HTTP Proxy IE外掛工具	http://www.iewatch.com
Firebug	PT輔助工具	Firebox外掛工具,可用於JavaScript程式碼除錯, Ajax指令觀察	https://addons.mozilla.org/firefox/1843/

推薦的Web安全工具(三)

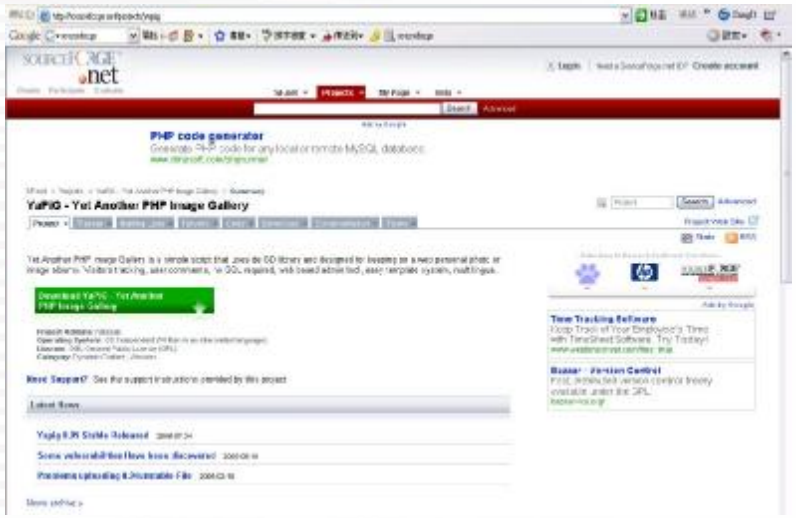
項目 \ 工具	種類	用法與效果	下載
Burp Suite	PT輔助工具	滲透測試工具，HTTP Proxy, Spider	http://Portswigger.net
Paros Proxy	PT輔助工具	獨立的HTTP Proxy	http://www.parosproxy.org
OWASP WebScarab	PT輔助工具	獨立的HTTP Proxy	http://www.owasp.org
Google	PT輔助工具	filetype:properties inurl:db intext:password	http://www.google.com/search?hl=en&q=[弱點特徵參數]+site%3A[目標網址] 
ModSecurity	應用程式防火牆	為Apache外掛，需替應用程式的每一支程式設定規則	http://www.modsecurity.org/

檢測範例：熱門PHP線上畫廊套件

YaPiG - Yet Another PHP Image Gallery

- 多國語系之套件 ： 英文, 法文, 德文, 義大利文, 俄文, 西班牙文
- SourceForge開放軟體入口網站極為熱門的專案 (上週最新活躍度) ： 91.51
- 每日瀏覽點擊次數近千人

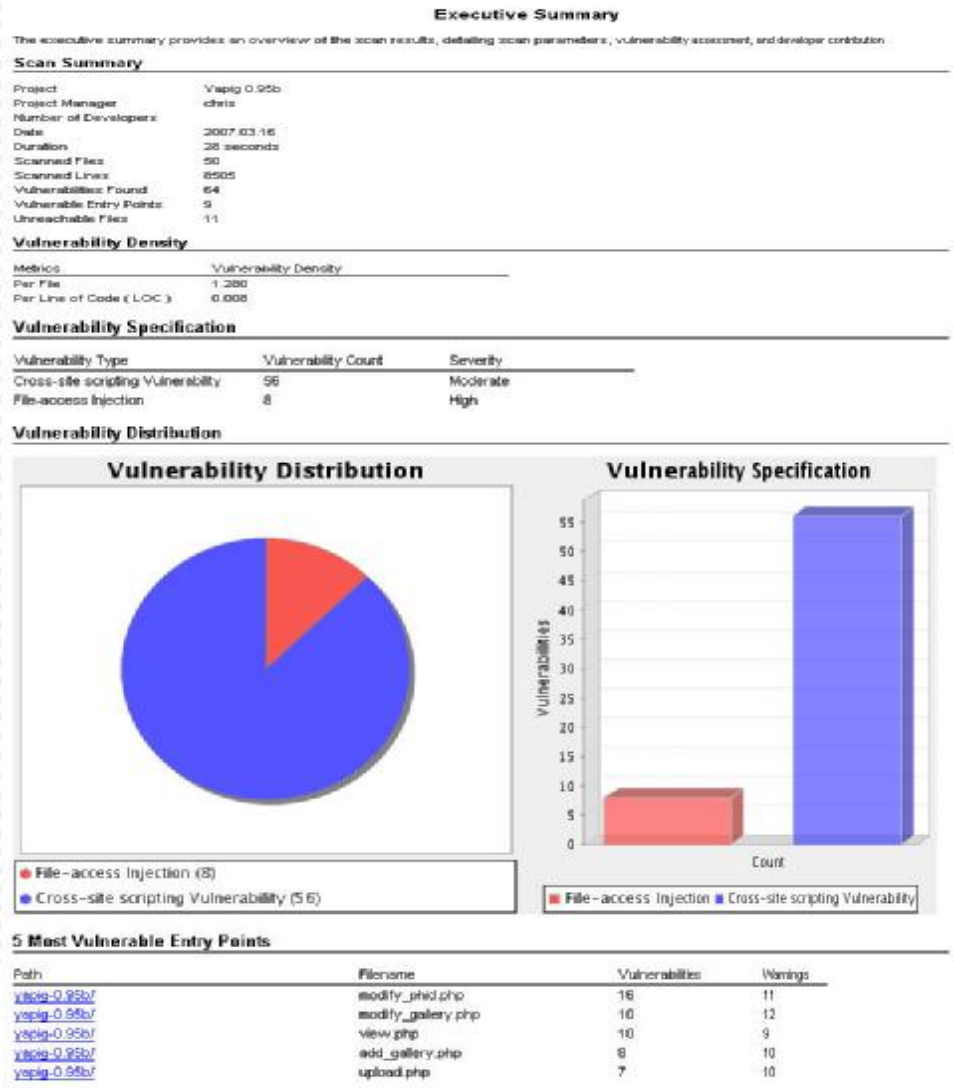
Date (UTC)	Rank	Total Pages [1]	Downloads	Project Web Hits
20 Mar 2007	N/D	2	0	42
19 Mar 2007	15,516	113	14	540
18 Mar 2007	17,945	66	16	507
17 Mar 2007	17,836	79	17	638
16 Mar 2007	17,683	108	25	1,078
15 Mar 2007	18,191	106	20	770
14 Mar 2007	17,964	80	12	780



- 典型具代表性之不安全的PHP專案
  - 已有多家資安公司發佈此軟體的弱點通報
- 檢測範例
  - 使用自動靜態分析工具來檢測YaPiG專案
- 攻擊示範 (Demo-Only)
  - (0day) thanks_comment.php, $D_REFRESH_URL
  - 單行程式碼極為複雜, 涉及的參數近十個, 僅有一個有問題
- 弱點發生原因: 脆弱可污染的進入點

檢測範例 (*YaPiG*)

- 檢測報告呈現的結果
- 此軟體安不安全?
  - 依循OWASP Top 10 弱點命名與檢測標的
  - 弱點分佈圖與統計
    56個XSS跨站腳本弱點
    2個檔案注入弱點
- 檔案大小?
  (50個檔案; 8,505行)
  - 耗時多久? (28秒)
  - 弱點密度? (1.2個/每檔案)
- 要從何處開始修正?
  - 單一檔案高達16個弱點



Executive Summary

The executive summary provides an overview of the scan results, detailing scan parameters, vulnerability assessment, and developer contribution

Scan Summary

Project	Yapig 0.95b
Project Manager	chris
Number of Developers	
Date	2007.03.16
Duration	28 seconds
Scanned Files	50
Scanned Lines	8505
Vulnerabilities Found	64
Vulnerable Entry Points	9
Unreachable Files	11

Vulnerability Density

Metrics	Vulnerability Density
Per File	1.280
Per Line of Code (LOC)	0.008

Vulnerability Specification

Vulnerability Type	Vulnerability Count	Severity
Cross-site scripting Vulnerability	56	Moderate
File-access Injection	8	High

Vulnerability Distribution

5 Most Vulnerable Entry Points

Path	Filename	Vulnerabilities	Warnings
yapig-0.95b/	modify_phid.php	16	11
yapig-0.95b/	modify_gallery.php	10	12
yapig-0.95b/	view.php	10	9
yapig-0.95b/	add_gallery.php	8	10
yapig-0.95b/	upload.php	7	10

資料來源：

滲透測試 vs. 程式碼檢測

項目 ＼ 工具	滲透測試工具(Nikto)	自動源碼檢測工具
背景	免費強大之滲透測試工具	Web Script程式碼檢查工具
功能	1. 檢查Server錯誤設定問題 (230種以上) 2. 檢查Web 檔案/CGI安全問題 (3300種)	1. 檢查最嚴重的Web問題 2. 防堵網頁竄改常用入口
測試結果 1. 涵蓋 2. 誤報 *測試標的:yapig0.95b	1. 找到Apache設定問題(TRACE缺失) 2. 2筆誤報XSS, SQL database dump (yapig不使用資料庫)	1. 找出56個XSS, 8個File Aceess Injection 2. /admin下的檔案
結論	1. 找出已知的設定問題 2. 適合與 Nessu搭配作為VA+PT方案	1. 可用於找出未被發現的的程式漏洞 2. 提供最佳偵測率,並找出錯誤源頭, 補足PT,VA先天不足之處

檢測流程三部曲：1.上傳程式碼

- 將原始程式碼, 上傳至檢測平台做掃瞄

資料來源：

檢測流程三部曲：
2. 觀看掃瞄進度與排程

- 弱點一覽
- 專案一覽
- 自動排程

個人資訊板

此頁面提供使用者基本資訊，諸如參與的專案、目前所找到的弱點等等。

錯誤列表 (2007/3/16 下午 4:20)

錯誤類型	檔案	嚴重等級	問題位置	簡述
File-access Injection	add_comment.php	4	116	the expression fopen($comments_file,"a+") was found vulnerable.
Cross-site scripting Vulnerability	slideshow.php	2	99	the expression print $the_url . "&phid=" . $phid_next was found vulnerable.
Cross-site scripting Vulnerability	slideshow.php	2	99	the expression print $interval was found vulnerable.
Cross-site scripting Vulnerability	slideshow.php	2	130	the expression print $the_url . "&phid=" . $phid . "&paused=1" was found vulnerable.
Cross-site scripting Vulnerability	slideshow.php	2	136	the expression print $the_url . "&phid=" . $phid_next was found vulnerable.

1 2 3 4 5 6 7 8 9 10 11 12 13

參與專案列表

專案名稱	角色	HTML報告	PDF報告	最新掃描日期	下次執行時間
GoopGallery	專案經理			尚未做過掃描	下次掃描將於：2007/3/21 上午 6:05 執行
AdnForum 1.0	專案經理			尚未做過掃描	下次掃描將於：2007/3/21 上午 6:05 執行
CoolForum	專案經理			尚未做過掃描	下次掃描將於：2007/3/21 上午 6:05 執行
FourTwoSevenBB	專案經理			尚未做過掃描	下次掃描將於：2007/3/21 上午 6:05 執行
gcontact_0.65	專案經理			2007年3月16日 下午04時15分05秒	下次掃描將於：2007/3/21 上午 6:05 執行

1 2

最後登入資訊

登入時間
2007年3月21日 下午02時04分27秒

資料來源：OWASP Taiwan
http://www.owasp.org.tw

檢測流程三部曲：
3.弱點的細部資訊

- 主要提供弱點的"證據"，在哪一行、哪個參數造成什麼問題

thanks_comment.php

Total Vulnerabilities: 1
Location: yapig-0.95b/template/default/thanks_comment.php
Lines of code: 37
Parse Time: 2 milliseconds

Line # 10

Vulnerability Type

Cross-site scripting Vulnerability

Vulnerable Expression

```
echo <<<THANKS <html> <!-- thanks_comment BEGIN --> <head> <meta http-equiv="Content-Type" content="text/html;
charset=ISO-8859-1" /> <meta http-equiv="Refresh" content="2; url=$D_REFRESH_URL" /> <title>$I_THANKS</title> </head> <body>
<div style="background-color: #EBEBEB; border-top: 1px solid #FFFFFF; border-left: 1px solid #FFFFFF; border-right: 1px solid
#AAAAAA; border-bottom: 1px solid #AAAAAA;"> <h4>$I_THANKS</h4> <p>$I_ADDED</p> <pre> <b>$I_TITLE</b>: $D_TITLE
<b>$I_AUTHOR</b>: $D_AUTHOR <b>$I_EMAIL</b>: $D_MAIL <b>$I_WEB</b>: $D_WEB <b>$I_MESSAGE</b>: $D_MESSAGE</pre>
<p>$I_IF_NOT_REFRESHED <a href="$D_REFRESH_URL">$I_PRESS_HERE</a></p> </div> </body> <!-- thanks_comment END --> </html> THANKS;
```

Code Snippet

```
9:
10: echo <<<THANKS
11:   <html>
```

Vulnerability Trace-back Notes

(tainted origin)

add_comment.php On line 146 of add_comment.php variable $D_REFRESH_URL gets assigned the tainted value $gid

```
146: $D_REFRESH_URL="view.php?gid=$gid&phid=$phid";
```

(vulnerability cause) *add_comment.php* On line 63 of add_comment.php variable $gid gets assigned the tainted value 'gid'

```
63: $gid=$_GET['gid'];
```

資料來源：OWASP Taiwan
http://www.owasp.org.tw

實務案例:
政府資安作業共通規範
GISCC網站
http://www.giscc.org.tw/

程式約80多MB
程式碼1萬6千行
散佈在上百個檔案

資安工作的體會

- 資安最大的威脅，就是不知道威脅
- 資安最大的危機，就是最大的轉機
- 資安最大的績效，就是看不到績效
- 錢不是資安的問題，問題是沒有錢
- 人是資安最大資產，卻是最大挑戰
- 資安認知最小投資，卻是最大回報

問題與討論