AT-A-GLANCE

# Protecting Applications from Critical Web Vulnerabilities

## HIGHLIGHTS

- The OWASP Top Ten project identifies the most critical security risks for online applications
- The Pulse Secure vWAF shields applications by applying business rules to block attacks
- Rapid deployment of virtual patches to enforce system-wide policies in real time

## Effective Application Security with Intelligent Application Security

The speed at which organizations must evolve their IT environments—and the inherent complexity and interconnectedness of those applications and environments—has increased the risk of programming or design errors that can leave applications and data vulnerable to attack.

At the same, it can take longer to fix security vulnerabilities once identified, and in some cases it may prove prohibitively expensive to locate the error, create the patch, and deploy the fix. However it is imperative that applications continue to function securely whether a patch or fix is in place or not; especially the Web applications located on the "front line" when it comes to both customer service and securing data and systems.

Application security must therefore provide a strong and intelligent defensive shield, allowing new code design, development, and deployment to move as quickly as required, while ensuring any vulnerabilities cannot be exploited. Current applications and their data are thus kept secure; despite the number of programming errors and glitches that will increasingly get through testing before being identified thanks to accelerated delivery timetables. Virtual application firewalls are the cornerstone in a creating such an effective and holistic application security system.

### Addressing the Most Critical Web Application Security Risks

IT departments wanting to understand how best to provide effective application security will find the Open Web Application Security Project (OWASP) "Top 10" an ideal place to begin. OWASP is an open community dedicated to helping organizations leverage trustworthy applications that are supported by a not-for-profit foundation and independent of any specific vendor. Its "Top 10 Most Critical Web Application Security Risks" is a regularly updated list of highlighting the security risks organizations face prioritized by levels of prevalence and risk. The Pulse Secure Virtual Web Application Firewall (vWAF) can address many of these critical security vulnerabilities, and in this document, we have highlighted five of the most common ways in which Pulse Secure vWAF can help:


**Figure 1:** The OWASP "Top Ten" Project is updated periodically: this diagram illustrates the 2013 report—next update due in 2H 2017.

## Injection Flaws

Injection flaws allow attackers to use hostile data that can trick the application into executing unauthorized commands or providing access to data without proper authorization. Such flaws make it possible for attackers to enter text into login screens and get access to passwords, directories, and other sensitive data. The Pulse Secure vWAF is able to detect and stop data traffic that contains suspected injection flaw payloads by validating all user input, which helps to prevent sensitive data being extracted illegally.

## Broken Authentication and Session Management

Web sites can sometimes expose security weaknesses, especially if placed under pressure either due to peak demand or malicious intent. Account credentials and session tokens are often not properly protected; unencrypted cookies and design flaws can enable attackers to circumnavigate authentication. This can allow attackers to compromise passwords, keys, or authentication tokens to assume other users' identities to commit identity theft and other crimes, such as credit card fraud.

By controlling user session timeouts and setting session limits, the Pulse Secure vWAF addresses some of the common design flaws that allow authentication to be bypassed while keeping vulnerable session information behind the firewall. It enforces processes that ensure users always start a new session on the chosen start page, evading one of the common methods attackers use to get around security stages. By validating a successful Web site login, the Pulse Secure vWAF prohibits any user from accessing pages that do not have proper authorization from the application.

The Pulse Secure vWAF also features a "Cookie Jar" Handler. This addresses the use of unencrypted or unsecure cookies by placing a "bad" cookie in a holding pen, and sending a secure "safe" cookie out in its place. The cookies are then automatically swapped back once the data is safely back behind the firewall. This prevents the use of such cookies to navigate around authentication and authorized entry points.

## Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is a slightly more sophisticated attack, but one that fundamentally still relies on very common Web vulnerabilities. Attackers execute a script in the victim's browser and then hijack user sessions, deface Web sites, introduce damaging code, and so on. The vulnerability arises whenever an application takes user supplied data and sends it to a Web browser without first validating or encoding that content. This is increasingly a risk as Web site designers seek to automate and speed up some processes to provide a faster, simpler user experience.

The Pulse Secure vWAF uses advanced text analysis to detect and deny traffic that contains suspected XSS payloads through validation of all user input. By stripping out the suspect data or data that should not be sent externally unencrypted, attackers are unable to capitalize on the weakness in the system.

## Sensitive Data Exposure

Information and data on credit cards, identifying information, and authentication credentials that require encryption protection at all times are often poorly protected by Web applications. Handling such information requires special precautions when exchanged with the browser to prevent it being inappropriately accessed, viewed, or even stolen.

The Payment Card Industry Wizard provided by the Pulse Secure vWAF delivers response filtering to hide sensitive data details when sent outside the firewall. The Wizard can recognize certain patterns of data that identify that data as security numbers, names, card numbers, and other sensitive information, and prevents it going outside the secure area in its readable form. It also confirms if a request was transmitted via SSL and enforces SSL encryption to create the multiple layers of security such data demands.

## Cross Site Request Forgery (CSRF)

More sophisticated still, and extremely destructive CSRF is a fundamental weakness in the way that transactions in Web applications are authorized. A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable Web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. This can occur when a user has several Web sites open and while looking at one application, another application or attacker targets one of the other open sites the user has not logged out of. For example, if a user had a social media account, an online store account, and a bank account all open at the same

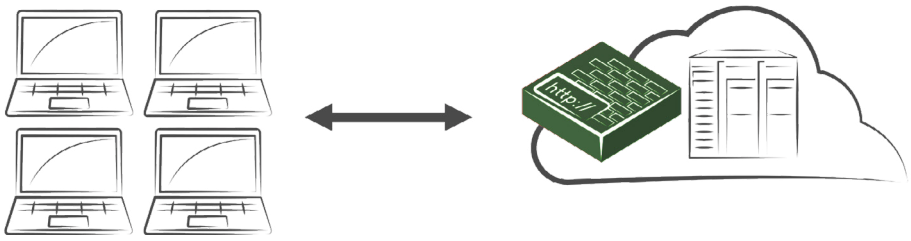


**Figure 2:** The Pulse Secure vWAF deployed as an integral part of the Pulse Secure Virtual Traffic Manager.

time while they are posting updates, they may unwittingly leaving the bank account application vulnerable to a CSRF attack via their browser.

Applications can be protected using the Pulse Secure vWAF form protection and form virtualization, which makes it impossible to exploit an application in this way. The Pulse Secure vWAF signs outgoing forms with a session-based key and acts on any changes, blocking activity if the correct session token is not used and closing sessions to prevent manipulation.

## The Pulse Secure Virtual Web Application Firewall

The Pulse Secure vWAF is a scalable solution for application-level security, providing intelligent protection against external attacks. As a virtual device, it can be easily scaled and optimized to provide the required level of protection and policy enforcement without impacting performance, removing bottlenecks from the network, and optimizing application availability. It supports both off-the-shelf solutions and complex custom applications, including third-party frameworks integrating easily into any environment, such as hybrid environments where virtual, physical, and cloud-based resources are in use.

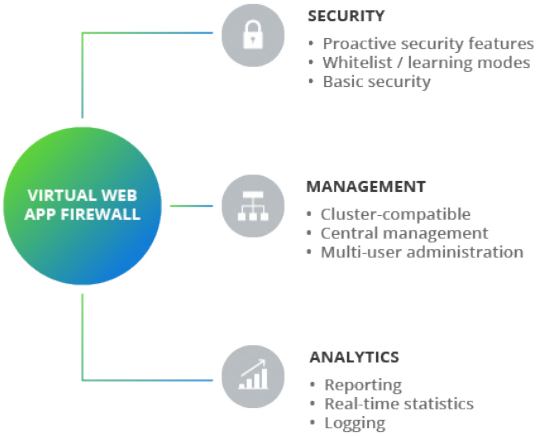


**Figure 3:** Pulse Secure vWAF provides multiple layers of protection.

The Pulse Secure vWAF shields applications by inspecting and blocking attacks such as SQL injection and XSS—identified by the OWASP as among the top ten most critical Web application security risks—by applying business rules to online traffic. And distributed and automated policy management ensures that all changes and fixes are deployed system-wide in real time, reducing any window of opportunity for attackers.

Learn more about Pulse Secure Virtual Web Application Solutions at http://www.pulsesecure.net/vadc/vwaf.

**Corporate and Sales Headquarters**
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net



Pulse Secure®