# Instituto Tecnológico Colonia CTC

# Seguridad Informática: Todo Ofertas

Entregado como requisito para la obtención del título Analista Programador.

Alumnos: Agustín Bartel - Octavio Etchevarrén - Alex Besozzi

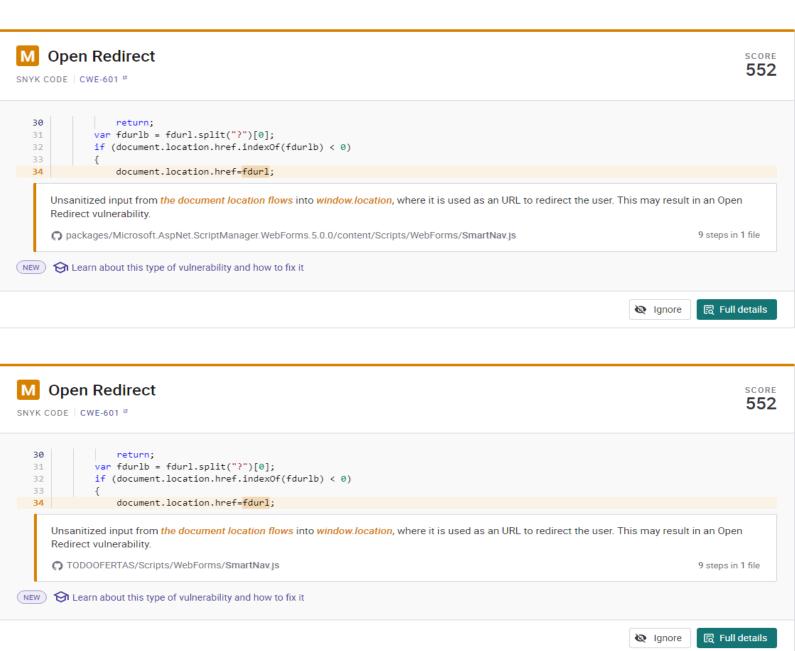
Tutor: Peter Fernández

Año: 2022

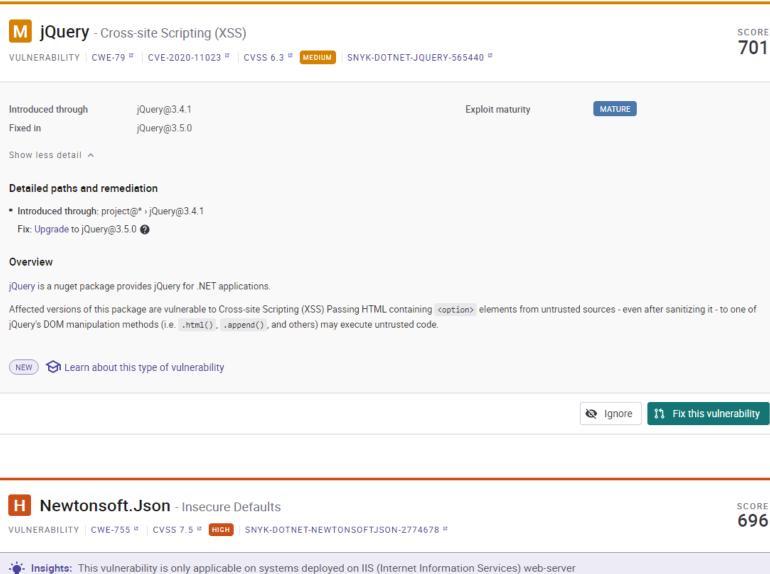
# Snyk:



#### Análisis de Código:



#### Vulnerabilidades:



inegrie. The varietability is only approached on systems aspisyed on the (internet information confidence) free serve

Introduced through Newtonsoft.Json@12.0.2 Exploit maturity

Fixed in Newtonsoft.Json@13.0.1

Show less detail ^

#### Detailed paths and remediation

Introduced through: project@\* > Newtonsoft.Json@12.0.2
 Fix: Upgrade to Newtonsoft.Json@13.0.1

#### Overview

Affected versions of this package are vulnerable to Insecure Defaults due to improper handling of StackOverFlow exception (SOE) whenever nested expressions are being processed. Exploiting this vulnerability results in Denial Of Service (DoS), and it is exploitable when an attacker sends 5 requests that cause SOE in time frame of 5 minutes.

 $\textbf{Note:} \ This\ vulnerability\ is\ only\ applicable\ to\ systems\ deployed\ on\ IIS\ (Internet\ Information\ Services)\ web-server and the property of the$ 



PROOF OF CONCEPT

# Posible solución:

- Actualizar jQuery y JSON a la última versión disponible.

## **Burp Suite**

#### SqlMap

```
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
 *] starting @ 18:17:11 /2022-08-17/
[18:17:12] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data' so you want to try URI injections in the target URL itself? [Y/n/q] y
No you want to try URI injections in the target URL itself? [Y/n/q] y

[18:17:20] [INFO] testing connection to the target URL

[18:17:20] [INFO] testing connection to the target URL

[18:17:20] [INFO] testing connection to the target URL on the target URL

[18:17:20] [MARNING] WAF/IPS identified as 'ASP.NET RequestValidationMode (Microsoft)'

Incompare that you want to continue with further target testing? [Y/n] y

[18:17:21] [MARNING] please consider usage of tamper scripts (option '--tamper')

[18:17:21] [INFO] testing if the target URL content is stable

[18:17:22] [MARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of just results, refer to user's manual paragraph 'Page comparison'

now do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c

[18:17:27] [INFO] testing if URL parameter '#1*' is does not appear to be dynamic

[18:17:27] [MARNING] URL parameter '#1*' does not appear to be dynamic

[18:17:27] [MARNING] URL parameter '#1*' does not appear to be dynamic

[18:17:27] [MARNING] URL parameter '#1*' does not appear to be dynamic

[18:17:27] [MARNING] URL parameter '#1*' does not appear to be dynamic
```

[\*] ending @ 18:17:34 /2022-08-17/

:\BurpSuiteCommunity>\_

#### Sql Injection

# **Login Administrador**

Cédula					
12345678					
Contraseña					
•••••	***************************************	•••••	•••••		
Ingresar					
Datos incorrecto	\$				

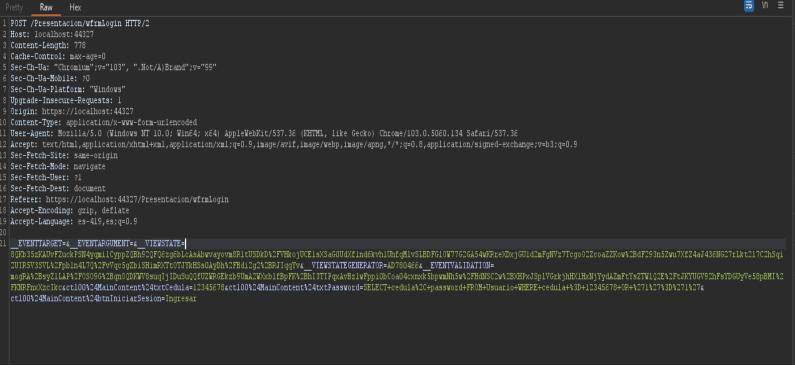
Datos incorrectos

#### **Datos ingresados:**

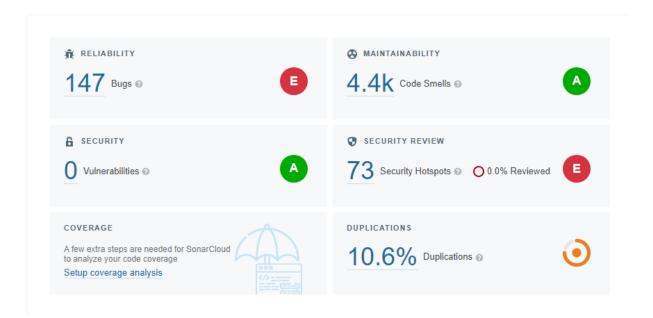
**Cédula:** 12345678

Contraseña: SELECT cedula, password FROM Usuario WHERE cedula

= 12345678 OR '1'='1'



## Sonar Cloud:



 Comprobando el detalle de los distintos bugs y advertencias de seguridad, encontramos que todos están relacionados con la librería jQuery y la biblioteca Bootstrap que se instalan por defecto al crear un proyecto ASP.NET.

#### Posible solución:

- Actualizar jQuery y Bootstrap a la última versión disponible.

## Aclaraciones:

 Somos conscientes que no debería haber un formulario que sea fácilmente accesible para registrar administradores. Lo incluímos para que el usuario que pruebe el programa pueda acceder a las distintas funciones que este tipo de usuarios tiene. Por ejemplo: Ingresar, eliminar o modificar promociones.