**php titan**

بسم الله الرحمن الرحيم اليوم بشرح بشكل بسيط عن [php titan](https://github.com/kira2040k/php_titan) اداة سويتها و وظيفتها تفحص اكواد php بنجرب اختبارات عليها بعدين سيناريو واقعي على كود موقع حقيقي

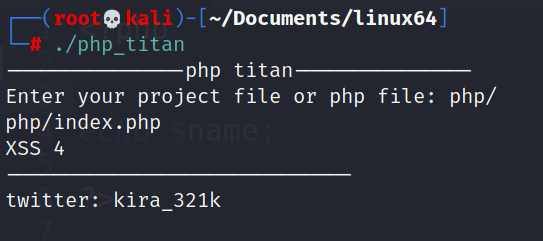
اول شي ابي اسوي اختبارات عشان نشوف ذكاء الاداة نفسها

​

Graphical user interface, text, application

Description automatically generated

​



​

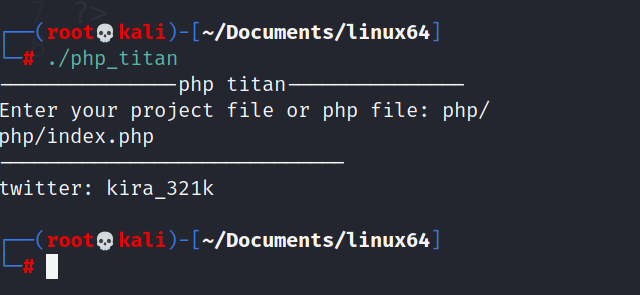
في الصورة الكود على اليسار و مخرجات الاداة على اليمين ف يقول ان فيه XSS في سطر 4

​

Text

Description automatically generated

​



​

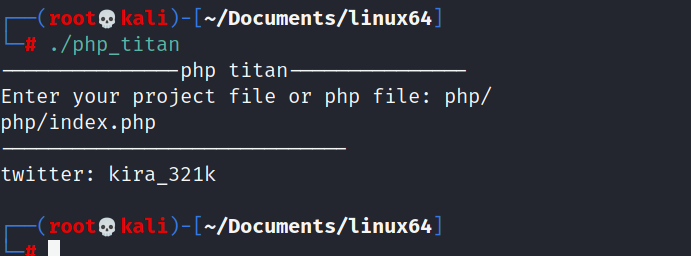
الكود هذا مافيه ثغرة ف الاداة عندها القدرة تميز اذا كان داخل المتغير نص او براميتر معين

​

Text

Description automatically generated

​



​

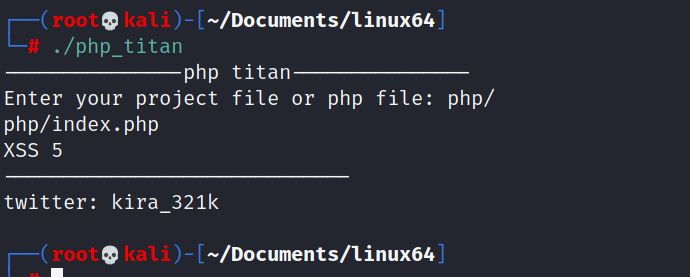
و هذا كود ثاني غير مصاب و الاداة ماقالت شي يعني الشغل للحين صح بدون اي اخطاء

​

Text

Description automatically generated

​



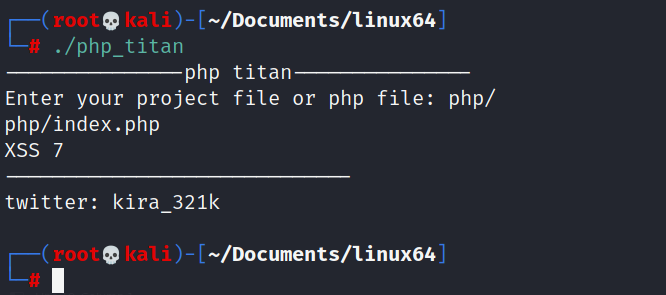
​

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

​



​

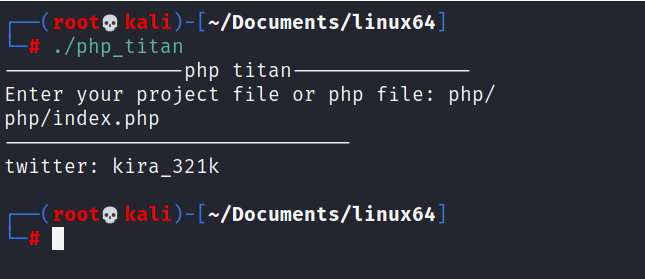


​

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

Text

Description automatically generated

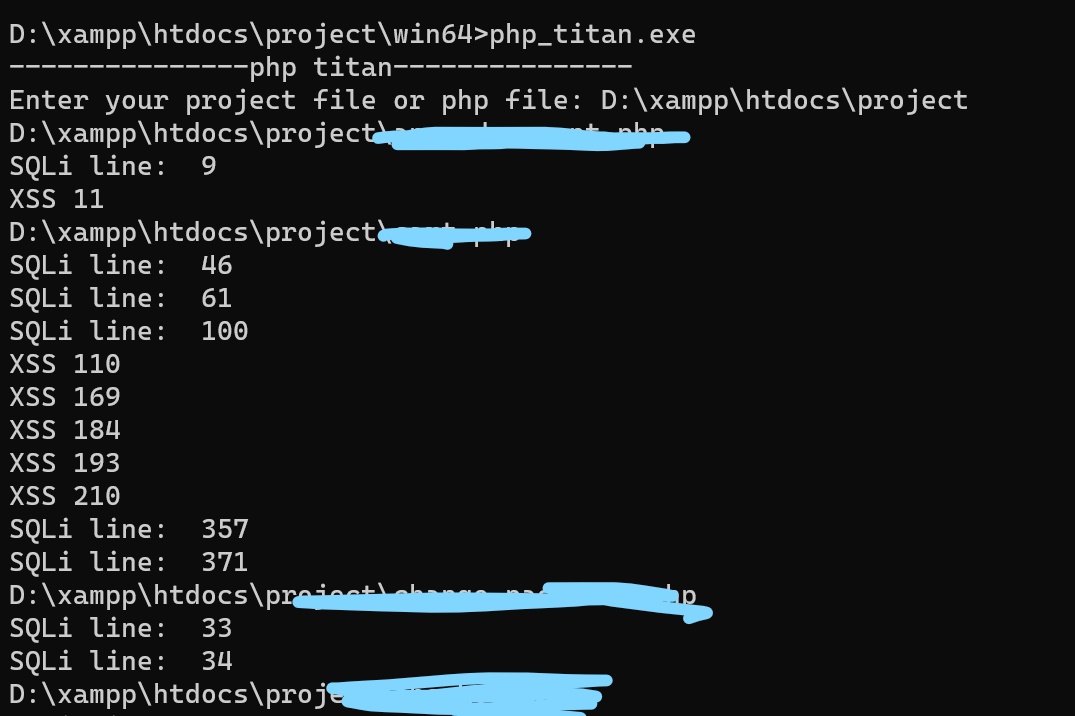


هنا لا اختلف الموضوع الكود فيه ثغرة XSS بس الاداة ماقالت فيه شي طيب وش الفايدة؟ ان الاداة ممكن تغلط شي طبيعي ف لا تعتمد عليها بشكل كبير ممكن تقول فيه ثغره و يطلع مافيه شي و العكس صحيح بس فايدتها ممكن تختصر عليك وقت في البحث عن الثغرات

**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

​

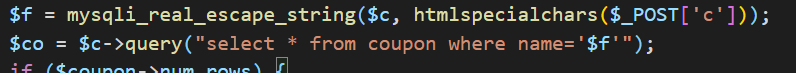


هنا الاداة تقول فيه ثغرات معينه ف بروح اشيك عليها الحين و تعطيني رقم السطر بركز على ثغرات SQLi و بترك XSS طبعا تكتشف الاداة ثغرات اكثر بس الموقع حمايته جيدة

Text

Description automatically generated

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

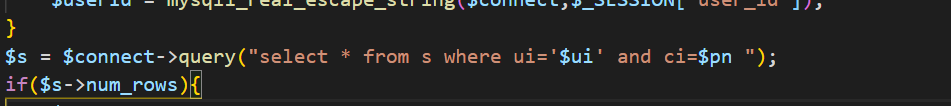


نفس الشي اللي فوق mysqli real escape string و بين ' نكمل فحص

Text

Description automatically generated with medium confidence

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



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