Brandon Roldan Follow
Oct 18, 2021 · 3 min read · Listen

Support Board 3.3.4 Arbitrary File Deletion to Remote Code Execution

Hi. In this writeup, i will show you a bug that i found. Allowing an Authenticated user to delete any file in the system in the Support Board 3.3.4 and also will show you a possible exploit scenario with it. Even though this is an authenticated bug, there is no csrf protection on it so we can chain it with csrf.

While reversing the functions, i found a function called delete-file

```
case 'delete-file':
    die(sb_json_response(sb_file_delete($_POST['path'])));
```

It accepts the post parameter path as an argument.

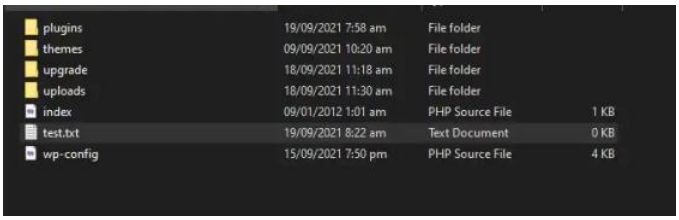
```
function sb_file_delete($path) {
    if (strpos($path, 'http') !== false) {
        $path = SB_PATH . '\uploads\\' . basename($path);
    }
    return unlink($path);
}
```

You can see that if the path parameter has http on it, it will delete the file in the SB_PATH\uploads . This implementation is pretty safe since we can only delete files in the /uploads directory which doesnt have that much impact

However, if you look at the code again.

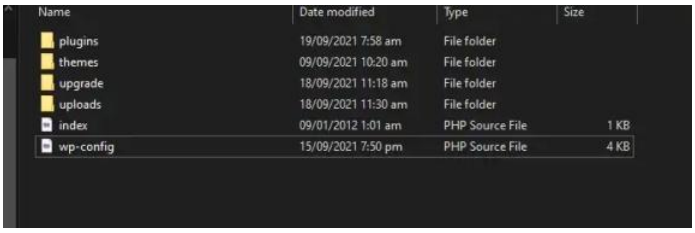
```
function sb_file_delete($path) {
    if (strpos($path, 'http') !== false) {
        $path = SB_PATH . '\uploads\\' . basename($path);
    }
    return unlink($path);
}
```

It will only delete files in the /uploads directory if the path contains the string http. If not, it will directly use our input in $path into the unlink. So if we supplied a file without the http, it will get deleted. For reproduction purpose, i made a file called test.txt in C:\xampp\htdocs\wordpress\wp-content

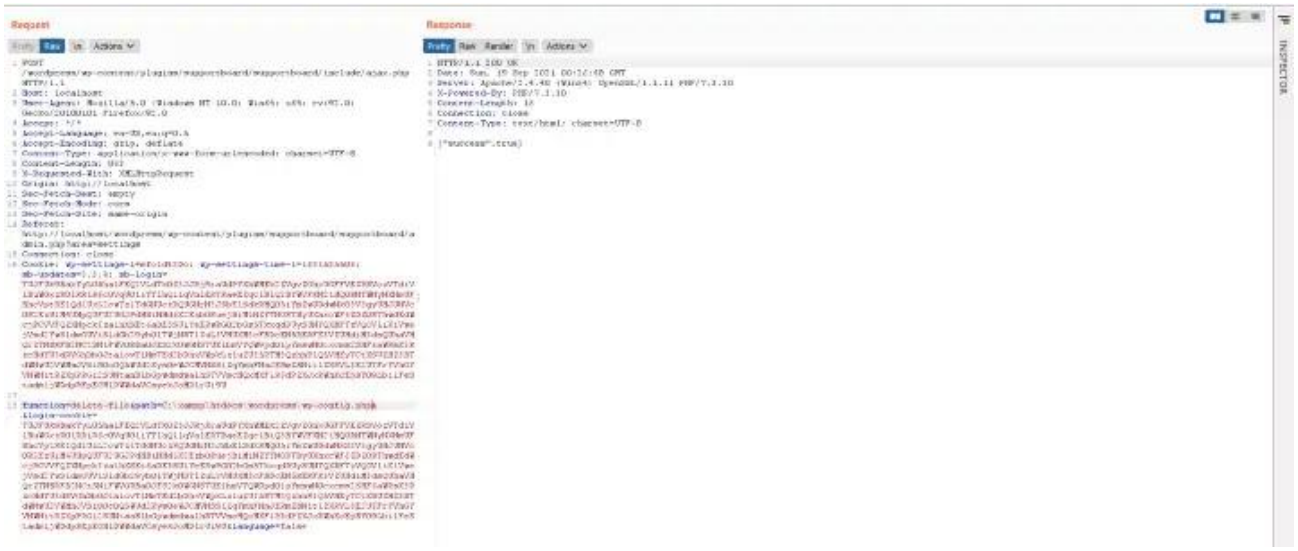


Now back to burpsuite, if we supply the location of this file, this file should be deleted.

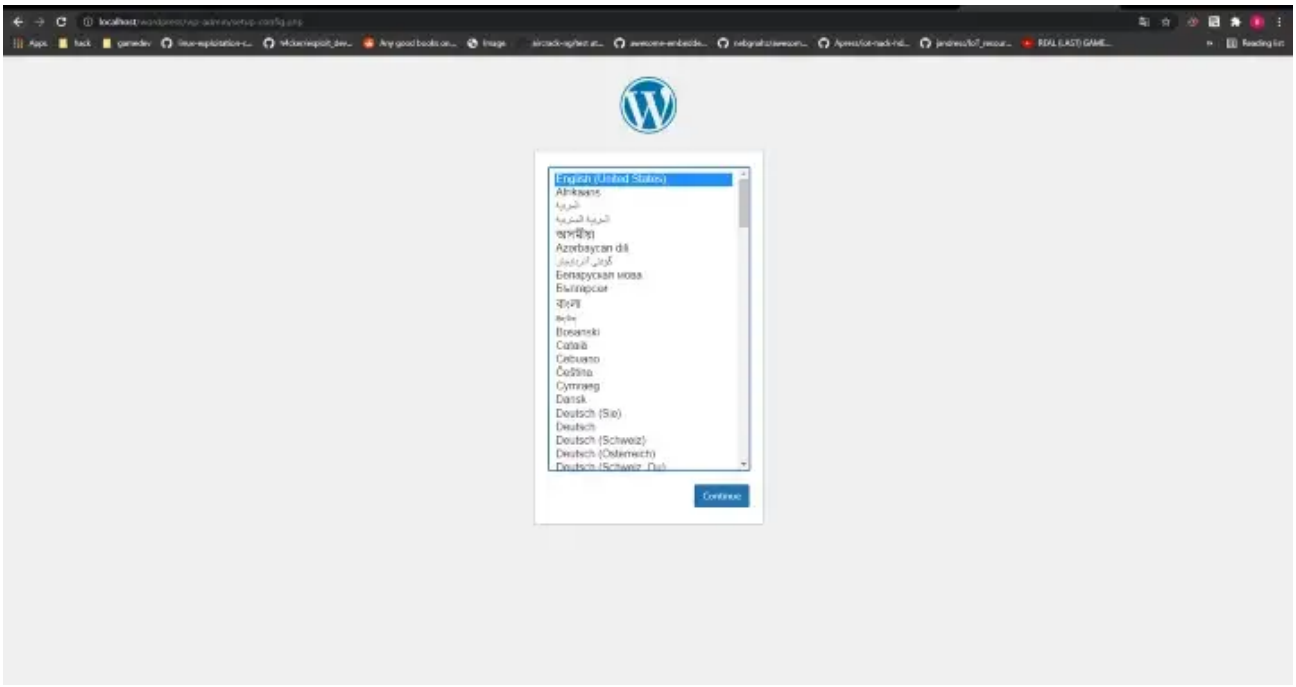
We can see that it succeed and our file is now deleted



So we got a bug now. Now like i said earlier, i will show you a possible exploit scenario with this. In a wordpress installation, there is a file called wp-config.php . It contains the config of a wordpress installation. When we delete this file, we can then reinstall the whole wordpress application. So lets try it out. Normally, this wp-config.php is commonly found in the root directory of wordpress. So i tried deleting it and it succeed



Now if we go to the site. We can reinstall the wordpress installation. In there, we can easily achieve rce



This is the end of my writeup, thanks for reading.

Update:

It is fixed now in the version 3.3.6.

```
function sb_file_delete($path) {
    $path = SB_PATH . '/uploads/' . basename($path);
    return unlink($path);
}
```

Thanks for reading

Word Press Hacking Infosec Bug Bounty Exploit