

## hyper SOURCE

Secure your web code

## Finden Sie die kritischen Sicherheitslücken in Ihrem Quellcode!

## Schwachstellen finden und beheben:

Cross-Site Scripting  
 SQL Injection  
 Command Injection  
 File Injection  
 XML/XPath Injection  
 Malicious File Inclusion

## Source Code Verification

## Präziser und automatisierter Sicherheits-Check mittels statischer Analyse

art of defence bietet mit **hypersource™** europaweit das einzige Source Code Analyse Tool auf Basis der patentierten Source Code Verification Technologie. Diese verwendet automatisierte statische Analyse, um die Sicherheit von Web-Anwendungs-Code während der Software-Entwicklung zu überprüfen. **hypersource™** verfügt über einen eingebauten Compiler und kann deshalb Code unabhängig vom 'build environment' scannen. Da der Quellcode direkt geprüft wird, werden Schwachstellen wie Cross-Site-Scripting oder SQL-Injection schnell und eindeutig gefunden; dazu bietet **hypersource™** verständliche Vorschläge zur Fehlerbehebung.

## Warum brauchen Sie hypersource™ ?

## Automatisierter sicherer Entwicklungs-Prozess

Sicherheit wird oft als ein reines 'Backend'-Problem betrachtet - erst die Produkt-Fertigstellung, dann die Sicherheit. Dabei wird versucht, Angriffe zu entschärfen oder Laufzeitfehler mit Änderungen oder Anpassungen zu korrigieren. Dies ist aber oft unwirksam - und immer kostspielig und zeitaufwändig. Denn meist werden hier Lösungen wie z.B. Schwachstellen Analyse, Penetrations-Tests oder manuelle Code Reviews eingesetzt, oft erst, wenn die Software bereits produktiv im Einsatz ist. Um hier umfassende Ergebnisse zu erzielen, müssen heute echte Web Application Security Experten in der Regel viel Zeit investieren – verbunden mit vergleichsweise hohen Kosten. **hypersource™** verändert mit seiner Source Code Verification Technologie dieses Vorgehen, indem es den Sicherheitsaspekt direkt in den Entwicklungsprozess integriert.

**Der hypersource™ Verification-Prozess ist vollständig automatisiert und kann wiederholt in jeder beliebigen Phase des Entwicklungsprozesses eingeplant werden. Das Ergebnis ist bessere und sichere Software.**

## Großer Anwendungsbereich und hohe Genauigkeit

Im Gegensatz zu Penetrations-Tests und anderen Verfahren, die auf Brute-Force-Angriffen basieren, erkennt die Source Code Verification die genaue Lage und die Wurzeln der Schwachstellen. Zudem verbessert sie Programmier-Methoden, produziert wenige 'False Positives' und erzeugt sicher keine schädlichen Nebeneffekte während des Analyse-Prozesses. **hypersource™** bietet alle Vorteile eines manuellen Code-Reviews – aber mit einer gewaltigen Kosten- und Zeitersparnis, weil die Analyse bereits in der Entwicklungsphase und automatisiert erfolgt. Während sogenannte Vulnerability Assessments (VA) meist nur bereits implementierte und weit verbreitete Software auf bekannte Schwachstellen untersucht, ermöglicht **hypersource™** die Analyse von kundenspezifischer oder firmenintern entwickelter Software. **hypersource™** verfolgt mittels Trace-Back alle Fehler bis zur Wurzel zurück und visualisiert jeden Schritt der Fehlerfortpflanzung vom Beginn bis zum Ende. So erleichtert **hypersource™** dem Entwickler das Verstehen der identifizierten Schwachstelle - und bietet dazu noch konkrete Vorschläge zur Fehlerbehebung.



## hypersource™

Das automatisierte Source Code-Analyse-Tool identifiziert Sicherheitslücken im Web Code und schlägt schon in den frühen Phasen der Entwicklung einer Web-Anwendung Fehlerbehebungen vor.

# hyperSOURCE™ Overview

hyperSOURCE™ wurde von Grund auf mit dem Ziel entwickelt, Web-Applikationen bereits möglichst früh in ihrem Lebenszyklus abzusichern. Bereits in der Entwicklungsphase kann hyperSOURCE™ Quellcode automatisiert analysieren und die Entwickler bei der Behebung entdeckter Schwachstellen unterstützen. Besonders wichtig war zudem die einfache Integration von hyperSOURCE™ in die bestehenden Entwicklungsprozesse. Deshalb besteht hyperSOURCE™ aus zwei Komponenten - integriert in einer einzigen web-basierten Appliance.

## hyperSOURCE™ Enterprise

### Innovative Security Features

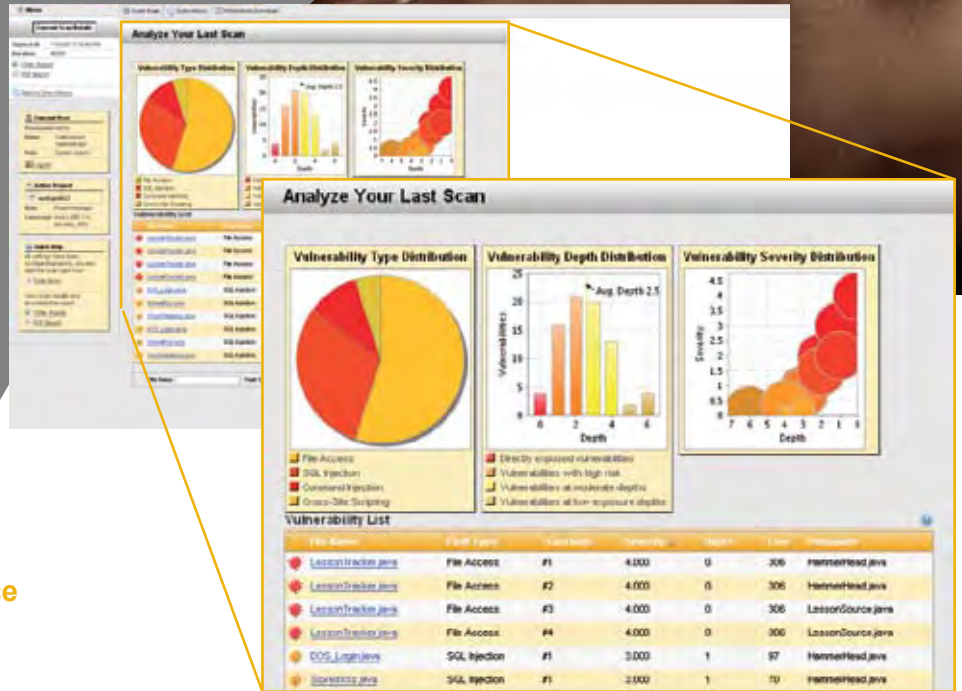
Eingebauter Parser und Übersetzer  
Tainted-Flow Analyse  
Smart Fix Recommendations

### Personalisierte Einstellungen

Rollenbasiertes Dashboard  
Individueller Report (html/pdf)  
Intelligente Hilfe-Funktion  
Mehr-Projekt-Fähigkeit

### Einfache Navigation im Web-Interface

Keine Software Installation- und Wartung  
Zentralisierte Konfiguration  
Zentralisiertes Wissensmanagement  
Automatische Reports per Email  
Automatisierte Regelmäßige Scans  
Flexible Quell-Auswahl (Dateien, SVN, zip, SAMBA, ftp)



hyperSOURCE™ Enterprise ist das erste automatisierte statische Source Code Analyse-Tool, das über ein web-basiertes Interface verfügt. Als Web 2.0 Appliance unterstützt hyperSOURCE™ Enterprise ohne großen Integrationsaufwand CSOs, CIOs und IT-Manager dabei, komplette Projekte und Teams mit rollenspezifischen Statusberichten zu managen und sehr große Mengen von Code zu analysieren. Zudem kann es einfach unternehmensweit eingesetzt werden, weil jeder Nutzer clientseitig nur einen Web Browser benötigt.

## hyperSOURCE™ Workbench

### Innovative Security Features

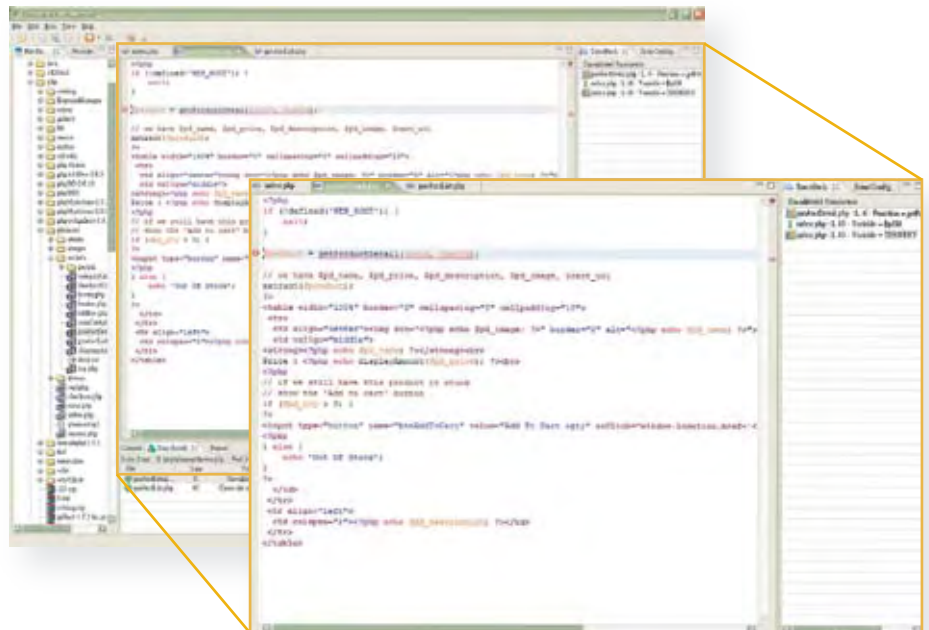
Trace-Back von Schwachstellen  
Cross-File Tainted-Flow Analyse  
Smart Fix Recommendations

### Integrierte Entwicklungsumgebung

Integrierte IDE und Plug-Ins  
Hervorheben des fehlerhaften Codes mit Hilfe von Quick Jump Index  
Syntax Highlighting

### Schnelles Assessment

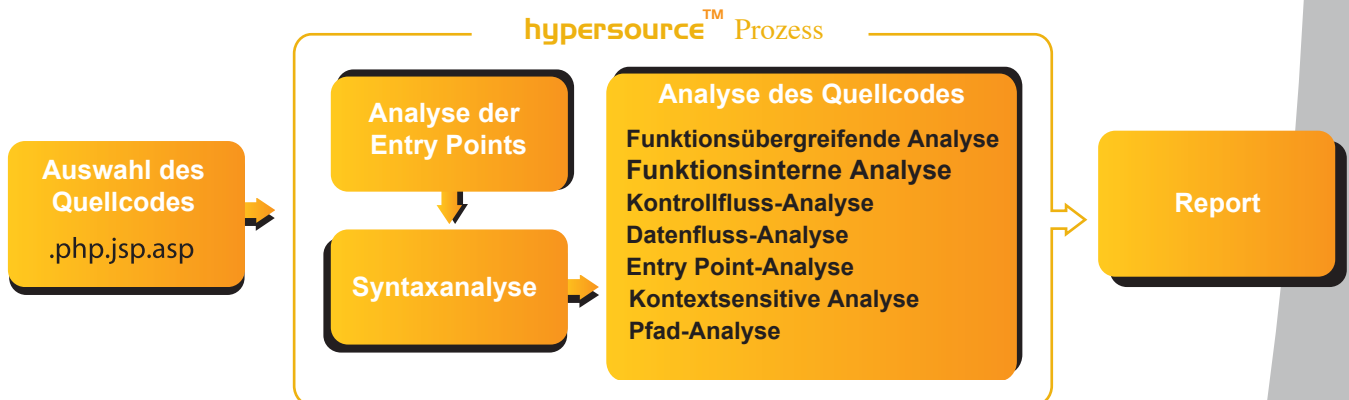
Einfache File-Navigation  
File-Basis Scanning  
HTML Report



hyperSOURCE™ Workbench ist das Werkzeug für die Software-Entwickler - mit einer einfach zu navigierenden Integrated Development Environment (IDE). Quellcode kann von jedem Repository abgerufen, gescannt, analysiert und gefixt werden, ohne die IDE zu verlassen. Features wie Traceback™ und Smart Remediation™ identifizieren die Wurzeln von Schwachstellen und schlagen Methoden zur Beseitigung vor.

## So funktioniert hypersource™.

**hypersource™** verwendet die neueste Verification-Technologie zur Analyse des Quellcodes. Hierbei wird zunächst ein Gesamtbild des Codes geformt; alle Funktionen werden analysiert und der Code wird systematisch auf Schwachstellen untersucht. Anschließend werden diese Schwachstellen Schritt für Schritt nachverfolgt und auf Schweregrad, Tiefe und Umfang geprüft. Damit ist **hypersource™** die derzeit fortschrittlichste, effektivste und umfassendste Source Code Analyse Lösung.



## hypersource™ im Einsatz

Mit **hypersource™ Enterprise** können Projektleiter den Stand ihrer Web-Applikations-Projekte jederzeit einfach überprüfen und hinsichtlich Sicherheit bewerten. Dazu sind nur folgende fünf Schritte notwendig:



*Jedes Unternehmen, das seine vertraulichen und geschäftskritischen Informationen in Webanwendungen schützen will, wird von **hypersource's™** übergreifendem Ansatz stark profitieren.*

- 1) Geschäftsführer und Führungskräfte erhalten einen Kurzüberblick auf Projektebene, der sowohl den Projektstatus als auch die Leistung und den Fortschritt des Projektteams darstellt.
- 2) CSOs und CIOs erhalten eine vollständige Quellcode-Analyse-Lösung, die nur eine einzige Installation erfordert, dennoch die gesamte Applikationsentwicklung unternehmensweit abdeckt und ein kontinuierliches Monitoring sowohl auf Projektebene als auch auf individueller Basis erlaubt.
- 3) Betriebs-Teams haben minimalen Aufwand – nur eine zentrale Appliance muss installiert und gewartet werden.
- 4) Entwicklungsleiter, Softwarearchitekten und Security Auditoren können zu jeder Zeit ihr personalisiertes Dashboard einfach über einen Web Browser aufrufen - es sind keine clientseitigen Installationen notwendig.

Mit einer bequem navigierbaren IDE bietet **hypersource™ Workbench** eine einfache und integrierte Plattform, um Code zu überprüfen und Schwachstellen zu identifizieren und zu beheben. Die integrierte Enterprise-Version bietet zudem planmäßige Scans, Email-Reporting und rollenbasierte Dashboards. Die Prozess-Effizienz wird so erheblich gesteigert, da eine fließende Kommunikation zwischen den einzelnen Abteilungen und Hierarchieebenen erleichtert wird.

## Unterstützte Plattformen

Windows  
UNIX-like (Linux/BSD)  
Mac OS X

## Unterstützte Web-Sprachen

PHP  
J2EE (JAVA/JSP)  
ASP  
.NET

## Kontakt

**art of defence GmbH**  
Bruderwöhrdstr. 15b  
93055 Regensburg  
Deutschland

Office: +49-941-604-889-78  
Fax: +49-941-604-889-837

Email: [sales@artofdefence.com](mailto:sales@artofdefence.com)

## Entwicklung von Web Applikationen und Softwareprodukten

In-house entwickelte Software wird meist regelmäßig durch Kollegen oder durch externe manuelle Code Reviews auf Schwachstellen überprüft – sehr zeit- und kostenaufwändig.

### Ein Fall für **hypersource**™

Die Entwickler können das Quellcode-Analyse-Tool routinemäßig einsetzen, um Schwachstellen möglichst früh und sehr schnell zu finden und zu beseitigen.

## Überprüfung von Outsourcing-Leistungen

Die Überprüfung von outgesourceten Projekten bedeutet immer einen immensen Zeit-, Arbeits- und Kostenaufwand - denn nicht jeder Entwickler ist ein Security-Experte.

### Ein Fall für **hypersource**™

Das statische Analyse-Tool übernimmt auch hier die Überprüfung und identifiziert Sicherheitslücken in outgesourceten Projekten.

## Fortgeschrittenes Penetration Testing

Viele Firmen verwenden heute Penetration-Testing-Tools zur Überprüfung von bereits entwickelter oder installierter Software. Diese haben in der Regel folgende Nachteile: 1. Begrenzte Tiefe der Analyse – komplexe und gravierende Sicherheitslücken werden übersehen und 2. Unklare Gegenmaßnahmen – Die Tools können den Entwicklern nicht die genaue fehlerhafte Stelle im Quellcode zeigen.

### Ein Fall für **hypersource**™

Source Code Verification identifiziert bekannte und unbekannte Schwachstellen, zeigt die fehlerhaften Stellen im Code präzise an und schlägt Lösungswege vor.

## Erkennen von Zero-Day-Exploits in Open Source Software

Open Source Software ist heute sehr weit verbreitet und kommt in ganz unterschiedlichen Applikationen im industriellen oder öffentlichen Sektor -z. B. in staatlichen oder militärischen Einrichtungen - zum Einsatz. Deshalb sind Schwachstellen in Open Source Komponenten inzwischen lukrative Angriffsziele für Angreifer aller Art. Unzählige frei zugängliche Open Source Komponenten bedeuten aber Milliarden von Code-Zeilen. Diese können nur durch automatisierte Tools wirksam und effizient überprüft werden.

### Ein Fall für **hypersource**™

Mit dem Quellcode Analyse-Tool spüren Sie Zero-Day-Exploits auf - bevor sie Hacker ausnutzen.

## Über art of defence

Die art of defence GmbH ist das europaweit einzige Unternehmen, das Sicherheits-Produkte für Web-Anwendungen über den gesamten Applikations-Lebenszyklus anbietet. Führende Banken, Finanzdienstleister und E-Commerce-Unternehmen setzen beim Schutz ihrer internen und externen Web-Anwendungen auf art of defence und erfüllen so Gesetzesauflagen und Industrie-Standards wie die Sicherheitsrichtlinien der Kreditkartenindustrie (PCI-Compliance).

Das Web Source Code Analyse-Tool **hypersource** erkennt die genaue Lage von Schwachstellen im Quellcode von Web-Anwendungen mittels automatisierter statischer Analyse. Es unterstützt CIOs, Sicherheitsverantwortliche und Entwickler rollenbasiert durch Status-Berichte und detaillierte Vorschläge zur Behebung der entdeckten Schwachstellen – ohne clientseitige Installation, nur über einen Web Browser.

Für den Schutz produktiver Web-Anwendungen bietet art of defence **hyperguard**, die Enterprise Web Application Firewall (WAF) der zweiten Generation. Mit ihr definieren Security-Verantwortliche das Verhalten von Web-Applikationen nach außen und können so Manipulationen und unberechtigte Zugriffe auf die hinter den Web-Anwendungen liegenden Datenbanken und operativen Systeme verhindern.

[www.artofdefence.com](http://www.artofdefence.com)