Fortify Audit Workbench

SANS Top 25 2011

ManagementPlatformWeb_CodeReview20230706

Table of Contents

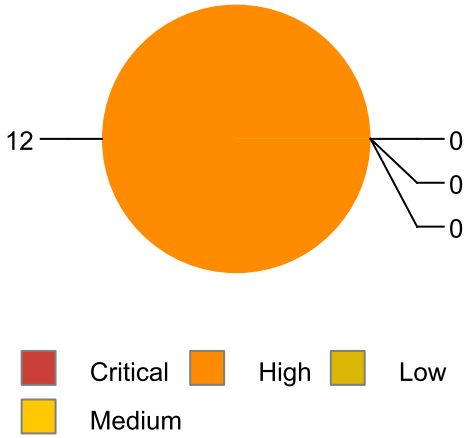
© Copyright [2008-2018] Micro Focus or one of its affiliates. The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Executive Summary

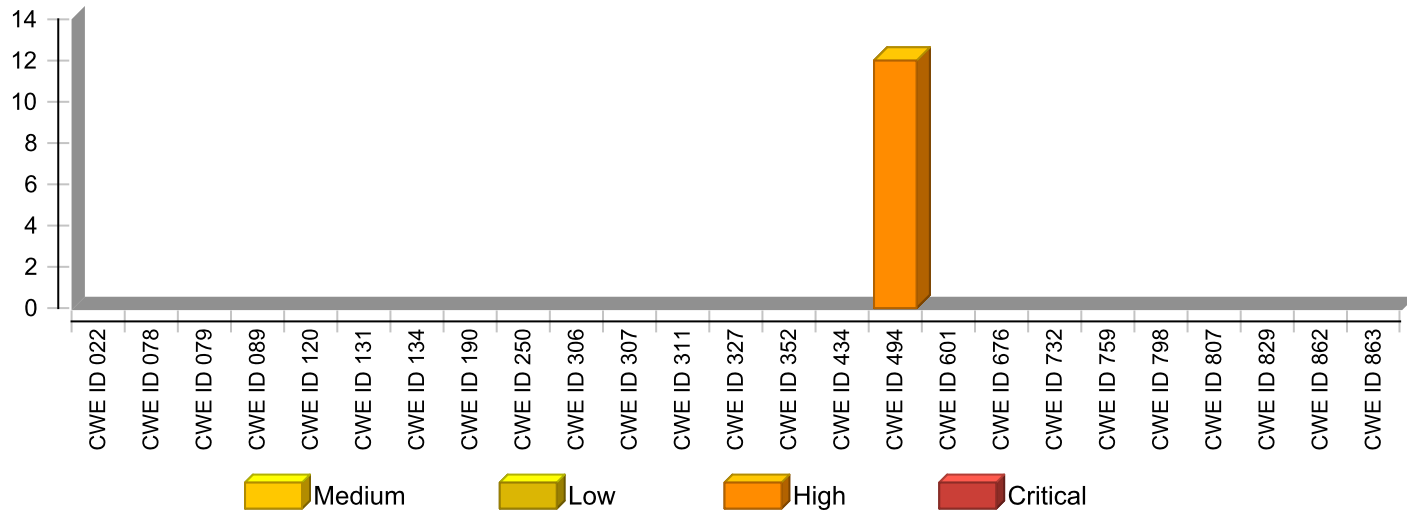
Project Name:	ManagementPlatformWe
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present

Issues by Folder



SANS Top 25 2011 groups	Total	Status
Insecure Interaction	0	**PASS**
Porous Defenses	0	**PASS**
Risky Resource Management	12	**FAIL**

Issues by SANS Top 25 2011 Categories



* The detailed sections following the Executive Summary contain specifics.

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Issue BreakDown

The following table summarizes the number of issues identified across the different SANS Top 25 2011 categories and broken down by Fortify Priority Order.

Risky Resource Management	Folder	Issues	Audited
Risky Resource Management - CWE ID 022		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Insecure Interaction	**Folder**	**Issues**	**Audited**
Insecure Interaction - CWE ID 078		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Insecure Interaction - CWE ID 079		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Insecure Interaction - CWE ID 089		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management	**Folder**	**Issues**	**Audited**
Risky Resource Management - CWE ID 120		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management - CWE ID 131		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management - CWE ID 134		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management - CWE ID 190		0	0
	Critical	0	0
	High	0	0

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management	Folder	Issues	Audited
Risky Resource Management - CWE ID 190		0	0
	Medium	0	0
	Low	0	0
Porous Defenses	**Folder**	**Issues**	**Audited**
Porous Defenses - CWE ID 250		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 306		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 307		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 311		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 327		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Insecure Interaction	**Folder**	**Issues**	**Audited**
Insecure Interaction - CWE ID 352		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Insecure Interaction - CWE ID 434		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management	**Folder**	**Issues**	**Audited**
Risky Resource Management - CWE ID 494		12	0
	Critical	0	0

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management	Folder	Issues	Audited
Risky Resource Management - CWE ID 494		12	0
	High	12	0
	Medium	0	0
	Low	0	0
Insecure Interaction	**Folder**	**Issues**	**Audited**
Insecure Interaction - CWE ID 601		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management	**Folder**	**Issues**	**Audited**
Risky Resource Management - CWE ID 676		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses	**Folder**	**Issues**	**Audited**
Porous Defenses - CWE ID 732		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 759		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 798		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 807		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Risky Resource Management	**Folder**	**Issues**	**Audited**
Risky Resource Management - CWE ID 829		0	0
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Porous Defenses	Folder	Issues	Audited
Porous Defenses - CWE ID 862		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
Porous Defenses - CWE ID 863		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0

NOTE:
1. Reported issues in the above table may violate more than one SANS Top 25 2011 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by SANS Top 25 2011, Folder, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

Risky Resource Management - CWE ID 022

对受限制目录路径名称的不当限制（“路径遍历”）。 CWE-22 声明：“软件使用外部输入来构建用于识别位于受限制父级目录下的文件或目录的路径名称，但是软件无法对路径名称中的特殊元素进行妥善转义处理，使得路径名称解析到了受限制目录之外的位置”。

No Issues

Insecure Interaction - CWE ID 078

对 OS 命令中使用的特殊元素的处理不当（“OS 命令注入”）。 CWE-78 声明：“软件使用来自上游组件的受外部影响的输入来构建完整或部分的 OS 命令，但是当将其发送给下游组件时软件无法或错误地转义处理了可以修改预期 OS 命令的特殊元素”。

No Issues

Insecure Interaction - CWE ID 079

Web 页面生成期间对输入的不当转义处理（“跨站脚本攻击”）。 CWE-79 声明：“软件将输入放入用作为其他用户服务的 Web 页面的输出之前，无法或错误地转义处理了用户可控制的输入”。

No Issues

Insecure Interaction - CWE ID 089

对 SQL 命令中使用的特殊元素转义处理不当（“SQL 注入”）。 CWE-89 声明：“软件使用来自上游组件的受外部影响的输入来构建完整或部分的 SQL 命令，但是当将其发送给下游组件时软件无法或错误地转义处理了可以修改预期 SQL 命令的特殊元素”。

No Issues

Risky Resource Management - CWE ID 120

复制缓冲区时不检查输入大小（“典型的缓冲区溢出”）。 CWE-120 声明：“如果程序将一个输入缓冲区复制到一个输出缓冲区，而不验证输入缓冲区的大小是否小于输出缓冲区的大小，这将导致缓冲区溢出”。

No Issues

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management - CWE ID 131

错误计算缓冲区大小。 CWE-131 声明：“分配缓冲区时软件没有正确地计算出要使用的大小，这将导致缓冲区溢出”。

No Issues

Risky Resource Management - CWE ID 134

不受控制的格式字符串。 CWE-134 声明：“软件在 printf 样式的函数中使用外部控制的格式字符串，这可以导致缓冲区溢出或数据表示问题”。

No Issues

Risky Resource Management - CWE ID 190

整数溢出或环绕。 CWE-190 声明：“当逻辑假设最终值将始终大于初始值时，软件执行可产生整数溢出或环绕的计算。当计算用于资源管理或执行控制时，这将产生其他弱点”。

No Issues

Porous Defenses - CWE ID 250

使用不必要的权限执行。 CWE-250 声明：“软件执行操作时使用级别高于最低要求级别的权限，这将产生新的弱点或扩大其他弱点所带来的影响”。

No Issues

Porous Defenses - CWE ID 306

缺少关键功能验证。 CWE-306 声明：“软件不对功能执行任何验证，该功能需要可证明的用户标识或将消耗大量资源”。

No Issues

Porous Defenses - CWE ID 307

对过多验证尝试的不当限制。 CWE-307 声明：“软件未实施有效措施以防止在短时间范围内进行多次失败的验证尝试，使得其更易遭受强力攻击”。

No Issues

Porous Defenses - CWE ID 311

缺少对敏感数据的加密。 CWE-311 声明：“软件未在存储或传输前加密敏感信息或重要信息”。

No Issues

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Porous Defenses - CWE ID 327

使用无效的或有风险的加密算法。 CWE-327 声明：“使用无效的或有风险的加密算法会产生不必要的风险，导致敏感信息暴露。”

No Issues

Insecure Interaction - CWE ID 352

跨站请求伪造 (CSRF)。 CWE-352 声明：“Web 应用程序不验证或无法确定格式标准的、有效的持续请求是否是提交请求的用户有意提供的”。

No Issues

Insecure Interaction - CWE ID 434

不限制上传危险类型的文件。 CWE-434 声明：“软件允许攻击者上传或传输危险类型的文件，这些文件可在产品环境中自动处理”。

No Issues

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management - CWE ID 494

在不检查完整性的情况下下载代码。 CWE-494 声明：“产品从远程位置下载源代码或可执行文件，并在未充分验证其来源和完整性的情况下执行代码”。

Dynamic Code Evaluation: Code Injection		High
Package: 00Lexi.01SVN.CountInsurance.branches.ManagementPlatformWeb.ManagementPlatformWeb_CodeReview2		
Location	**Analysis Info**	**Analyzer**
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.js:2809	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.js:2786	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.js:2809	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.js:2786	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.js:3436	**Sink:** setInterval() **Enclosing Method:** pollInteralLogs() **Source:** Read window.location **from** Operation() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.js:1253	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.min.js:1	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.min.js:1	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeCountNet.Insurance.ManagemerScripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** pollInteralLogs() **Source:** Read window.location **from** t() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/CountNet.Insurance.ManagementPlatformWeb/Scripts/ai.0.22.9-build00167.min.js:1	SCA

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management - CWE ID 494

在不检查完整性的情况下下载代码。 CWE-494 声明：“产品从远程位置下载源代码或可执行文件，并在未充分验证其来源和完整性的情况下执行代码”。

Dynamic Code Evaluation: Code Injection		High
Package: 00Lexi.01SVN.CountInsurance.branches.ManagementPlatformWeb.ManagementPlatformWeb_CodeReview20230706.packages.Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167.content.scripts		
Location	**Analysis Info**	**Analyzer**
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:2809	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:2786	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:2809	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:2786	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:3436	**Sink:** setInterval() **Enclosing Method:** pollInteralLogs() **Source:** Read window.location **from** Operation() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.js:1253	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	SCA
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** trackPageView() **Source:** Read window.location **from** trackPageView() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	SCA

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Risky Resource Management - CWE ID 494

在不检查完整性的情况下下载代码。 CWE-494 声明：“产品从远程位置下载源代码或可执行文件，并在未充分验证其来源和完整性的情况下执行代码”。

Dynamic Code Evaluation: Code Injection		High
Package: 00Lexi.01SVN.CountInsurance.branches.ManagementPlatformWeb.ManagementPlatformWeb_CodeReview20230706.packages.Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167.content.scripts		
Location	**Analysis Info**	**Analyzer**
00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	**Sink:** setInterval() **Enclosing Method:** pollInteralLogs() **Source:** Read window.location **from** t() **In** 00Lexi/01SVN/CountInsurance/branches/ManagementPlatformWeb/ManagementPlatformWeb_CodeReview20230706/packages/Microsoft.ApplicationInsights.JavaScript.0.22.9-build00167/content/scripts/ai.0.22.9-build00167.min.js:1	SCA

Insecure Interaction - CWE ID 601

将 URL 重定向至不可信赖的站点（“打开重定向”）。 CWE-601 声明：“Web 应用程序接收了一个用户控制的输入，该输入指定了一个到外部站点的链接，并在重定向中使用该链接。这样就会使钓鱼攻击变得更容易”。

No Issues

Risky Resource Management - CWE ID 676

使用有潜在危险的函数。 CWE-676 声明：“程序调用有潜在危险的函数，如果使用不正确，可能会导致产生漏洞，但也可以安全地使用该函数”。

No Issues

Porous Defenses - CWE ID 732

关键资源权限分配错误。 CWE-732 声明：“软件为安全关键资源指定权限，允许非指定的操作者读取或修改资源”。

No Issues

Porous Defenses - CWE ID 759

使用不带 Salt 的单向散列。 CWE-759 声明：“软件对输入使用了单向加密散列，应该是不可逆的，例如密码，但该软件在输入中也未使用 salt”。

No Issues

© Copyright [2008-2018] Micro Focus or one of its affiliates.

Porous Defenses - CWE ID 798

使用硬编码凭证。 CWE-798 声明：“软件包含硬编码凭证，例如密码或加密密钥，用于自身的入站验证、外部组件的出站通信或者内部数据的加密”。

No Issues

Porous Defenses - CWE ID 807

确定是否安全时依赖不可信赖的输入。 CWE-807 声明：“应用程序使用一种依赖于输入的存在或输入值的保护机制，但是不可信赖的操作者可以跳过保护机制修改输入”。

No Issues

Risky Resource Management - CWE ID 829

包含来自不可信赖的控制范围的功能。 CWE-829 声明：“软件导入、需要或包含来自预期控制范围以外的可执行功能（例如库）”。

No Issues

Porous Defenses - CWE ID 862

缺少授权。 CWE-862 声明：“软件未在操作者尝试访问资源或执行操作时执行授权检查”。

No Issues

Porous Defenses - CWE ID 863

授权错误。 CWE-863 声明：“软件在操作者尝试访问资源或执行操作时进行了授权检查，但不正确。这样就允许攻击者跳过原本的访问限制”。

No Issues

© Copyright [2008-2018] Micro Focus or one of its affiliates.