Manual Fortify

Eclipse y Visual Studio

ShieldNow BlueTeam Services

Email: blueteam@shieldnow.co

Web: https://shieldnow.co

Contenido

Introducción……...3

1. Instalación de Fortify Static Code Analyzer……..……..3

1.1 Instalación desde Marketplace..……..3

2. Análisis de un proyecto……..……9

2.1 Ejecución de la herramienta……..……9

2.2 Análisis del error: Path Manipulation……...13

Introducción

HP Fortify localiza vulnerabilidades de seguridad en las soluciones y paquetes sin ejecutar el código, luego muestra los resultados del escaneo en Visual Studio o Eclipse. Los resultados incluyen una lista de problemas descubiertos, descripciones del tipo de vulnerabilidad que representa cada problema y sugerencias sobre cómo solucionarlos. El paquete de HP Fortify Visual Studio o Eclipse son administrados por HP Fortify Static Code Analizer y HP Fortify Coding Rulepacks y soportan los siguientes lenguajes:

- ASP.NET
- C#
- C/C++
- ASP
- HTML
- Java
- JavaScript
- PHP
- PL/SQL
- Python
- VB.NET
- VBScript
- Visual Basic
- XML

1. Instalación de Fortify Static Code Analyzer

Requerimientos:

- Entorno de desarrollo instalado
- Archivo de licencia de HPE Security Fortify
- Archivo HPE_Security_Fortify_SCA_and_Apps_17.20_windows_x64

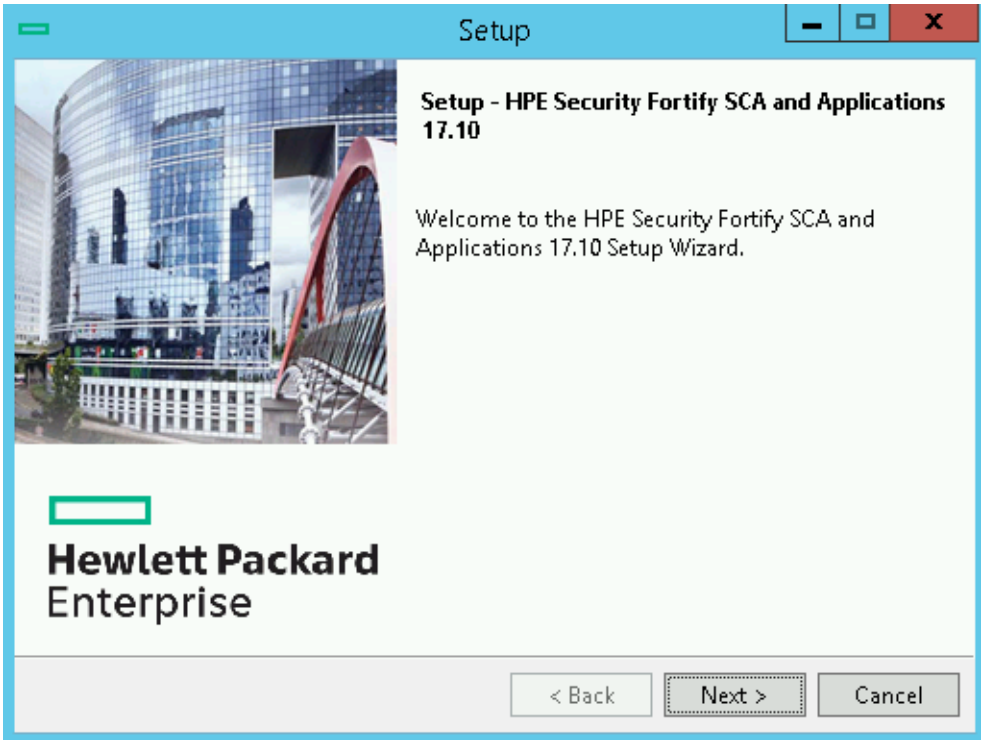

Figura 1. Wizard HPE Security Fortify SCA

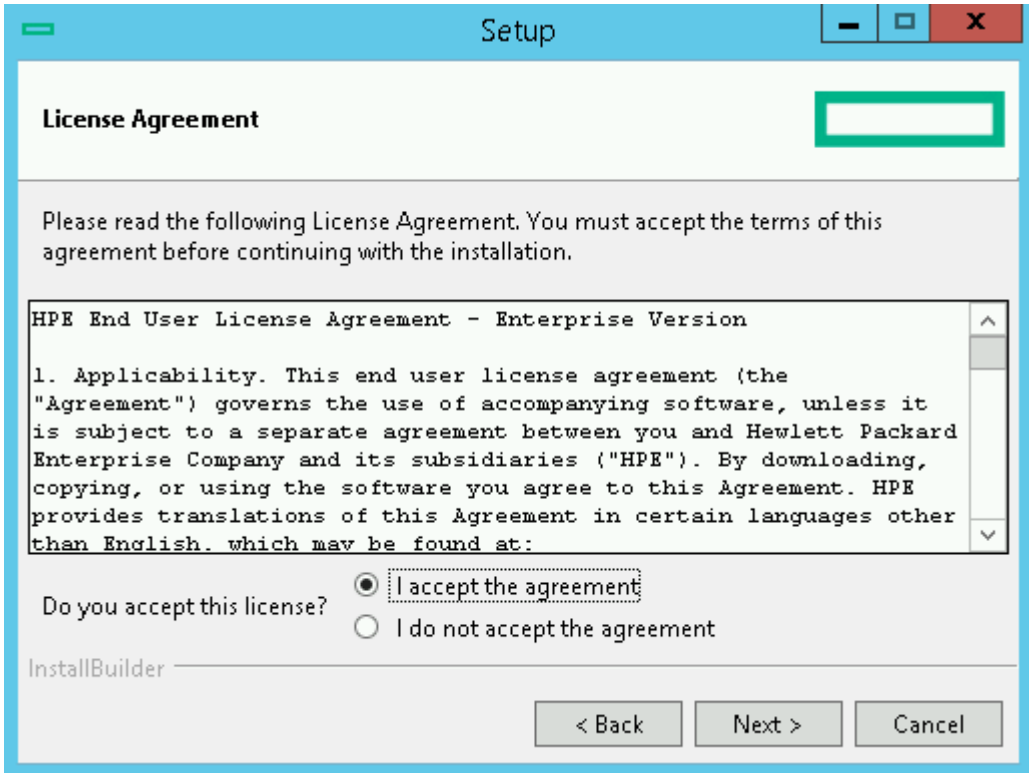

Figura 2. Términos de licencia

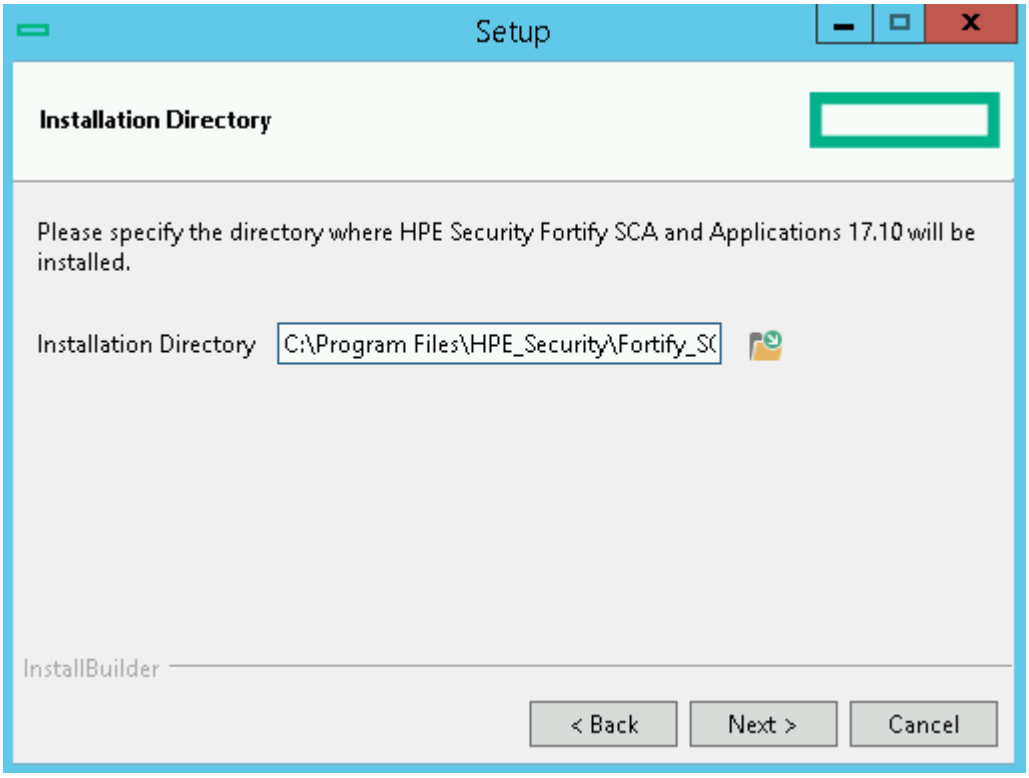

Figura 3. Directorio de instalación

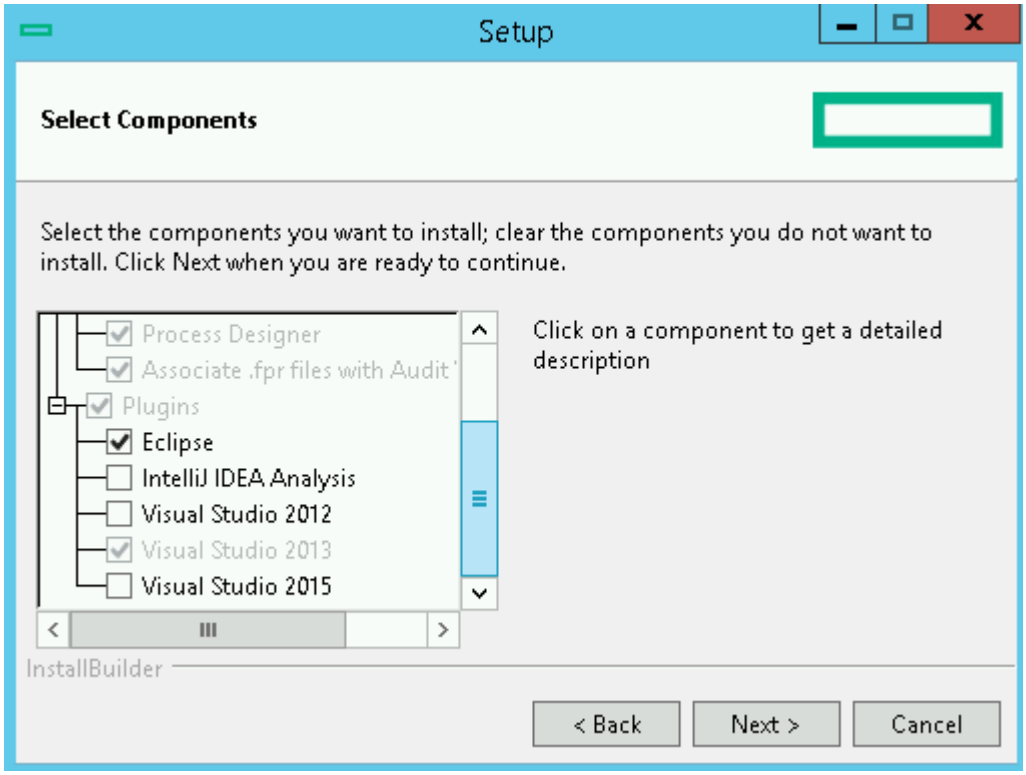

Figura 4. Selección del componente a instalar

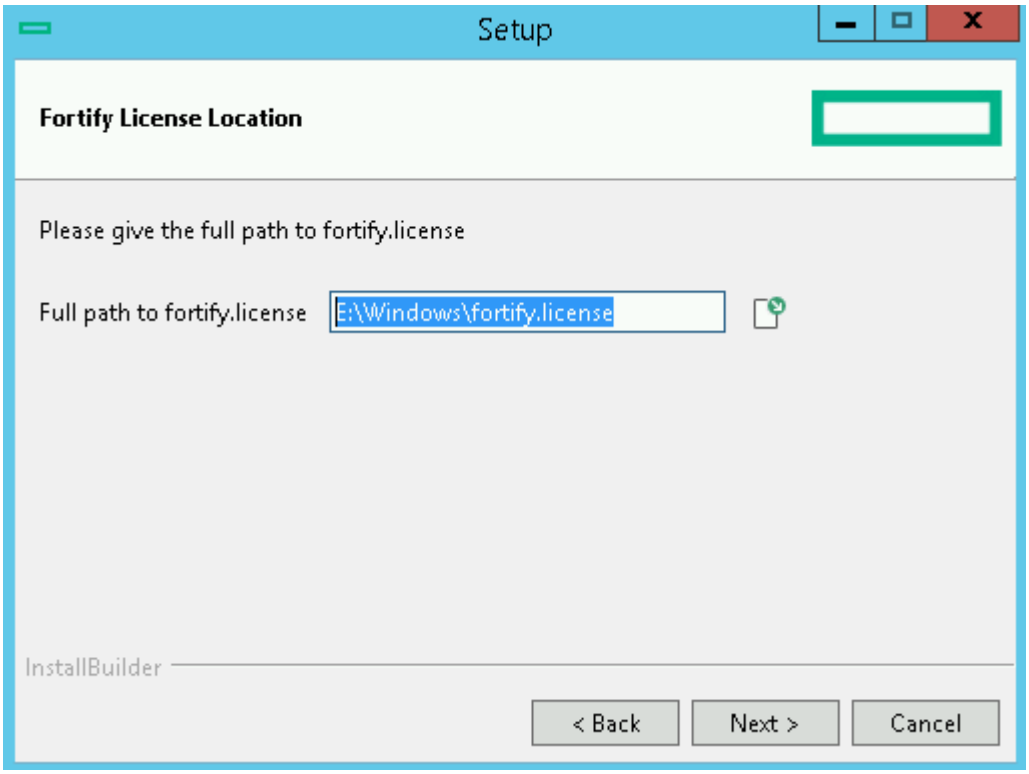

Figura 5. Archivo de licencia

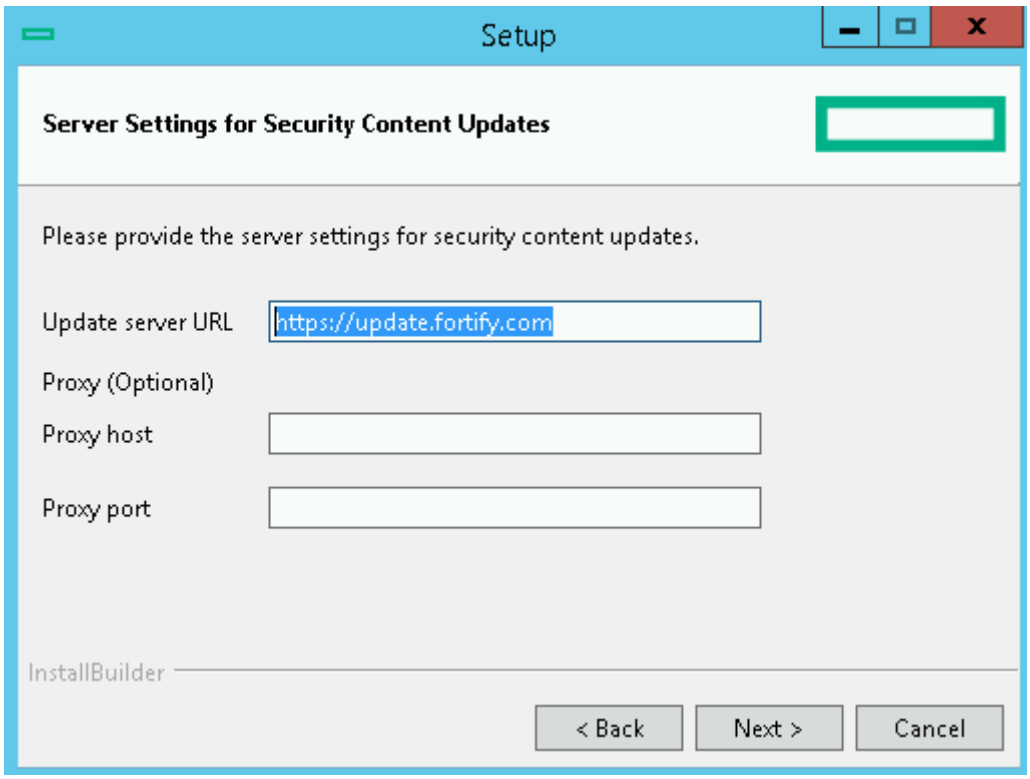

Figura 6. Servidor de actualizaciones

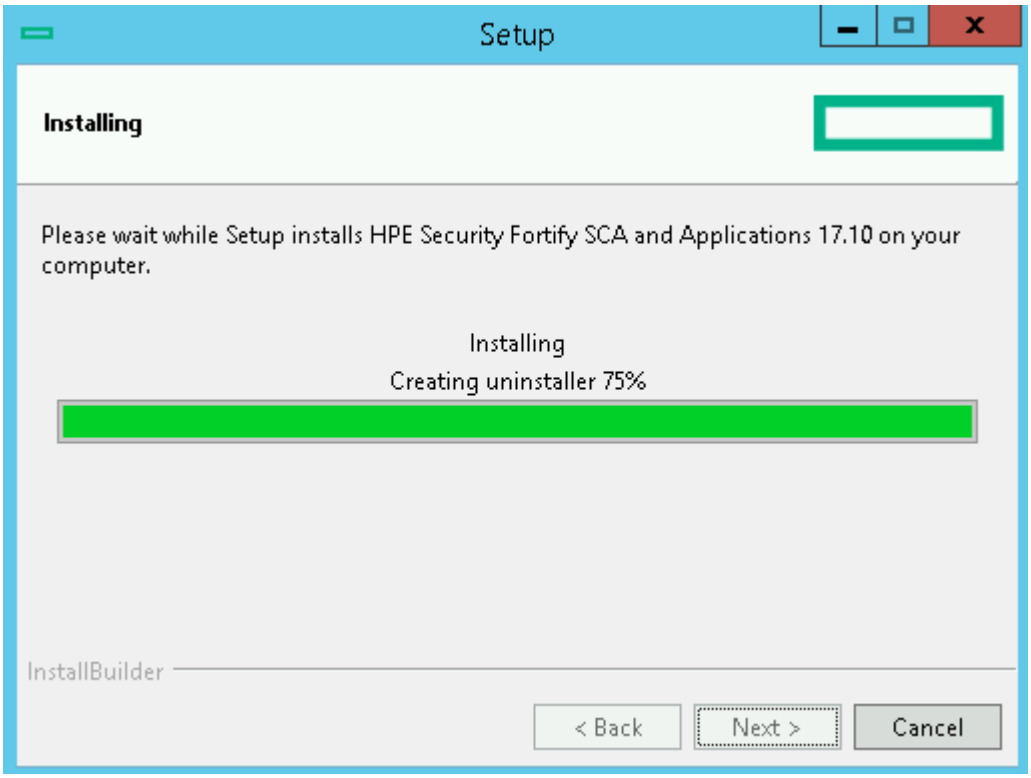

Figura 7. Servidor de actualizaciones

1.1 Instalación desde Marketplace

HPE Fortify se integra con el entorno de desarrollo de Eclipse y agrega la capacidad de escanear y analizar toda la base de códigos de un proyecto y aplicar cientos de reglas de seguridad de software que identifican las vulnerabilidades en código de Java. Los resultados se muestran dentro del IDE, junto con descripciones de cada uno de los problemas de seguridad y sugerencias para su eliminación.

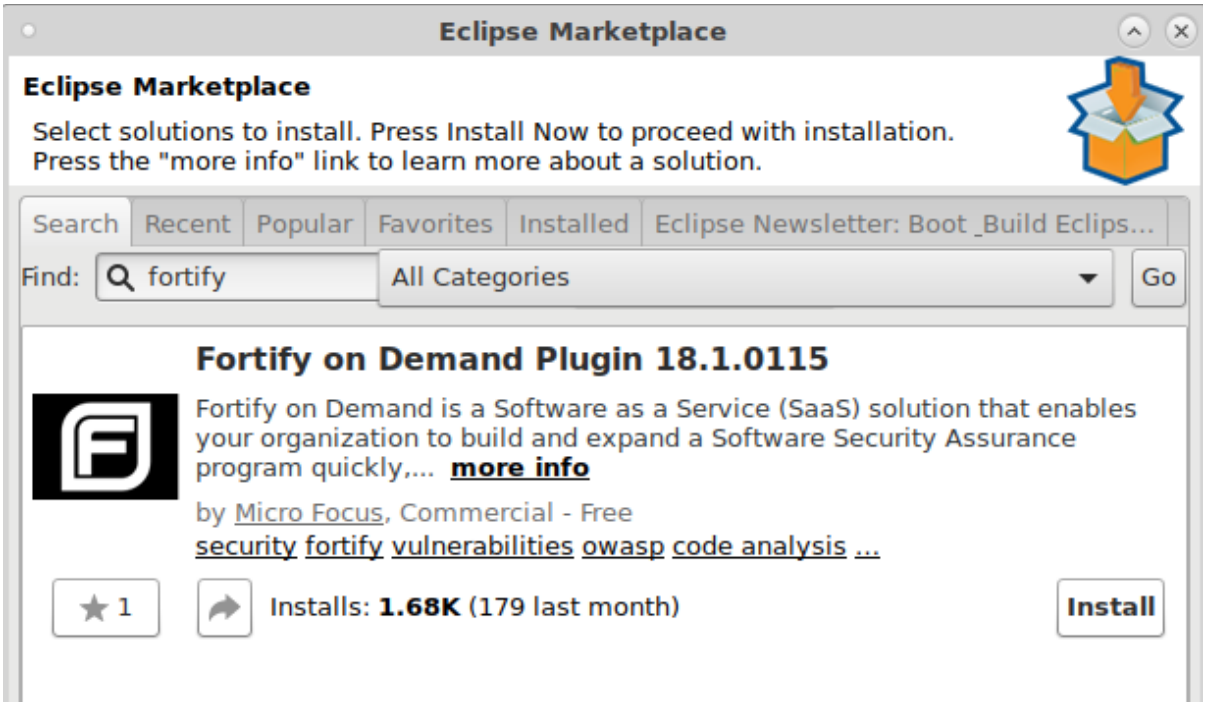

Figura 8. Eclipse Marketplace

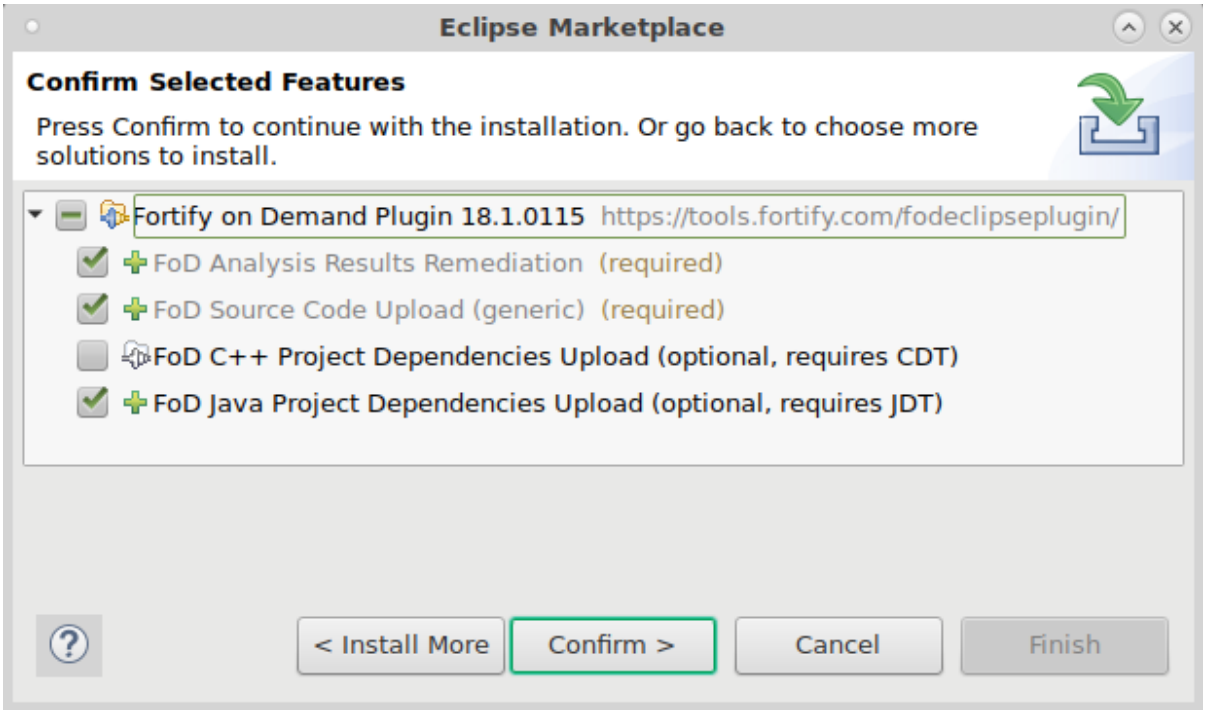

Figura 9. Componentes de Fortify

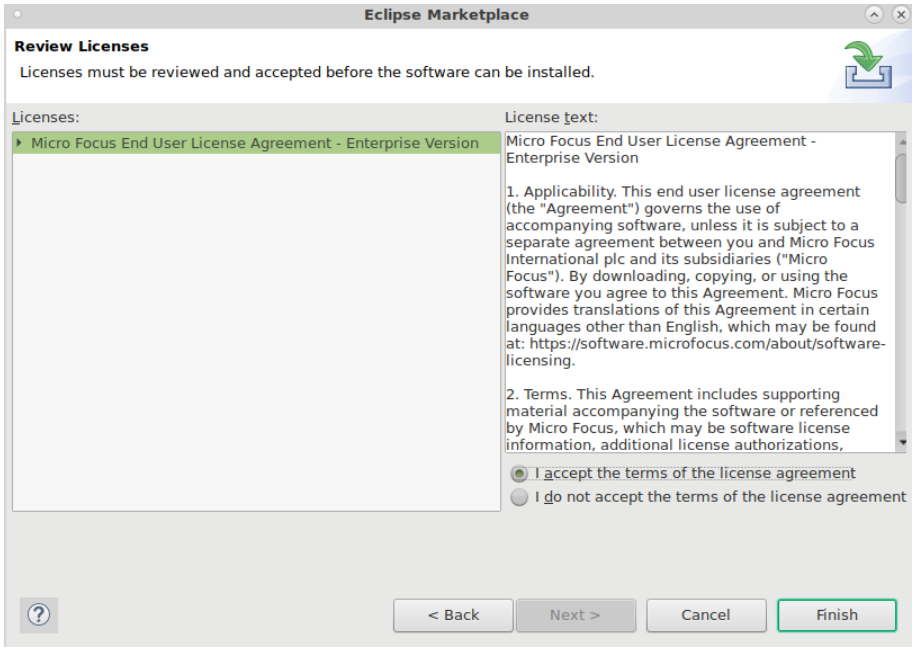

Figura 10. Términos de licencia

2. Análisis de un proyecto

2.1 Ejecución de la herramienta

Una vez instalado el plugin se ejecuta el análisis de la solución y/o proyecto.

Menú: FORTIFY / Analyze Solution

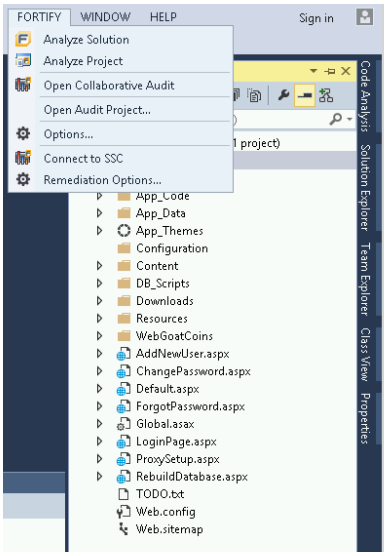

Figura 11. Ejecución del análisis

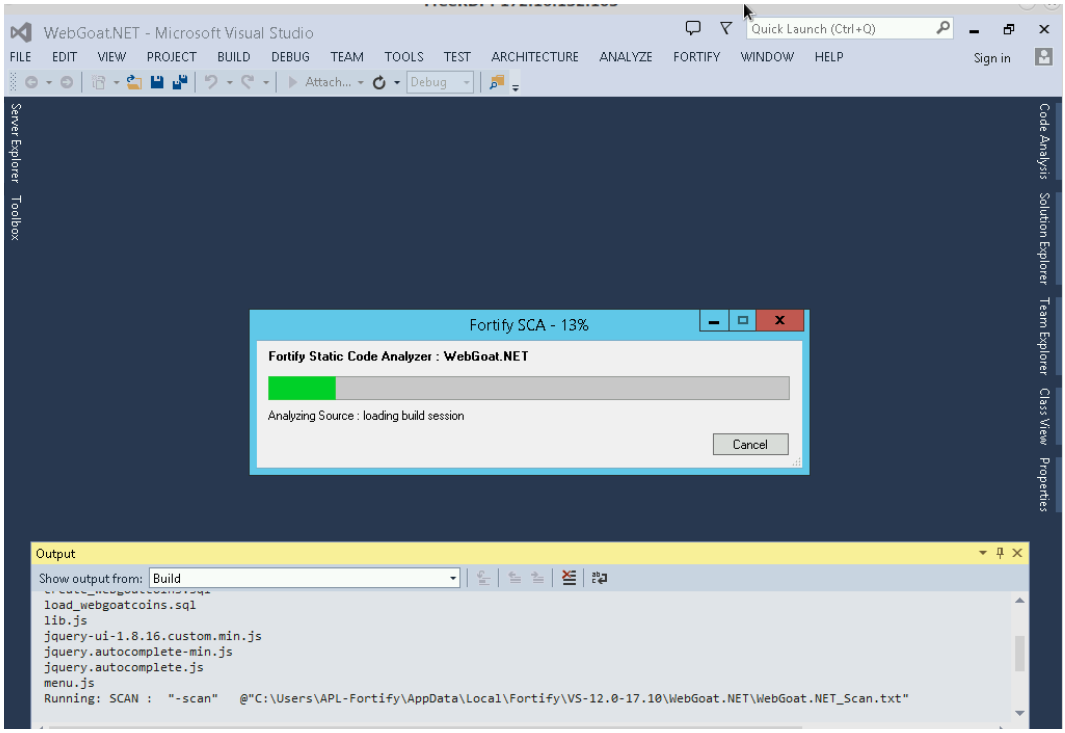

Figura 12. Proceso del análisis

Al finalizar el escaneo se sugiere la sincronización con el Software Security center

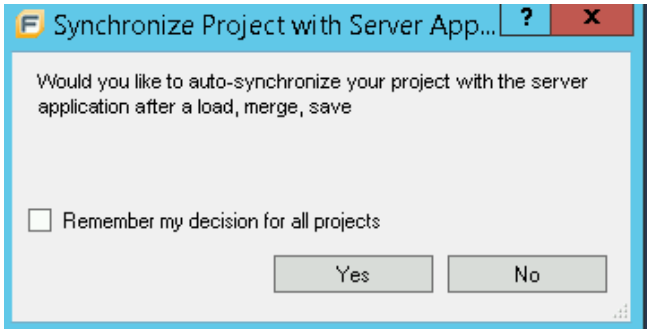

Figura 13. Sincronización del análisis

El resultado del escaneo es agrupado por el nivel de criticidad de los hallazgos: (Critical, High, Medium, Low)

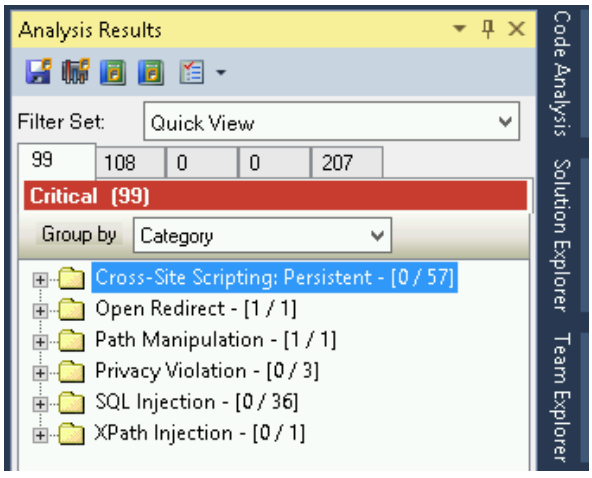

Figura 14. Hallazgos

2.2 Análisis del error: Path Manipulation

```
string filename = Request.QueryString["filename"];
if(filename != null)
{
    try
    {
        ResponseFile(Request, Response, filename, MapPath("~/Downloads/" + filename), 100);
    }
    catch (Exception ex)
    {
        Console.WriteLine(ex.Message);
        lblStatus.Text = "File not found: " + filename;
    }
}
```

Figura 15. Código vulnerable

Resumen de la vulnerabilidad

Un atacante podría controlar la ruta del archivo enviado por parámetro al método MapPath () en PathManipulation.aspx.cs línea 38, lo que les permite acceder o modificar archivos protegidos. Los errores de manipulación de ruta ocurren cuando se cumplen las dos condiciones siguientes:
1. Un atacante puede especificar una ruta utilizada en una operación en el sistema de archivos.
2. Al especificar el recurso, el atacante obtiene una capacidad que de otro modo no estaría permitida.
Por ejemplo, el programa puede dar al atacante la capacidad de sobrescribir el archivo especificado o ejecutarlo con una configuración controlada por el atacante.

En este caso, el atacante puede especificar el valor que ingresa al programa en get_QueryString() en PathManipulation.aspx.cs linea 33, y este valor se usa para acceder a un recurso del sistema de archivos en MapPath () en PathManipulation.aspx.cs en la línea 38.

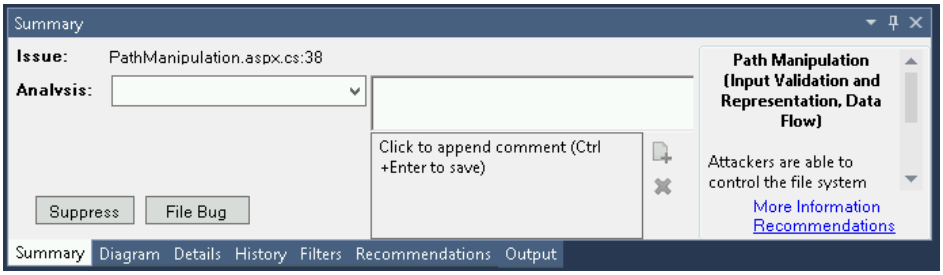

Figura 16. Resumen

Diagrama

Crea una representación gráfica del orden de ejecución de la vulnerabilidad sobre el código, la profundidad de la llamada y el tipo de expresión del problema seleccionado en el panel de problemas. La pestaña muestra información relevante para el tipo de regla. El eje vertical muestra el orden de ejecución.

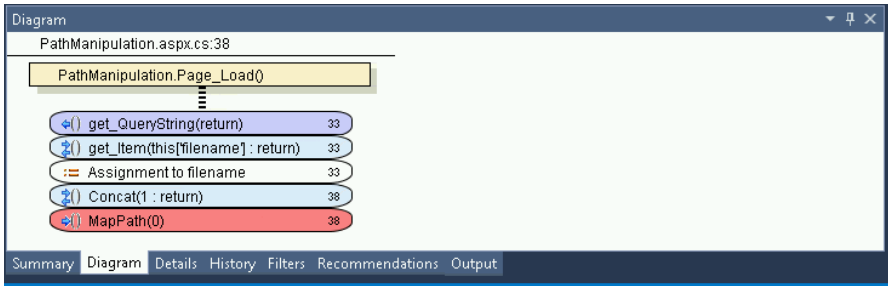

Figura 15. Diagrama

Detalle

Muestra la descripción y explicación del problema.

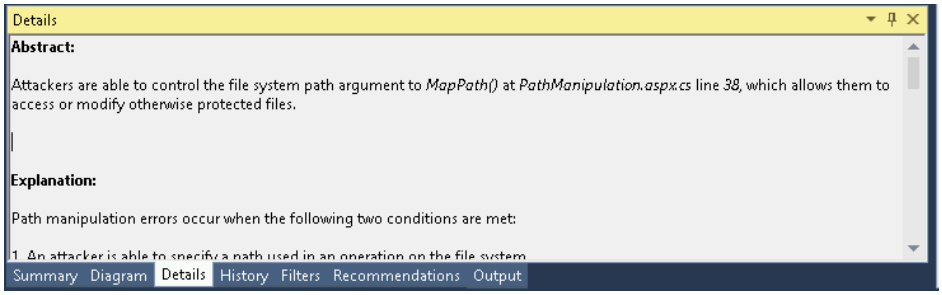

Figura 17. Detalle

Recomendaciones

Recomendaciones a implementar con el fin de mitigar la vulnerabilidad.

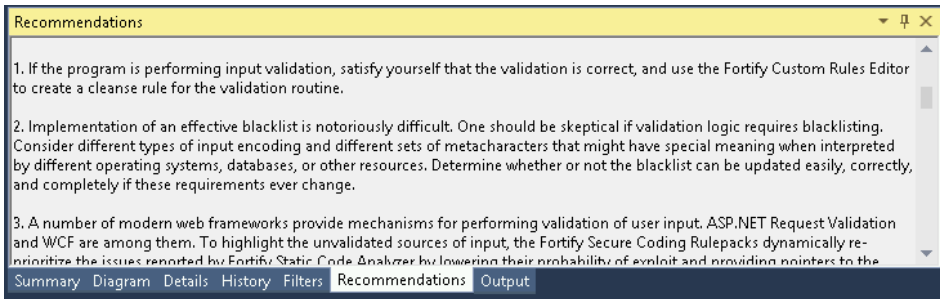

Figura 18. Recomendaciones

Este resultado del análisis permite ser exportado para su posterior análisis en Audit Workbench o SSC

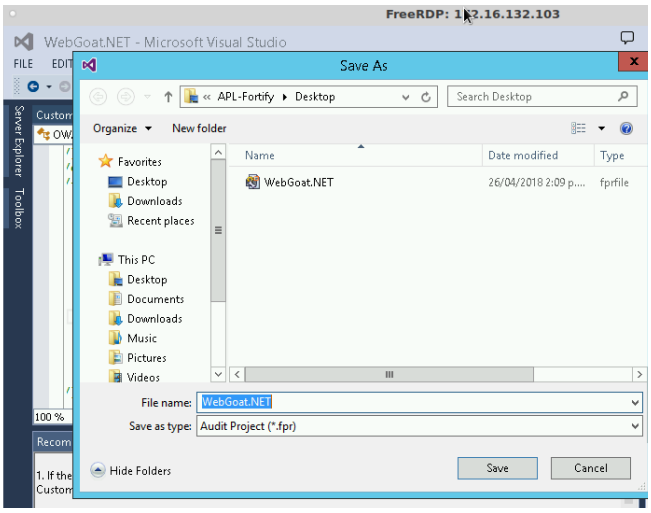

Figura 19. Exportar informe

2. HPE Security Fortify Audit Workbench

Audit Workbench es un complemento HPE Security Fortify Static Code Analyzer (Fortify Static Code Analyzer) con una interfaz gráfica de usuario que puede usar para organizar, investigar y priorizar los resultados de análisis.
Desde Audit Workbench, puede ver y auditar archivos FPR desde HPE Security Fortify Software Security Center, HPE Security Fortify Runtime Application Protection y HPE Security Fortify con los complementos de escaneo para IDE.

Figura 20. Software Audit Workbench

Audit Workbench utiliza una base de conocimiento de reglas para aplicar estándares de codificación segura aplicables a la base de código para el análisis estático. El contenido de HPE Security Fortify Software Security (contenido de seguridad) consiste en Rule Packs de codificación segura y metadatos externos los cuales incluyen asignaciones de las categorías de HPE Security a categorías alternativas (como CWE, OWASP Top 10 y PCI DSS).

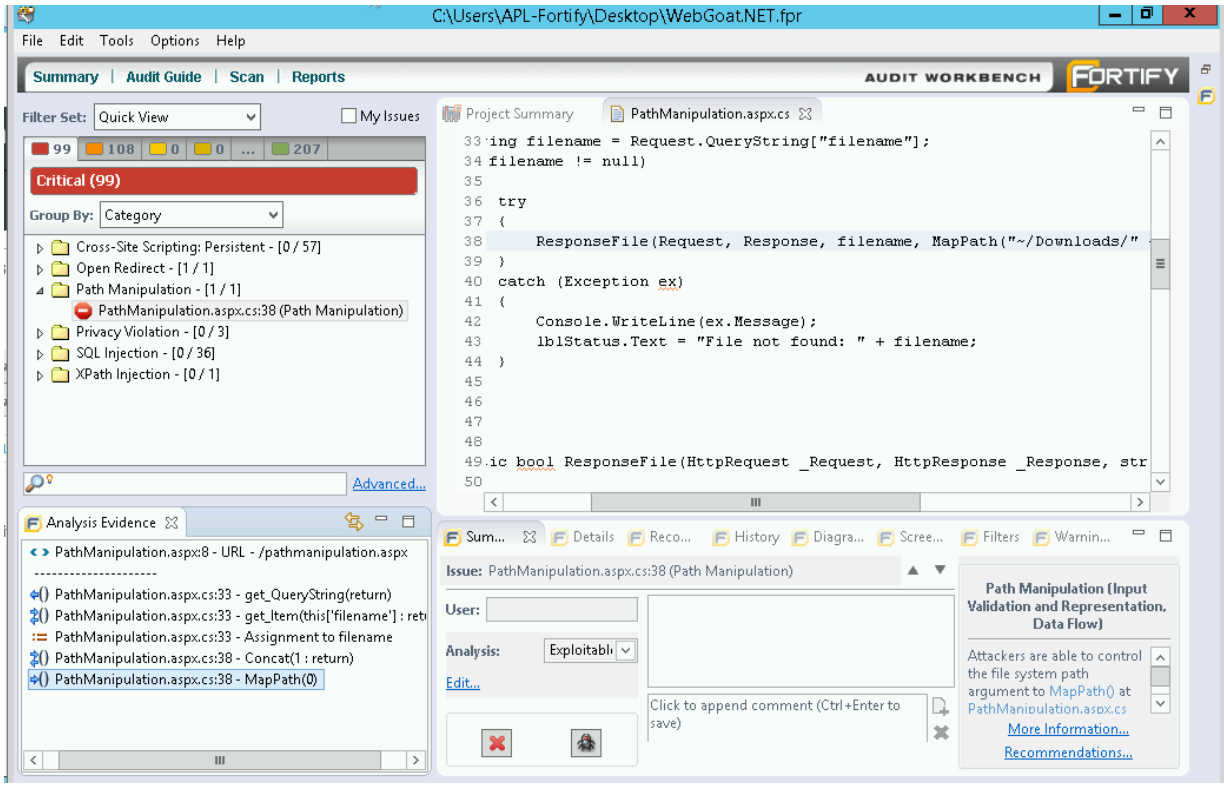

Figura 21. Resultado de un escaneo