Un servidor web afectado por esta vulnerabilidad que tenga un formulario de contacto, que permita a los usuarios enviar emails:



El valor “$$\_post[“mail”] es usado en las cabeceras de correo electrónico, pudiendo aprovechar un intruso y enviar un valor malicioso en al campo del email, como:

*“atacante@example.com\r\nCC: victima@example.com”*, indicando el salto de línea en el texto y la cabecera del correo:

*From: atacante@example.com*

*CC: victima@example.com*

Por todo ello, recomienda actualizar a la versión superior para no perder el control total del contenido de los encabezados del correo electrónico.

Los scripts de los CGI pueden estar escritos en lenguajes de programación diferentes, imaginemos que lo tenemos en Python, tomando como parámetro la URL y lo acepte en la web sin validar o escapar esa entrada de usuario (imagen\_1) De esta forma el valor del parámetro “name” se inserta directamente en la web, pudiendo un atacante modificarlo, y enviar una URL maliciosa (imagen\_2)

La solución es restablecer el acceso a la aplicación vulnerable y actualizar o parchear por el soporte técnico, no existiendo exploits públicos disponibles.



