NULL Byte

درود

امروز میخوام در مورد null byte یه صحبتی بکنم!

اولین چیزی که باید بگم اینه که این کد رو نباید با 0(صفر) اشتباه گرفت!

نال بایت ، در واقع بایت به زبان Hex است و به این صورت نشون داده میشه : ("%00")

در اصل اون به این صورت نوشته میشه ۰/ ، در زبان PHP نال بایت به عنوان یک کاراکتر نال شناخته میشه! این به ابن معنی است که String ما بعد از نال بایت بایسته !

زبان PHP در C نوشته شده و این ویژگی نال بایت خودش رو هم از C به ارث برده .

مشکل به همینجا ختم نمیشه! Unix هم در C نوشته شده و همین خاصیت پایان دادن به رشته ها(Strings) رو داره.خب بگذارید یک مثال براتون بزنم :

```
<?
$file = $HTTP_GET_VARS['file'];
$file = $file.'.txt';
fopen($file, 'r');
?>
```

میبینید این کد قصد داره با استفاده از متغیر file یک فایل دیگر که فقط پسوند اون میتونه txt باشه رو باز کنه(در خط ۳ با استفاده از تابع File open).

خب اگه ما اسم فایلمون رو به این صورت بهش بدیم :

```
phppage.php%00
```

به نظر شما چی میشه؟ این فایل در اسکریپت به این صورت قرار میگیره :

```
phppage.php%00.txt
```

در اینجا نال بایت ما باعث خاطمه یافتن یا به اصتلاح بیگانه terminate شدن رشته میشه و کد ما به صورت phppage.php تعبیر میشه و صفحه phppage.php باز میشه!

پس ما با استفاده از نال بایت در php میتونیم هر فایلی با هر پسوندی رو باز کنیم!!!!

نویسنده : SNAKE