ESDS VTMScan

VIRTUAL VAPT (vVAPT) CERT-In Certification

For your web security

ESDS Software Solution Pvt. Ltd.

esds

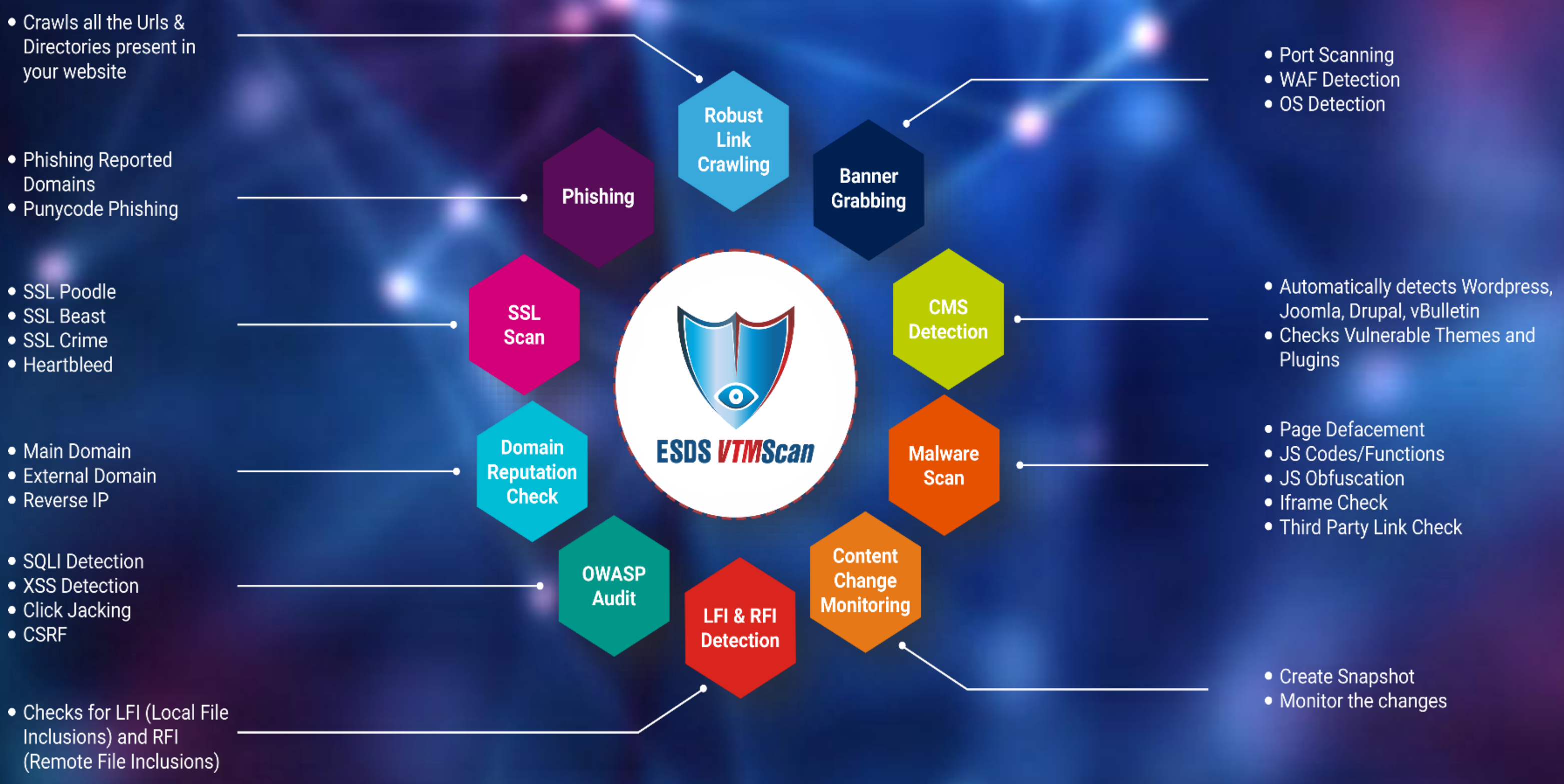
enabling futurability...

About VIRTUAL VAPT (vVAPT)

Virtual VAPT service of ESDS comes with a complete security audit of your web applications / web sites for CERT-in Certification followed by regular vulnerability scanning with ESDS VTMScan. ESDS deliver this service in 2 phases.

- **Phase 1 – Web Application Security Audit by** a CERT-in empaneled Agency
- **Phase 2 – VTMScan Annual scanning service for web application** (Based on selected plans)

That makes it the most unique offering in the security market today for a complete security assessment of critical web presence of client.



Robust Link Crawling
- Crawls all the Urls & Directories present in your website

Phishing
- Phishing Reported Domains
- Punycode Phishing

SSL Scan
- SSL Poodle
- SSL Beast
- SSL Crime
- Heartbleed

Domain Reputation Check
- Main Domain
- External Domain
- Reverse IP

OWASP Audit
- SQLI Detection
- XSS Detection
- Click Jacking
- CSRF

LFI & RFI Detection
- Checks for LFI (Local File Inclusions) and RFI (Remote File Inclusions)

Banner Grabbing
- Port Scanning
- WAF Detection
- OS Detection

CMS Detection
- Automatically detects Wordpress, Joomla, Drupal, vBulletin
- Checks Vulnerable Themes and Plugins

Malware Scan
- Page Defacement
- JS Codes/Functions
- JS Obfuscation
- Iframe Check
- Third Party Link Check

Content Change Monitoring
- Create Snapshot
- Monitor the changes

Scope of Work

The scope is limited to: WEB Applications / Web sites

Phase 1 – Web Application Security Audit by a CERT-in empaneled Agency

Application Security Audit

Application Security Audit is the process of actively evaluating all the components to ensure that they have been developed within the guidelines of security best practices. It is an important step during the process of certifying applications. During this step, the modules are individually tested for a number of weaknesses and properties. The application only passes the review if it exhibits all required properties. Errors in development (known variously as bugs, flaws or vulnerabilities) could allow an attacker to gain access to the confidential information or deny authorized users to access the Application; with potentially catastrophic results.

Application Security Audit is of great importance to avoid security holes in the application itself. It improves the reliability, stability and performance of the application. The results of the application testing are delivered in a comprehensive report highlighting the vulnerabilities and mitigating the risk.

Application Security Testing

There are two types of testing carried out for the complete check of the Web Application i.e. Functional Test and Internal logic test. Black box testing assesses the functional operating effectiveness and White box testing assesses the effectiveness of software program logic. We would be carrying out the Black Box testing for the application. As the Application has various roles defined for various users we will be carrying role based functionality testing to ascertain any security flaws.

The First level Application Audit would highlight the vulnerabilities in the Application like Cross Site Scripting, vulnerability to SQL Injections, Buffer Overflows, Invalidated Inputs, insecure storage etc. These would need to be addressed by the Developers, post which the second or third level audits would be undertaken, if required. Removal of flaws and vulnerabilities from the Application depends on the capabilities of the Application Developers, and the subsequent level audits are driven by this necessity.

Security Audit as per OWASP Standard

The standard used for Web Application Testing is OWASP (Open Web Application Security Project). The OWASP 2017 Top Ten represents a broad consensus about what are the most critical application security flaws. The following table summarizes the OWASP 2017 Top Ten Most Critical Application Security Vulnerabilities:

Top Ten Most Critical Application Security Vulnerabilities	
A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3- Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A4- XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5- Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6- Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7- Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8- Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9- Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defense and enable various attacks and impacts.
A10- Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Review

Review of the system will be headed by the web Application Manger. Review of the progress shall be done on daily basis and the reporting body shall be the Program Manager.

Consultants

ESDS shall deploy the following CERT-in empanelled agency consultants:

- Application Manager.
- Attack and Penetration experts.

Methodology

The first step followed is to analyses the Web-application / website / API application for appropriate security measures built into the Web Application & API application. This analysis is necessary to create a baseline so that one understands the present state better and can thus appreciate findings and recommendations.

The project entails a First Level Audit of the website/API applications, post which the Development Team would correct the vulnerabilities projected in the Audit Report. On successful patching up of the vulnerabilities, a certificate will be issued for website / web application. The methodology followed is as follows:

- Understand the scope and purpose of the Web Application/API Applications. Review the web application structure and specifications so as to understand the basic design of the Website.

- For the web application under review, identify, document and understand the "high value objects" that a malicious attacker would seek to steal or exploit (e.g., user IDs, customer data, passwords).

- Devise attacks or methods using techniques to obtain the desired data objects.

- Once Website security is handled, check if a valid/invalid user can use the Website in a manner so as to subvert the underlying security model of the system.

- Various attacks are devised on each component and then relevant vulnerabilities are demonstrated.

Deliverable of Phase -1

Application Security Audit Report based upon Black box assessment with the Vulnerabilities and Flaws highlighted along with recommendations.

What we require from you. We propose that you will provide:

1. A briefing by the development team on workflow of the Application and sharing of digital signatures and other relevant documents.

2. Client will provide access of server (through VPN) which require security audit.
Testing shall be done offsite.

3. Client will provide the staging/ live server with the hosted Application which is to be audited along with the usernames, passwords and digital signatures for testing.

4. Client may require support of Application development team for clarification and functional testing and patching up of the vulnerabilities in the web pages.

5. Client will provide timely review and comment within two business days on all interim, draft and final deliverables, unless mutually agreed upon, based upon the size of deliverable, for a different timeline.

6. CERT-in empaneled agency will provide for working space for up to two Consultants, access to computing and communication resources (including internet connection) for enabling report documentation, coordination with base teams and effective feedback with the management and project teams.

7. CERT-in empaneled agency will designate a Single point of contact to co-ordinate the activities.

Phase 2 – VTMScan Annual scanning service for web application (Based on selected plans)

VTMScan Features:

1. Domain Reputation
2. PORT scans
3. SQL injection
4. Malware Scans
5. RFI Scans
6. LFI Scan
7. Cross Site Scripting
8. URL monitoring
9. CMS scan
10. OS Detection
11. Click Jacking
12. CSRF
13. SSL Scan
14. WAF Detection
15. Content Change Monitoring
16. Banner Grabbing

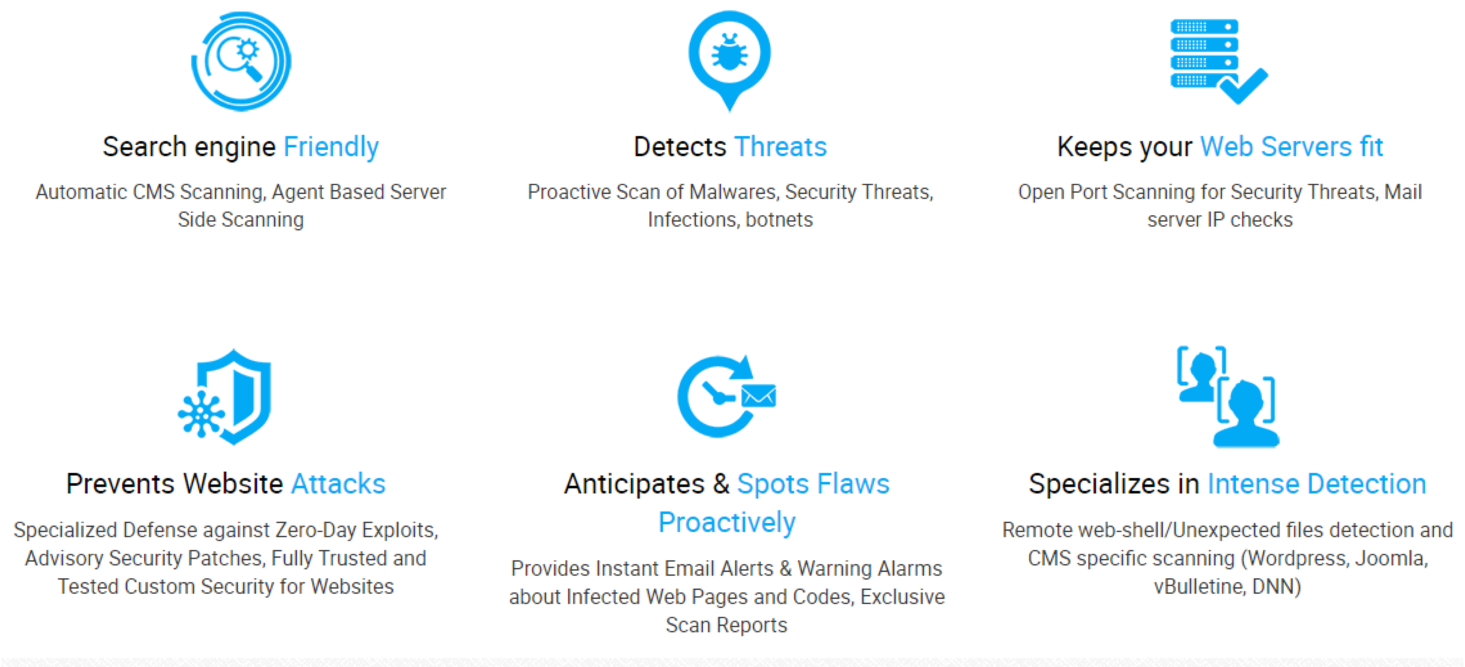
All this modules are tightly integrated with each other to provide a proactive scanning of domain.

Domain Reputation:

- Checks domain reputation in Google , SURBL , Malware Patrol , clean MX, Phish Tank
- Domain mail server IP check in 58 Real time Black hole list and DNS based black hole list

PORT Scans :

- Checks for Open ports on the server and services running on it.
- An open port could be potentially a threat to the server if not properly managed



Search engine Friendly

Automatic CMS Scanning, Agent Based Server Side Scanning

Detects Threats

Proactive Scan of Malwares, Security Threats, Infections, botnets

Keeps your Web Servers fit

Open Port Scanning for Security Threats, Mail server IP checks

Prevents Website Attacks

Specialized Defense against Zero-Day Exploits, Advisory Security Patches, Fully Trusted and Tested Custom Security for Websites

Anticipates & Spots Flaws Proactively

Provides Instant Email Alerts & Warning Alarms about Infected Web Pages and Codes, Exclusive Scan Reports

Specializes in Intense Detection

Remote web-shell/Unexpected files detection and CMS specific scanning (Wordpress, Joomla, vBulletine, DNN)

SQL injection:

- Scans for MySQL , MSSQL, PGSQL & Oracle database
- Checks for poorly filtered or in-correct escaped SQL queries into parsing variable data received from user input

Malware Scans:

- Scans for Page defacement and JavaScript's codes against generic signatures
- Special algorithm developed to detect JavaScript Obfuscation
- Third party links found in page are checked in Google malware database

Cross Site Scripting:

- XSS enables attackers to inject client side scripts into web pages viewed by others
- Scans each and every form in the webpages and scans for GET and POST request to detect XSS

LFI & RFI Scan:

- Scans for pages which hacker can include a remote or a local file via script from web browser
- Occurs due to Pages are not sanitized
- Can lead to other attacks like DDoS , Data Theft etc.

CMS Scan:

- Automatically detects CMS (word press, Joomla,etc.)
- Scans all themes , Plugins, Unprotected admin area
- Brute forcing for passwords
- File path disclosure scanning

OS Detection:

- Checks Operating system and its version of Web Server
- Verifies OS and its version with Malware database

Click Jacking:

- It is a practice of manipulating a website user's activity by concealing hyperlinks beneath legitimate clickable content.
- VTMScan checks if any defense mechanism is used by website developer to protect it.

CSRF:

- Attack that occurs when a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site
- Try to detect them by checking each form if it contains an unpredictable token for each user.

SSL Scan:

- Checks Authenticity of SSL Certificate
- Checks if algorithm used in SSL are weak or not.
- Detects if SSL Certificate is expired.

WAF Detection:

- Detects if website is protected by Web Application Firewall
- Sends malicious payloads to website and checks if any defense mechanism is used by website which is blocking or filtering requests

Content Change Monitoring:

- Creates a snapshot of current state of your website
- Compares each time current state of website with snapshot and informs if any changes are observed on website

Banner Grabbing:

- Creates a snapshot of current state of your website
- Compares each time current state of website with snapshot and informs if any changes are observed on website

Reports:

- Scan Report with Recommendations: Complete Report
- Content Change Report: Report containing CCM results.
- URL Report: Report containing full list of websites