Exploit #1:

The first exploit involves XSS during the “Large File Upload Error” interaction. A media file that’s 20MB or larger titled “Dinosaurs secret life<img src=x onerror=alert(1)>.png” must be added to wordpress. By adding this image, you can generate an error in wordpress that’s susceptible to javascript code; the resulting file will result in an alert box with the number 1.

Exploit #2:

The second exploit involves posting a comment that is 64KB or larger. By writing the following javascript in a comment: “<a title='x onmouseover=alert(unescape(/hello%20world/.source)) style=position:absolute;left:0;top:0;width:5000px;height:5000px '></a> and putting 64KB worth of characters in between the 5000px and the single quote, the comment is truncated by MySQL and the code passes through undetected. The result from this code is an alert box that says “Hello World”.

Exploit #3;

The third exploit involves writing a line of javascript into either a post or a page that says “<a href="[caption code=">]</a><a title=" onmouseover=alert('test') ">link</a>”. Due to wordpress’ shortcode processing, the code is read as “<a href="</a><a title=" onmouseover=alert('test') ">link</a”, which results in an alert box that says “test” when the post made is hovered over with the mouse.