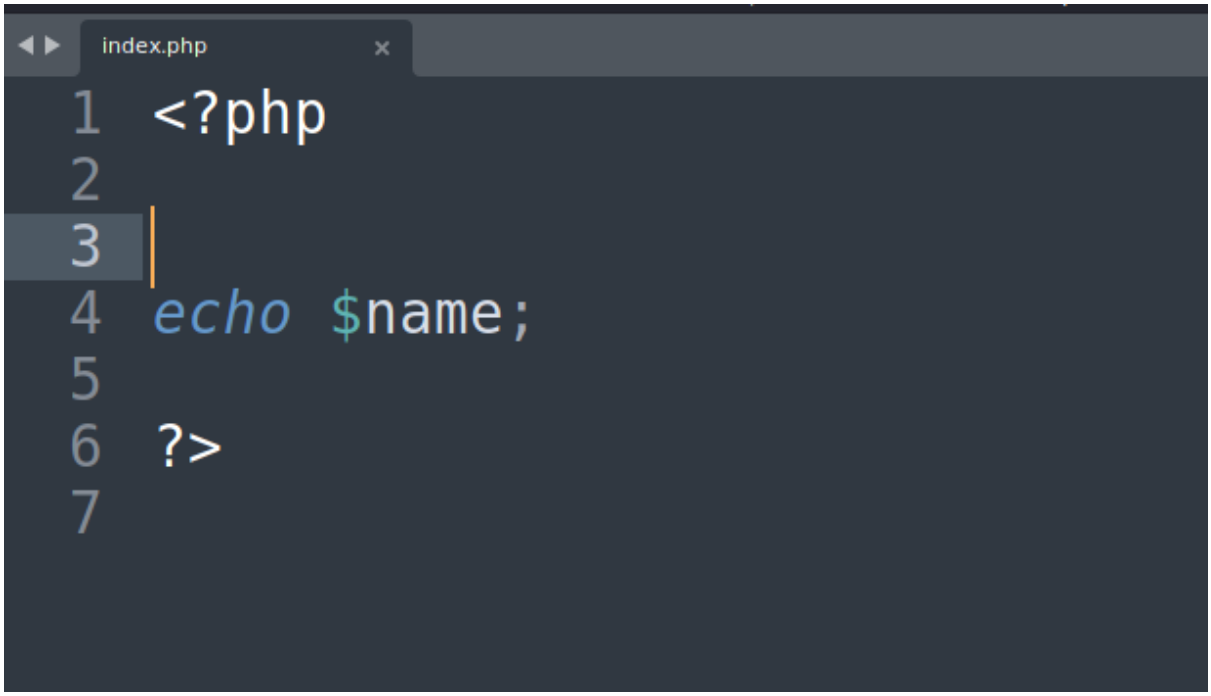
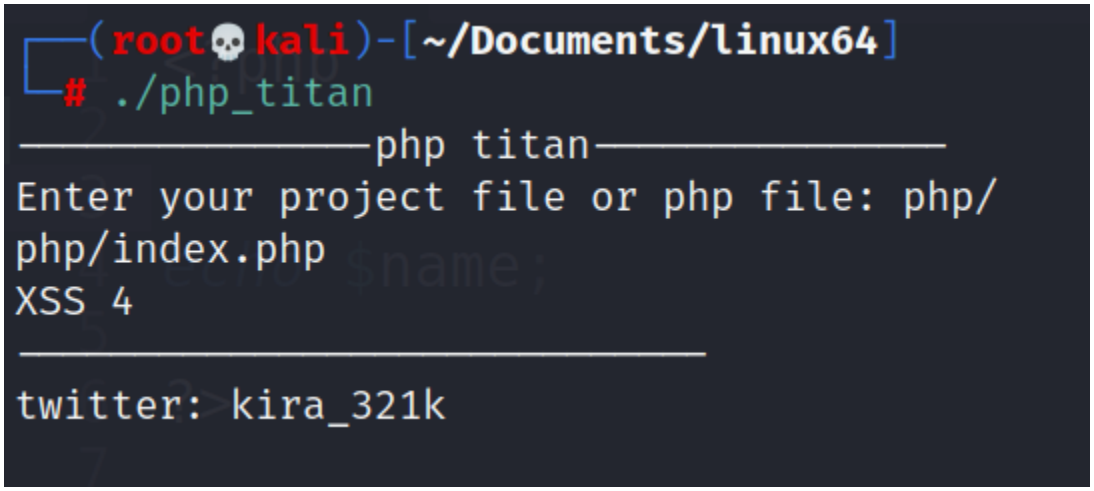
php titan

بسم الله الرحمن الرحيم اليوم بشرح بشكل بسيط عن php titan اداة سويتها و وظيفتها تفحص اكواد php بنجرب اختبارات عليها بعدين سيناريو واقعي على كود موقع حقيقي
اول شي ابي اسوي اختبارات عشان نشوف ذكاء الاداة نفسها





في الصورة الكود على اليسار و مخرجات الاداة على اليمين ف يقول ان فيه XSS في سطر 4

```php
<?php

$name = "hello";

echo $name;

?>

```

```
┌──(root💀kali)-[~/Documents/linux64]
└─# ./php_titan
─────────────────php titan─────────────────
Enter your project file or php file: php/
php/index.php
─────────────────────────────────
twitter: kira_321k

┌──(root💀kali)-[~/Documents/linux64]
└─#
```

الكود هذا مافيه ثغرة ف الاداة عندها القدرة تميز اذا كان داخل المتغير نص او براميتر معين

```php
<?php

$name = htmlspecialchars($_GET['name']);

echo $name;

?>
```

```
┌──(root💀kali)-[~/Documents/linux64]
└─# ./php_titan
──────────────php titan──────────────
Enter your project file or php file: php/
php/index.php
──────────────────────────────────────
twitter: kira_321k

┌──(root💀kali)-[~/Documents/linux64]
└─#
```

و هذا كود ثاني غير مصاب و الاداة ماقالت شي يعني الشغل للحين صح بدون اي اخطاء

```php
<?php

$name = htmlspecialchars($_GET['name']);

echo $name . $_GET["username"];

?>
```

```
┌──(root💀kali)-[~/Documents/linux64]
└─# ./php_titan
─────────────────php titan─────────────────
Enter your project file or php file: php/
php/index.php
XSS 5
────────────────────────────────────
twitter: kira_321k

┌──(root💀kali)-[~/Documents/linux64]
└─#
```

في الصورة هذي المتغير name ماهو مصاب بس فيه جنبه براميتر username مصاب و قدرت الاداة تقول لنا ان فيه ثغرة

```php
<?php

$name = htmlspecialchars($_GET['name']);

$username = $_GET["username"];

echo $name . "Welcome" .$username;

?>
```

```
┌──(root💀kali)-[~/Documents/linux64]
└─# ./php_titan
──────────────php titan──────────────
Enter your project file or php file: php/
php/index.php
XSS 7
─────────────────────────────────
twitter: kira_321k

┌──(root💀kali)-[~/Documents/linux64]
└─#
```

نفس الفكرة قاعد احاول اخلي الاداة تغلط بس الى الان كل شي يمشي بشكل صحيح

```php
<?php

$xss = $_GET['name'];

echo '<a href="http://example.com/page?input="' . htmlspecialchars($xss) . '">Link</a>';

?>
```

```
┌──(root💀kali)-[~/Documents/linux64]
└─# ./php_titan
──────────────php titan──────────────
Enter your project file or php file: php/
php/index.php
─────────────────────────────────
twitter: kira_321k

┌──(root💀kali)-[~/Documents/linux64]
└─#
```

هنا لا اختلف الموضوع الكود فيه ثغرة XSS بس الاداة ماقالت فيه شي طيب وش الفايدة؟ ان الاداة ممكن تغلط شي طبيعي ف لا تعتمد عليها بشكل كبير ممكن تقول فيه ثغره و يطلع مافيه شي و العكس صحيح بس فايدتها ممكن تختصر عليك وقت في البحث عن الثغرات

سيناريو واقعي

بالسيناريو هذا بستخدم سورس لموقع و فيه صفحات كثير ف صعب اني افحصه صفحه صفحه لأن اكواده كثيرة ف ودي اختصر الوقت و استخدم الاداه اذا مالقيت شي ممكن اسويها بشكل يدوي

```
D:\xampp\htdocs\project\win64>php_titan.exe
---------------php titan---------------
Enter your project file or php file: D:\xampp\htdocs\project
D:\xampp\htdocs\project[redacted]
SQLi line:  9
XSS 11
D:\xampp\htdocs\project[redacted]
SQLi line:  46
SQLi line:  61
SQLi line:  100
XSS 110
XSS 169
XSS 184
XSS 193
XSS 210
SQLi line:  357
SQLi line:  371
D:\xampp\htdocs\project[redacted]
SQLi line:  33
SQLi line:  34
D:\xampp\htdocs\proj[redacted]
```

هنا الاداة تقول فيه ثغرات معينه ف بروح اشيك عليها الحين و تعطيني رقم السطر بركز على ثغرات SQLi و بترك XSS طبعا تكتشف الاداة ثغرات اكثر بس الموقع حمايته جيدة

```php
$comment = mysqli_real_escape_string($connect,$_POST['comment']);
$userId = mysqli_real_escape_string($connect,$_POST['userId']);
$ci = mysqli_real_escape_string($connect,$_POST['ci']);
$video = mysqli_real_escape_string($connect,$_POST['video']);
$connect->query("insert into comments(`uid`,`ci`,`comment`,`video`) values('$userId','$ci','$comment','$video')");
```

هنا الاداة تقول ان فيه SQLi اذا كنت فاهم في php بتعرف انه مافيه SQLi هنا و السبب انه مستخدم داله mysqli real escape string و هذي الاداة تحميك من SQLi مو بشكل كامل الا اذا حطيت بين المتغير ' مثل الكود اللي فوق امن ف بروح لسطر الثاني او ملف ثاني الاداة تقول فيه ثغرة

```php
$f = mysqli_real_escape_string($c, htmlspecialchars($_POST['c']));
$co = $c->query("select * from coupon where name='$f'");
if ($coupon->num_rows) {
```

نفس الشي اللي فوق mysqli real escape string و بين ' نكمل فحص

```php
$_SESSION['b'] = null;
$arrayC = [];
$cc = $connect->query("select id from c where id=$b");
```

هنا لو نلاحظ مافيه فلترة بس مسوي real escape string بس مو ظاهره بالصورة بس انه نسى يضيف ' و عندنا تحكم بمتغير b ف هنا فيه ثغرة

```php
}
$s = $connect->query("select * from s where ui='$ui' and ci=$pn ");
if($s->num_rows){
```

و هنا حط ' في وحده و الثانيه بدون ف فيه ثغرة

ملخص

شفنا الاداة انها ممكن تخطي مو بس بهذي الاداة كل الادوات بالعالم فيها نسبة خطأ و سوينا سينارو واقعي و اكتشفنا ثغرتين SQLi طبعا لو نكمل يمكن نلاقي اكثر و ماشفنا ثغرات XSS ف ممكن اطلع عليها