

Práctica 1 - Seguridad Informática

Pedro Tamargo

Juan José Tambo

24 de septiembre de 2020

Índice

1. Tarea 1: Experimentar con las funciones en Bash	1
2. Tarea 2: Configuración de programas CGI	1
3. Tarea 3: pasar datos a Bash a través de las variables de entorno	1
4. Tarea 4: Lanzamiento del Ataque Shellshock	1
5. Tarea 5: Obtención de un Shell inverso a través de un ataque Shellshock	1

1. Tarea 1: Experimentar con las funciones en Bash

Para esta sección se ha creado una función `foo` y se ha ejecutado el siguiente código:

Cambiar esto

```
foo=`() echo "Prueba vulnerabilidad"; ; echo "Soy vulnerable";`  
echo $foo  
export foo  
bash_shellshock
```

Tras la ejecución de este código podemos observar como el intérprete *BASH_SHELLSHOCK* es vulnerable (Figura 1).

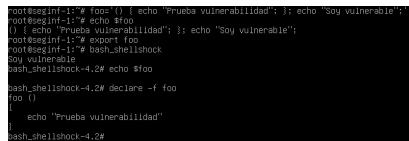


Figura 1: Intérprete afectado por el ataque *shellshock*

2. Tarea 2: Configuración de programas CGI

Hola

3. Tarea 3: pasar datos a Bash a través de las variables de entorno

Hola

4. Tarea 4: Lanzamiento del Ataque Shellshock

Hola

5. Tarea 5: Obtención de un Shell inverso a través de un ataque Shellshock

Hola