MSP1 | Cyber Security Solutions & Services

Web Application Protection

MSP1 protects your websites and web applications with an enterprise-class web application firewall (WAF), enhanced by advanced bot protection, spam and malware detection, error monitoring, content protection and source code encryption.

MSP1 WAP is your main line of defence against all web application attacks, including all OWASP Top 10 threats like cross-site scripting (XSS), SQL injection (SQLI), cross-site request forgery (CSRF) and remote file inclusion (RFI).

FEATURES

- SQL injection protection
- XSS protection
- Clickjacking protection
- MIME Mismatch attack protection
- Secure connection
- Hides PHP information
- Sanitization
- Mass requests prevention
- Spam & DNSBL protection
- Proxy protection
- Tor protection
- Malware protection
- Bad Bot / Fake Bot protection
- Content Protection
- Error Monitoring
- Source code encryption

- Blocks all attacks ensuring protection.
- Logs every attack for further analysis and 'proactive' action as necessary.
- Automatically bans anyone attempting attack.
- Sends email notifications when someone attempts attack.

SQL INJECTION

Technique where malicious users inject SQL commands into an SQL statement, via web page input. Injected SQL commands can alter SQL statement and compromise the security of a web application.

- XSS Protection: Sanitizes infected requests
- Clickjacking Protection: Detects and blocks clickjacking attempts
- MIME Mismatch Attack Protection: Prevents attacks based on MIME-type mismatch
- Secure connection: Compels use of secure connection
- Hide PHP Information: Hides PHP version to remote requests
- Request Sanitization: Sanitizes all fields, inputs, forms and requests

MASS REQUESTS/ FLOOD ATTACK

A type of Distributed Denial of Service (DDoS) attack in which the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application.

SPAM & DNSBL

Electronic Spamming is the use of electronic messaging systems to send irrelevant or unsolicited messages over the Internet, for the purposes of advertising, phishing, spreading malware, etc. repeatedly to the same site or domain.

A DNS-based Blackhole List (DNSBL) or Real-time Blackhole List (RBL) is a list of IP addresses which are most often used to publish the addresses of computers or networks linked to spamming.

PROXY

A computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, a computer user sends requests to the proxy server which then processes the request and returns what the user was wanting.

- Detection Method #1: Connects with an online Proxy checker and verifies if the visitor is using a Proxy
- Detection Method #2: Checks visitor's HTTP headers for Proxy elements
- Detection Method #3: Scans visitor's ports to detect if behind a Proxy or not.

TOR

A free software for enabling anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. TOR works much like the Open Proxies; however, it's mostly used by legitimate visitors who just want to remain anonymous in Internet. However, it can be abused by malicious visitors.

CONTENT PROTECTION PREVENTS

- Default right menu from popping
- Image download or copy
- Contents and objects 'Drag' and 'Drop'
- Screenshots and printing
- Usage of pages in offline mode
- Page loading into someone else's frame
- Content selection.

CONTENT PROTECTION DISABLES

- 'Cut', 'Copy', Paste' option and prevents copying of contents
- 'View Source' option

LOG MANAGEMENT

Logging errors is recommended best practice, even for production site(s). Checking those logs however might seem like a chore. MSP1 Web App Protection Monitoring module brings all entries from error logs to this page.

- Log file is automatically detected from server/ host configuration
- Only the end of file is read; hence, no memory overflow issues
- Optimized to work well with very large log files

HTML ENCRYPTION

Converts web page contents to a non-easily understandable format. This helps protect code from being stolen to great extent. Its disadvantage is that the pages will be seen on JavaScript enabled browsers only.

DEVELOP CUSTOM RULES

A simple-to-use dashboard lets you configure rules according to your specific security needs based on signals, such as IP reputation, URL slug, client type, number of requests and geo-data.

EXCEPTION HANDLING

Every application has its own logic and there is no one size fits all security solution. With MSP1 you have the option to override every default security rule with your own whitelisting policies.

MSP1 Cyber Security Solutions & Services

MSP1 helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, we enable businesses to transform the way they manage their information security and compliance programs.

With automation, tools and intelligence, we find better ways for businesses to overcome their security challenges. Our qualified security assessors, ethical hackers and other experts are some of the industry's most trusted sources for risk assessments, threat research, forensic investigations, and security training.

North America
46721 Fremont Blvd,
Fremont, CA 94538
United States
+1 (408) 769 5030
https://msp1services.com

India
11/11 Kamdhenu, Hariom
Nagar, Mulund East
Mumbai 400081, India
+ 91 9769757668