

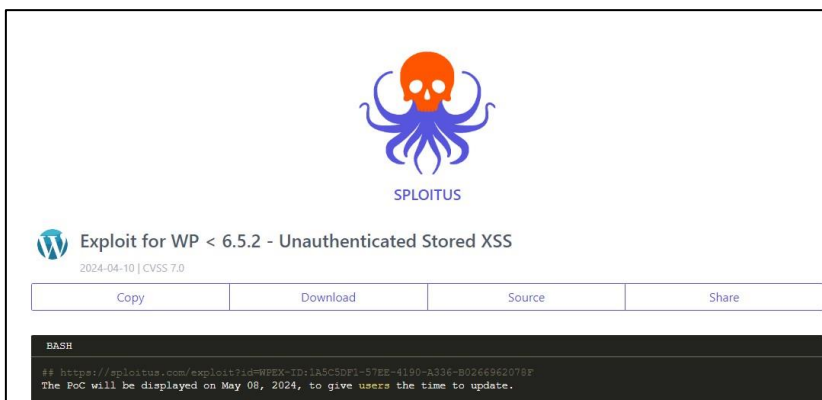
VULNERABILIDAD XSS WORDPRESS < 6.5

Los desarrolladores de WordPress lanzaron recientemente la versión “6.5.2”, en el cual solucionan una vulnerabilidad de “Cross-site Scripting” afectando a las versiones 6.x y anteriores.

La vulnerabilidad se veía afectada a través del nombre del autor, en el bloque del Avatar, ya que no escapaba correctamente los atributos, dejando lugar a la ejecución de un “Cross-Site Scripting” almacenado. Sin embargo, con una instalación de WordPress por defecto en los bloques de comentarios, esta vulnerabilidad también podría ser ejecutada sin autenticación.

Se recomienda actualizar a la última versión de WordPress “v6.5.2”, o en caso contrario, cualquier versión posterior a 6.x.

Se recomienda tomar las debidas precauciones y actualizaciones antes del día 8/5/2024, ya que se hará publica la prueba de concepto.



The screenshot shows the SploitUs interface for an exploit titled "Exploit for WP < 6.5.2 - Unauthenticated Stored XSS". It includes a skull and octopus logo, a table with "Copy", "Download", "Source", and "Share" buttons, and a terminal window with the following text:

```
BASH
## https://sploit.us.com/exploit?id=WPX-ID:1A5CSDPI-5TEE-4190-A336-B0266962078P
The PoC will be displayed on May 08, 2024, to give users the time to update.
```



Referencia:

<https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/>