Hardening Guide for OWASP Compliance
Abstract

This guide will provide an overview of the OWASP related security features and procedures built into the EventTracker product and the checks and balances made in its development cycle. This document also goes into the details of how the EventTracker application can be deployed and hardened as per the OWASP recommendations. It also highlights the steps taken during the development cycle to plug possible security loop holes.

Audience

This guide helps EventTracker users to secure EventTracker application.
# Table of Contents

Abstract .................................................................................................................................................. 1  
Audience .............................................................................................................................................. 1  
Overview ............................................................................................................................................... 3  
Categories of OWASP .......................................................................................................................... 3  
Information Gathering .......................................................................................................................... 3  
Configuration Management .................................................................................................................. 5  
Authentication Testing ......................................................................................................................... 9  
Authorization Testing ............................................................................................................................ 13  
Business Logic Testing .......................................................................................................................... 15  
Data Validation Testing ........................................................................................................................ 15  
Denial of Service Testing ...................................................................................................................... 19  
Web Services Testing ............................................................................................................................ 21  
AJAX Testing .......................................................................................................................................... 21
Overview

The Open Web Application Security Project (OWASP) is an open-source application security project.

Goal of OWASP:

- Protect EventTracker users against high risk problem areas
- Ensure web application security
- Reduce the surface area for an attacker to hack EventTracker application

Categories of OWASP

There are 10 categories available for testing. They are:

1. Information Gathering
2. Configuration Management
3. Authentication Testing
4. Session Management
5. Authorization Testing
6. Business Logic Testing
7. Data Validation Testing
8. Denial of Service Testing
9. Web Services Testing
10. AJAX Testing

All the categories are applicable for EventTracker except Web Services testing.

Information Gathering

Collecting as much information as possible about a target application, by using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used.

There are a few test cases in this section. Details about the test cases are given below.

Test Case ID: OWASP-IG-001

Test Name: Spiders, Robots and Crawlers, Not Applicable for EventTracker

Description: Web spiders/robots/crawlers retrieve a web page and then recursively traverse hyperlinks to retrieve further web content.
Resolution: EventTracker is an intranet application. Even though it is hosted on a website, crawler does not crawl through the EventTracker pages if it is not logged in.

Test Case ID: OWASP-IG-002

Test Name: Search Engine Discovery/Reconnaissance, Not Applicable for EventTracker

Description: This test case describes how to search the Google Index and remove the associated web content from the Google Cache.

Remarks: EventTracker is not a search engine based application.

Test Case ID: OWASP-IG-003

Test Name: Identify application entry points, Applicable for EventTracker

Description: Enumerating the application and its attack surface is a key precursor before any thorough testing can be undertaken, as it allows the tester to identify likely areas of weakness. This test case aims to help identify and map out areas within the application that should be investigated once enumeration and mapping has been completed.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-IG-004

Test Name: Testing for Web Application Fingerprint, Applicable for EventTracker

Description: Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-IG-005

Test Name: Application Discovery, Applicable for EventTracker

Description: A paramount step in testing for web application vulnerabilities is to find out which particular applications are hosted on a web server. Many applications have known vulnerabilities and known attack strategies that can be exploited in order to gain remote control or to exploit data.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-IG-006

Test Name: Analysis of Error Codes, Applicable for EventTracker

Description: Often during a penetration test on web applications we come up against many error codes generated from applications or web servers. It's possible to cause these errors to be displayed by using a particular request, either specially crafted with tools or created manually. These codes are very useful to penetration testers during their activities because they reveal a lot of information about databases, bugs, and other technological components directly linked with web applications.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Configuration Management

Analysis of the infrastructure and topology architecture can reveal information about a web application. Information such as source code, HTTP methods permitted, administrative functionality, authentication methods and infrastructural configurations can be obtained.

Test Case ID: OWASP-CM-001

Test Name: SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity), Applicable for EventTracker

Description: SSL and TLS are two protocols that provide, with the support of cryptography, secure channels for the protection, confidentiality, and authentication of the information being transmitted. Considering the criticality of these security implementations, it is important to verify the usage of a strong cipher algorithm and its proper implementation.

Resolution: Customers must configure SSL for IIS by using trusted and valid certificates.

Please refer the topic ‘Secure IIS Web Server’ in Hardening Guide for EventTracker Server

Test Case ID: OWASP-CM-002

Test Name: DB Listener Testing, Not Applicable for EventTracker

Description: During the configuration of a database server, many DB administrators do not adequately consider the security of the DB listener component. The listener could reveal sensitive data as well as configuration settings or running database instances if insecurely configured and probed with manual or automated techniques.

Remarks: This test case is only for Oracle database and EventTracker does not support Oracle Database.
Test Case ID: OWASP-CM-003

Test Name: Infrastructure Configuration Management Testing, Applicable for EventTracker

Description: It takes only a single vulnerability to undermine the security of the entire infrastructure, and even small and (almost) unimportant problems may evolve into severe risks for another application on the same server. Here we test to verify this.

Resolution: User should disable remote connection to IIS. If enabling remote connection to IIS is required then, default username and password like admin should be avoided.

To disable remote connection in IIS, follow the steps mentioned below.

1. Select the Start button, select Control Panel, and then select Administrative Tools.
2. Select Internet Information Services (IIS) Manager.

3. In the Connections pane, click the server node in the tree.
4. To open the Management Service feature, double-click Management Service.

![Figure 1](image-url)
5. Disable **Enable Remote Connections** option, if it is checked.

**Test Case ID:** OWASP-CM-004

**Test Name:** Application Configuration Management Testing, Applicable for EventTracker

**Description:** Web applications hide some information that is usually not considered during the development or configuration of the application itself. This data can be discovered in the source code, in the log files or in the default error codes of the web servers.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-CM-005

**Test Name:** Testing for File Extensions Handling, Applicable for EventTracker

**Description:** The file extensions present in a web server or a web application make it possible to identify the technologies which compose the target application. File extensions can also expose additional systems connected to the application.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-CM-006

**Test Name:** Old, backup and unreferenced files, Applicable for EventTracker

**Description:** Redundant, readable and downloadable files on a web server, such as old, backup and renamed files, are a big source of information leakage. It is necessary to verify the presence of these files because they may contain parts of source code, installation paths as well as passwords for applications and/or databases.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-CM-007

**Test Name:** Infrastructure and Application Admin Interfaces, Applicable for EventTracker

**Description:** Many applications use a common path for administrative interfaces which can be used to guess or brute force administrative passwords. This test tends to find admin interfaces and understand if it is possible to exploit it to access to admin functionality. Many applications use a common path for administrative interfaces which can be used to guess or brute force administrative passwords.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-CM-008

**Test Name:** Testing for HTTP Methods and XST, Applicable for EventTracker

**Description:** In this test, we check that the web server is not configured to allow potentially dangerous HTTP commands (methods) and that Cross Site Tracing (XST) is not possible.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.
Authentication Testing

Authentication is the process of attempting to verify the digital identity of the sender of a communication.

Test Case ID: OWASP-AT-001

Test Name: Credentials transport over an encrypted channel, Applicable for EventTracker

Description: Here, the tester will just try to understand if the data that users put into the web form, in order to log into a web site, are transmitted using secure protocols that protect them from an attacker or not.

Resolution: Customers must configure SSL for EventTracker by using trusted and valid certificates. Please refer the topic ‘Secure IIS Web Server’ in Hardening Guide for EventTracker Server.

Test Case ID: OWASP-AT-002

Test Name: Testing for user enumeration, Applicable for EventTracker

Description: The scope of this test is to verify if it is possible to collect a set of valid users by interacting with the authentication mechanism of the application. This test will be useful for the brute force testing, in which we verify if, given a valid username, it is possible to find the corresponding password.

Resolution: Customers should follow security recommendations of Active Directory as per Microsoft guidelines. Also it is recommended that customers should not add default or guessable user accounts into the EventTracker group.

Please refer the topic ‘Harden Windows Server’ in Hardening Guide for EventTracker Server.

Test Case ID: OWASP-AT-003

Test Name: Testing for Guessable (Dictionary) User Account, Applicable for EventTracker

Description: Here we test if there are default user accounts or guessable username/password combinations (dictionary testing)

Resolution: Customers should follow security recommendations of Active Directory as per Microsoft guidelines. Also it is recommended that customers should not add default or guessable user accounts into the EventTracker group.

Please refer the topic ‘Harden Windows Server’ in Hardening Guide for EventTracker Server.
Test Case ID: OWASP-AT-004

Test Name: Brute Force Testing, Applicable for EventTracker

Description: When a dictionary type attack fails, a tester can attempt to use brute force methods to gain authentication. Brute force testing is not easy to accomplish for testers because of the time required and the possible lockout of the tester.

Resolution: EventTracker depends on Windows Authentication which can be either Active Directory or local host based. Customers should follow security recommendations of Active Directory as per Microsoft guidelines.

Please refer the topic ‘Harden Windows Server’ in Hardening Guide for EventTracker Server.

Test Case ID: OWASP-AT-005

Test Name: Testing for bypassing authentication schema, Applicable for EventTracker

Description: Other passive testing methods attempt to bypass the authentication schema by recognizing that not all of the application's resources are adequately protected. The tester can access these resources without authentication.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-AT-006

Test Name: Testing for vulnerable remember password and password reset, Partially Applicable for EventTracker

Description: Here we test how the application manages the process of "password forgotten". We also check whether the application allows the user to store the password in the browser ("remember password" function).

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-AT-007

Test Name: Testing for Logout and Browser Cache Management, Applicable for EventTracker

Description: Here we check that the logout and caching functions are properly implemented.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-AT-008

Test Name: Testing for CAPTCHA, Not Applicable for EventTracker

Description: CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used by many web applications to ensure that the response is not generated by a computer. CAPTCHA implementations are often vulnerable to various kinds of attacks even if the generated CAPTCHA is unbreakable.

Remarks: EventTracker application does not have any CAPTCHA

Test Case ID: OWASP-AT-009

Test Name: Testing Multiple Factors Authentication, Not Applicable for EventTracker

Description: Multiple Factors Authentication means to test the following scenarios: One-time password (OTP) generator tokens, Crypto devices like USB tokens or smart cards, equipped with X.509 certificates, Random OTP sent via SMS, Personal information that only the legitimate user is supposed to know [OUTOFWALLET].

Remarks: EventTracker does not support Multiple Factors Authentication

Test Case ID: OWASP-AT-010

Test Name: Testing for Race Conditions, Applicable for EventTracker

Description: A race condition is a flaw that produces an unexpected result when timing of actions impact other actions. An example may be seen on a multithreaded application where actions are being performed on the same data. Race conditions, by their very nature, are difficult to test for.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Session Management

Test Case ID: OWASP-SM-001

Test Name: Testing for Session Management Schema, Applicable for EventTracker

Description: This describes how to analyze a Session Management Schema, with the goal to understand how the Session Management mechanism has been developed and if it is possible to break it to bypass the user session.

Resolution: Customers are recommended to configure SSL for IIS by using trusted and valid certificates for session variables to traverse through encrypted channel.

Please refer the topic ‘Secure IIS Web Server’ in Hardening Guide for EventTracker Server.
Test Case ID: OWASP-SM-002

Test Name: Testing for Cookies attributes, Applicable for EventTracker

Description: Cookies are often a key attack vector for malicious users (typically, targeting other users) and, as such, the application should always take due diligence to protect cookies. In this section, we will look at how an application can take the necessary precautions when assigning cookies and how to test that these attributes have been correctly configured.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-SM-003

Test Name: Testing for Session Fixation, Applicable for EventTracker

Description: When an application does not renew the cookie after a successful user authentication, it could be possible to find session fixation vulnerability and force a user to utilize a cookie known to the attacker.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-SM-004

Test Name: Testing for Exposed Session Variables, Applicable for EventTracker

Description: Session Tokens represent confidential information because they tie the user identity with his own session. It’s possible to test if the session token is exposed to this vulnerability and try to create a replay session attack.

Resolution: Customers are recommended to configure SSL for IIS by using trusted and valid certificates for session variables to traverse through encrypted channel. Please refer the topic ‘Secure IIS Web Server’ in Hardening Guide for EventTracker Server.

Test Case ID: OWASP-SM-005

Test Name: Testing for CSRF (Cross-site Request Forgery), Applicable for EventTracker

Description: Cross Site Request Forgery describes a way to force an unknowing user to execute unwanted actions on a web application in which he is currently authenticated.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Authorization Testing

Test Case ID: OWASP-AZ-001

Test Name: Testing for Path Traversal, Applicable for EventTracker

Description: In this test case, we test if it is possible to find a way to execute a path traversal attack and access reserved information.

Resolution: Directory browsing in IIS should be disabled and files with extensions (.log & .logs) should not be served directly.

To disable directory browsing in IIS follow the steps given below:

1. Select the Start button, select Control Panel, and then select Administrative Tools.
2. Select Internet Information Services.
   OR
   Select the Start button, select the Run command prompt.
3. Enter Inetmgr in the Open textbox and then click OK.
4. Right click Default Web Site, select Properties.
Default Web Site Properties window displays.

5 Select **Home Directory** tab.

![Default Web Site Properties window](image)

6 Uncheck **Directory browsing** if it is selected.

**Test Case ID:** OWASP-AZ-002

**Test Name:** Testing for bypassing authorization schema, Applicable for EventTracker

**Description:** This kind of test focuses on verifying how the authorization schema has been implemented for each role/privilege to get access to reserved functions/resources.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-AZ-003

Test Name: Testing for Privilege Escalation, Applicable for EventTracker

Description: During this phase, the tester should verify that it is not possible for a user to modify his or her privileges/roles inside the application in ways that could allow privilege escalation attacks.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Business Logic Testing


Access rights of various user roles and groups are different. Every role or group has different constraints and privileges been assigned to them.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Data Validation Testing

Test Case ID: OWASP-DV-001

Test Name: Testing for Reflected Cross Site Scripting, Applicable for EventTracker

Description: In Cross Site Scripting (XSS) testing, we test if it is possible to manipulate the input parameters of the application so that it generates malicious output. We find XSS vulnerability when the application does not validate our input and creates an output that is under our control.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-002

Test Name: Testing for Stored Cross Site Scripting, Applicable for EventTracker

Description: In Stored Cross Site Scripting, we check if stored data are potentially exposed to this type of attack.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-DV-003

**Test Name:** Testing for DOM based Cross Site Scripting, Applicable for EventTracker

**Description:** In DOM-based cross site scripting, we test if the active content, such as a JavaScript function, a DOM element can be controlled by an attacker or not.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-004

**Test Name:** Testing for Cross Site Flashing, Not Applicable for EventTracker

**Description:** ActionScript is the language, based on ECMAScript, used by Flash applications when dealing with interactive needs. Flash applications are often embedded in browsers; vulnerabilities could be present in flawed Flash applications.

**Remarks:** EventTracker does not have any Flash images.

Test Case ID: OWASP-DV-005

**Test Name:** SQL Injection, Applicable for EventTracker

**Description:** In SQL injection testing, we test if it is possible to inject data into the application so that it executes a user-controlled SQL query in the back-end DB.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-006

**Test Name:** LDAP Injection, Applicable for EventTracker

**Description:** LDAP injection testing is similar to SQL Injection testing. The differences are that we use the LDAP protocol instead of SQL and that the target is an LDAP Server instead of a SQL Server.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-007

**Test Name:** ORM Injection, Not Applicable for EventTracker

**Description:** ORM injection testing is similar to SQL Injection Testing, as well. In this case, we use a SQL Injection against an ORM generated data access object model.

**Remarks:** EventTracker is not an ORM supported application.
Test Case ID: OWASP-DV-008

Test Name: XML Injection, Applicable for EventTracker

Description: In XML injection testing, we test if it possible to inject a particular XML document into the application. We find an XML injection vulnerability if the XML parser fails to make appropriate data validation.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-009

Test Name: SSI Injection, Applicable for EventTracker

Description: In SSI injection testing, we test if it is possible to inject into the application data that will be interpreted by SSI mechanisms. A successful exploitation of this vulnerability allows an attacker to inject code into HTML pages or even perform remote code execution.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-010

Test Name: XPath Injection, Applicable for EventTracker

Description: In XPath injection testing, we test if it is possible to inject data into an application so that it executes user-controlled XPath queries.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-011

Test Name: IMAP/SMTP Injection, Applicable for EventTracker

Description: In IMAP/SMTP injection testing, we test if it possible to inject arbitrary IMAP/SMTP commands into the mail servers, due to input data not properly sanitized.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Test Case ID: OWASP-DV-012

Test Name: Code Injection, Applicable for EventTracker

Description: In code injection testing, we check if it is possible to inject into an application data that will be later executed by the web server.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-013

Test Name: OS Commanding, Applicable for EventTracker

Description: In command injection testing, we will try to inject an OS command through an HTTP request into the application.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-014

Test Name: Buffer overflow, Applicable for EventTracker

Description: In these tests, we check for different types of buffer overflow vulnerabilities.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-015

Test Name: Incubated vulnerability, Applicable for EventTracker

Description: Incubated testing is a complex testing that needs more than one data validation vulnerability to work.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DV-016

Test Name: Testing for HTTP Splitting/Smuggling, Applicable for EventTracker

Description: Describes how to test for an HTTP Exploit, as HTTP Verb, HTTP Splitting, and HTTP Smuggling.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.
Denial of Service Testing

Test Case ID: OWASP-DS-001

Test Name: Testing for SQL Wildcard Attacks, Applicable for EventTracker

Description: SQL Wildcard Attacks are about forcing the underlying database to carry out CPU-intensive queries by using several wildcards. This vulnerability generally exists in search functionalities of web applications. Successful exploitation of this attack will cause Denial of Service.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DS-002

Test Name: Locking Customer Accounts, Applicable for EventTracker

Description: In this test we check whether an attacker can lock valid user accounts by repeatedly attempting to log in with a wrong password.

Resolution: EventTracker depends on Active Directory [AD] for authentication and this scenario is mainly based on AD settings. Customers should follow security recommendations of Active Directory as per Microsoft guidelines.

Please refer the topic ‘Harden Windows Server’ in Hardening Guide for EventTracker Server.

Test Case ID: OWASP-DS-003

Test Name: Testing for DoS Buffer Overflows, Applicable for EventTracker

Description: In this test, we check whether it is possible to cause a denial of service condition by overflowing one or more data structures of the target application.

Remarks: The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DS-004

Test Name: User Specified Object Allocation, Not Applicable for EventTracker

Description: In this test, we check whether it is possible to exhaust server resources by making it allocate a very high number of objects.

Remarks: EventTracker does not support these settings.
Test Case ID: OWASP-DS-005

**Test Name:** User Input as a Loop Counter, Not Applicable for EventTracker

**Description:** In this test we check whether it is possible to force the application to loop through a code segment that needs high computing resources, in order to decrease its overall performance.

**Remarks:** EventTracker does not support this setting.

Test Case ID: OWASP-DS-006

**Test Name:** Writing User Provided Data to Disk, Applicable for EventTracker

**Description:** With this test, we check that it is not possible to cause a DoS condition by filling the target disks with log data

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DS-007

**Test Name:** Failure to Release Resources, Applicable for EventTracker

**Description:** With this test, we check that the application properly releases resources (files and/or memory) after they have been used.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.

Test Case ID: OWASP-DS-008

**Test Name:** Storing too Much Data in Session, Applicable for EventTracker

**Description:** In this test, we check whether it is possible to allocate big amounts of data into a user session object to make the server exhaust its memory resources.

**Remarks:** The security recommendations are incorporated in the product development and user’s intervention is not required.
Web Services Testing

There are no web services in EventTracker. Hence this category is not applicable for EventTracker Enterprise.

AJAX Testing

AJAX (Asynchronous JavaScript and XML) is a group of interrelated web development techniques used on the client-side to create asynchronous web applications. With Ajax, web applications can send data to, and retrieve data from, a server asynchronously (in the background) without interfering with the display and behavior of the existing page.

There are no AJAX components in EventTracker. Hence this category is not applicable for EventTracker Enterprise.