http://www.e-spincorp.com *website*
info@e-spincorp.com *email*

E-SPIN

SERVICE DESCRIPTION

WEB APPLICATION SECURITY SCANNING

Prepared By:

Vincent Lim
Group General Manager
Solutions and Business Consulting

E-SPIN Group of Companies

PROPRIETARY NOTICE

This proposal contains confidential information of E-SPIN, which is provided for the sole purpose of permitting the receipt to evaluate the proposal submitted herewith. In consideration of receipt of this proposal, the receipt agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents. There is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from E-SPIN, or becomes publicly known through no fault of recipient, or is received without obligation of confidentiality to E-SPIN.

TABLE OF CONTENTS

LIST OF FIGURE

EXECUTIVE SUMMARY

[customer] stated operation requirement to perform independent or 3rd party penetration test service for the web portal / web application / custom web site / intranet application / extranet application for new roll out application for security, audit and compliance purpose for their [own or their end client]. We understand your requirements and we are going to work with you to meet those requirements by deliver the service as per required (based on standard package fixed deliverables and scope of service work subscribed, as well as additional service that your may consider before, during and after based on the consulting session). It is our intention to prove this statement through our proposal and by demonstrating our company commitment to a solution that last not product or service approach to solve your service requirement. Our package solution allows us to provide component or service mix that you are require for current and cater for your future without over investment.

The document also serve as statement of service work for penetration test service deliverables.

We are confidence capable to deliver the said project within the timeline package set, the detail project timeline is provide detail outline for how various tasks in perform based on the schedules in project timeline section.

For the standard one IP or URL fixed scope web penetration test service as per detailed scope of work highlight within the service description is as subscribe fee, it take total up to three (3) Man Day (MD) to deliver, inclusive of security recommendation report, whether use it for project vulnerability baseline scan or use for project closure for quality assurance purpose. E-SPIN can always provide full infrastructure penetration testing and site security assessment project that cover complete enterprise wide security, risk and compliance operation, strategic or project requirement. Please consult our consultant based on the scope of work and infrastructure/site/project equipments, network, application involved or event involve supplying, installing, training and maintaining.

WEB APPLICATION SECURITY SCANNING SERVICE

Below are the standard web application security scanning services fixed deliverables:

- It is typical use for web site, web application, portal application (whether intranet or extranet) security assessment, penetration test to found out exploitable vulnerability and identified them into report and provide some suggestion how to close those vulnerabilities being identified
- The service serve the purpose of helping client (1) to evaluate the vulnerability of the application and network components related to the system to potential malicious attacks which may compromise the system integrity, confidentiality, and availability; (2) to identify flaws and loopholes on the application against security breach, if done from outside it is external oriented, if done from inside, it is internal oriented.
- Planned date for service delivering subject upfront confirmation, and require official letter of authorization and permission sort out from partner with the end client or other party involved.
- The scope of work is carry out based on the given one external or internal accessible IP/URL and at least one set of credential to cover target scanning system.

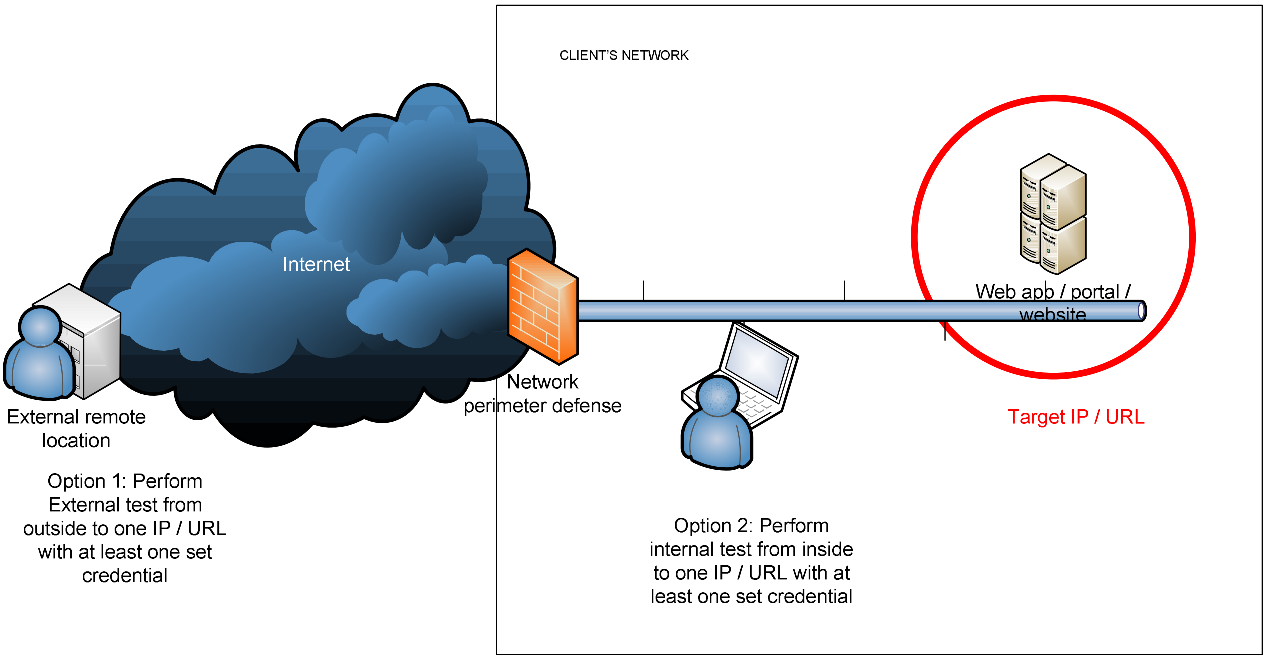

CLIENT'S NETWORK
Internet
External remote location
Option 1: Perform External test from outside to one IP / URL with at least one set credential
Network perimeter defense
Web app / portal / website
Target IP / URL
Option 2: Perform internal test from inside to one IP / URL with at at least one set credential

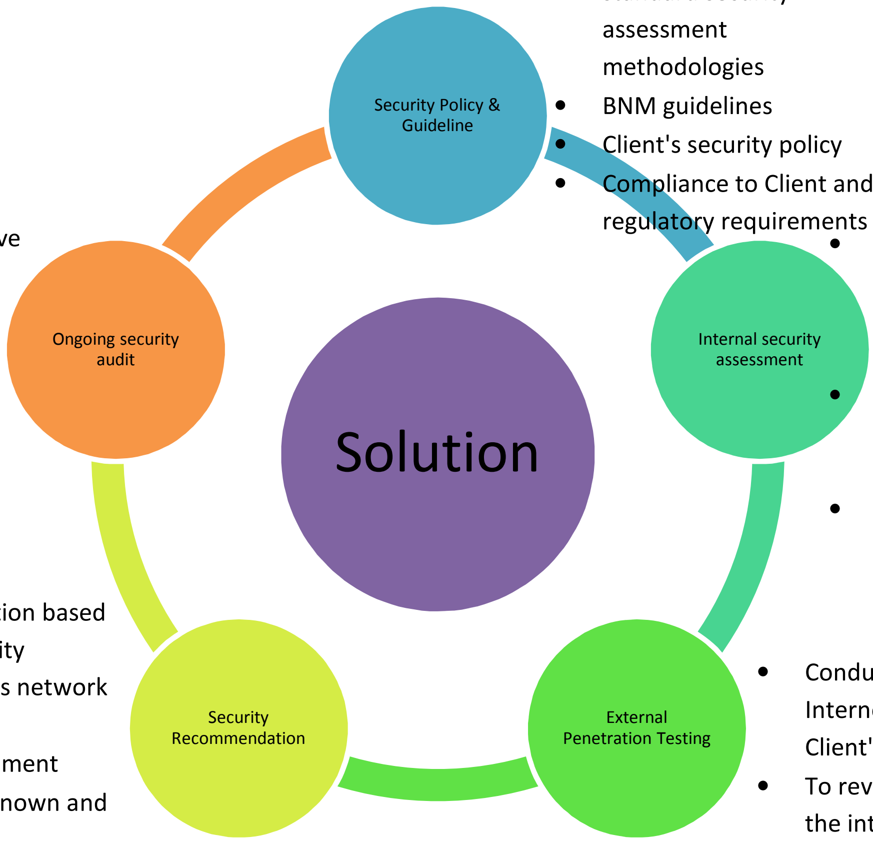
Figure 1 Standard System Diagram from external or internal web application security scanning

More detail scope of service as below:

- Evaluate the possibility of malicious attacks on the system and network which may compromise the system integrity, confidentiality, and availability (for this case, web application system or website/portal application)
- company use industry standard security and vulnerability assessment tools, which may include those employed by "hackers"
- company will perform the service during the scanning time, and generate report to summarize all the vulnerabilities found and recommendation report
- network security scanning is not the scope of subscribe service, , however, partner and client can always may consider doing two time scanning, one from outside, one from inside, please discuss it before, during, after the service deliver as additional complementary service subscription
- vulnerability fixing / mitigation module development and system hardening is not the scope of subscribe service, however, partner and client can always discuss it before, during, after the service deliver as additional complementary service subscription

OUR APPROACH

We have adopted a customer-centred and conservative approach for this project. We focus on the “end-to-end” solution delivery that make the solution work for the customer, it is completeness as single solution without forgot unique constraint within customer working environment. Furthermore, it has being factor in the subscribe service may perform multiple time in future date to build up baseline, project closure or ongoing routine security check, audit and reporting (if Client required this type of service arrangement). This is very practical and common approach for external and then perform internal scan to audit and submit the report for various security, risk and compliance authorities.


Security Policy & Guideline
Internal security assessment
External Penetration Testing
Security Recommendation
Ongoing security audit
Solution

- standard security assessment methodologies
- BNM guidelines
- Client's security policy
- Compliance to Client and regulatory requirements

- local LAN IP vulnerabilities for IP enabled system and device
- Windows/UNIX/Linux workstation & server
- Network equipment (eg switches, router, firewall, AP, SLB)

- Conduct outside Internet boundary of Client's network
- To reveal how much of the internal security risk are exposed to the public and external hackers

- security recommendation based on results of the security assessment and client's network design
- security policy enforcement
- advisory to minimize known and controllable risk

- ongoing proactive, preventive security audit to ensure security and vulnerability control in order

Figure 2 E-SPIN's Full service capability overview and approach

We have the capability to perform infrastructure security assessment, penetration testing, to security hardening, vulnerability fixing and mitigation module development. The complete solution approach for full project engagement include combination of policy & guideline study, internal security assessment, external penetration testing, security recommendation as a full infrastructure security service complete solution package.

This approach is appropriate since there are usually have some uncertainty on your final confirmation, in terms of the work arrangements and preferences for infrastructure security assessment. This approach allows both Client and E-SPIN to make adjustments to the final execution plan before any full investment commitment. And we can roll out the project in phase by phase manner to deliver the service required.

SCOPE OF WEB APPLICATION SECURITY ASSESSMENT

- Below table summarize the web application security assessment service scope of work in easy to understand manner compare with full infrastructure security assessment service.

Item	Task	Frequency
1.0	Study on relevant security policies/guidelines on client environment	No inclusive for pure web app security assessment service subscription. However, Client may always top up and subscribe for the additional service for this
2.0	Internal security assessment covers the scoped Web Application, Operating System, Database, Web Server	No inclusive for pure web app security assessment service subscription. However, in certain circumstance, it can count as one time service delivery, ie three man day service for per URL/IP given with at least one credential. But if app/database/web server spread across multiple server, it take longer time and charge more extra man day.
3.0	External penetration testing	Inclusive, and count as one time service delivery, ie three man day service for per URL/IP given with at least one credential. If CLIENT require us to perform internal and external, it combine total man day required.

4.0	Security assessment and recommendation report	Inclusive, as part of the report deliverables. With security assessment and security recommendation report

STUDY ON RELEVANT SECURITY POLICIES/GUIDELINES SERVICE (IF SUBSCRIBE)

The task here involve study the relevant policies and guidelines to create a security assessment checklist (this is an outline, not a detailed technical checklist) based on a combination of the following:

1) Standard security assessment methodologies
2) Central Bank / Regulatory guidelines
3) Client's security policy

Security assessment will be conducted such that all areas in the checklist are covered in compliance to the Client's and regulatory requirements.

INTERNAL SECURITY ASSESSMENT COVERS WEB APPLICATION, OPERATING SYSTEM, DATABSE, WEB SERVER (IF SUBSCRIBE)

The internal security assessment is conducted within the Client's local area network to identify vulnerabilities of IP-enabled network nodes.

The IP nodes could be any IP-enabled systems or devices, including:

a) MS Windows-based servers and workstations
b) UNIX or Linux servers and workstations
c) Switches, routers, firewalls, access servers and wireless access points

<u>EXCEPT</u>: proprietary or legacy systems such as mainframes, FEP, AS/400, etc.

Security assessment will only be conducted over the network using proven assessment methodologies and tools. No system-level assessment will be conducted.

The tested vulnerabilities will include:

- Operating system vulnerabilities
- TCP/IP protocol (IP/TCP/UDP) vulnerabilities
- Common application protocol (HTTP,FTP,SMTP,SNMP,etc) vulnerabilities
- Buffer overflow vulnerabilities
- Network-enabled backdoors and trojans
- Vulnerabilities in popular applications, e.g. IIS, MS-Exchange, Lotus Notes, etc.

- Weak system configuration resulting in vulnerable exposure
- In Depth Web Application Vulnerabilities (please refer to next page for detail)

List of Web Application vulnerabilities covered in detail:

* Version Check
o Vulnerable Web Servers
o Vulnerable Web Server Technologies – such as “PHP 4.3.0 file disclosure and possible code execution.

* CGI Tester
o Checks for Web Servers Problems – Determines if dangerous HTTP methods are enabled on the web server (e.g. PUT, TRACE, DELETE)
o Verify Web Server Technologies

* Parameter Manipulation
o Cross-Site Scripting (XSS) – over 40 different XSS variations are tested.
o SQL Injection
o Code Execution
o Directory Traversal
o File Inclusion
o Script Source Code Disclosure
o CRLF Injection
o Cross Frame Scripting (XFS)
o PHP Code Injection
o XPath Injection
o Full Path Disclosure
o LDAP Injection
o Cookie Manipulation
o Arbitrary File creation (AcuSensor Technology)
o Arbitrary File deletion (AcuSensor Technology)
o Email Injection (AcuSensor Technology)
o File Tampering (AcuSensor Technology)
o URL redirection
o Remote XSL inclusion

* MultiRequest Parameter Manipulation
o Blind SQL/XPath Injection

* File Checks
o Checks for Backup Files or Directories - Looks for common files (such as logs, application traces, CVS web repositories)
o Cross Site Scripting in URI
o Checks for Script Errors

* Directory Checks
o Looks for Common Files (such as logs, traces, CVS)
o Discover Sensitive Files/Directories
o Discovers Directories with Weak Permissions
o Cross Site Scripting in Path and PHPSESSID Session Fixation.
o Web Applications
o HTTP Verb Tampering

- Text Search
    - Directory Listings
    - Source Code Disclosure
    - Check for Common Files
    - Check for Email Addresses
    - Microsoft Office Possible Sensitive Information
    - Local Path Disclosure
    - Error Messages
    - Trojan shell scripts (such as popular PHP shell scripts like r57shell, c99shell etc)

- Weak Passwords
    - Weak HTTP Passwords

- GHDB Google Hacking Database
    - Over 1200 GHDB Search Entries in the Database

- Port Scanner and Network Alerts
    - Port scans the web server and obtains a list of open ports with banners
    - Performs complex network level vulnerability checks on open ports such as:
        - DNS Server vulnerabilities (Open zone transfer, Open recursion, cache poisoning)
        - FTP server checks (list of writable FTP directories, weak FTP passwords, anonymous access allowed)
        - Security and configuration checks for badly configured proxy servers
        - Checks for weak SNMP community strings and weak SSL cyphers
        - and many other network level vulnerability checks!

Other vulnerability tests may also be performed using the manual tools provided, including:

- Input Validation
- Authentication attacks
- Buffer overflows
- Blind SQL injection
- Sub domain scanning

Web Application Vulnerabilities cover in detailed (below just sample, as it keep expand and update)

- Zomplog v.3.7.6 Local File Inclusion Security Vulnerability
- Zomplog 3.4 SQL Injection and Cross-Site Scripting Security Vulnerability
- Zeroboard v.4.1.pl5 Multiple Remoote File Inclusion Security Vulnerability
- Zend Cart 1.2.6 admin_email SQL Injection Vulnerability Security Vulnerability
- YACS v.6.6.1 File Inclusion Security Vulnerability
- Cross Site Scripting Security Vulnerability
- XOOPS v.2.0.11 SQL Injection and Authentification Bypass Security Vulnerability
- XHP CMS v.0.5 File Upload Security Vulnerability
- XHP CMS v.0.5.1 Cross-Site Scripting Security Vulnerability
- WWWThreads Forum Cross-Site Scripting Security Vulnerability
- XPath Injection vulnerability Security Vulnerability
- WSN Forum 1.21 id SQL Injection Vulnerability Security Vulnerability
- Directories with write permissions enabled Security Vulnerability
- WoWRoster v.1.5.0 Remote File Inclusion Security Vulnerability
- WordPress v.2.1.2 (year) Cross-Site Scripting Security Vulnerability
- WordPress v.2.1.1 - Compromised Installation Security Vulnerability
- WordPress v.2.0.6 Trackback (Zend Hash Del Key Or Index) Injection Security Vulnerability
- WordPress v.2.0.5 Trackback UTF-7 SQL Injection Security Vulnerability
- WordPress v.2.0.3 SQL Injection Security Vulnerability
- WordPress_v.2.0.1_Path_Disclosure.xml Security Vulnerability
- Wordcircle v.2.14 SQL Injection, Login Bypass and Cross-Site Scripting Security Vulnerability
- WizForum 1.20 Multiple SQL Injection Security Vulnerability
- Wili-CMS v.0.11 File Inclusion Security Vulnerability
- WhiteAlbum v.2.5 SQL Injection Security Vulnerability
- Web Wiz Forums v.8.05 (MySQL version) SQL Injection Security Vulnerability
- Web server default welcome page Security Vulnerability
- Web Quiz Pro v.1.0 Cross-Site Scripting Security Vulnerability
- Web Content System v.2.7.1 File Inclusion Security Vulnerability
- WebspotBlogging v.3.0 SQL Injection and Login Bypass Security Vulnerability
- Webspell v.4.01.02 Local File Inclusion Security Vulnerability
- Webspell v.4.01.01 Database Data Disclosure Security Vulnerability
- WebDAV Enabled Security Vulnerability
- WebCalendar v.1.00 (send_reminders.php) Remote File Inclusion Security Vulnerability
- Web-News v.1.6.3 File Inclusion Security Vulnerability
- W2B Online Banking Cross-Site Scripting Security Vulnerability
- W-Agora v.4.2.1 Multiple Security Vulnerabilities
- W-Agora 4.2.0 Cross-Site Scripting Security Vulnerability
- VP-ASP Shopping Cart v.6.09 Multiple Security Vulnerabilities
- Vote Pro v.4.0 Remote Command Execution Security Vulnerability
- Videodb (Mambo component) v.0.3 Remote File Inclusion Security Vulnerability
- Vego Links Builder v.2.00 SQL Injection and Login Bypass Security Vulnerability
- URL redirection Security Vulnerability

- Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1 Security Vulnerability
- Typo3 v.3.8.1 Path Disclosure Security Vulnerability
- TWiki rev Parameter Remote Command Execution Security Vulnerability
- Trojan shell script Security Vulnerability
- TRACK method is enabled Security Vulnerability
- TRACE method is enabled Security Vulnerability
- TOPo v.2.2.178 Remote Code Execution Security Vulnerability
- TOPo v.2.2.178 Cross-Site Scripting Security Vulnerability
- ToendaCMS v.1.0.0 (FckEditor) File Upload Security Vulnerability
- Toast Forums v.1.6 Cross-Site Scripting Security Vulnerability
- Timesheet PHP 1.2.1 SQL Injection Security Vulnerability
- Tim-online PHPBB v1.2.4RC3 (Mambo component) Remote File Inclusion Security Vulnerability
- Tiki Wiki v.1.9.4 JHot.PHP Remote Command Execution Security Vulnerability
- Tiki Wiki v.1.9.3.1 Cros-Site Scripting Security Vulnerability
- Thyme v.1.3 Cross-Site Scripting Security Vulnerability
- Techno Dreams Products login.asp SQL Injection Vulnerability Security Vulnerability
- Teca Diary Personal Edition v.1.0 SQL Injection Security Vulnerability
- TeamCal Pro v.2.8.001 File Inclusion Security Vulnerability
- SZUserMgnt v.1.4. SQL Injection and login Bypass Security Vulnerability
- Survey System 1.1 SURVEY_ID parameter SQL Injection Security Vulnerability
- SunShop Shopping Cart v.3.5 Cross-Site Scripting Security Vulnerability
- ssCMS v.2.1.0 Cross-Site Scripting Security Vulnerability
- SQuery v.4.5 (phpNuke module) Remote File Inclusion Security Vulnerability
- SQL injection Security Vulnerability
- Source code disclosure Security Vulnerability
- SmartSiteCMS v1.0 Remote File Inclusion Security Vulnerability
- SKForum v.1.5 Cross-Site Scripting Security Vulnerability
- SiteEnable v.3.3 Cross-Site Scripting Security Vulnerability
- Simplog v.0.9.1 File Inclusion Security Vulnerability
- Simplog v.0.9.1 Cross-Site Scripting Security Vulnerability
- Simplog SQL Injection Security Vulnerabilities
- Simple PHP Blog v.0.4.7.1 Local File Inclusion Security Vulnerability
- Simpleboard v1.1.0 (Mambo component) Remote File Inclusion Security Vulnerability
- SimpleBlog v.3.0 SQL Injection Security Vulnerability
- SimpleBlog v.2.1 SQL Injection Security Vulnerability
- SimpleBBS v.1.1 name PHP Code Injection Security Vulnerability
- Signkorn Guestbook v.1.1 File Inclusion Security Vulnerability
- Sensitive data not encrypted Security Vulnerability
- SendCard v.3.4.0 Unautorized Administrative Access Security Vulnerability
- sCssBoard 1.12 search_term Cross-Site Scripting Security Vulnerability
- Script source code disclosure Security Vulnerability
- ScriptMagix Recipes v.2.0 Multiple SQL Injection Security Vulnerability
- ScriptMagix Lyrics v.2.0 (recid) SQL Injection Security Vulnerability
- ScriptMagix Jokes v.2.0 Multiple SQL Injection Security Vulnerability
- SazCart v.1.5 File Inclusion Security Vulnerability

- SaveWebPortal v.3.4 Remote File Inclusion Security Vulnerability
- SAPID CMS v.1.23rc3 Remote File Inclusion Security Vulnerability
- Snitz Forums 2000 v.3.4.05 post.asp Cross-Site Scripting Security Vulnerability
- RunCMS v.1.3a5 Cross-Site Scripting Security Vulnerability
- Qwiki v.1.5.1 Cross-Site Scripting Security Vulnerability
- QuizShock v.1.6.1 Cross-Site Scripting Security Vulnerability
- QuickEStore v.7.9 SQL Injection and Path Diclosure Security Vulnerability
- QontentOneCMS v1.0 Cross-Site Scripting Security Vulnerability
- PUT Method Enabled Security Vulnerability
- Publicist v.0.95 SQL Injection, Path Disclosure and Cross-Site Scripting Security Vulnerability
- ProjectApp_v.3.3_Cross-Site_Scripting.xml Security Vulnerability
- PRINTER ISAPI filter mapped Security Vulnerability
- pppBlog v.0.3.8 Local File Disclosure Security Vulnerability
- Possible sensitive files Security Vulnerability
- PortalApp v.3.3 Cross-Site Scripting Security Vulnerability
- Popper v.1.41.r2 File Inclusion Security Vulnerability
- PmWiki v.2.1.19 File Inclusion Security Vulnerability
- PmWiki 2.0.12 q-Parameter Cross-Site Scripting Security Vulnerability
- PluggedOut Blog v.1.9.9c SQL Injection Security Vulnerability
- Pivot v1.30 RC2 Multiple Input Validation Security Vulnerabilities
- PHP Zend_Hash_Del_Key_Or_Index Security Vulnerability
- PHP version older than 5.2.1 Security Vulnerability
- PHP version older than 4.4.1 Security Vulnerability
- PHP version older than 4.3.8 Security Vulnerability
- PHP upload arbitrary file disclosure vulnerability Security Vulnerability
- PHP unspecified remote arbitrary file upload vulnerability Security Vulnerability
- PHP undefined Safe_Mode_Include_Dir safemode bypass Security Vulnerability
- PHP socket_iovec_alloc() integer overflow Security Vulnerability
- PHP Simple Shop v.2.0 Remote File Inclusion Security Vulnerability
- PHP Safedir Restriction Bypass Vulnerabilities Security Vulnerability
- PHP POST file upload buffer overflow vulnerabilities Security Vulnerability
- PHP multiple vulnerabilities Security Vulnerability
- PHP mail function ASCII control character header spoofing Security Vulnerability
- PHP HTTP POST incorrect MIME header parsing Security Vulnerability
- PHP HTML Entity Encoder Heap Overflow Security Vulnerability
- PHP error logging format string Security Vulnerability
- PHP code injection Security Vulnerability
- PHP Classifieds v.6.20 SQL Injection and Login Bypass Security Vulnerability
- PHP Classifieds v.6.20 Cross-Site Scripting Security Vulnerability
- PHP Advanced Transfer Manager v.1.21 File Inclusion Security Vulnerability
- PHP Advanced Transfer Manager System Disclosure and Remote Code Execution (Windows) Security Vulnerability
- PHP Advanced Transfer Manager System Disclosure and Remote Code Execution (Unix) Security Vulnerability
- PHP 4.3.0 file disclosure and possible code execution Security Vulnerability

- PHPX v.3.5.15 Multiple SQL Injection and Cross-Site Scripting Security Vulnerability
- PhpWebThings 1.4.4 forum.php SQL Injection Security Vulnerability
- phpWebFTP v.3.2 Local File Inclusion (windows) Security Vulnerability
- phpWebFTP v.3.2 Local File Inclusion (unix) Security Vulnerability
- PHPTB 2.0 Code Injection Security Vulnerabilities
- phpSysInfo 2.3 Cross-File Scripting Security Vulnerability
- PHPStatus v.1.0 SQL Injection and Login Bypass Security Vulnerability
- PHPSESSID session fixation Security Vulnerability
- PHPNuke v.7.9 Cross-Site Scripting Security Vulnerability
- PHPNuke v.7.9 SQL Injection Security Vulnerability
- PHPNuke Remote Directory Traversal Security Vulnerability
- PHPNuke Remote Directory Traversal (Unix) Security Vulnerability
- PHPNuke 7.6 Multiple SQL Injection Security Vulnerability
- PHPNuke 7.5 (admin_styles.php) Remote File Inclusion Security Vulnerability
- phpMyFAQ 1.5.1 SQL Injection Security Vulnerability
- phpMyAdmin Path Disclosure and Response Splitting Security Vulnerability
- phpMyAdmin "grab_globals.lib.php" Directory Traversal Vulnerability Security Vulnerability
- phpMyAdmin Cross-Site Scripting Security Vulnerability
- phpListPro v.2.0.0 File Inclusion Security Vulnerability
- PhpLinkExchange v.1.0 Remote File Inclusion Security Vulnerability
- phpLDAPadmin Command Execution Security Vulnerability
- PHPKB v.1.5 Cross Site Scripting Security Vulnerability Security Vulnerability
- PHPjournaler v.1.0 SQL Injection Security Vulnerability
- PHPinfo page found Security Vulnerability
- PhpHostBot v.1.0 Remote File Inclusion Security Vulnerability
- PHPGreetz 0.99 Remote File Include Vulnerability Security Vulnerability
- PhpGedView v.3.3.7 File Inclusion and PHP Code Injection Security Vulnerability
- phpFullAnnu v.5.1 File Inclusion Security Vulnerability
- PHPEasyData Pro v.2.2.2 SQL Injection Security Vulnerability
- phpCommunityCalendar login bypass, SQL injection and cross site scripting Security Vulnerability
- PHPCollab v.2.4 SQL Injection Security Vulnerability
- phpCOIN v.1.2.2 Cross-Site Scripting Security Vulnerability
- phpBB XS Build 058 File Inclusion and Cross-Site Scripting Security Vulnerability
- phpBB Addon: Hacks List v.1.20 Local File Inclusion Security Vulnerability
- phpBB 2.0.15 Viewtopic.php Remote Code Execution Vulnerability Security Vulnerability
- phpArcadeScript v.2.0 Cross-Site Scripting Security Vulnerability
- PHP4 multiple vulnerabilities Security Vulnerability
- PHP4 IMAP module buffer overflow Security Vulnerability
- PHP.exe Windows CGI for Apache may let remote users view files on the server Security Vulnerability
- PHP-Fusion 6.00.109 SQL Injection Security Vulnerability
- PhotoPost v.4.6 File Inclusion Security Vulnerability
- photokorn v.1.542 SQL Injection Security Vulnerability
- Phorum v.5.1.18 (admin.php) Cross-Site Scripting Security Vulnerability
- Pentacle In-Out Board v.6.03.0.0080 SQL Injection and Login Bypass Security Vulnerability
- PEAR XML_RPC 1.3.0 Remote Command Execution Security Vulnerability

- Pearl For Mambo v.1.6 Remote File Inclusion Security Vulnerability
- Pearl Forums 2.4 SQL Injection Security Vulnerability
- PBLang 4.65 System Disclosure and Remote Code Execution Security Vulnerability
- Particle Blogger v.1.2.0 (posid) SQL Injection Security Vulnerability
- Pagesetter v.6.2.0 (PostNuke module) Local File Inclusion Security Vulnerability
- paBugs v.2.0b3 File Inclusion Security Vulnerability
- oaboard 1.0 SQL Injection Security Vulnerability
- Owl v.0.82 File Inclusion Security Vulnerability
- Ottoman v.1.1.2 File Inclusion Security Vulnerability
- osCommerce v.2.2 Cross-Site Scripting Security Vulnerability
- Orca Forum 4.3.b msg SQL Injection Security Vulnerability
- OrbitHYIP v.2.0 Cross-Site Scripting Security Vulnerability
- OpenPHPNuke v.2.3.3 File Inclusion Security Vulnerability
- OpenERM v.2.8.1 File Inclusion Security Vulnerability
- OpenEdit v.4.0 Cross-Site Scripting Security Vulnerability
- oaboard v.1.0 SQL Injection Security Vulnerability
- N/X CMS v.4.1 File Inclusion Security Vulnerability
- NZ Ecommerce Cross Site Scripting and SQL Injection Security Vulnerability
- Nodez v.4.6.1.1 Cross-Site Scripting and Local File Inclusion Security Vulnerability
- NKads v.1.0.a3 Login SQL Injection Vulnerability Security Vulnerability
- Netquery "host" Parameter Arbitrary Command Execution Security Vulnerability
- NetOffice v.2.5.3-pl1 SQL Injection Security Vulnerability
- My Gaming Ladder v.7.0 File Inclusion Security Vulnerability
- MyTopix v.1.2.3 SQL Injection And Path Disclosure Security Vulnerability
- MySource 2.14.0 Cross-Site Scripting and File Inclusion Security Vulnerabilities
- MyPHP CMS v.0.3 Remote File Inclusion Security Vulnerability
- myEvent v.1.4 Multiple Security Vulnerabilities
- MyBulletinBoard v.1.1.5 SQL injection Security Vulnerability
- MyBuletinBoard v.1.1.7 Cross-Site Scripting Security Vulnerability
- MyBuletinBoard v.1.0.2 Table Prefix Weakness Security Vulnerability
- myBloggie SQL Injection and login bypas Security Vulnerability
- myBloggie v.2.1.4 SQL Injection Security Vulnerability
- Musicbox v.2.3 SQL Injection Security Vulnerability
- Musicbox v.2.3 Cross-Site Scripting Security Vulnerability
- MultiCalendars-v.3.0-SQL-Injection Security Vulnerability
- MODx v.0.9.2.1 File Inclusion Security Vulnerability
- miniBloggie v.1.0 SQL Injection and Login Bypass Security Vulnerability
- MiniBILL v.1.2.4 File Inclusion Security Vulnerability
- Minerva v.238a File Inclusion Security Vulnerability
- Microsoft IIS Cookie Variable Information Disclosure Security Vulnerability
- MercuryBoard v.1.1.4 SQL Injection Security Vulnerability
- MaxxSchedule v.1.0 Cross-Site Scripting Security Vulnerability
- MAXdev MD-Pro v.1.0.76 Path Disclosure Security Vulnerability
- MAXdev MD-Pro v.1.0.76 Cross-Site Scripting Security Vulnerability
- Mantis 1.00 File Inclusion and SQL Injection Vulnerabilities (Windows) Security Vulnerability

- Mantis 1.00 File Inclusion and SQL Injection Vulnerabilities (Unix) Security Vulnerability
- Mambo v.4.5.3h SQL Injection and Login Bypass Security Vulnerability
- Mambo v.4.5.2 (tar.php) Remote File Inclusion Security Vulnerability
- Mambo up to v.4.6.1 SQL Injection and Login Bypass Security Vulnerability
- MailGust 1.9 SQL Injection Security Vulnerability
- Maian Weblog v.2.0 SQL Injection Security Vulnerability
- Maian Events v.1.00 SQL Injection Security Vulnerability
- Magic News Lite v.1.2.3 Code Injection Security Vulnerability
- Macromedia Dreamweaver Remote Database Scripts Security Vulnerability
- lucidCMS 1.0.11 SQL Injection and Login Bypass Security Vulnerability
- Loudmouth (Mambo component) v.4.0 Remote File Inclusion Security Vulnerability
- Loudblog v.0.4 File Inclusion and PHP Code Injection Security Vulnerability
- LocazoList Classifieds v.1.03c SQL Injection Security Vulnerability
- Lizard Cart CMS v.1.0.4 id parameter SQL Injection Security Vulnerability
- LinPHA v.1.0 Local File Inclusion Security Vulnerability
- Leadhound 2006-04-28 Cross Site Scripting Security Vulnerability
- LDAP Injection vulnerability Security Vulnerability
- JiRo's FAQ Manager v.1.x SQL Injection Security Vulnerability
- JetPhoto Server v.1.x Cross-Site Scripting Security Vulnerability
- Jamroom v.3.0.16 Cross-Site Scripting Security Vulnerability
- iWare Professional v.5.0.4 Remote Code Execution Security Vulnerability
- Invision Power Board v2.1.6 SQL injection Security Vulnerability
- Invision Power Board v.2.0.3 Cross-Site Scripting Security Vulnerability
- IntranetApp v.3.3 Cross-Site Scripting Security Vulnerability
- Interspire FastFind v.2006-10-09 Cross-Site Scripting Security Vulnerability
- Integramod Portal v.2.0 File Inclusion Security Vulnerability
- Instant Photo Gallery v.1.0 SQL Injection Security Vulnerability
- IIS server variables backup file Security Vulnerability
- Internet Information Server returns IP address in HTTP header (Content-Location) Security Vulnerability
- IIS extended unicode directory traversal vulnerability Security Vulnerability
- IISWorks ASP KnowledgeBase v2.x Cross-Site Scripting Security Vulnerability
- IDQ ISAPI filter mapped Security Vulnerability
- IDC ISAPI filter mapped Security Vulnerability
- IDA ISAPI filter mapped Security Vulnerability
- HTW ISAPI filter mapped Security Vulnerability
- HTR ISAPI filter mapped Security Vulnerability
- GreenBeast CMS v.1.3 File Upload Security Vulnerability
- Google Search Appliance UTF-7 Cross-Site Scripting Security Vulnerability
- Google API Search Engine v.1.3.1 Script Cross-Site Scripting Security Vulnerability
- Gemini v.2.0 Cross Site Scripting Security Vulnerability
- GeekLog v1.4.0 Remote File Inclusion Security Vulnerability
- GeekLog v1.4.0 FckEditor File Upload Security Vulnerability
- Gcards v.1.45 SQL Injection and Login Bypass Security Vulnerability
- Gcards 1.44 limit parameter SQL Injection Security Vulnerability
- Gallery "g2_itemId" Disclosure of Sensitive Information (Windows) Security Vulnerability

- Gallery "g2_itemId" Disclosure of Sensitive Information (Unix) Security Vulnerability
- Gallery v.2.03 Local File Inclusion Security Vulnerability
- Galleria v1.0 (Mambo component) Remote File Inclusion Security Vulnerability
- Full path disclosure Security Vulnerability
- Frontpage Extensions Enabled Security Vulnerability
- Frontpage authors.pwd available Security Vulnerability
- FreeWebshop v.2.2.1 SQL Injection and Local File Inclusion Security Vulnerability
- Freekot v.1.01 SQL Injection and Login Bypass Security Vulnerability
- freeForum 1.1 thread SQL Injection Security Vulnerability
- Flyspray 0.9.8 Cross-Site Scripting Security Vulnerability
- Flushcms v1.0.0.pre2 Remote File Inclusion Security Vulnerability
- File inclusion Security Vulnerability
- FAQ System 1.1 Multiple SQL Security Vulnerabilities
- ezContents v.2.0.3 Multiple Security Vulnerabilities
- eyeOS Project v.0.8.9 PHP Code Execution Security Vulnerability
- eWebquiz v.8.0 (QuizID) SQL Injection Security Vulnerability
- Etomite CMS v.0.6.1 SQL Injection Security Vulnerability
- Etomite CMS v.0.6.1 File Upload Security Vulnerability
- Enterprise Connector v.1.02 Multiple SQL Vulnerabilities Security Vulnerability
- Envolution v.1.1.0 Cross-Site Scripting and SQL Injection Security Vulnerability
- Enhanced Simple PHP Gallery v.1.7 Cross-Site Scripting and Path Disclosure Security Vulnerability
- Email address found Security Vulnerability
- EkinBoard 1.0.3 config.php SQL Injection, Board Take Over, Cross-Site Scripting Security Vulnerability
- Eggblog v.3.6 SQL Injection Security Vulnerability
- eFiction v.3.1 (path_to_smf) Remote File Inclusion Security Vulnerability
- eFiction 1.1 Cross Site Scripting and SQL Injection Security Vulnerability
- EDirectoryPro 2006-05-09 SQL Injection Security Vulnerability
- EasyMoblog v.0.5.1 Cross-Site Scripting Security Vulnerability
- e107 v0617 SQL Injection and Code Execution Security Vulnerability
- E-School Management System v.1.0 Cross-Site Scripting Security Vulnerability
- e-moBLOG v.1.3 SQL Injection and Login Bypass Security Vulnerability
- Drupal v.4.7.2 Cross-Site Scripting Security Vulnerability
- Dragonfly CMS v.9.0.6.1 Cross-Site Scripting Security Vulnerability
- dotproject v.2.0.1 File Inclusion and Information Disclosure Security Vulnerability
- dotNetBB v2.42EC.SP3 Cross-Site Scripting Security Vulnerability
- DokuWiki v.2006-03-09b dwpage.php Remote Code Execution Security Vulnerability
- DokuWiki v.2006-03-09b Cross-Site Scripting Security Vulnerability
- DoceboLMS 2.04 System Disclosure (Unix) Security Vulnerability
- Directory Traversal Security Vulnerability
- Directory Listing Security Vulnerability
- Directories with executables permission enabled Security Vulnerability
- Digital Scribe 1.4 Login Bypass, SQL Injection and Remote Code Execution Security Vulnerability
- Diesel Joke Sike v.2006.05.25 SQL Injection Security Vulnerability
- DEV web management system v1.5 SQL Injection and Cross-Site Scripting Security Vulnerability
- DeluxeBB v1.08 SQL injection Security Vulnerability

- DELETE Method Enabled Security Vulnerability
- Cyphor 0.19 SQL Injection, Board Takeover, Cross-Site Scripting Security Vulnerability
- CyberBuild 06.05.03 SQL Injection and Cross-Site Scripting Security Vulnerability
- CVS Web Repository Security Vulnerability
- Common files Security Vulnerability
- Cute News v.1.4.5 Cross-Site Scripting Security Vulnerability
- Cute News 1.4.1 Local File Inclusion Security Vulnerability
- CuteNews 1.4.1 Shell Injection Security Vulnerability
- CubeCart v.2.0.7 Cross-Site Scripting Security Vulnerability
- Cross Site Scripting in URI Security Vulnerability
- Cross Site Scripting in path Security Vulnerability
- XFS vulnerability Security Vulnerability
- CRLF injection/HTTP response splitting Security Vulnerability
- CRE Loaded v.6.15 files.php File Upload Security Issue Security Vulnerability
- Creative Community Portal v.1.1 SQL Injection Security Vulnerability
- Absolute FAQ Manager v.4.0 Cross-Site Scripting Security Vulnerability
- Aardvark Topsites PHP v.4.2.2 File Inclusion Security Vulnerability
- Acidcat v.2.1.13 SQL Injection Security Vulnerability
- Active Auction Pro v.7.0 (catid) SQL Injection Security Vulnerability
- Active Newsletter v.4.3 (NewsPaperID) SQL Injection Security Vulnerability
- Active Photo Gallery 20070326 (catid) SQL Injection Security Vulnerability
- Active Trade v.2.x (catid) SQL Injection Security Vulnerability
- Ades Guestbook v.2.0 Cross-Site Scripting Security Vulnerability
- ADN Forum v.1.0b SQL Injection and Cross-Site Scripting Security Vulnerability
- ADOdb Insecure Test Scripts Security Issues Security Vulnerability
- ADP Forum v.2.0.2 users Exposure of User Credentials Security Vulnerability
- Advanced Guestbook v.2.3.1 File Inclusion Security Vulnerability
- FAQ 1.0 SQL Injection Security Vulnerability
- Ajax Portal v.3.0 SQL Injection Security Vulnerability
- Alex Guestbook v.4.0.1 Cross Site Scripting Security Vulnerability
- AlstraSoft Affiliate Network Pro v.7.2 Multiple Security Vulnerabilities
- Alstrasoft Article Manager Pro v.1.6 SQL Injection, Path Disclosure and Cross-Site Scripting Security Vulnerability
- AlstraSoft Template Seller Pro 3.25 File Inclusion, Code Injection, SQL Injection and Login Bypass Security Vulnerability
- Amazon Store Manager v1.0 Cross-Site Scripting Security Vulnerability
- AndoNET Blog SQL Injection Security Vulnerability
- Andromeda v.1.9.3.4 Cross-Site Scripting Security Vulnerability
- Apache 2.x Version Older Than 2.0.46 Security Vulnerability
- Apache 2.0.39 Win32 Directory Traversal Security Vulnerability
- Apache 2.0.44 Win32 File Reading Vulnerability Security Vulnerability
- Apache 2.x Version Equal to 2.0.51 Security Vulnerability
- Apache 2.x Version Older Than 2.0.43 Security Vulnerability
- Apache 2.x Version Older Than 2.0.45 Security Vulnerability
- Apache 2.x Version Older Than 2.0.47 Security Vulnerability

- Apache 2.x Version Older Than 2.0.48 Security Vulnerability
- Apache 2.x version older than 2.0.49 Security Vulnerability
- Apache 2.x Version Older than 2.0.51 Security Vulnerability
- Apache 2.x version older than 2.0.55 Security Vulnerability
- Apache Configured to Run as Proxy Security Vulnerability
- Apache Error Log Escape Sequence Injection Security Vulnerability
- Apache HTTP CONNECT method is enabled Security Vulnerability
- Apache Mod_Rewrite Off-By-One Buffer Overflow Security Vulnerability
- Apache Mod_SSL Log Function Format String Security Vulnerability
- Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Security Vulnerability
- Apache Server-Info Enabled Security Vulnerability
- Apache Server-Status Enabled Security Vulnerability
- Apache Version Older than 1.3.27 Security Vulnerability
- Apache Version Older than 1.3.28 Security Vulnerability
- Apache Version Older than 1.3.29 Security Vulnerability
- Apache Version Older than 1.3.31 Security Vulnerability
- Apache Version Older than 1.3.34 Security Vulnerability
- Apache Version up to 1.3.33 htpasswd Local Overflow Security Vulnerability
- Apache Win32 Batch File Remote Command Execution Security Vulnerability
- Application Error Message Security Vulnerability
- Articlebeach v.2.0 File Inclusion Security Vulnerability
- Artmedic Newsletter v.4.1.2 Remote Code Execution Security Vulnerability
- ASP Survey v1.10 SQL Injection and Login Bypass Security Vulnerability
- ASP.NET Application Trace Enabled Security Vulnerability
- ASP.NET Debugging Enabled Security Vulnerability
- ASP.NET Path Disclosure Security Vulnerability
- Atlantis Knowledge Base Software v.3.0 SQL Injection Security Vulnerability
- ATUTOR 1.5.1 SQL Injection, Local File Inclusion and Command Execution Security Vulnerability
- ATUTOR v.1.5.3 Cross Site Scripting Security Vulnerability
- Ay-System CMS-v.2.6-File-Inclusion Security Vulnerability
- b2Evolution-v.1.8.6 Cross-Site Scripting Security Vulnerability
- Backup files Security Vulnerability
- Battleaxe Software Forums v.2.0 Cross-Site Scripting Security Vulnerability
- Big Webmaster Guestbook v.1.02 Cross-Site Scripting Security Vulnerability
- Bit5blog v.8.1 SQL Injection and Login Bypass Security Vulnerability
- Blind SQL/XPath injection Security Vulnerability
- BLOG:CMS v4.0.0 SQL Injection Security Vulnerability
- bMachine v.2.9b Cross-Site Scripting Security Vulnerability
- BP Blog v.7.0 (layout) SQL Injection Security Vulnerability
- BTI-Tracker v.1.3.2 File Deletion Vulnerability Security Vulnerability
- Calendarix v.1.6 SQL Injection and Login Bypass Security Vulnerability
- Calendarix v.1.x Cross-Site Scripting Security Vulnerability
- CALimba v.0.99.2 Sql Injection and Login Bypass Security Vulnerability
- Cattadoc v.3.0 File Disclosure
- CcCounter v.2b (dir) Cross-Site Scripting Security Vulnerability

- Check for Apache Versions up to 1.3.25, 2.0.38 Security Vulnerability
- Chi Kien Uong Advanced Poll 2.03 Cross-Site Scripting Security Vulnerability
- Chipmunk Forum Cross-Site Scripting Security Vulnerability
- Chipmunk Topsites Cross-Site Scripting Security Vulnerability
- Claroline v.1.7.4 Local File Inclusion and Cross Site Scripting Security Vulnerability
- Claroline v.1.7.7 File Inclusion Security Vulnerability
- classifiedZONE v.1.2 Cross-Site Scripting Security Vulnerability
- Clever Copy v.3.0 SQL Injection Security Vulnerability
- Code execution Security Vulnerability
- Codegrrl Arbitrary Code Execution and Local File Inclusion Security Vulnerability
- ColdFusion path disclosure Security Vulnerability
- ColdFusion User-Agent Cross-Site Scripting Security Vulnerability
- Community Builder Component v.1.0 File Inclusion Security Vulnerability
- Confixx 3 Professional v.3.1.2 SQL Injection Security Vulnerability
- Connect Daily v.3.2.9 Cross-Site Scripting Security Vulnerability
- CONTROLzx HMS v.3.3.4 Cross-Site Scripting Security Vulnerability
- Cookie manipulation Security Vulnerability
- Coppermine Photo Gallery v.1.4.2 relocate_server.php Exposure of Configuration Security Vulnerability
- Coppermine Photo Gallery v.1.x (phpNuke module) Remote File Inclusion Security Vulnerability
- cPanel v.10.8.2.118 Cross-Site Scripting Security Vulnerability
- WebCalendar v.4.0 SQL Injection Security Vulnerability
- 99articles File Inclusion Security Vulnerability

EXTERNAL PENETRATION TESTING

The external penetration testing will be conducted outside the Internet boundary of the Client's network, typically from E-SPIN's office.

An external assessment will help to reveal the exposure of the Client's network to the Internet. It will also provide information on how much of the internal security risks are exposed to the public.

NETWORK, SYSTEM, DATABASE, SERVER, WEB APPLICATION, DATA, PROCESS SECURITY RECOMMENDATION

Security recommendation will be provided based on the following:

1) a study on the Client's network design
2) results of the security assessment

Technical recommendations will be provided to advise the Client on best practices to improve the network, application, system, server, database, data, and process security posture.

STATEMENT OF SCOPE OF SERVICE WORK (SOW)

The scope of work and responsibilities for the IT security assessment services shall be as follows:

1) E-SPIN shall perform security assessment on the Client's network using proven penetration testing methodologies and tools. The scope of assessment is strictly limited to IP-enabled systems and devices as per fixed scope of work The assessment will be conducted during normal business operating hours (9am – 5pm on weekdays).
2) E-SPIN shall analyse the security assessment results and submit a report cover all the security assessment service deliverables.
3) E-SPIN shall provide network, system, database, application, web, data and server security recommendations for remedial actions for discovered vulnerabilities as well as to improve the general security best practice for the items covered within the scope of work only.

OUT-OF-SCOPE

The following are NOT INCLUDED in this proposal

1. Implementation of the mitigating measures and recommendations, unless the additional service is subscribe with additional service fee involve.
2. System reconfiguration, fine-tuning, patching, etc, unless the additional service is subscribed with additional service fee involve.
3. Security hardening, vulnerability fixing and mitigation module development, security consulting, unless the additional service is subscribe with additional service fee involve

DELIVERABLES

Item	Task	Frequency
1	Security Assessment Report	One time
2	Security Recommendation Report	One time

Reports will be submitted within 5 working days from the date of completion of each exercise, and in two set of e copy, one for End client, one for E-SPIN filing.

CLIENT’S RESPONSIBILITIES

It is expected of the Client to fulfil the following responsibilities during the course of the project:

1. The client shall ensure the network and application to be assessed is up and operational throughout the penetration testing exercise. All servers and network devices to be assessed shall be powered up and operational when the assessment is conducted.
2. The Client shall provide E-SPIN’s personnel with access to its internal networks and servers, typically an Ethernet network point connected to the same network segment as the server farm
3. The Client shall furnish a list of systems and devices to be assessed.
4. Optional - The Client shall provide all the required logs to E-SPIN in a timely manner or outsourcing to E-SPIN. The Client shall ensure that logging is enabled on the relevant systems.

PROJECT TASKS

Item	Task	Duration	Frequency
1	Study on security policies/guidelines	5 days	one time, if subscribe
2	Internal security assessment	5 days	one time, if subscribe
3	External penetration testing	3 days	one time, if subscribe
4	Conduct of post scan of the web application security (to enable pre- and post- scan comparison)	3 days	one time, if subscribe
4	security recommendation	3 days	one time, if subscribe

SAMPLE AGREEMENT

Security Assessment Service Agreement

<CLIENT NAME> (hereafter referred to as the client) explicitly agrees to employ the services of E-SPIN (hereafter referred to as E-SPIN) for conducting a security assessment of its network.

The following are the terms of this engagement:

1. The client is in legal valid possession of the network and wishes E-SPIN to provide the security assessment of its network.
2. E-SPIN will employ crafted tools for scanning and analyzing vulnerabilities on the network. The client agrees to the use of such tools by E-SPIN and indemnifies against any possible recourse, either by the client or its service provider.
3. E-SPIN will restrict itself to analyzing the vulnerabilities of the network shall not penetrate into network or devices. E-SPIN will take utmost care not to compromise the system, intentionally or otherwise, and will only present the vulnerability or attack that can be used to gain access or glean information of the system. E-SPIN assures complete confidentiality and trust in conducting the penetration test. If the client wishes, E-SPIN can enter into a separate non-disclosure agreement with the client to ensure confidentiality of the information.
4. E-SPIN has signed non-disclosure agreement with its employee who would be conducting the said assessment. A full report with the vulnerability found and log of activities will be provided to the client upon the completion of the assignment.
5. Due to the sensitivity of the report, E-SPIN will provide only a two copy to the authorized person of client and the circulation of the report shall be in consultation with E-SPIN.

E-SPIN and the client express their agreement to the terms described above in full.

For E-SPIN	For <CLIENT NAME>
Vincent Lim	
General Manager	
Date:	Date:

SAMPLE NON-DISCLOSURE AGREEMENT (NDA)

E-SPIN

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the “Agreement”) is made between E-SPIN, and <client’s name>

(“COMPANY”) and entered into this ___day of , 20___.

In consideration of the mutual promises and covenants contained in this Agreement for the mutual disclosure of confidential information to each other, the parties hereto agree as follows:

1) Confidential Information and Confidential Materials
   a) “Confidential Information” means nonpublic information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. “Confidential Information” includes, without limitation, information relating to released or unreleased Disclosing Party software or hardware products, the marketing or promotion of any Disclosing Party product, Disclosing Party’s business policies or practices, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement
   b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party’s breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party prior to Disclosing Party’s disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party; or (iv) is independently developed by Receiving Party.
   c) “Confidential Materials” shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

2) Restrictions
   a) Receiving Party shall not disclose any Confidential Information to third parties. However, Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided Receiving Party shall give Disclosing Party reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent.
   b) Receiving Party shall take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information. Receiving Party may disclose Confidential Information or Confidential Material only to Receiving Party’s employees or consultants on a need-to know basis. Receiving Party will have executed or shall execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement.
   c) Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party’s business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3) Rights and Remedies

a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

b) Receiving Party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

c) Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

4) Miscellaneous

a) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

b) In case of any dispute, both the parties agree for neutral third party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. Only if the dispute cannot be settled during the above process, the parties may approach the courts of Malaysia, who shall have the exclusive jurisdiction in such matters.

c) If either party employs attorneys to enforce any rights arising out of or relating to this Agreement, the prevailing party shall be entitled to recover reasonable attorney's fees through due process of law.

d) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

e) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

f) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

For E-SPIN	For <Client Name>
(signature)	(signature)
Name:	Name:
Designation:	Designation:
Date:	Date:

ASSESSMENT TOOLS

The following are the list of tools potentially used by the assessment team. However, the actual selection of tools is at the discretion of the lead assessment consultant.

ACUNETIX OR BURP SUITE PRO WEB APPLICATION VULNEARBILITIES SCANNER AND REPORTER

Acunetix or Burp Suite Pro WVS is worldwide leading "hacking" tool kit that use by worldwide leading security expert to perform web application vulnerabilities scanning by attacking the web application just like true hacker does to exploit for any vulnerabilities, cover full ranges of attacks and vulnerabilities areas:

It is also common use for generate professional and workable reports based on the findings for developer or submit for compliance authorities.

GFI LANGUARD NETWORK SECURITY SCANNER AND PORT SCANNER

It is common deployed and widely use commercial tool to perform network port scanning and use to generate professional and workable reports based on the findings for developer or submit for compliance authorities. It can use for automated and distributed vulnerabilities fix and patches.

NESSUS

Nessus is a free, powerful, up-to-date and easy to use client-server based remote security scanner. A security scanner is a software which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way. Unlike many other security scanners, Nessus will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability. Nessus is very fast, reliable and has a modular architecture.

SAMSPADE

SamSpade for Windows is a freeware, network query tool. It allows the Windows user to access a number of network tools previously only available for Unix users. Feature set includes ping, nslookup, whois, IP block, dig, traceroute, finger, zone transfer, address scan, website crawl, URL decoder and much more.

WGET

GNU Wget is a freely available network utility to retrieve files from the World Wide Web using HTTP and FTP, the two most widely used Internet protocols. It works non-interactively, thus enabling work in the background, after having logged off. The recursive retrieval of HTML pages, as well as FTP sites is supported -- you can use Wget to make mirrors of archives and home pages, or traverse the web like a WWW robot (Wget understands /robots.txt). Mirroring web content offline allows offline analysis of web site.

DOMTOOLS

Domtools is a suite of DNS utilities to enumerate all DNS records of a target host. You can list all hosts under a particular domain; retrieve detail information about a particular site, list MX records, etc.

NETSCANTOOLS

NetScanTools Pro is a set of internet information gathering utilities presented in a convenient tabbed window. Use it to determine ownership of IP addresses, translate IP addresses to hostnames, scan networks, port probe target computers for services, test firewalls, validate email addresses, find DHCP servers, determine ownership of domains, communicate with SNMP enabled devices, list the computers in a domain and much more.

HPING

hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired by the Unix ping command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. hping is a great tool to perform firewall testing, advanced port scanning, network testing, using different protocols, TOS, fragmentation, manual path MTU discovery, advanced traceroute under all the supported protocols, remote OS fingerprinting, remote uptime guessing and TCP/IP stacks auditing.

FIREWALK

Firewalking is a technique developed by Mike D. Schiffman and David E. Goldsmith that employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks. Firewalk the tool employs the technique to determine the filter rules in place on a packet forwarding device. The newest version of the tool, firewalk/GTK introduces the option of using a graphical interface and a few bug fixes. Firewalk is the best tool to perform firewalking.

NMAP

Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available.

NETCAT

Netcat has been dubbed the network Swiss army knife. It is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool; since it can create almost any kind of connection you would need and has several interesting built-in capabilities. Netcat is now part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions. The current version for Unix was released in 1996 by hobbit. This Windows version was released by Chris Wysopal in 1998. Both hobbit and Chris are part of @stake, Inc.

FESZER

This utility will log parameters to certain string operations exported from MSVCRT.dll, such as *printf(), strcat(), etc. It can help in detecting format string vulnerabilities and buffer overflows in a blind auditing environment.

CERBERUS WEBSCAN

This is a web security scanner designed to find known web server security issues.

WEBPROXY

WebProxy 1.0 is a cross-platform/browser security tool for use in auditing web sites. Installed as a proxy for your browser, WebProxy allows you to intercept, modify, log, and re-submit requests, both HTTP and HTTPS. Editing capabilities include parsing of query parameters, request headers, and POST parameters, as well as cookie editing. The convenient "browse from here" capability allows you to edit and resubmit previous requests and continue browsing on from the returned page. Request interception allows on-the-fly editing of requests based on a matching regular expression. There is also dynamic certificate generation. Use WebProxy for SQL injection, cookie manipulation, parameter testing, or simply monitoring of requests.

NBTDUMP

This utility dumps NetBIOS information from Windows NT, Windows 2000 and *NIX Samba servers such as shares, user accounts with comments etc and the password policy.

TCPDUMP

Tcpdump prints out the headers of packets on a network interface that match the boolean expression. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -b flag, which causes it to read from a saved packet file rather than to read packets from a network interface.   In all cases, only packets that match expression will be processed by tcpdump. WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX.

DSNIFF

dsniff is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g., due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

ETHEREAL

Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

STROBE

Strobe is a network/security tool that locates and describes all listening TCP ports on a (remote) host or on many hosts in a bandwidth utilisation maximising, and process resource minimizing manner.

SARA

SARA or Security Auditor's Research Assistant is a third generation Unix-based security analysis tool based on the famous first generation SATAN model. It fully complies with the SANS Top 20 specification, SANS/ISTS Certified, performs remote self scan and API facilities.

CHEOPS

Cheops is an open sourced Network User Interface. It is designed to be the network equivalent of a Swiss-army knife, unifying your network utilities. Cheops does for the network what a file manager does for your filesystem. Cheops hopes to provide the system administrator and the user a powerful tool for locating, accessing, diagnosing, and managing network resources, all with the click of a button. Cheops is capable of map ping your network nodes in a graphical layout.

DUMPSEC

SomarSoft's DumpSec is a security auditing program for Microsoft Windows® NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information. DumpSec is a must-have product for Windows NT systems administrators and computer security auditors.

ENUM

enum is a tool that combines almost all possible attacks against NETBIOS based communication and computers supporting such communication. Especially it will provide an attacker with information about: - users and computers - shares - password policy It establishes a NETBIOS Null Session and keeps it open during the attack. Based on dictionaries or given values this tool will try to guess passwords.

ITS4

ITS4 is a simple tool that statically scans C and C++ source code for potential security vulnerabilities. It is a command-line tool that works across Unix and Windows platforms. ITS4 scans source code, looking for function calls that are potentially dangerous. For some calls, ITS4 tries to perform some code analysis to determine how risky the call is. In each case, ITS4 provides a problem report, including a short description of the potential problem and suggestions on how to fix the code.

STUNNEL

The Stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd-startable) or remote server. It can be used to add SSL functionality to commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the programs' code. Stunnel can be used to interface with SSL enabled application testing.

WHISKER

Whisker is a CGI scanner with impressive features that makes it much better than most CGI scanners. Whisker will verify that the CGI directory exists, and that the CGI itself exists, reducing the number of false positives. The server type and version is checked prior to any testing, reducing checks for unsupported CGIs. Virtual Hosting is fully supported, allowing Whisker to test vulnerabilities against sub-domains within the same server (a feature not supported by all CGI scanners). URL encoding that hides scans from IDS programs, something like '/cgi-bin/phf?' is requested by its mime encoding equivalent: '/%63%67%69%2d%62%69%6e/%66%69%6e%67%65%72' which causes most IDS programs to not detect the scan.

JUGGERNAUT

Juggernaut is a robust network tool for the Linux OS. It contains several modules offering a wide degree of functionality. Juggernaut has been tested successfully on several different Linux machines on several different networks. However, your mileage may vary depending on the network topologies of the environment (i.e. Smart hubbing will kill much of the packet sniffing functionality...) and, to a lesser extent, the machine running Juggernaut. Juggernaut can be used to perform TCP session hijacking.

HUNT

The main goal of the HUNT project is to develop tool for exploiting well known weaknesses in the TCP/IP protocol suite. It implements some "new" features which are not seen in any other products. Capable of performing session hijacking, it supports connection synchronization after attack and ARP relay too.

IRPAS

IRPAS is a collection of tools to assess routers. While several circumstances can lead to a denial of service attack, the tools try to implement routing protocol functionality as described by the papers, therefore enabling the user of these tools (probably you) to design its own customized attack. IRPAS are capable of manipulating routes on gateway devices to bypass ACLs.

NEMESIS

Nemesis is a command-line UNIX network packet injection suite. Nemesis is used to Generate and spoof various types packets.

EGRESSOR

This freeware tool from MITRE is intended to assist information security specialists in conducting a vulnerability analysis of their network by identifying potential weaknesses in their network configuration. Briefly, the client generates a stream of packets, some of which are spoofed. The server listens for test packets, and determines if spoofed packets were received as part of the test. The server then generates a report of the results, indicating whether spoofed packets were received or not. Figure 1 shows the two scenarios that the tool can find including the html versions of the reports. There is also a "daemon" option which causes the server to run indefinitely.

FRAGROUTER

Fragrouter forces all traffic to fragment, which demonstrates how easy it is for hackers/crackers to do the same in order to evade intrusion detection. This accepts incoming traffic then fragments it according to various rules (IP fragmentation with various sizes and overlap, TCP segmentation again with various sizes and overlaps, TCP insertion in order to de-synchronize the connection, etc.).

TCPREPLAY

tcpreplay is a tool to replay saved tcpdump or snoop files at arbitrary speeds. This program was written in the hopes that a more precise testing methodology might be applied to the area of network intrusion detection, which is still a black art at best. Many NIDSs fare poorly when looking for attacks on heavily-loaded networks. tcpreplay allows you to recreate real network traffic from a real network for use in testing.

SNEEZE

Sneeze is a Snort false-positive generator written in perl. It will read normal Snort rules files, parse them, and generate packets that will hopefully trigger those same rules. Sneeze can be configured to use specific network devices, source ports, spoofed IPs, as well as loop a specified amount of times or forever. Sneeze provides a way to safely test an IDS in a controlled manner and provides useful output to track what you are sending as triggers. Sneeze has been tested with Snort 1.8 and its rules.

SNOT

Snot is an arbitrary packet generator that uses snort rules files as its source of packet information. It attempts at all times to randomize information that is not contained in the rule, to hamper the generation of 'snot detection' snort rules. It can be used as an IDS evasion tool, by using specific decoy hosts, or just something to keep your friendly IDS monitoring staff busy.

STICK

This is an IDS stress tool used to evaluate the bottle neck point in an IDS in an operational environment. Stick will not be released anytime soon for the exception of IDS vendors. The tool uses the Snort rule set and produces a C program via lex that when compiled will produce an IP packet capable of triggering that rule from a spoofed IP range (or all possible IP addresses) into a target IP range. A function is produced for each rule and a loop then executes these rules in a random order. The tool currently produces these at about 250 alarms per second.

MUTATEV2

MUTATEv2 an IDS evasion tool from Efrain Torres for assisting in system enumeration, port scanning, and vulnerability testing.

L0PHTCRACK

LC4 is the latest version of the award-winning password auditing and recovery application, L0phtCrack. It provides two critical capabilities to Windows® network administrators. LC4 helps administrators secure Windows-authenticated networks through comprehensive auditing of Windows NT and Windows 2000 user account passwords. LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

JOHN THE RIPPER

John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, and BeOS. Its primary purpose is to detect weak Unix passwords, but a number of other hash types are supported as well.

WEBSLEUTH

It is the fastest, most efficient Research Tool available for the Net. More than just a search engine an entirely new kind of tool. It makes it easy to sift through the vast ocean of information available on the Internet, maximizing speed and productivity without missing any details. It examines sites by word, content, and context, "Thinking" about and analyzing your information query. It instantly begins retrieving and indexing your data in an easy-to-use, encyclopedic format at the same time filtering out duplicate or irrelevant data including "404 File Not Found". And, by displaying an abstract of each page it reads. WebSleuth can cut hours off your research time by getting you the right information in record time. It's like having your own personal research assistant right on your desktop. WebSleuth applies the best combination of machine intelligence and human intelligence to the pursuit of information. For Windows 95 & NT 4.0

METIS

Metis is a tool I wrote to collect information from the content of web sites. Written in Java and is composed of 2 packages, the web spider engine and the data analysis part.

ACHILLES

Achilles is a tool designed for testing the security of web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session. A typical HTTP proxy will relay packets to and from a client browser and a web server. Achilles will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission. For example, during a normal HTTP SSL connection a typical proxy will relay the session between the server and the client and allow the two end nodes to negotiate SSL. In contrast, when in intercept mode, Achilles will pretend to be the server and negotiate two SSL sessions, one with the client browser and another with the web server. As data is transmitted between the two nodes, Achilles decrypts the data and gives the user the ability to alter and/or log the data in clear text before transmission.

HTDIG

The ht://Dig system is a complete World Wide Web indexing and searching system for a domain or intranet. This system is not meant to replace the need for powerful internet-wide search systems like Lycos, Infoseek, Google and AltaVista. Instead it is meant to cover the search needs for a single company, campus, or even a particular sub section of a web site. As opposed to some WAIS-based or web-server based search engines, ht://Dig can easily span several web servers. The type of these different web servers doesn't matter as long as they understand common protocols like HTTP.

CONCLUSION AND RECOMMENDATION

CONCLUSION

The proposed package Solution revealed an opportunity not just to perform the service for yours and at the same time equipped your IT security with the proposed tools to perform ongoing and routine security assessment internally. It is especially practical and widely adopt for the industry to scan and audit custom in house application and fix it internally without disclosure to too many outsider.

The proposed package solution delivers following immediate benefits:

1. Perform the required penetration test service that is needed prior for the new application roll out into production. We help you to exploit vulnerabilities and report to and close as much vulnerabilities as possible before the application consider “secure” for the production.
2. Optional IT Security assessment product training and knowledge transfer and equipped yours with the tools kit for ongoing internal security assessment, audit and reporting operation.

RECOMMENDATIONS

For security gain accordingly to Client criteria and requirements, the propose solution package should approve and funding to kickoff the project. So Client can resolve current security concern within the timeline given and at the same time build up the internal strength for ongoing manual and automated security check and audit capacity.

At a minimum, your should approve the project to start for the penetration test service portion to resolve current security concern, and scale up the operation accordingly in the future (ie equipped with the tool kits and acquired the operating knowledge for internal security assessment and audit operation.