Hardening Guide

OWASP Compliance

Publication Date

March 06, 2024

Abstract

This guide provides an overview of the OWASP-related security features and procedures built into Netsurion Open XDR and the checks and balances made in its development cycle.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.x.

Audience

This guide is for the users of the Netsurion Open XDR Web console.

Table of Contents

1 Overview

The **Open Web Application Security Project** (OWASP) is an open-source application security project. The primary goals of OWASP are given below:

- Protect Netsurion Open XDR users against high-risk threats.
- Ensure web application security.
- Reduce the surface area for an attacker to hack the Netsurion Open XDR Web console.

2 Categories of OWASP

There are ten categories available for testing as given below:

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 Netsurion Open XDR except **Web Services testing**.

3 Information Gathering

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

Test Case ID: OWASP-IG-002
Test Name: Search Engine Discovery/Reconnaissance, not applicable for Netsurion Open XDR
Description: This test case describes how to search the Google Index and remove the associated web content from Google Cache.
Remarks: Netsurion Open XDR is not a search engine-based application.

Test Case ID: OWASP-IG-003
Test Name: Identify application entry points, applicable for Netsurion Open XDR
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 have been completed.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-IG-004
Test Name: Testing for Web Application Fingerprint, applicable for Netsurion Open XDR
Description: Knowing the version and type of the running web server allows the testers to determine known vulnerabilities and the appropriate exploits to use during testing.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-IG-005
Test Name: Application Discovery, applicable for Netsurion Open XDR
Description: A paramount step in testing for web application vulnerabilities is to find out which applications are hosted on a web server. Many applications have known vulnerabilities and known attack strategies that can be exploited to gain remote control or to exploit data.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-IG-006
Test Name: Analysis of Error Codes, applicable for Netsurion Open XDR
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 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 into the product development and user intervention is not required.

4 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.

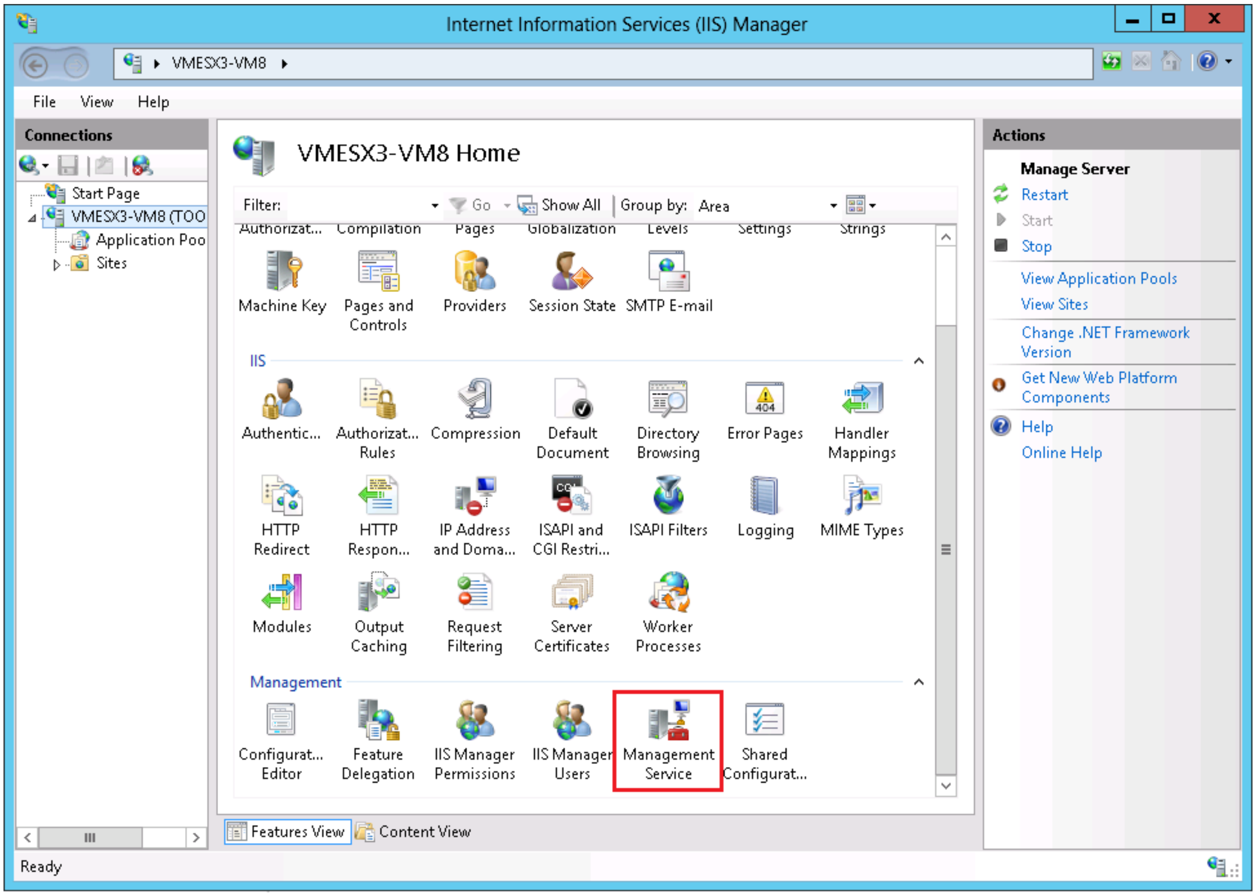
Test Case ID: OWASP-CM-001
Test Name: SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity), applicable for Netsurion Open XDR
Description: SSL and TLS are two protocols that provide, with the support of cryptography, secure channels for the protection, confidentiality, and authentication 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.
Refer the topic ‘Secure IIS Web Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-CM-002
Test Name: DB Listener Testing, not applicable for Netsurion Open XDR
Description: During the configuration of a database server, many Database 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 the Oracle database and Netsurion Open XDR does not support Oracle Database.

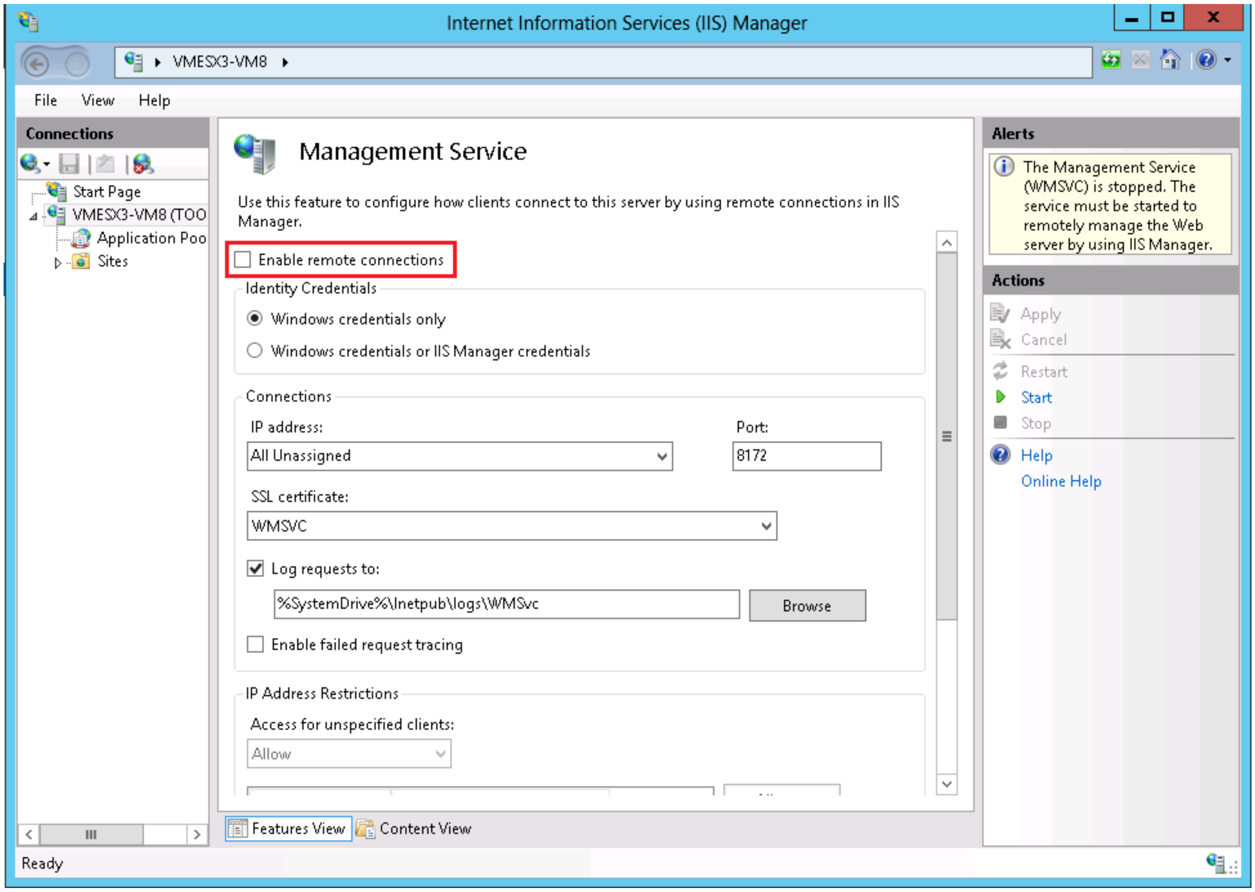
Test Case ID: OWASP-CM-003
Test Name: Infrastructure Configuration Management Testing, applicable for Netsurion Open XDR
Description: It takes only a single vulnerability to undermine the security of the entire infrastructure, and even small and (almost) unimportant problems may evolve into severe risks for another application on the same server.
Resolution: The 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 the remote connection in IIS, follow the steps mentioned below:

1. Click 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**.



Management Service

Use this feature to configure how clients connect to this server by using remote connections in IIS Manager.

□ Enable remote connections

Identity Credentials

● Windows credentials only

○ Windows credentials or IIS Manager credentials

Connections

IP address: All Unassigned

Port: 8172

SSL certificate: WMSVC

☑ Log requests to: %SystemDrive%\Inetpub\logs\WMSvc [Browse]

□ Enable failed request tracing

IP Address Restrictions

Access for unspecified clients: Allow

The Management Service (WMSVC) is stopped. The service must be started to remotely manage the Web server by using IIS Manager.

5. Disable the **Enable Remote Connections** option if it is selected.

Test Case ID: OWASP-CM-004
Test Name: Application Configuration Management Testing, applicable for Netsurion Open XDR
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 the default error codes of the web servers.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-CM-005
Test Name: Testing for File Extensions Handling, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-CM-006
Test Name: Old, Backup, and Unreferenced files, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-CM-007
Test Name: Infrastructure and Application Admin Interfaces, applicable for Netsurion Open XDR
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 them to access 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 into the product development and user intervention is not required.

Test Case ID: OWASP-CM-008
Test Name: Testing for HTTP Methods and XST, applicable for Netsurion Open XDR
Description: In this test, we check that the web server is not configured to allow potentially dangerous HTTP commands (methods), and cross-site tracing (XST) is not possible.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

5 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 Netsurion Open XDR
Description: Here, the tester will just try to understand if the data that users put into the web form, to log onto a website, is transmitted using secure protocols that protect them from an attacker or not.
Resolution: Customers must configure SSL for Netsurion Open XDR by using trusted and valid certificates. Refer the topic ‘Secure IIS Web Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-AT-002
Test Name: Testing for user enumeration, applicable for Netsurion Open XDR
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 brute force testing, in which we verify if, given a valid username, it is possible to find the corresponding password.
Resolution: Customers should follow the security recommendations of Active Directory as per Microsoft guidelines. Also, it is recommended that customers should not add default or guessable user accounts to the Netsurion Open XDR group.
Refer the topic ‘Harden Windows Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-AT-003
Test Name: Testing for Guessable (Dictionary) User Account, applicable for Netsurion Open XDR
Description: Here, we test if there are default user accounts or guessable username/password combinations (dictionary testing).
Resolution: Customers should follow the security recommendations of Active Directory as per Microsoft

guidelines. Also, it is recommended that customers should not add default or guessable user accounts to the Netsurion Open XDR group.
Refer the topic ‘Harden Windows Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-AT-004
Test Name: Brute Force Testing, applicable for Netsurion Open XDR
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: Netsurion Open XDR depends on Windows Authentication which can be either Active Directory or local host-based. Customers should follow the security recommendations of Active Directory as per Microsoft guidelines.
Refer the topic ‘Harden Windows Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-AT-005
Test Name: Testing for bypassing authentication schema, applicable for Netsurion Open XDR
Description: Other passive testing methods attempt to bypass the authentication schema by recognizing that not all the application's resources are adequately protected. The tester can access these resources without authentication.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-AT-006
Test Name: Testing for vulnerable remember password and password reset, partially applicable for Netsurion Open XDR
Description: Here, we test how the application manages the process of forgetting passwords. 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 into the product development and user intervention is not required.

Test Case ID: OWASP-AT-007
Test Name: Testing for Logout and Browser Cache Management, applicable for Netsurion Open XDR
Description: Here we check that the logout and caching functions are properly implemented.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-AT-008
Test Name: Testing for CAPTCHA, not applicable for Netsurion Open XDR
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: Netsurion Open XDR application does not have any CAPTCHA.

Test Case ID: OWASP-AT-009
Test Name: Testing Multiple Factors Authentication, not applicable for Netsurion Open XDR
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: Netsurion Open XDR does not support Multiple Factors Authentication.

Test Case ID: OWASP-AT-010
Test Name: Testing for Race Conditions, applicable for Netsurion Open XDR
Description: A race condition is a flaw that produces an unexpected result when the timing of actions impacts other actions. An example may be seen in 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 into the product development and user intervention is not required.

6 Session Management

Test Case ID: OWASP-SM-001
Test Name: Testing for Session Management Schema, applicable for Netsurion Open XDR
Description: This describes how to analyze a Session Management Schema, 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 channels.
Refer the topic ‘Secure IIS Web Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-SM-002
Test Name: Testing for Cookies attributes, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-SM-003
Test Name: Testing for Session Fixation, applicable for Netsurion Open XDR
Description: When an application does not renew the cookie after successful user authentication, it could be possible to find a session fixation vulnerability and force a user to utilize a cookie known to the attacker.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-SM-004
Test Name: Testing for Exposed Session Variables, applicable for Netsurion Open XDR
Description: Session Tokens represent confidential information because they tie the user's identity with his 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 channels.

Refer the topic ‘Secure IIS Web Server’ in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-SM-005
Test Name: Testing for CSRF (Cross-site Request Forgery), applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

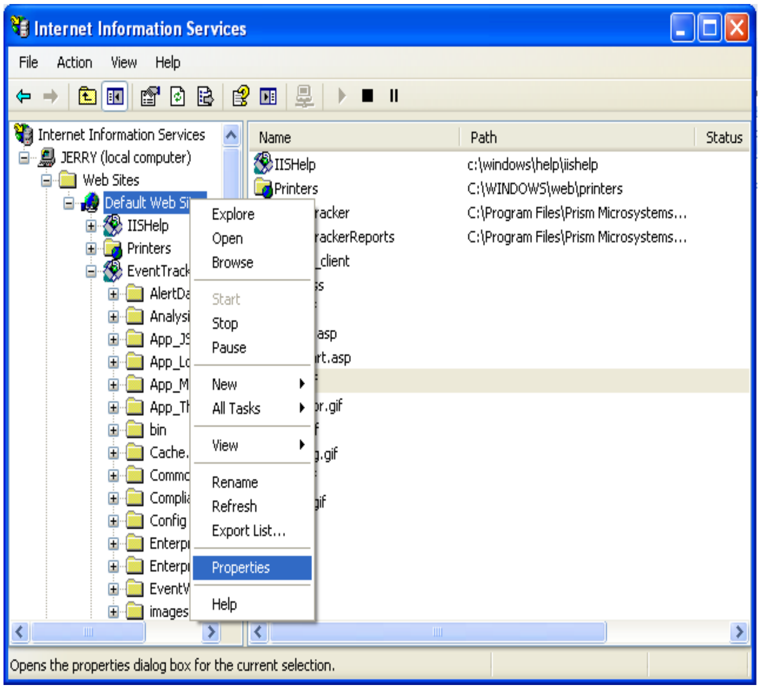
7 Authorization Testing

Test Case ID: OWASP-AZ-001
Test Name: Testing for Path Traversal, applicable for Netsurion Open XDR
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 and . logs should not be served directly.
To disable directory browsing in IIS, follow the steps given below:

1. Click the **Start** button, select **Control Panel**, and then select **Administrative Tools**.
2. Select **Internet Information Services**.

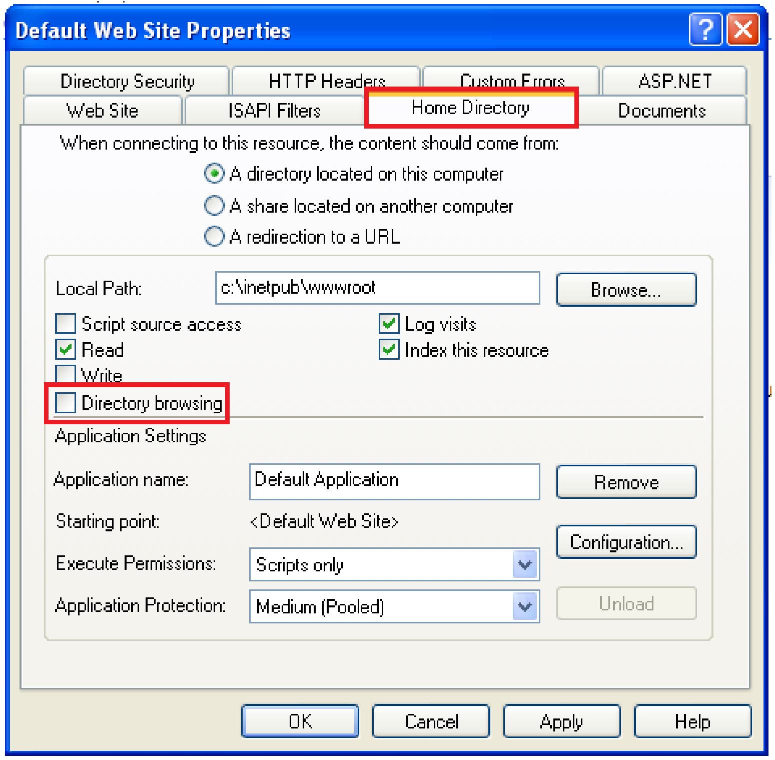
(OR)

1. Click the **Start** button, and select the **Run** command prompt.
2. Type **inetmgr** and then click **OK**.
3. Right-click **Default Web Site**, and select **Properties**.
4. **The Default Web Site Properties** window will be displayed.



Opens the properties dialog box for the current selection.

3. Select the **Home Directory** tab.



When connecting to this resource, the content should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local Path: c:\inetpub\wwwroot

□ Script source access
☑ Read
□ Write
□ Directory browsing
☑ Log visits
☑ Index this resource

Application Settings

Application name: Default Application
Starting point: <Default Web Site>
Execute Permissions: Scripts only
Application Protection: Medium (Pooled)

4. Unselect **Directory browsing** if it is selected.

Test Case ID: OWASP-AZ-002
Test Name: Testing for bypassing authorization schema, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-AZ-003
Test Name: Testing for Privilege Escalation, applicable for Netsurion Open XDR
Description: During this phase, the tester should verify that a user can't modify his or her privileges/roles inside the application in ways that could allow privilege escalation attacks.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

8 Business Logic Testing

Testing for business logic flaws in a multi-functional dynamic web application requires thinking in unconventional ways. Access rights of various user roles and groups are different. Every role or group has different constraints and privileges assigned to them.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

9 Data Validation Testing

Test Case ID: OWASP-DV-001
Test Name: Testing for Reflected Cross Site Scripting, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-002
Test Name: Testing for Stored Cross Site Scripting, applicable for Netsurion Open XDR
Description: In Stored Cross Site Scripting, we check if the stored data is potentially exposed to this type of attack.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-003
Test Name: Testing for DOM based Cross Site Scripting, applicable for Netsurion Open XDR
Description: In DOM-based cross-site scripting, we test if the active content, such as a JavaScript function, or a DOM element can be controlled by an attacker or not.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-004
Test Name: Testing for Cross Site Flashing, not applicable for Netsurion Open XDR
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: Netsurion Open XDR does not have any Flash images.

Test Case ID: OWASP-DV-005
Test Name: SQL Injection, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-006
Test Name: LDAP Injection, applicable for Netsurion Open XDR
Description: LDAP injection testing is like 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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-007
Test Name: ORM Injection, not applicable for Netsurion Open XDR
Description: ORM injection testing is like SQL Injection Testing, as well. In this case, we use an SQL Injection against an ORM-generated data access object model.
Remarks: Netsurion Open XDR is not an ORM-supported application.

Test Case ID: OWASP-DV-008
Test Name: XML Injection, applicable for Netsurion Open XDR
Description: In XML injection testing, we test if it is 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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-009
Test Name: SSI Injection, applicable for Netsurion Open XDR
Description: In SSI injection testing, we test if it is possible to inject into the application data that will be interpreted by SSI mechanisms. 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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-010
Test Name: XPath Injection, applicable for Netsurion Open XDR
Description: In XPath injection testing, we have tested if it is possible to inject data into an application so that it executes user-controlled XPath queries.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-011
Test Name: IMAP/SMTP Injection, applicable for Netsurion Open XDR
Description: In IMAP/SMTP injection testing, we test if it is possible to inject arbitrary IMAP/SMTP commands into the mail servers, because the input data is not properly sanitized.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-012
Test Name: Code Injection, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DV-013
Test Name: OS Commanding, applicable for Netsurion Open XDR
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 into the product development and user

intervention is not required.

Test Case ID: OWASP-DV-014
Test Name: Buffer overflow, applicable for Netsurion Open XDR
Description: In these tests, we check for different types of buffer overflow vulnerabilities.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-015
Test Name: Incubated vulnerability, applicable for Netsurion Open XDR
Description: Incubated testing is a complex test that needs more than one data validation vulnerability to work.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

Test Case ID: OWASP-DV-016
Test Name: Testing for HTTP Splitting/Smuggling, applicable for Netsurion Open XDR
Description: Describes how to test for an HTTP Exploit, such as HTTP Verb, HTTP Splitting, and HTTP Smuggling.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

10 Denial of Service Testing

Test Case ID: OWASP-DS-001
Test Name: Testing for SQL Wildcard Attacks, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DS-002
Test Name: Locking Customer Accounts, applicable for Netsurion Open XDR
Description: In this test, we check whether an attacker can lock valid user accounts by repeatedly attempting to log in with the wrong password.
Resolution: Netsurion Open XDR depends on Active Directory [AD] for authentication and this scenario is mainly based on AD settings. Customers should follow the security recommendations of Active Directory as per Microsoft guidelines.
Refer the topic 'Harden Windows Server' in the Hardening Guide for Netsurion Open XDR Server.

Test Case ID: OWASP-DS-003
Test Name: Testing for DoS Buffer Overflows, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DS-004
Test Name: User Specified Object Allocation, not applicable for Netsurion Open XDR
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: Netsurion Open XDR does not support these settings.

Test Case ID: OWASP-DS-005
Test Name: User Input as a Loop Counter, not applicable for Netsurion Open XDR
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, to decrease its overall performance.
Remarks: Netsurion Open XDR does not support this setting.

Test Case ID: OWASP-DS-006
Test Name: Writing User Provided Data to Disk, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DS-007
Test Name: Failure to Release Resources, applicable for Netsurion Open XDR
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 into the product development and user intervention is not required.

Test Case ID: OWASP-DS-008
Test Name: Storing too Much Data in Session, applicable for Netsurion Open XDR
Description: In this test, we check whether it is possible to allocate large amounts of data into a user session object to make the server exhaust its memory resources.
Remarks: The security recommendations are incorporated into the product development and user intervention is not required.

11 Web Services Testing

There are no web services in Netsurion Open XDR. Hence this category is not applicable for Netsurion Open XDR Enterprise.

12 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 Netsurion Open XDR. Hence this category is not applicable.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support