SiteLock™
Security for Online Business

How SiteLock Protects Against
The OWASP Top 10 Threats

Find Fix Prevent

Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SiteLock's scanner detects and notifies you of injection vulnerabilities. Our Expert Services team can repair these flaws permanently, while our website firewall serves as a "virtual patch" during these repairs.

Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions or deface websites.

The SiteLock scanner detects and notifies you of cross-site scripting. Our Expert Services team can repair these flaws permanently while our website firewall protects your site during these repairs.

Insecure Direct Object References

Insecure direct object references may occur because applications do not always verify that the user is authorized for the target object. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

The SiteLock website firewall helps prevent insecure direct object reference attacks by using reviews of user input, in addition to known attack vectors and behaviors.

Broken Authentication and Session Management

Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.

The SiteLock website firewall helps protect your site from session attacks by tracing bots, tools and behaviors of these types of attacks. SiteLock gives you this protection without rewriting or intruding on an application's session management functionality.

Cross-Site Request Forgery (CSRF)

A CSRF attack creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or other techniques. If the user is authenticated, the attacker succeeds. CSRF takes advantage of Web applications that allow attackers to predict all the details of the transaction. Since browsers send credentials like session cookies automatically, attackers can create malicious web pages which generate forged requests that are indistinguishable from legitimate ones.

The SiteLock website scanning technology identifies CSRF vulnerabilities and alerts you to their location for resolution. With the SiteLock website firewall you can leverage referral usage patterns and external feeds. Our firewall uses a blacklisting security model to detect potential malicious behavioral patterns and offending sites.

Contact Us
Phone: (877) 257-9263
International: +1 (415) 390-2500
SiteLock.com

SiteLock™
Security for Online Business

How SiteLock Protects Against The OWASP Top 10 Threats

Find Fix Prevent

Security Misconfiguration

Security misconfiguration can happen at any level of an application attack, including the platform, web server, application server, framework, and custom code. Such flaws can give attackers access to default accounts, unused pages, unpatched flaws, unprotected files, and directories to gain unauthorized access to system data.

The SiteLock scanner identifies and pinpoints server misconfigurations. Our website firewall applies generic and application specific security measures to accommodate for security misconfiguration and creates specific "virtual patching" for issues that it finds.

Insecure Cryptographic Storage

Many web applications do not properly protect sensitive data such as credit cards, Social Security Numbers (SSNs), and authentication credentials with appropriate encryption or hashing. Attackers may use this weakly protected data to conduct identity theft, credit card fraud, or other crimes.

The SiteLock security suite of solutions does not directly store any of your confidential data. Your customers will not put their data at risk for attacks with our website firewall in place.

Failure to Restrict URL Access

Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

The SiteLock website firewall applies application specific as well as signature and client-based illegal resource access policies. Our website firewall can prevent even the most sophisticated, targeted access attempts.

Insufficient Transport Layer Protection

Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.

The SiteLock website firewall and Content Delivery Network (CDN) fully support HTTPS traffic while the SiteLock website scanner can identify areas that need encryption and alert you when the proper controls are not in place.

Invalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

The SiteLock security suite can ensure that your website does not redirect traffic to malicious destinations. Our website firewall also analyzes the application behavior to mitigate known vulnerabilities and help prevent unauthenticated redirects and forwards.

Contact Us
Phone: (877) 257-9263
International: +1 (415) 390-2500
SiteLock.com