

Oracle web applications can help dramatically increase productivity, accessibility, knowledge sharing and revenues. With an ever-increasing variety of digital threats it is essential that web applications of all varieties remain accessible, and secure. Failure to protect against current and emerging threats can have potentially crippling effects upon organisations of all kinds.

OraScan from NGSSoftware is a detailed auditing application developed to assess the security of Oracle web applications regardless of environment. OraScan allows system administrators to audit the security of bespoke online applications and front-end servers. The detailed level of auditing supported by OraScan allows users to be assured in their digital defence strategies.

## Product Overview

OraScan forms part of NGSSoftware's suite of Intelligent Next Generation Security Assessment tools. OraScan has been developed to provide system administrators with the facility to successfully conduct detailed audits of bespoke Oracle web applications regardless of their deployment.

OraScan performs a comprehensive and detailed security vulnerability audit of Oracle web applications focusing on the discovery of flaws (e.g. SQL Injection, Cross Site Scripting, Remote Command Shell execution etc). OraScan can additionally be deployed to audit the configuration of Oracle IAS web server, ensuring that no security vulnerabilities are present within the base software architecture.

OraScan consists of six unique scanning phases:

### Spidering

OraScan incorporates advanced spidering technology to enumerate the structure of Oracle web applications to a deep level. Following this enumeration phase, OraScan employs a series of checks in order to evaluate the structure of all the functional aspects of the application.

### PL/SQL Checks

OraScan verifies the configuration of the HTTP interface to PL/SQL, checking Database Access Descriptor configuration, default package accessibility, and verifying that known mod\_plsql bugs (such as directory traversal) are not present.

### JSP Checks

OraScan checks for SQL Injection and Cross Site Scripting bugs in JSP scripts. It also verifies that checked servers are not vulnerable to known Oracle JSP issues such as source code disclosure.

### Oracle Defaults Checks

Oracle iAS adds large numbers of default scripts to the web server, some of which are potentially highly dangerous. OraScan checks for the existence of these scripts, as well as pointing out commonly visible configuration files and components (such as the Soap Router servlet).

### SQL Injection Checks

OraScan will automatically insert test values into potentially vulnerable URLs. The response is then parsed for recognised ODBC error messages. This automation of a tedious process for large sites uncovers many obscure means of exploitation that may be missed by a manual audit.

### Cross Site Scripting

Cross Site Scripting checks in OraScan insert JavaScript to create a pop-up box into potentially vulnerable URLs. OraScan tests for successful code execution within the client's security context, due to poor input validation.

## Global leadership

NGS leads the world in a number of key areas, including:

- Enterprise level application vulnerability research, database security, the development of sophisticated security software and expert consulting services.
- The NGS Team includes internationally renowned security researchers and CHECK Team leaders.
- Our Research Team is constantly hard at work to combat the ever-growing and increasingly sophisticated threats to software security.
- Based in the United Kingdom we provide our services to some of the largest and most demanding organisations around the globe.
- NGS have published more advisories regarding high-level enterprise application vulnerabilities than any other security company.
- NGS are a trusted computer security partner for some of the largest companies in the world – and for many key government departments.

## Features and Benefits

OraScan has a number of key benefits, including:

### Extensive Auditing Capabilities

OraScan is capable of auditing a variety of application level technologies. These include: PL/SQL, JSP, SQLJSP and XSQL.

### Reporting

OraScan provides a range of output formats for scan results. Results can be returned in either plain text, rich text format, HTML and dynamic HTML.

### Detailed Application Enumeration

The multi-layered scanning approach of OraScan allows it to develop a detailed perspective of applications. Thanks to the unique spidering technology of the application, OraScan can discover vulnerabilities that would otherwise have remained as hidden elements within Oracle web applications.

### Wide Variety of Audits

OraScan provides detailed auditing of Oracle web applications operating on any server platform. As well as systematically probing applications for security vulnerabilities, OraScan can additionally audit the configuration of Oracle IAS web servers to discover potentially unchecked flaws within the architecture of the base platform.

Currently, OraScan is the only application capable of fully auditing bespoke web applications on Oracle servers.

## System Requirements

System: Microsoft Windows NT 4.0 (Service pack 6a)  
 Microsoft Windows Server 2003  
 Microsoft Windows 2000  
 Microsoft Windows XP  
 Hardware: 500MHz Pentium III (minimum)  
 Memory: 512Mb RAM (minimum)  
 Disk space: 20Mb free disk space

### ACCREDITATIONS



**CLAS**

CESG Listed Adviser Scheme



**CTAS**

CESG Tailored Assurance Service



QUALIFIED SECURITY  
ASSESSOR

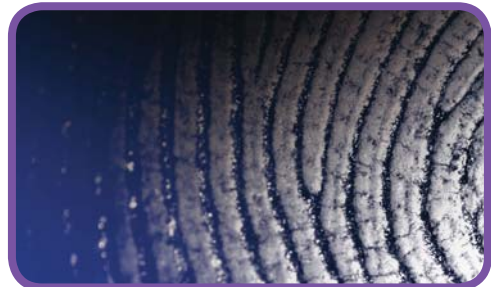


**CHECK**

IT Health Check Service

### Our customers include:

- Comic Relief
- Microsoft
- Commerzbank
- McAfee
- Centennial Software
- Eracent



### Why NGS?

NGSSoftware draws on both the insights of our world-beating research department and the highly practical expertise of our consultancy services; this helps ensure NGSSoftware's solutions are some of the most effective and up-to-date you can find.