



COMPUWARE

Rendre l'informatique encore plus performante

Compuware : Présence globale, Acteur local

Présence globale :

- 1,2 milliard de \$ en 2005
- 8 700 personnes
- 23 000+ clients
- Présent dans 47 pays
- 3 Laboratoires R&D
- 40% du chiffre d'affaires en Europe

Acteur local :

- 190 personnes
- 100 consultants spécialisés
- 1000 clients

LA REPONSE COMPUWARE

Pour rendre l'informatique encore plus performante

Compuware IT Governance Solution

Offres intégrées : services, méthodologie, meilleures pratiques

CAQS

CARS

CAPS

CAMS

Productivité du
Développement

OptimalJ
Uniface
DevPartner
DevEnterprise

Assurance Qualité
et tests

QAcenter
Vantage
File-AID

Performance et
Disponibilité

Vantage

Évolutions et
Maintenance

DevPartner
DevEnterprise
QAcenter

MVS, L4G, Java, C, .Net, Web services, VoIP, progiciels, bases de données ...

RAPPEL DE LA COUVERTURE FONCTIONNELLE DE DEVPARTNER STUDIO

- DETECTION AUTOMATIQUE D'ERREURS ET FUITES MEMOIRE
- ANALYSE ET OPTIMISATION DES PERFORMANCES CPU
- ANALYSE DES PERFORMANCES MEMOIRE
- COUVERTURE DE CODE
- RESPECT DES STANDARDS DE CODAGE
- DIAGNOSTIC D'EXECUTION LOCALE OU DISTRIBUEE D'APPLICATIONS
- MESURE DE PERFORMANCES RESEAU ET DISQUE DUR
- SIMULATION DE DYSFONCTIONNEMENT
- DETECTION DE FAILLES DE SECURITE (ASP.NET uniquement)
- COMPARER VOS ENVIRONNEMENTS D'EXECUTION

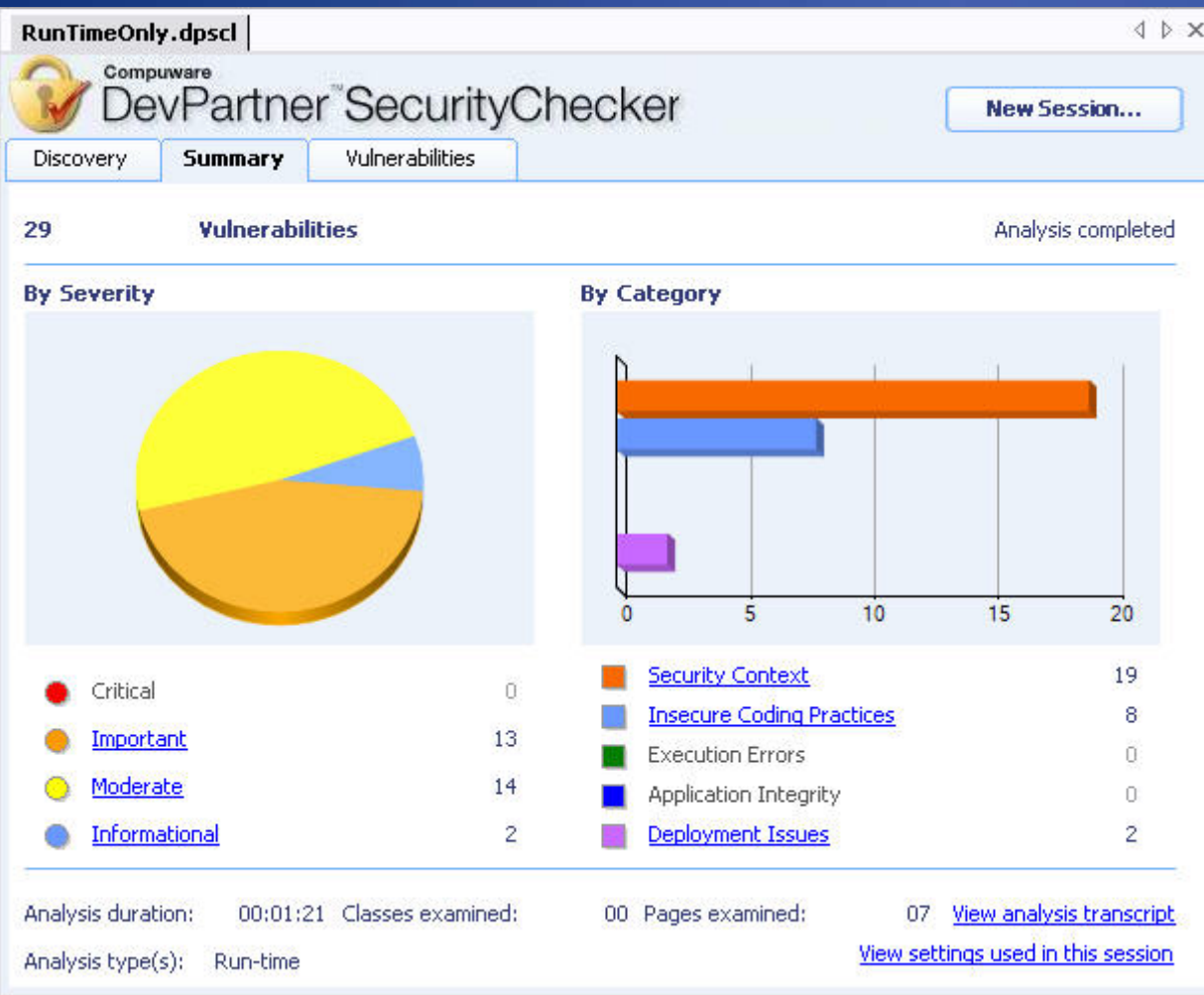
SECURITYCHECKER

Détection des failles de sécurité Web ASP.NET

- Plus de 200 règles pour la sécurisation de code
- 3 modes d'utilisations:
 - **Compile Time Analysis:** Analyse en phase de développement
 - **Runtime analysis:** Analyse en phase de débogage
 - **Integrity analysis:** Analyse en phase de pré déploiement
- Classification des erreurs par catégories et par niveau de sévérité
- Suggestion de correction pour chaque erreur identifiée

Run-Time analyze

- Debug phase
- Run-Time vulnerabilities, like
 - Permission Vulnerabilities
 - Database Access
 - Registry Access
 - Account Privileges
 - etc...



Niveau de détail et code source

The screenshot displays the Compuware DevPartner SecurityChecker interface. The main window shows a list of vulnerabilities under the 'Vulnerabilities' tab. The selected vulnerability is 'ValidateRequest disabled in page (1033)', which is categorized as 'Insecure Coding Practices' and has a severity of 'Critical'. The file path is 'E:\Inetpub\wwwroot\PDANET\account.aspx'.

The 'SecurityChecker Vulnerability Details' window provides an explanation for this issue:

ValidateRequest disabled in page (1033)

Explanation:
The ValidateRequest attribute of the Page directive has been disabled:

```
<%@ Page ValidateRequest="false"%>
```

This will prevent the page request from being validated for malicious input, most notably cross-site scripting attacks. The input entered into the fields of the page is compared against a variety of common cross-site scripting attack signatures. If an input matches, a HttpRequestValidationException is thrown. While this ASP.NET feature prevents many cross-site scripting attacks, it does not prevent all of them, especially the newer attacks.

By default, all page requests are validated

The 'CompileOnly.dpscl account.aspx' window shows the source code for the selected file. The 'Client Objects & Events' window is open, showing the following code:

```
<%@ Page Language="vb" Debug="true" AutoEventWireup="false" validateRequest="false" CodeBehind="Account.aspx.vb" Inherits="Account" %>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
  <HEAD>
    <title>Compuware Products Demonstration Application</title>
    <meta name="GENERATOR" content="Microsoft Visual Studio.NET 7.0">
```

Base de connaissance

DevPartner SECURITYCHECKER

Bénéfices

- Identifier automatiquement les failles de sécurités
- Disposer de plus de 350 règles de sécurisation du code Web .NET
- Mettre à jour ces verrous face aux dernières techniques de piratage:
 - SQL Injection,
 - XSS Attack
 - Droits d'exécutions,
 - Parameter tampering
 - Cross site script attack, etc...
- Accélérer l'apprentissage du langage Web.NET et la correction des bugs

Cible technologique:

MICROSOFT

APPLICATIONS WEB (ASP.NET)



COMPUWARE®