EventTracker

Actionable Security Intelligence

Statement of Compliance for WASC Threat Classification

Personal and Confidential

Abstract

EventTracker architecture mainly comprises of two components, Web and Engine. EventTracker and its components rely on Operating System, IIS webserver and SQL database for its functional requirements. With the increase in data management, it is important to safeguard EventTracker application and its pre-requisites against various known security threats.

One of the standard references to known security threats list is available is the Threat Classification (TC) of the Web Application Security Consortium (WASC) which is made up of an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web. As an active community, WASC facilitates the exchange of ideas and organizes several industry projects. WASC consistently releases technical information, contributed articles, security guidelines, and other useful documentation. Businesses, educational institutions, governments, application developers, security professionals, and software vendors all over the world utilize our materials to assist with the challenges presented by web application security.

The WASC Threat Classification outlines the attacks and weaknesses that can lead to the compromise of a website, its data, or its users. EventTracker adheres with standard threat classification of WASC which will help to identify security loopholes and take necessary mitigation and making EventTracker less vulnerable to web security threats.

This document is a statement of compliance against the WASC-TC.

References

***OWASP Guidelines**
https://www.owasp.org/index.php/Main_Page

WASC Threat Classification
http://projects.webappsec.org/w/page/13246978/Threat%20Classification

WASC Guidelines

Attacks	Description	Supported Features
Abuse of Functionality	The overall configuration of the application with external and internal entities must be handled securely.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Brute Force Credentials	Since users need to remember passwords, they often select easy to memorize words or phrases as passwords, making a brute force attack using a dictionary useful.	Not Applicable EventTracker depends on Windows Authentication which can be either Active Directory or local host based
Buffer Overflow	A Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold. Exploiting a buffer overflow allows an attacker to modify portions of the target process' address space.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Content Spoofing	Content Spoofing is an attack technique that allows an attacker to inject a malicious payload that is later misrepresented as legitimate content of a web application.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Credential/Session Prediction	Credential/Session Prediction is a method of hijacking or impersonating a web site user. Deducing or guessing the unique value that identifies a session or user accomplishes the attack. Also, known as Session Hijacking, the consequences could allow attackers the ability to issue web site requests with the compromised user's privileges.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Cross-Site Scripting	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
Cross-Site Request Forgery	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent to perform an action as the victim.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Denial of Service	Any attempt to make a machine or network resource unavailable to its intended users should not be successful.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Fingerprinting	The most common methodology for attackers is to first footprint the target's web presence and enumerates as much information as possible. With this information, the attacker may develop an accurate attack scenario, which will effectively exploit vulnerability in the software type/version being utilized by the target host.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Format String	Format String Attacks alter the flow of an application by using string formatting library features to access other memory space.	Continuous security process been adopted. EventTracker adheres to OWASP guidelines and was handled this vulnerability as a part of it. Also, it is maintained as a part of Security Development Life Cycle process.
HTTP Response Smuggling	HTTP response smuggling is a technique to "smuggle" 2 HTTP responses from a server to a client, through an intermediary HTTP device that expects (or allows) a single response from the server.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
HTTP Response Splitting	The attack consists of making the server print a carriage return (CR, ASCII 0x0D) line feed (LF, ASCII 0x0A) sequence followed by content supplied by the attacker in the header section of its response, typically by including them in input fields sent to the application. Per the HTTP standard (RFC 2616), headers are separated by one CRLF and the response's headers are separated from its body by two. Therefore, the failure to remove CRs and LFs allows the attacker to set arbitrary headers, take control of the body, or break the response into two or more separate responses.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
HTTP Request Smuggling	HTTP Request Smuggling is an attack technique that abuses the discrepancy in parsing of non-RFC compliant HTTP requests between two HTTP devices (typically a front-end proxy or HTTP-enabled firewall and a back-end web server) to smuggle a request to the second device "through" the first device. This technique enables the attacker to send one set of requests to the second device while the first device sees a different set of requests. In turn, this facilitates several possible exploitations, such as partial cache poisoning, bypassing firewall protection and XSS.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
HTTP Request Splitting	HTTP Request Splitting is an attack that enables forcing the browser to send arbitrary HTTP requests, inflicting XSS and poisoning the browser's cache. The essence of the attack is the ability of the attacker, once the victim (browser) is forced to load the attacker's malicious HTML page, to manipulate one of the browser's functions to send 2 HTTP requests instead of one HTTP request. Two such mechanisms have been exploited to date: the XMLHttpRequest object (XHR for short) and the HTTP digest authentication mechanism.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
Integer Overflows	An Integer Overflow is the condition that occurs when the result of an arithmetic operation, such as multiplication or addition, exceeds the maximum size of the integer type used to store it. When an integer overflow occurs, the interpreted value will appear to have “wrapped around’ the maximum value and started again at the minimum value.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
LDAP Injection	LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Mail Command Injection	Mail Command Injection is an attack technique used to exploit mail servers and webmail applications that construct IMAP/SMTP statements from user-supplied input that is not properly sanitized.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Null Byte Injection	Null Byte Injection is an active exploitation technique used to bypass sanity checking filters in web infrastructure by adding URL-encoded null byte characters (i.e. %00, or 0x00 in hex) to the user-supplied data. This injection process can alter the intended logic of the application and allow malicious adversary to get unauthorized access to the system files.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
OS Commanding	OS Commanding is an attack technique used for unauthorized execution of operating system commands.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
Path Traversal	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Predictable Resource Location	Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Remote File Inclusion (RFI)	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.
Routing Detour	The WS-Routing Protocol (WS-Routing) is a protocol for exchanging SOAP messages from an initial message sender to an ultimate receiver, typically via a set of intermediaries.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.
Session Fixation	Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
SOAP Array Abuse	XML SOAP arrays are a common target for malicious abuse. SOAP arrays are defined as having a type of "SOAP-ENC: Array" or a type derived there from. SOAP arrays have one or more dimensions (rank) whose members are distinguished by ordinal position.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.
SSI Injection	SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server. SSI Injection exploits a web application's failure to sanitize user-supplied data before they are inserted into a server-side interpreted HTML file.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
SQL Injection	SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
URL Redirector Abuse	URL Redirection to Untrusted Site ('Open Redirect')	Not Applicable EventTracker does not support this feature.
XPath Injection	XPath Injection is an attack technique used to exploit applications that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
XML Attribute Blowup	XML Attribute Blowup is a denial of service attack against XML parsers.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

Attacks	Description	Supported Features
XML External Entities	This technique takes advantage of a feature of XML to build documents dynamically at the time of processing.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.
XML Entity Expansion	The XML Entity expansion attack, exploits a capability in XML DTDs that allows the creation of custom macros, called entities that can be used throughout a document. By recursively defining a set of custom entities at the top of a document, an attacker can overwhelm parsers that attempt to completely resolve the entities by forcing them to iterate almost indefinitely on these recursive definitions.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.
XML Injection	XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
XQuery Injection	XQuery Injection is a variant of the classic SQL injection attack against the XML XQuery Language.	Not applicable. EventTracker Enterprise does not use XQuery language in its development.