英屬維京群島商時間軸科技股份有限公司
OWASP弱點測試報告書
專案項目：淡江資管系網

Author: Taien Wang(請製表人自行填寫)
Published: June 01, 2013(請製表人自行填寫)
Version: 1.0

編輯歷程

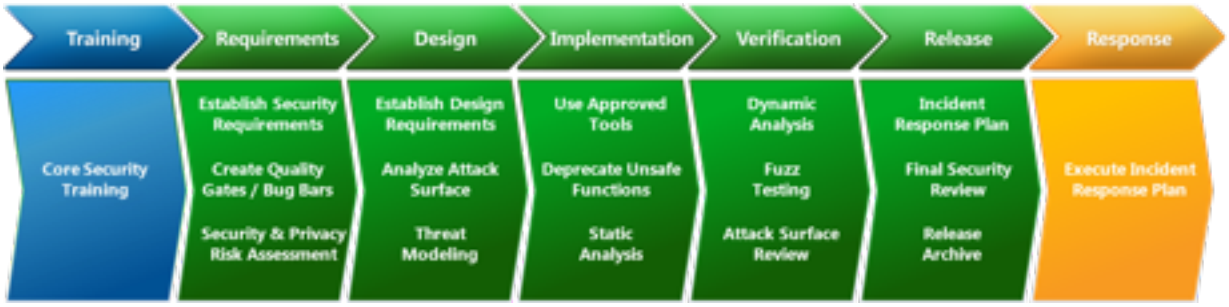
時間	版本	說明	編輯人
2013.01.01	1.0	參考軟體安全相關資料與翻譯OWASP v3.0 Code Review Guide撰寫此報告書	Taien Wang

OWASP弱點測試報告書章節

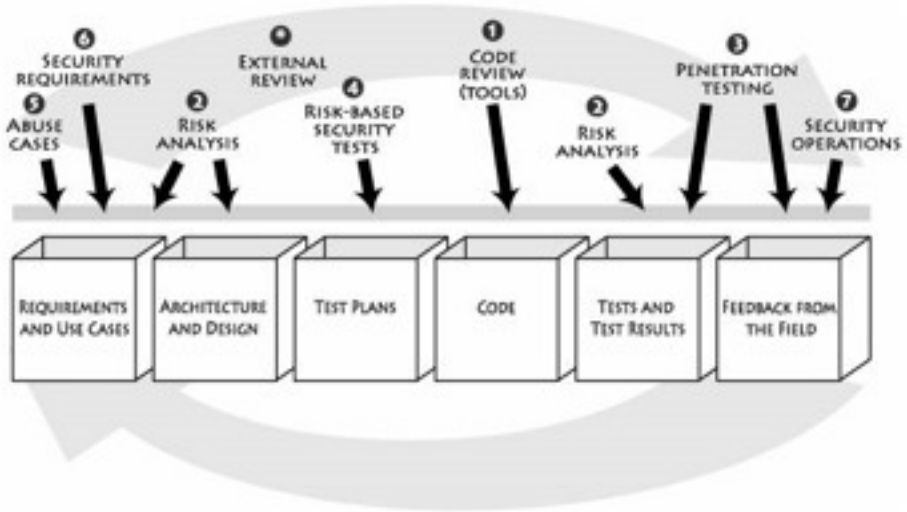
1. 測試設計

弱點測試依循微軟建議的安全性開發生命週期(Security Development Lifecycle，SDL)驗證安全性與軟體安全權威Gary McGraw提出的軟體安全接觸點(Touchpoint)滲透測試需求建置，詳細網頁程式安全參考開放Web軟體安全計畫(Open Web Application Security Project，OWASP)檢驗手冊與項目進行安全檢驗。

實際弱點挖掘使用自動化工具與手動調試，並在檢測結束後留下掃描相關紀錄檔(如html)並填寫本文件。



微軟 - 安全性開發生命週期



Gary McGraw – 七個軟體安全接觸點

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

OWASP - 十大網路應用程式攻擊

參考文獻

1. Microsoft, “Security Development Lifecycle”
2. Gray McGraw, “Software Security, Building Security In”
3. Open Web Application Security Project, “Owasp Testing Guide”, v3
4. Open Web Application Security Project, “Code Review Guide”, v1.1

2. 測試工具

本次針對 OWASP 測試所使用之工具列表如下：

Paros

Web 滲透測試工具，可透過代理伺服器(Proxy)方式作參數分析檢測，並可攔截HTTP/HTTPS傳輸內容，對HTTP相關數據進行修改。

http://www.parosproxy.org

OWASP Zed Attack Proxy

OWASP官方發布的交互試Web應用程式弱點掃描工具，除了提供自動掃描外還提供一些用於手動檢測分析弱點的工具。為OWASP十大工具之一。

http://code.google.com/p/zaproxy/

WebScarab

Web 滲透測試工具，可用來作參數分析檢測，並可攔截HTTP/HTTPS傳輸內容，對HTTP相關數據進行修改。

http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

(以上工具視實際作業增刪修改)

3. 測試字串

透過工具和手動測試，針對各項網站應用程式之參數，送出各種字串並判讀回應之訊息，底下為測試字串。

SQL Injection測試字串

a'

'+or+1=1#

'+or+1=1%23

'+or+1=1

'+or+1=1/*

x'+AND+userid+IS+NULL;--

x'+AND+email+IS+NULL; --

anything'+OR+'x'='x

x'+AND 1=(SELECT COUNT(*) FROM tabname); --

x'+AND+members.email+IS+NULL; --

x'+OR+full_name+LIKE+'%Bob%

';exec master..xp_cmdshell 'ping 10.10.10.1'--

Cross Site Scripting測試字串

<IMG SRC="javascript:alert('XSS');">

<IMG SRC=javascript:alert('XSS')>

<IMG SRC=JaVaScRiPt:alert('XSS')>

<IMG SRC=javascript:alert("XSS")>

<IMG SRC=`javascript:alert("'XSS"')`>

<IMG """><SCRIPT>alert("XSS")</SCRIPT>">

<BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XSS")>

<<SCRIPT>alert("XSS");//<</SCRIPT><IMG SRC=javascript:alert('XSS')>

<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>

<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>

Overflows測試字串：

- ### Integer Overflows

-1

0

0x100

0x1000

0x3fffffff

0x7ffffffe

0x7fffffff

0x80000000

0xfffffffe

0xffffffff

0x10000

0x100000

- ### Format String Errors

%s%p%x%d

.1024d

%.2049d

%p%p%p%p

%x%x%x%x

%d%d%d%d

%s%s%s%s

%99999999999s

%08x

%%20d

%%20n

%%20x

%%20s

%s%s%s%s%s%s%s%s%s%s

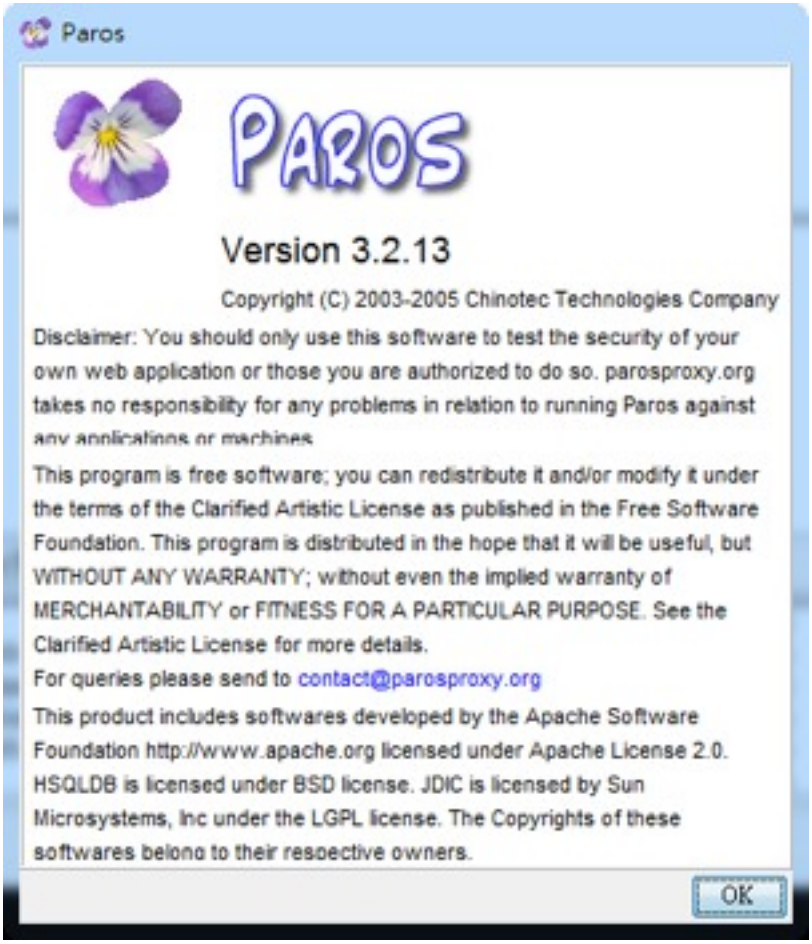
%p%p%p%p%p%p%p%p%p%p

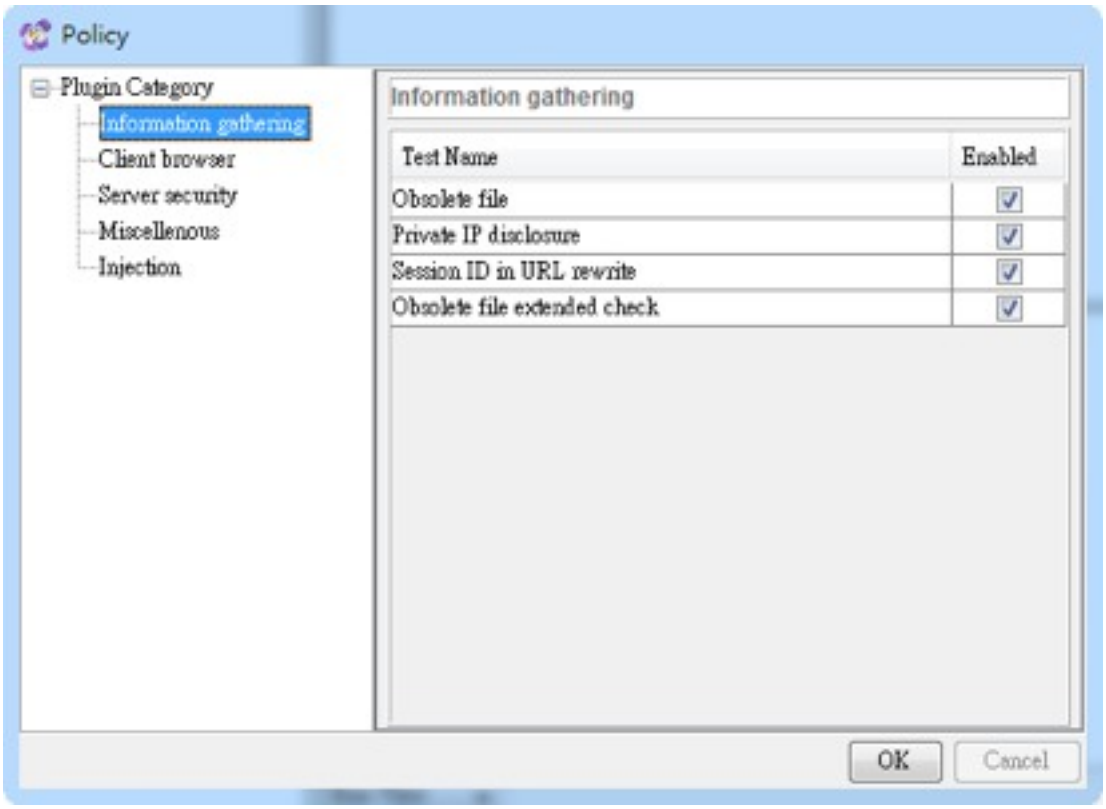
%#0123456x%08x%x%s%p%d%n%o%u%c%h%l%q%j%z%Z%t%i%e%g%f%a%C%S%08x%%

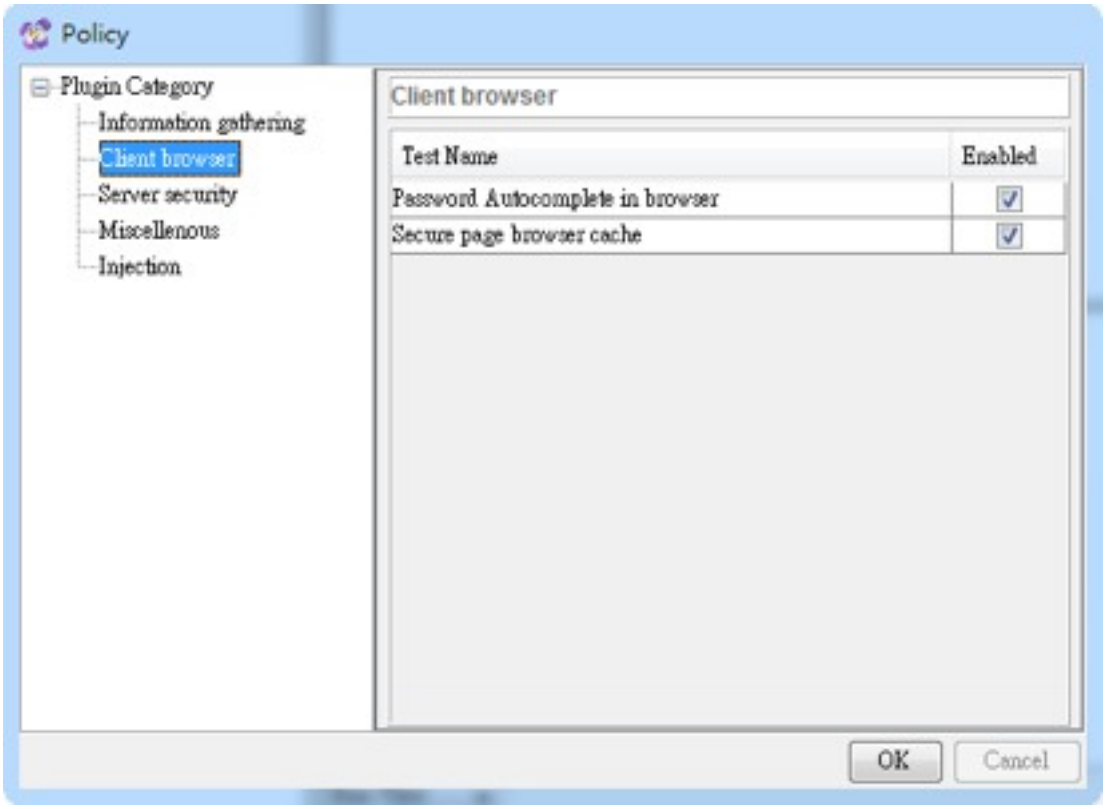
%s x 129

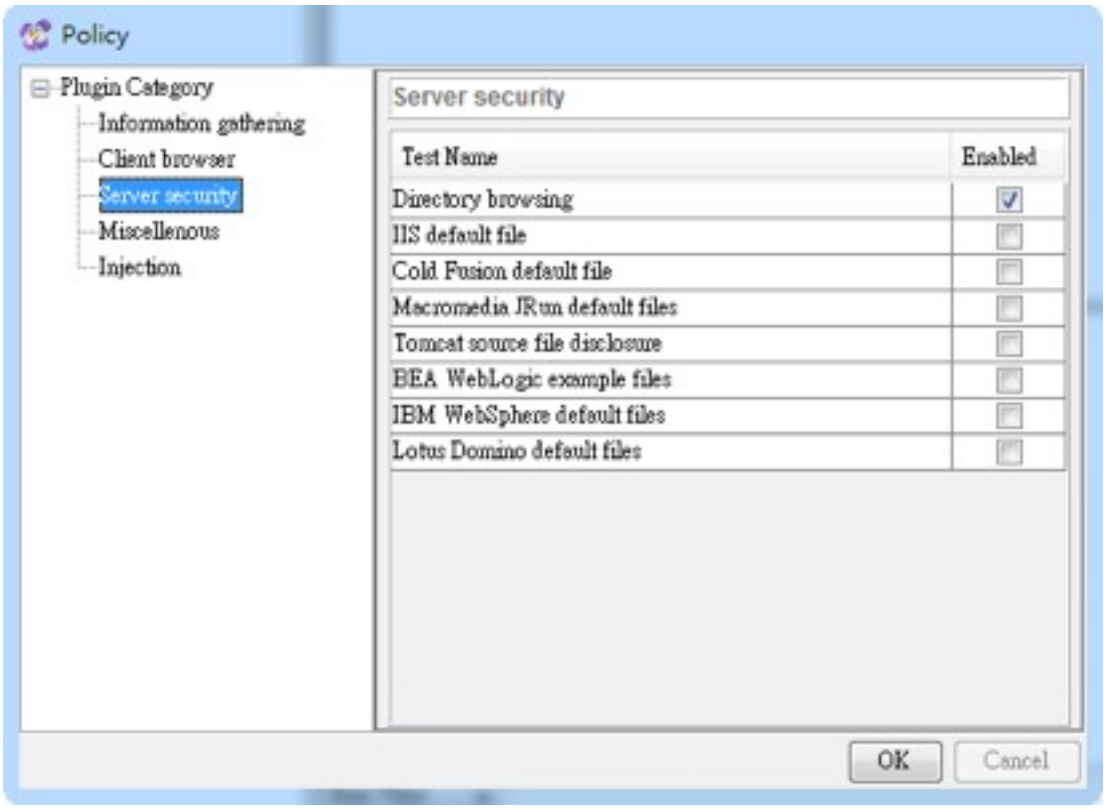
4. 測試工具設定

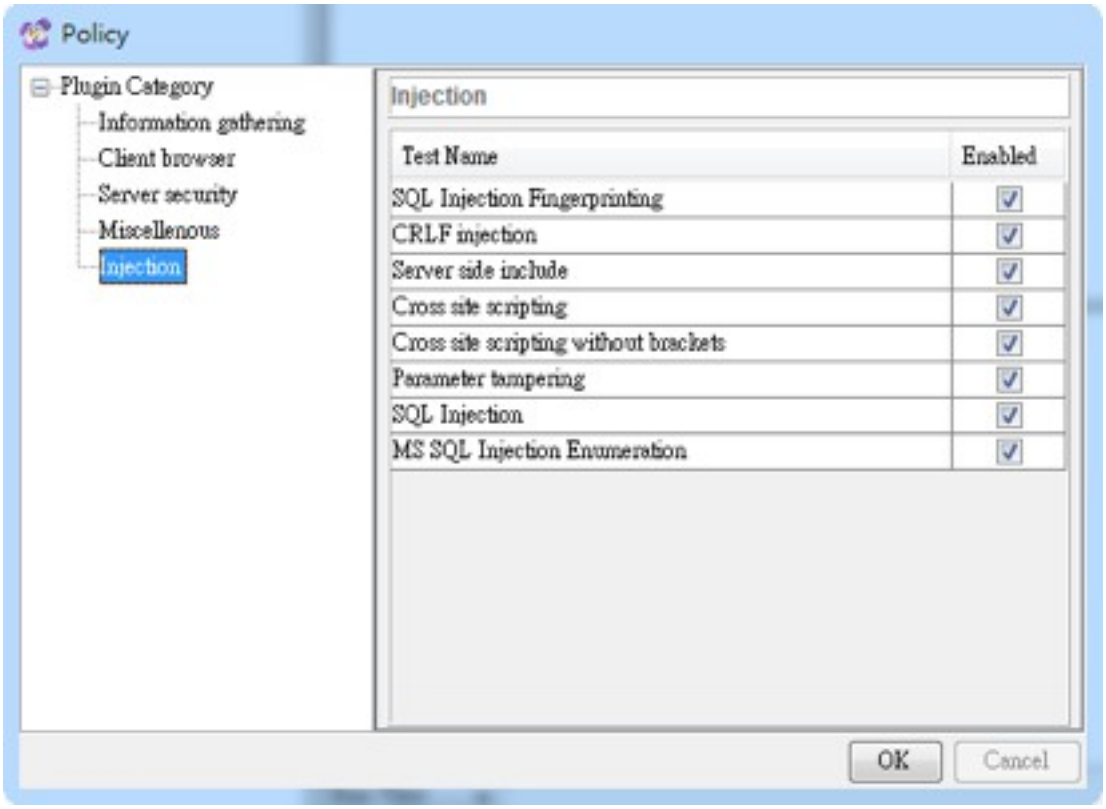
Paros



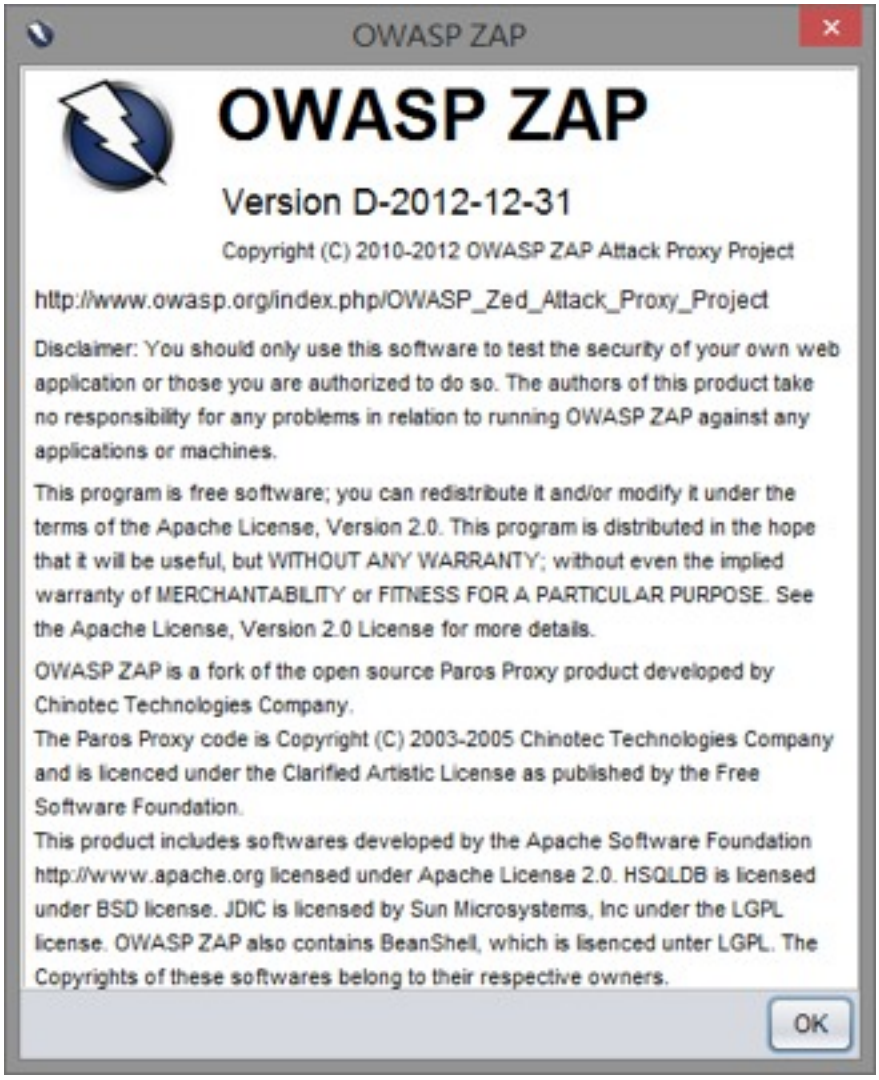

Policy
Plugin Category
Information gathering
Client browser
Server security
Miscellenous
Injection
Information gathering
Test Name
Enabled
Obsolete file
Private IP disclosure
Session ID in URL rewrite
Obsolete file extended check
OK
Cancel

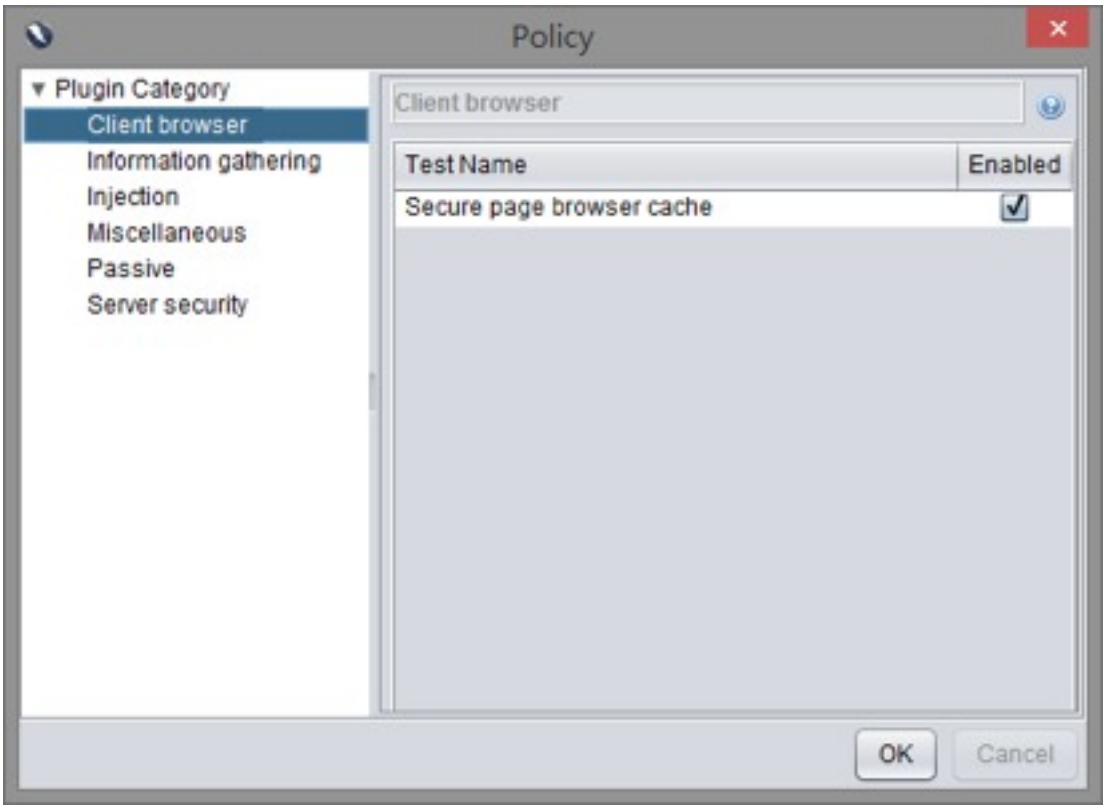

Policy
Plugin Category
Information gathering
Client browser
Server security
Miscellenous
Injection
Client browser
Test Name
Enabled
Password Autocomplete in browser
Secure page browser cache
OK
Cancel

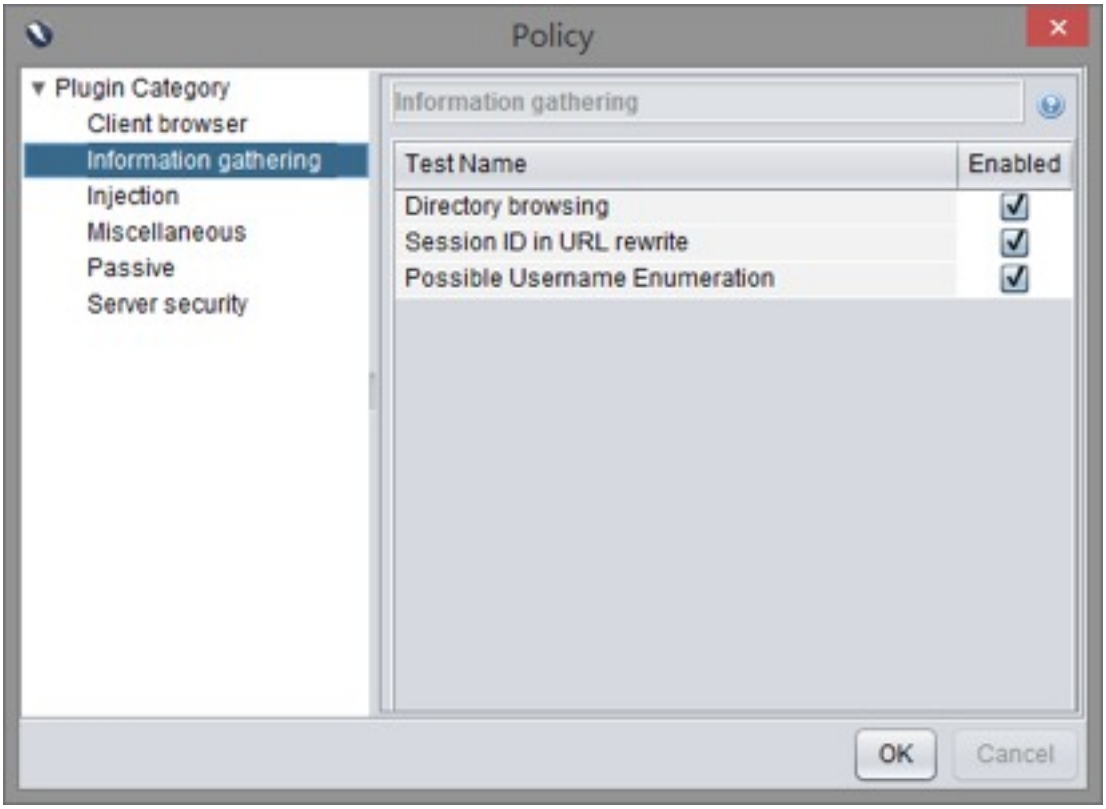

Policy
Plugin Category
Information gathering
Client browser
Server security
Miscellenous
Injection
Server security
Test Name
Enabled
Directory browsing
IIS default file
Cold Fusion default file
Macromedia JRun default files
Tomcat source file disclosure
BEA WebLogic example files
IBM WebSphere default files
Lotus Domino default files
OK
Cancel

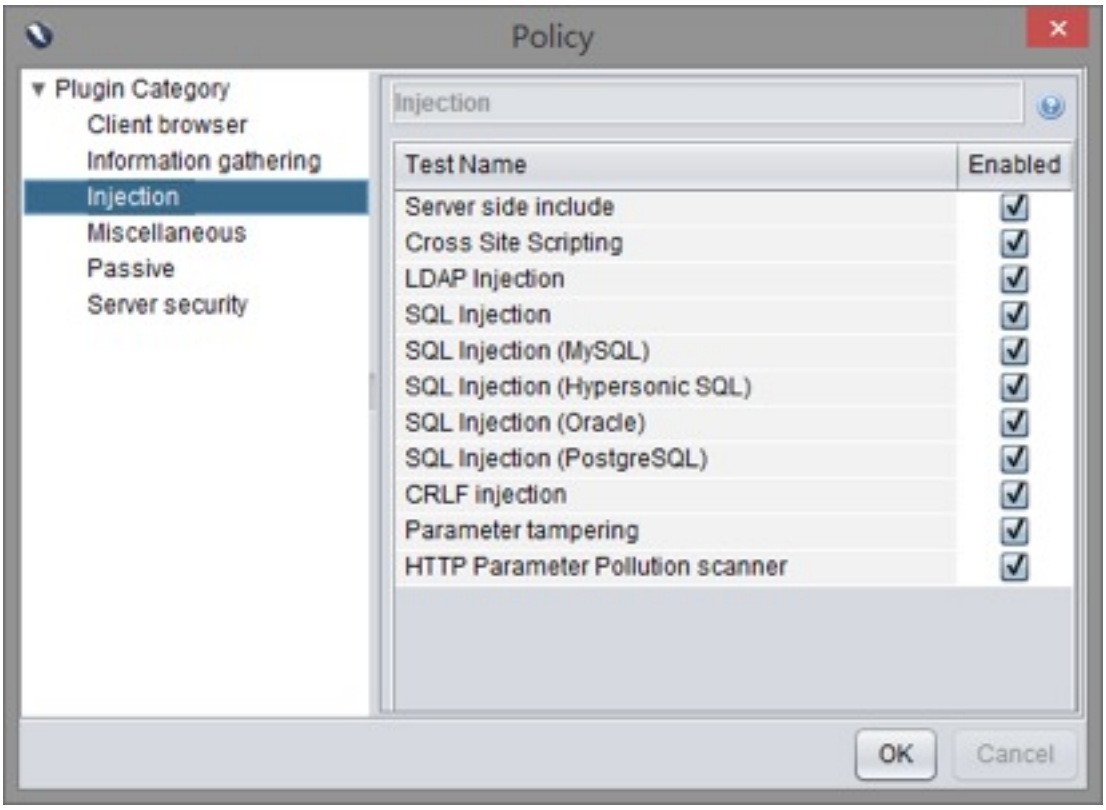

Policy
Plugin Category
Information gathering
Client browser
Server security
Miscellenous
Injection
Injection
Test Name
Enabled
SQL Injection Fingerprinting
CRLF injection
Server side include
Cross site scripting
Cross site scripting without brackets
Parameter tampering
SQL Injection
MS SQL Injection Enumeration
OK
Cancel

OWASP Zed Attack Proxy

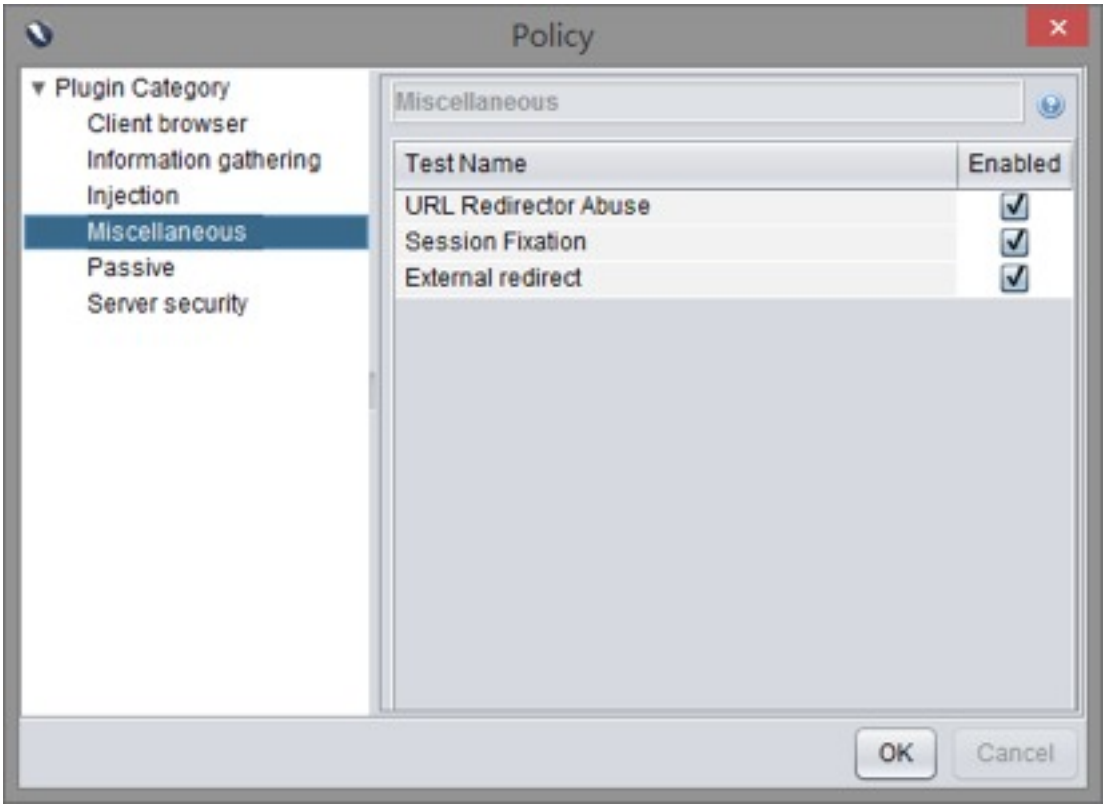


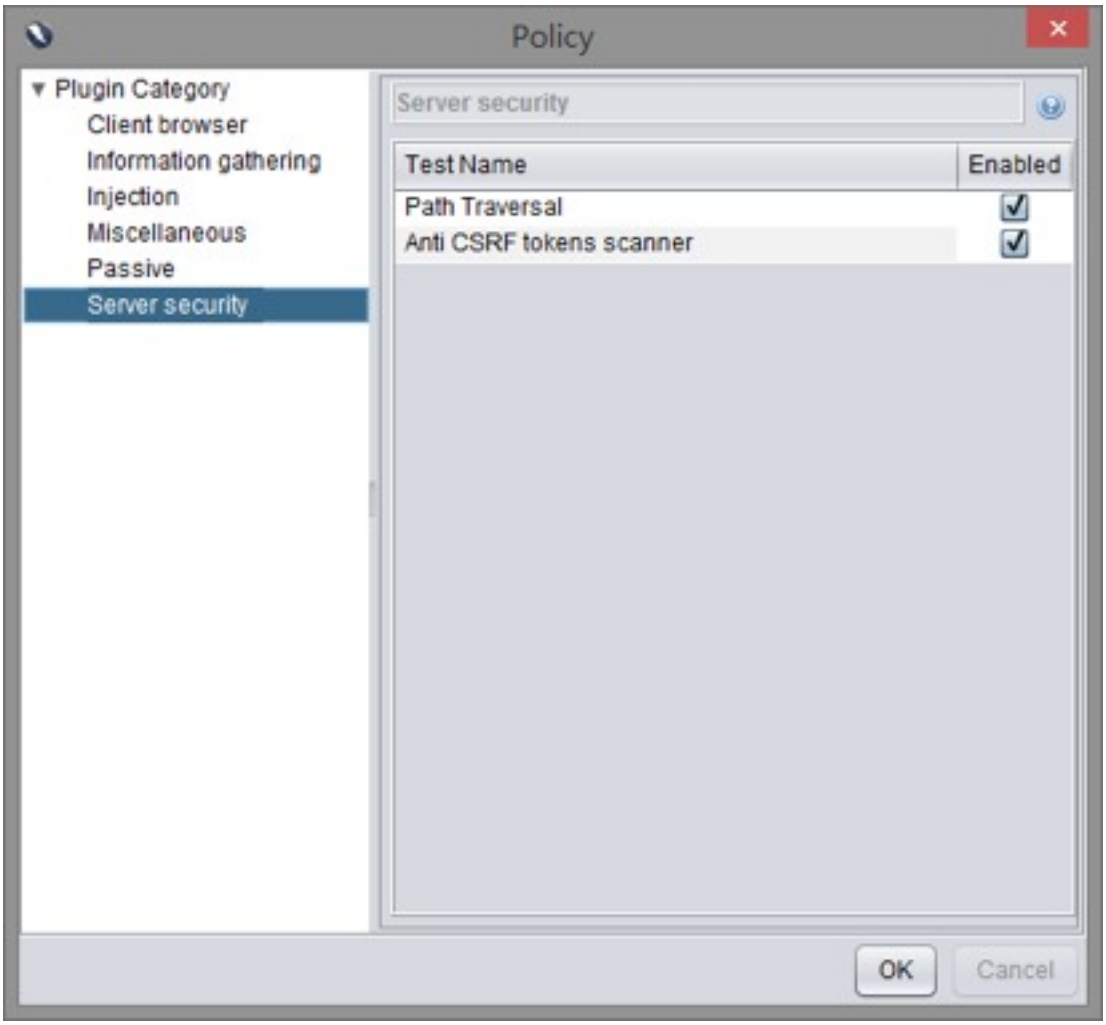

Policy
Plugin Category
Client browser
Information gathering
Injection
Miscellaneous
Passive
Server security
Client browser
Test Name
Enabled
Secure page browser cache
OK
Cancel


Policy
Plugin Category
Client browser
Information gathering
Injection
Miscellaneous
Passive
Server security
Information gathering
Test Name
Enabled
Directory browsing
Session ID in URL rewrite
Possible Username Enumeration
OK
Cancel

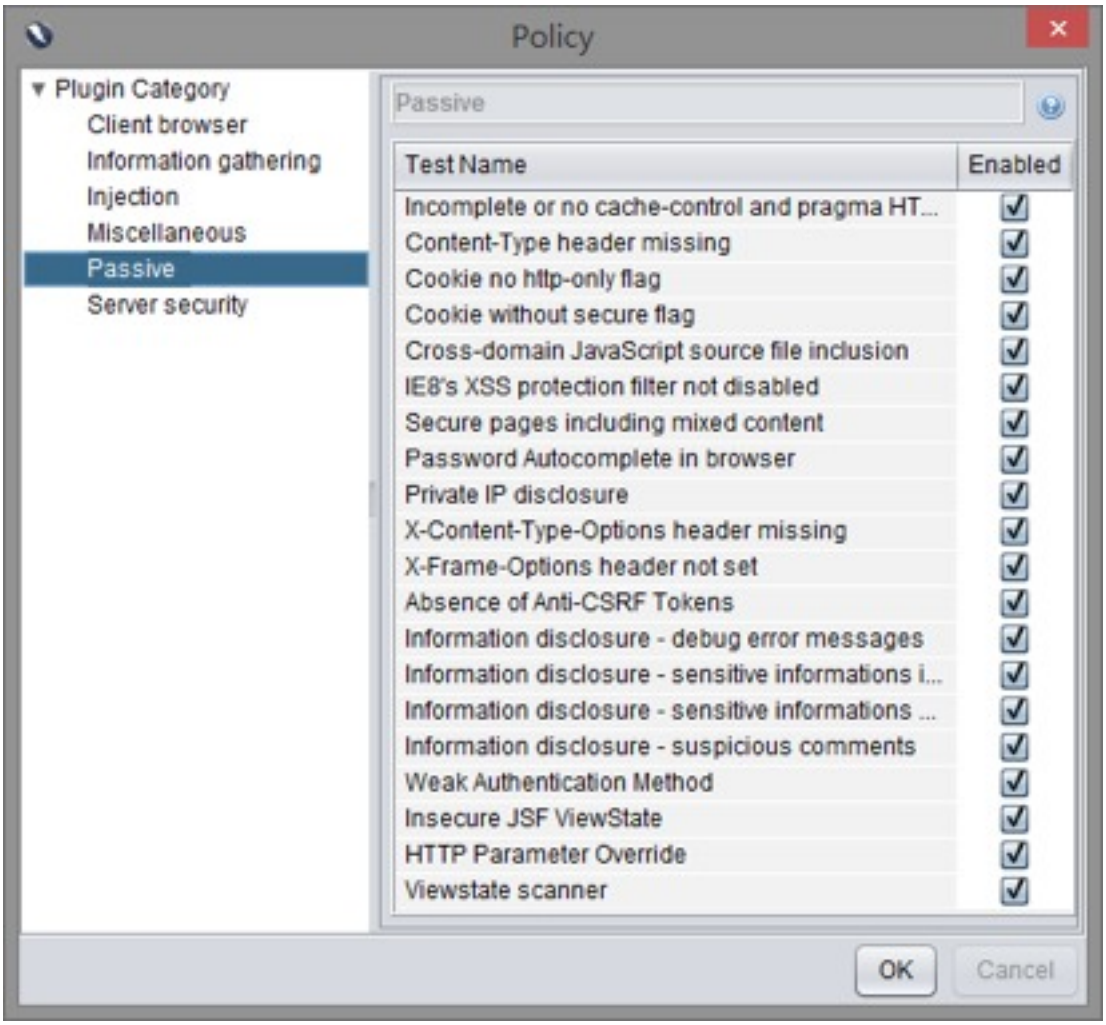


(SQL Injection視實際操作選取需要測試的類型，可加快速度與減少誤判)



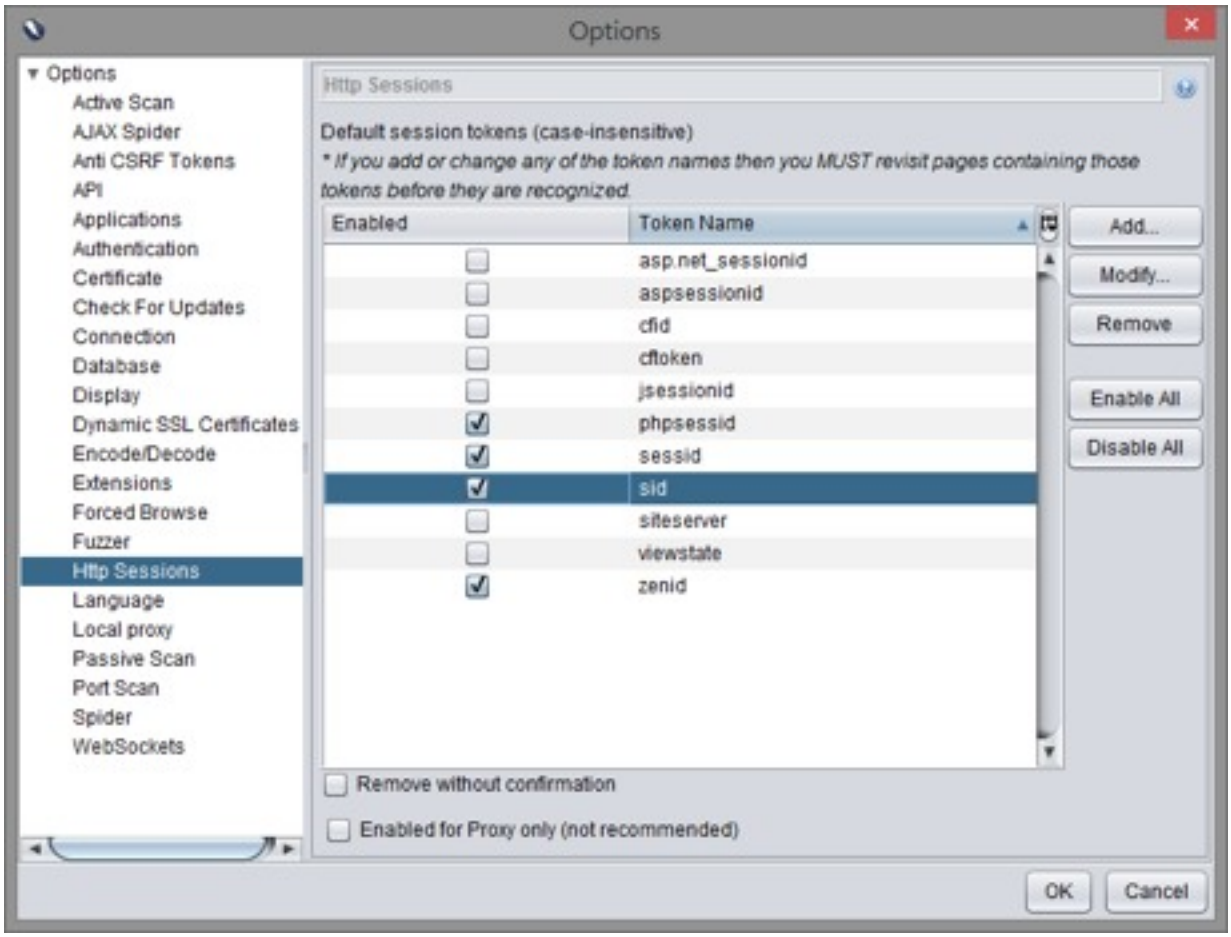


(視情況是否檢測CSRF，如不檢測請取消打勾，請將下面5、7章節的OWASP-SM-005選項刪除)



(視情況是否檢測CSRF，如不檢測請取消Absence of Anti-CSRF Tokens打勾，請將5、7章節的OWASP-SM-005選項刪除)

(如關閉以下Content-Type header missing、Cookie no http-only flag、Cookie without secure flag、Cross-domain JavaScript source file inclusion、X-Content-Type-Options header missing、X-Frame-Options header not set，請將5、7章節的OWASP-SM-002選項刪除，如關閉Password Autocomplete in browser，請將5、7章節的OWASP-AT-006選項刪除)


Options
Options
Active Scan
AJAX Spider
Anti CSRF Tokens
API
Applications
Authentication
Certificate
Check For Updates
Connection
Database
Display
Dynamic SSL Certificates
Encode/Decode
Extensions
Forced Browse
Fuzzer
Http Sessions
Language
Local proxy
Passive Scan
Port Scan
Spider
WebSockets
Http Sessions
Default session tokens (case-insensitive)
* If you add or change any of the token names then you MUST revisit pages containing those tokens before they are recognized.
Enabled
Token Name
asp.net_sessionid
aspsessionid
cfid
cftoken
jsessionid
phpsessid
sessid
sid
siteserver
viewstate
zenid
Add...
Modify...
Remove
Enable All
Disable All
Remove without confirmation
Enabled for Proxy only (not recommended)
OK
Cancel

5. 測試項目

針對網站主機所進行的OWASP 測試項目如下：

設定管理(Configuration Management Testing)

OWASP編號	項目	說明
OWASP-CM-001	SSL/TLS測試	憑證是否過期，是否採用弱加密？
OWASP-CM-002	資料庫監聽測試	Oracle資料庫是否有運行資料庫監聽？
OWASP-CM-003	基礎建設配置管理測試	主機是否有防火牆，甚至是網頁應用程式防火牆，與定期更新系統或第三方程式弱點？
OWASP-CM-004	應用配置管理測試	主機是否有正確設定可避免取得敏感資訊，紀錄如何存放與稽核？
OWASP-CM-005	檔案擴展處理測試	是否有些敏感資訊檔案.inc、.asa等可直接被存取？
OWASP-CM-006	過時、備份與未使用的檔案	系統中是否存在過時、備份與未使用的檔案？
OWASP-CM-007	基礎架構與應用管理介面	一般用戶使否可存取管理介面或功能？
OWASP-CM-008	HTTP方法與XST測試	主機中是否存在其他HTTP方法(HEAD、GET、POST、PUT、DELETE、TRACE、OPTIONS、CONNECT)可供非正常存取？

資訊收集(Information Gathering)

OWASP編號	項目	說明
OWASP-IG-001	蜘蛛、機器人與爬蟲器	檢測搜尋引擎搜尋設定robots.txt是否設定安全？
OWASP-IG-002	搜尋引擎發現與偵查	是否可利用搜尋引擎檢視挖掘機敏資訊？
OWASP-IG-003	應用入口識別	在GET\POST等HTTP請求中是否有敏感訊息？
OWASP-IG-004	Web應用指紋測試	是否可正確知道網頁伺服器版本，語言版本？
OWASP-IG-005	應用發現	是否可發現非主程式的額外應用？
OWASP-IG-006	錯誤代碼分析	是否有未經處理的主機直接錯誤訊息？

驗證(Authentication Testing)

OWASP編號	項目	說明
OWASP-AT-001	加密通道憑證傳輸	使用者輸入資料是否使用安全協議傳輸，以避免遭受攻擊？
OWASP-AT-002	用戶枚舉	是否可透過蒐集找到有效用戶與正確密碼？
OWASP-AT-003	可猜解用戶字典攻擊	透過字典攻擊是否可以破解用戶？
OWASP-AT-004	暴力測試	透過暴力攻擊是否可以破解用戶？
OWASP-AT-005	繞過驗證模式測試	是否可不經過驗證，取得原本需經驗證才可使用的授權？
OWASP-AT-006	記住密碼與密碼重置弱點測試	是否可透過密碼重置取得他人帳號權限？機敏等級較高系統應禁止記住密碼
OWASP-AT-007	註銷與瀏覽器暫存管理測試	在註銷連線後該連線是否真的無法再使用？瀏覽器在註銷連線後是否還有敏感資訊？
OWASP-AT-008	CAPTCHA測試	CAPTCHA是否容易被繞過破解？
OWASP-AT-009	多因素驗證測試	基於演算法或密碼學設計的驗證機制，是否可以配猜出或破解？
OWASP-AT-010	競爭條件測試	在多執行續同時運作時是否會有衝突？

連線管理(Session Management)

OWASP編號	項目	說明
OWASP-SM-001	連線管理模式測試	是否是在安全和非預知的情況下產生cookies和其他連線驗證碼？
OWASP-SM-002	Cookies屬性測試	Cookies是否設定Secure、HttpOnly、Domain與是否可竄改取得更高權限？
OWASP-SM-003	連線固定測試	在連線固定狀況下，是否可利用該弱點挾持用戶連線？
OWASP-SM-004	連線變數洩漏測試	連線ID(SessionID)是否加密？如無是否利用HTTPS保護？
OWASP-SM-005	CSRF測試	攻擊者是否可在用戶登入後暗中進行其他操作？

授權測試(Authorization Testing)

OWASP編號	項目	說明
OWASP-AZ-001	目錄與路徑洩漏	是否可找到一種方法來執行目錄洩漏並獲取隱藏資訊？
OWASP-AZ-002	繞過授權模式測試	是否可不經過驗證取得隱藏功能？
OWASP-AZ-003	權限提升測試	用戶是否可透過權限提升攻擊不經過正常管道提升權限？

商業邏輯測試(Business logic testing)

OWASP編號	項目	說明
OWASP-BL-001	商業邏輯測試	是否有影響正常商業邏輯的狀況？

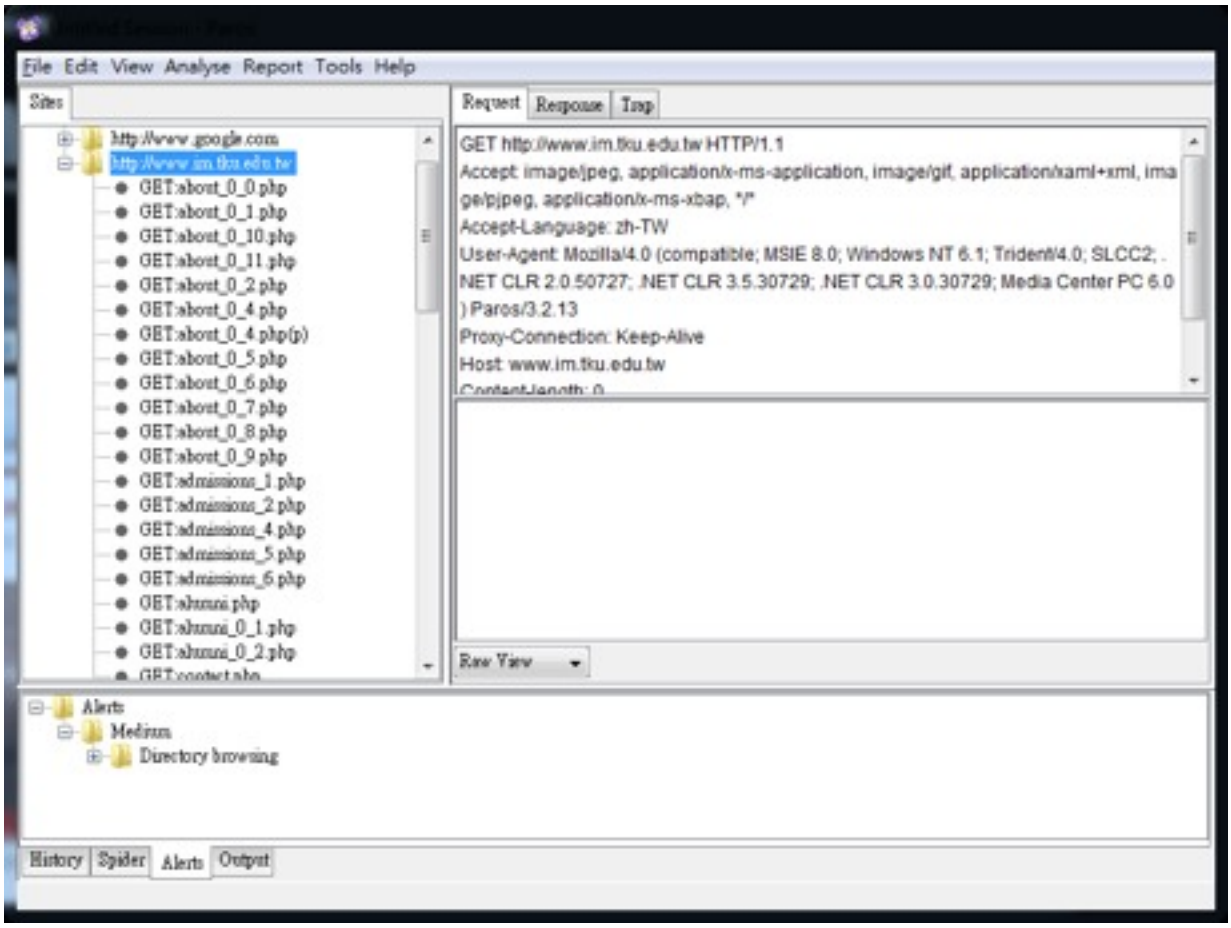
資料驗證測試(Data Validation Testing)

OWASP編號	項目	說明
OWASP-DV-001	跨站腳本反射測試	Reflected XSS
OWASP-DV-002	跨站腳本儲存測試	Stored XSS
OWASP-DV-003	跨站腳本DOM測試	DOM XSS
OWASP-DV-004	Flash跨站測試	Cross Site Flashing
OWASP-DV-005	SQL注入	檢查是否有Oracle、MySQL、SQL Server、MS ACCESS、PostgreSQL、Sqlite注入？
OWASP-DV-006	LDAP注入	LDAP Injection
OWASP-DV-007	ORM注入	ORM Injection
OWASP-DV-008	XML注入	XML Injection
OWASP-DV-009	SSI注入	SSI Injection
OWASP-DV-010	XPath注入	XPath Injection

OWASP-DV-011	IMAP/SMTP注入	IMAP/SMTP Injection
OWASP-DV-012	Code注入	是否可在應用程式中注入由Web伺服器執行的程式碼？
OWASP-DV-013	OS命令	是否可在HTTP請求中注入OS命令？
OWASP-DV-014	緩衝區溢出	檢查是否有Heap、Stack、格式化字串溢出?

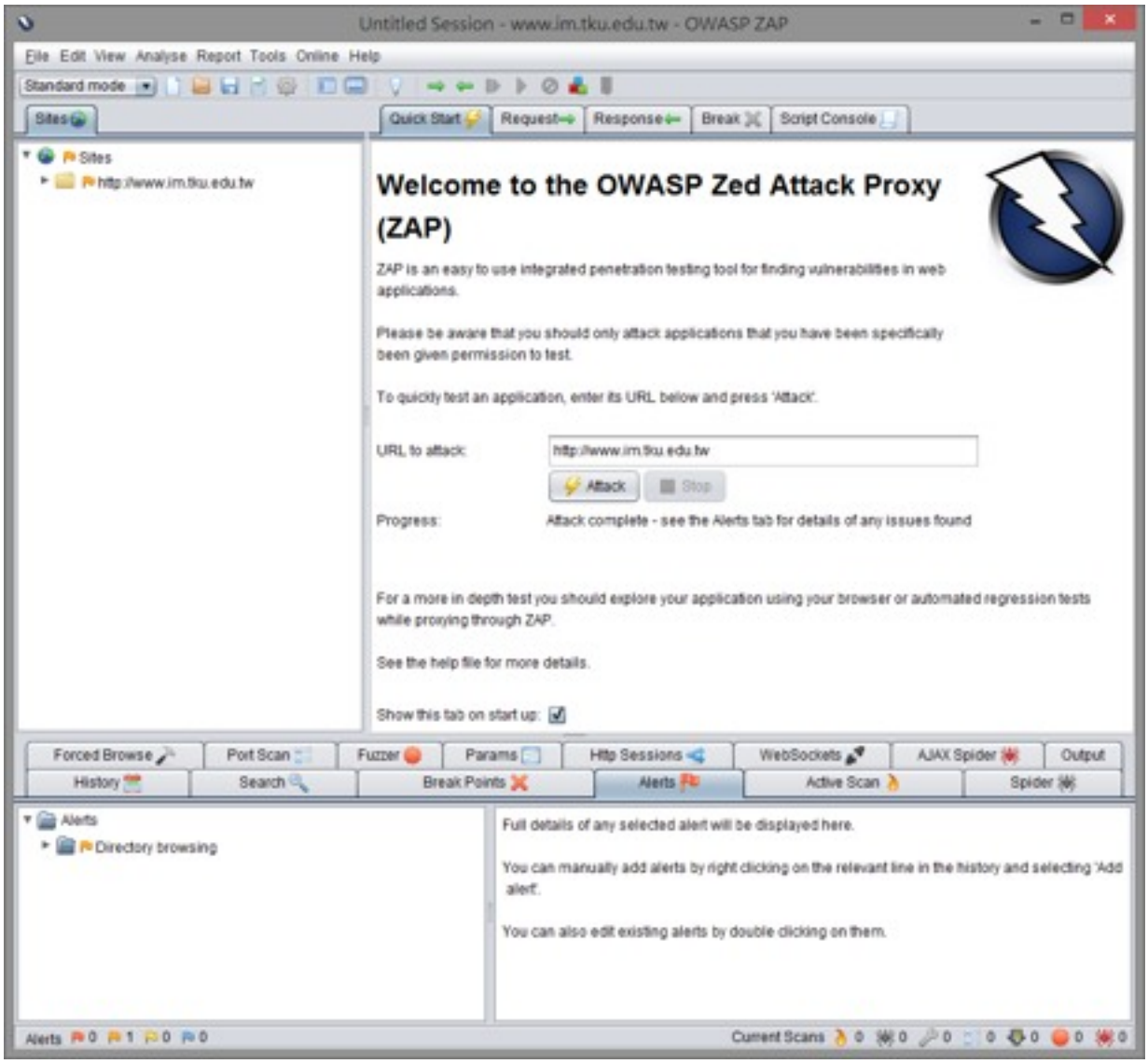
6. 測試截圖

Paros掃描



(盡量修正到完全沒有Alert)

ZAP掃描



(盡量修正到完全沒有Alert)

7. OWASP測試結果

目標：http://www.im.tku.edu.tw(請自行修改)

專案項目：淡江資管系開發專案(請自行修改)

OWASP檢驗結果

OWASP編號	項目	測試結果
OWASP-CM-001	SSL/TLS測試	通過
OWASP-CM-002	資料庫監聽測試	非使用Oracle資料庫
OWASP-CM-003	基礎建設配置管理測試	通過
OWASP-CM-004	應用配置管理測試	通過
OWASP-CM-005	檔案擴展處理測試	通過
OWASP-CM-006	過時、備份與未使用的檔案	通過
OWASP-CM-007	基礎架構與應用管理介面	通過
OWASP-CM-008	HTTP方法與XST測試	通過
OWASP-IG-001	蜘蛛、機器人與爬蟲器	通過
OWASP-IG-002	搜尋引擎發現與偵查	通過
OWASP-IG-003	應用入口識別	通過
OWASP-IG-004	Web應用指紋測試	通過
OWASP-IG-005	應用發現	通過
OWASP-IG-006	錯誤代碼分析	通過
OWASP-AT-001	加密通道憑證傳輸	不支援HTTPS
OWASP-AT-002	用戶枚舉	通過
OWASP-AT-003	可猜解用戶字典攻擊	通過
OWASP-AT-004	暴力測試	通過
OWASP-AT-005	繞過驗證模式測試	通過
OWASP-AT-006	記住密碼與密碼重置弱點測試	客戶需要瀏覽器記憶密碼
OWASP-AT-007	註銷與瀏覽器暫存管理測試	通過
OWASP-AT-008	CAPTCHA測試	通過
OWASP-AT-009	多因素驗證測試	通過
OWASP-AT-010	競爭條件測試	通過
OWASP-SM-001	連線管理模式測試	通過
OWASP-SM-002	Cookies屬性測試	通過
OWASP-SM-003	連線固定測試	通過
OWASP-SM-004	連線變數洩漏測試	不支援HTTPS
OWASP-SM-005	CSRF測試	通過
OWASP-AZ-001	目錄與路徑洩漏	通過
OWASP-AZ-002	繞過授權模式測試	通過
OWASP-AZ-003	權限提升測試	通過
OWASP-BL-001	商業邏輯測試	通過

OWASP-DV-001	跨站腳本反射測試	通過
OWASP-DV-002	跨站腳本儲存測試	通過
OWASP-DV-003	跨站腳本DOM測試	通過
OWASP-DV-004	Flash跨站測試	通過
OWASP-DV-005	SQL注入	通過
OWASP-DV-006	LDAP注入	通過
OWASP-DV-007	ORM注入	通過
OWASP-DV-008	XML注入	通過
OWASP-DV-009	SSI注入	通過
OWASP-DV-010	XPath注入	通過
OWASP-DV-011	IMAP/SMTP注入	通過
OWASP-DV-012	Code注入	通過
OWASP-DV-013	OS命令	通過
OWASP-DV-014	緩衝區溢出	通過