All this text wasn’t written by me (Tiago a.k.a TigaxMT).

All of it was transcribed by me from HackerOne video lessons.

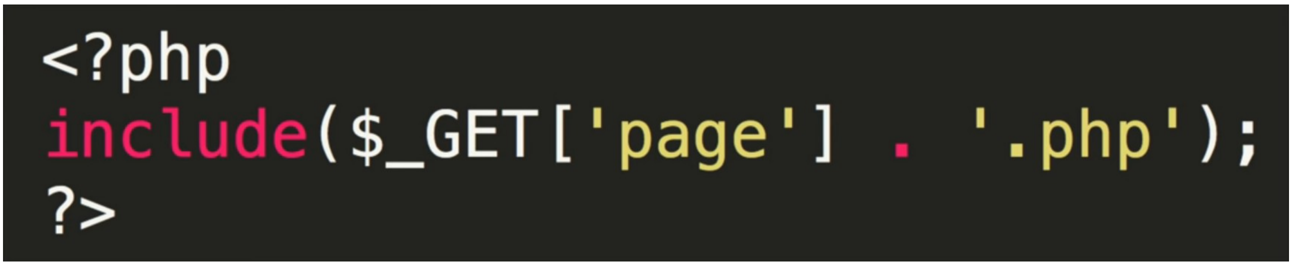
All credits and thanks go to them.

Null Termination

The null character (\x00, %00 etc) is used to terminate C strings. That is, you a have a series of characters ending with a null in memory. We don’t often test web apps written in Cm so why is that relevant?
Well, most dynamic language implementations are written in C, including Python, PHP, Ruby, and most others. This legacy comes in handy.

SCENARIO

Looking at a simple inclusion script, we have code like this:



```php
<?php
include($_GET['page'] . '.php');
?>
```

Simple inclusion of page from GET + ‘.php’

But what if we want to read, say, etc/passwd ? If we throw a null byte at the end of the page variable, it might only read up to that point when opening the file, allowing is to read any file we want.
So we try ?page=/etc/passwd%00 and we will see a passwd file in the page.

IMPLICATIONS

This bug could allow you to truncate strings at will, based on where in the application you’re attempting to reach.
When reading files, PHP uses native C functions (as most runtimes do), and due to a lack of proper string handling, this bug pops up all over the place.

TESTING

I strongly recommend you throw null bytes into anything related to file handling, particularly when dealing with PHP.
Most browser will strip %00 from requests, or truncate them there. Burp will allow you to embed literal nulls as well as URLencoded (%00) nulls.
You’ll find very interesting bugs if you do this regularly.