<< به نام خداوند بخشنده مهربان >>

الإمامُ الصّادقُ عليه‌السلام :

إنَّ لِكُلِّ شَيءٍ زَكاةً ، وزَكاةُ العِلمِ أن يُعَلِّمَهُ أهلَهُ

امام صادق عليه‌السلام :

هرچیزی‌زکاتی دارد و زکات دانش، آموختن آن است به اهلش

نام مقاله : آموزش نرم افزار dirbuster در بک ترک

نویسنده : ایلیا زمانی

ایمیل : Norton_sym@yahoo.com

صفحه شخصی فیسبوک : https://fb.com/iliya.norton1

آشنایی با کلمه buster :

buster در لغت به دو معنا به کار برده می شود ==> شگفت انگیز و شکننده یا خوردکننده که در این مقاله بیشتر مفهوم شکننده یا خورد کننده مد نظر است و به صورت (باستر) تلفظ می شود

Dirbuster چیست :

که در اصل directory buster می باشد و به صورت (دایرکتوری باستر di'rektərē bəstər_) تلفظ می شود

این نرم افزار بر اساس زبان کامل برنامه نویسی جاوا طراحی شده است در واقع کاراصلی این نرم افزار brute force کردن وشناسایی اسامی دایرکتوری ها و فایل ها در وب سرورها می باشد وهمه در خواست های http از جمله 404، 403، 200 ، 500 بروت می کند این نرم افزار هیچ اکسپلویتی انجام نمیدهد در ضمن در حملات black-box از این نرم افزار استفاده می شود هکر ها معمولا دنبال وب سرور هایی هستن که ضعف هایی در خود دارند تا بتوانند اسیب وارد کنند و مدیر وب سرور برای جلوگیری از وارد شدن آسیب ها معمولا اقدام به پنهان کردن فایل ها یا دایرکتوری ها می کنند که

دلیل استفاده از این نرم افزار پیدا کردن فایل های و دایرکتوری های مخفی است

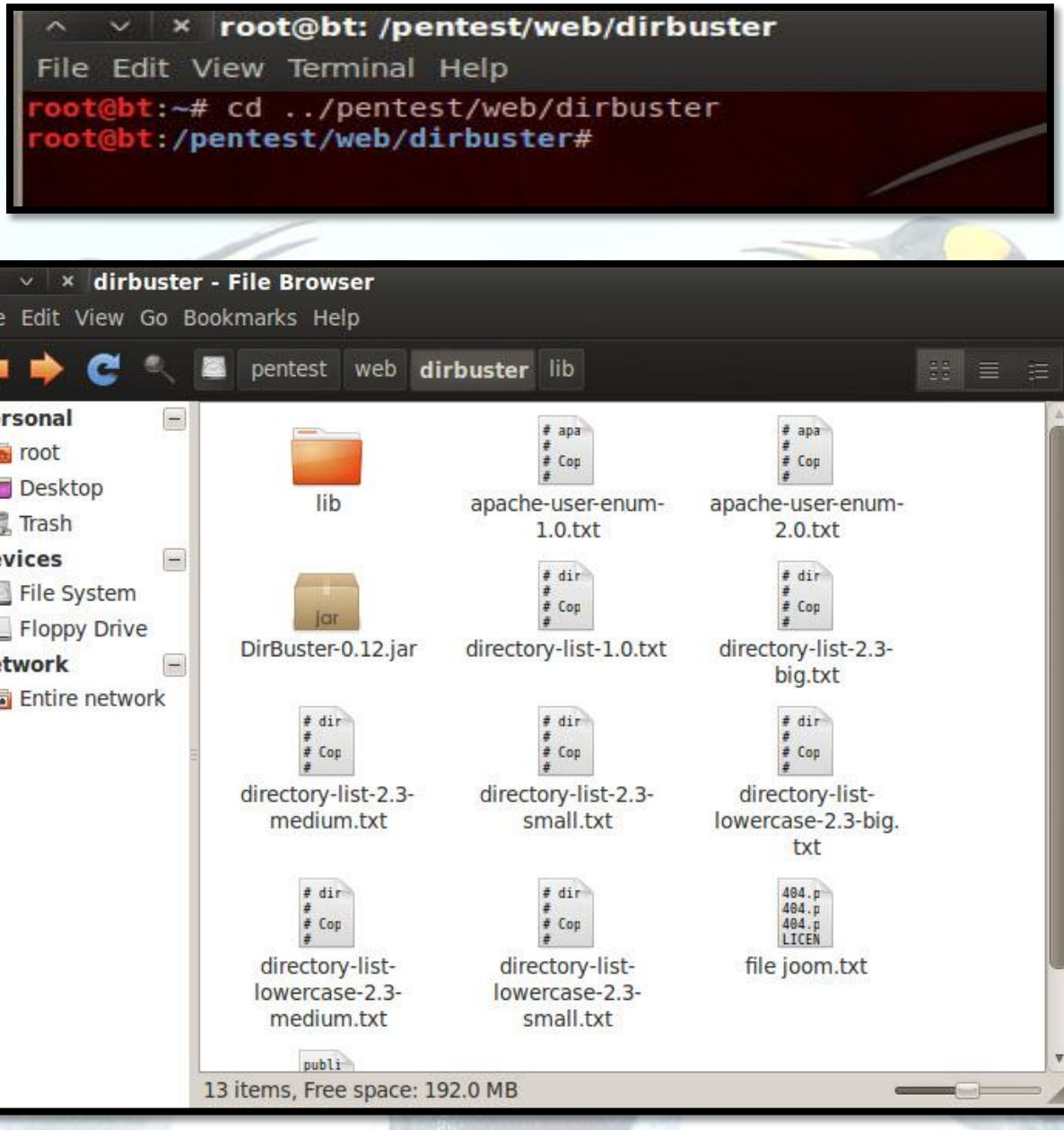
brute force : که به معنی حمله بی رحم می باشد و به صورت (بروت فورس broot fôrs) تلفظ می شود ، وظیفه دارد تا الگو های رمز شده را رمز نگاری کند که کلیه حالات ممکن را در یک زمان قابل قبول انجام می دهدتا بتواند رمز را شناسایی کند حملات بروت فورس برای شکستن encryption وکلید های رمزنگاری شده است که در موراد پیشرفته و کریپتوگرافی های سطح بالاDES-AESاز dictionary attackاستفاده می شود در این حملات از دیکشنری های قوی همراه با همه حروف ها عدد ها و کاراکتر ها استفاده می شود تا الگو رمز نگاری شود

همه توضیحات داده شد حالا بریم برای کار با نرم افزار.....

برای اجرای دایر باستر در بک ترک اول وارد محیط ترمینال می شویم و با دستور

Cd ../pentest/web/dirbuster

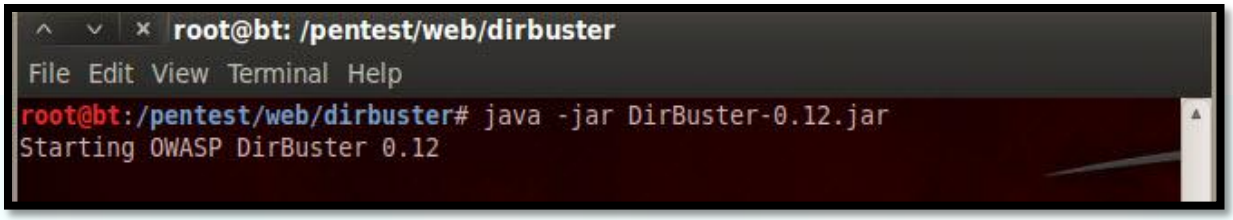
به مسیر دیر باستر می رویم



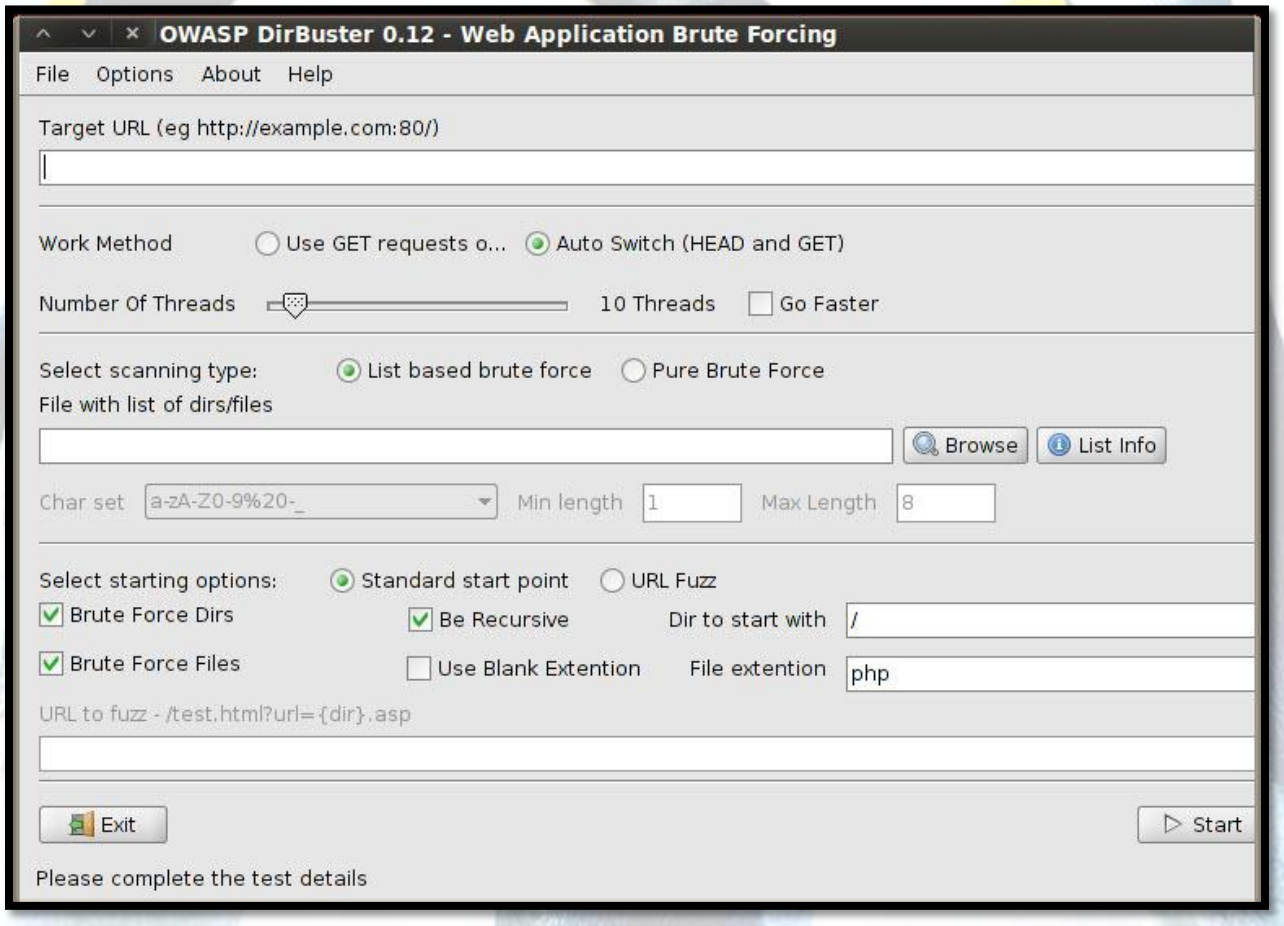
وحالا با دستور

Java -jar DirBuster-0.12.jar

نرم افزار دایر باستر را اجرا میکنیم



وبا محیط گرافیکی زیر رو به رو می شویم



این محیط از چهار قسمت تشکیل شده است

قسمت اول دادن تارگت به برنامه

http://site.com

http://www.easy-family-boating-recipes.com

قسمت دوم انتخاب متود کار برنامه

1) use Get request
2) Auto Switch (Get and Head)
3) Number Of threads

1) استفاده ازدر خواست تابع Get

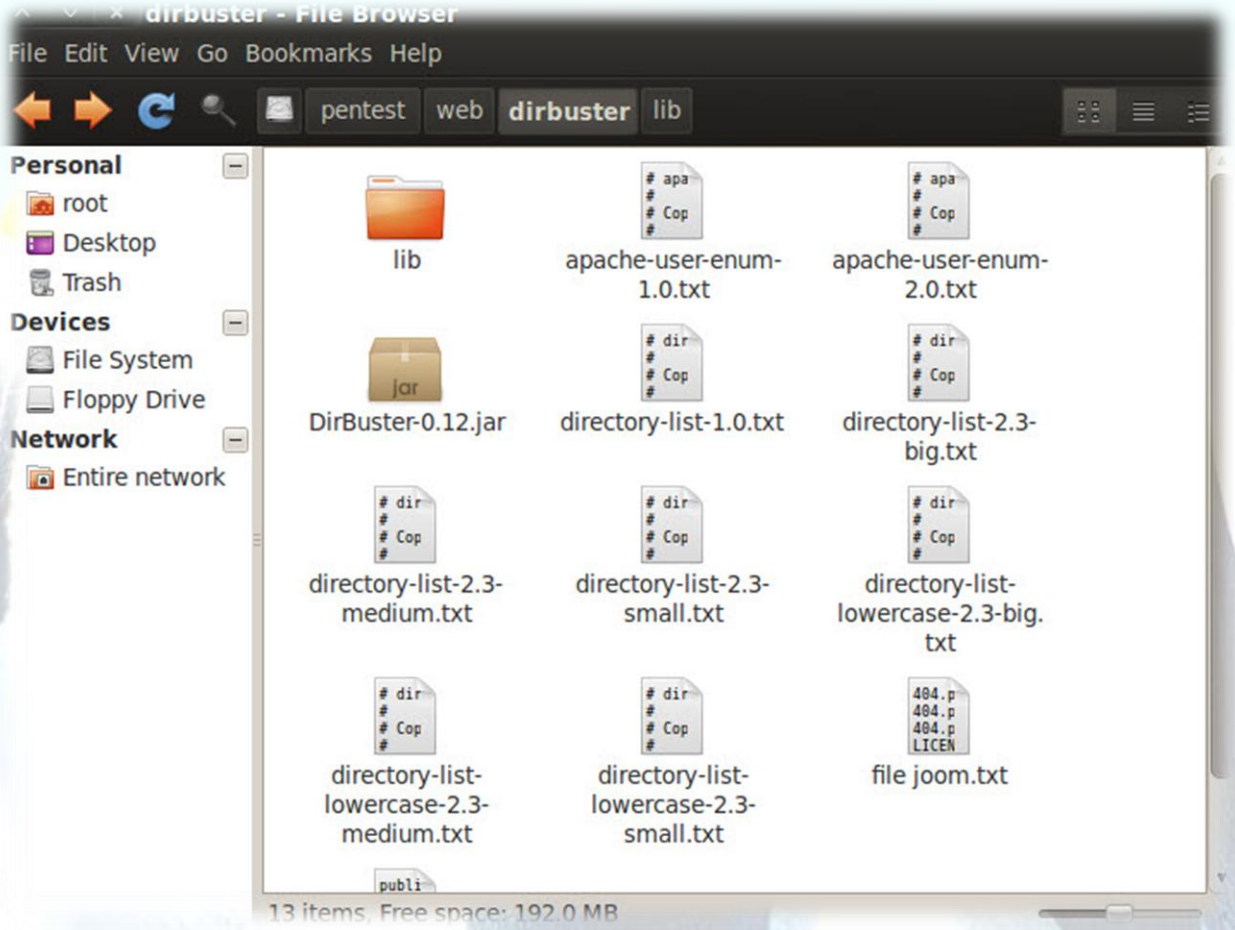
2) استفاده از توابع خودکار Get و Head (پیشنهاد میکنم از این گزینه استفاده کنید چون از دو توابع با هم استفاده میکنه)

3) سرعت خواندن (روی 100 قرار دهید)

قسمت سوم قرار دادن لیست برای بروت

1) List based Brute force
2) Pure Brute force

1) استفاده از لیست پایه (که به صورت قبلی در پوشه دایرباستر قرار داده شده است)



2) استفاده از لیست (که به صورت پیش فرض در برنامه قرار داده شده است)

قسمت چهارم انتخاب امکانات برنامه برای شروع

1)standard start point

1/1) Brute force dirs
1/2) Brute force files
1/3) Be recursive

1/4) Use Blank Extention

گزینه های پیش فرض 1.2.3 تیک خورده است بهتراز همانطور بماند وگزینه 4 استفاده از اکتنشن های خالی است که از پسوند های اسم استفاده میکند

2) url fuzz

نام فایلی است که در انتهای تارگت برای اسکن قرار می گیرد

در آخر سعی کنید از پروکسی استفاده کنید تا روند کار بهتر شود و از مسیر

Option/option advanced / http option

پروکسی اضافه کنید

دلایل استفاده از پروکسی :

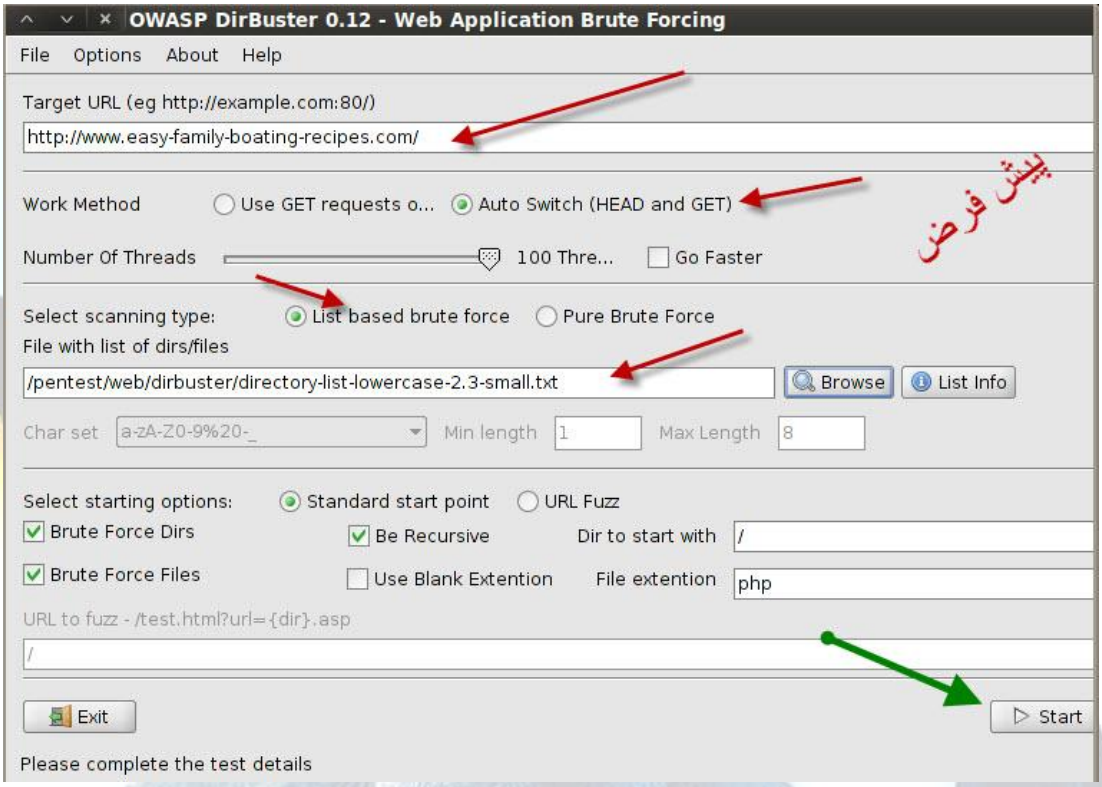
.ترافیک شبکه ای که ازش استفاده می کنیم پروکسی می تواند تغییر دهد

.. پروکسی میتواند کوکی ها رو مسدود کند

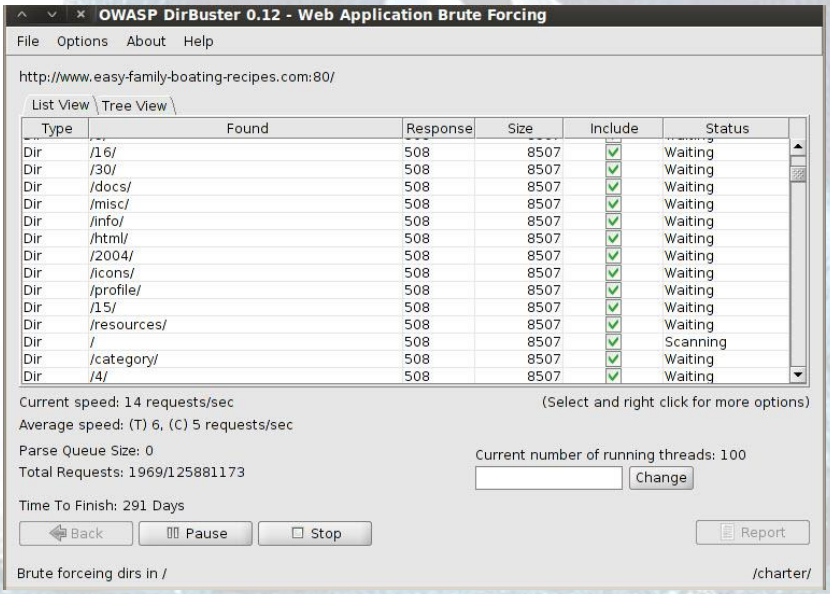
... استفاده از پروکسی است که به سرور وصل می شود و در نتیجه ip ما مخفی می ماند

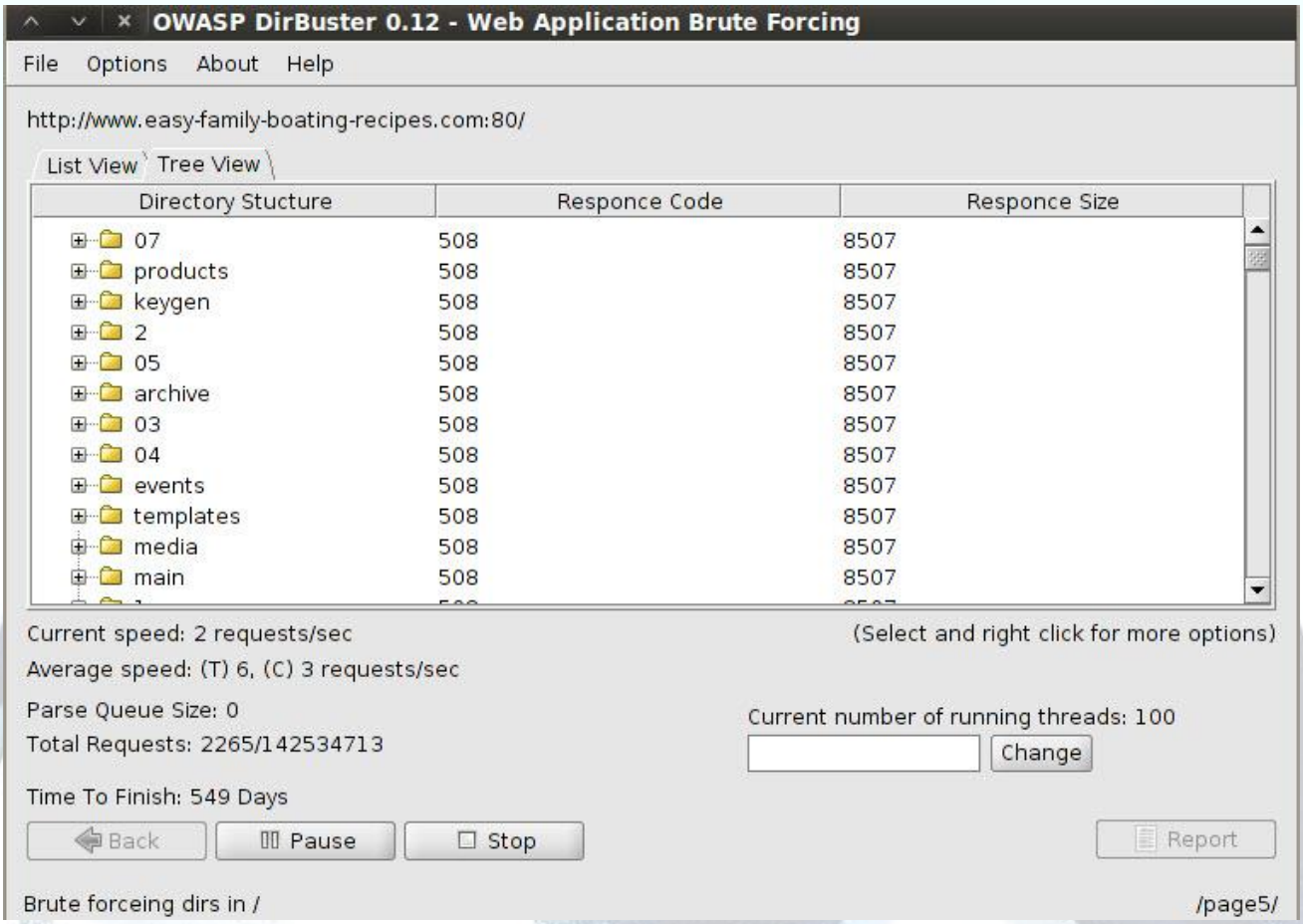
....از پهنای باند کمتری استفاده میکند

شروع کار :

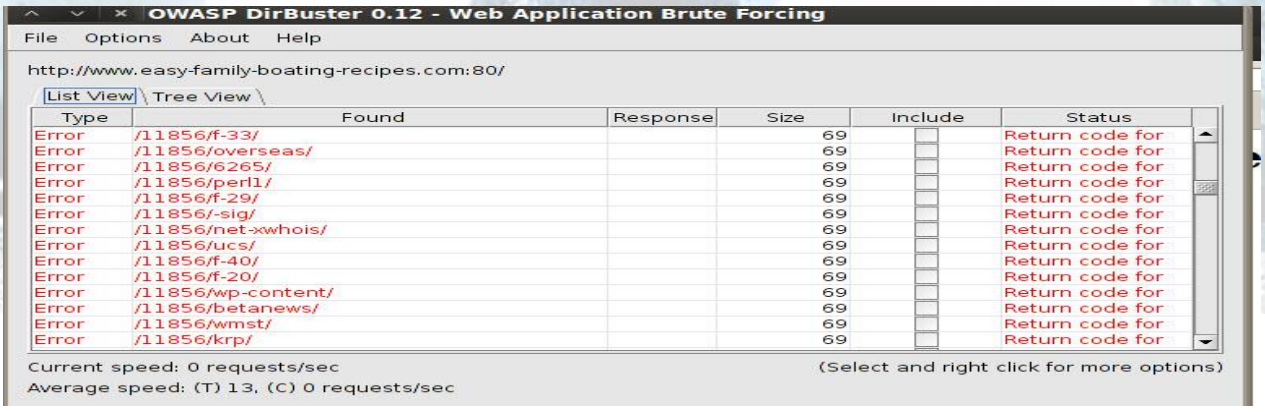


لیست اسامی را که انتخاب کرده بودیم بر روی وب سایت بروت می کند

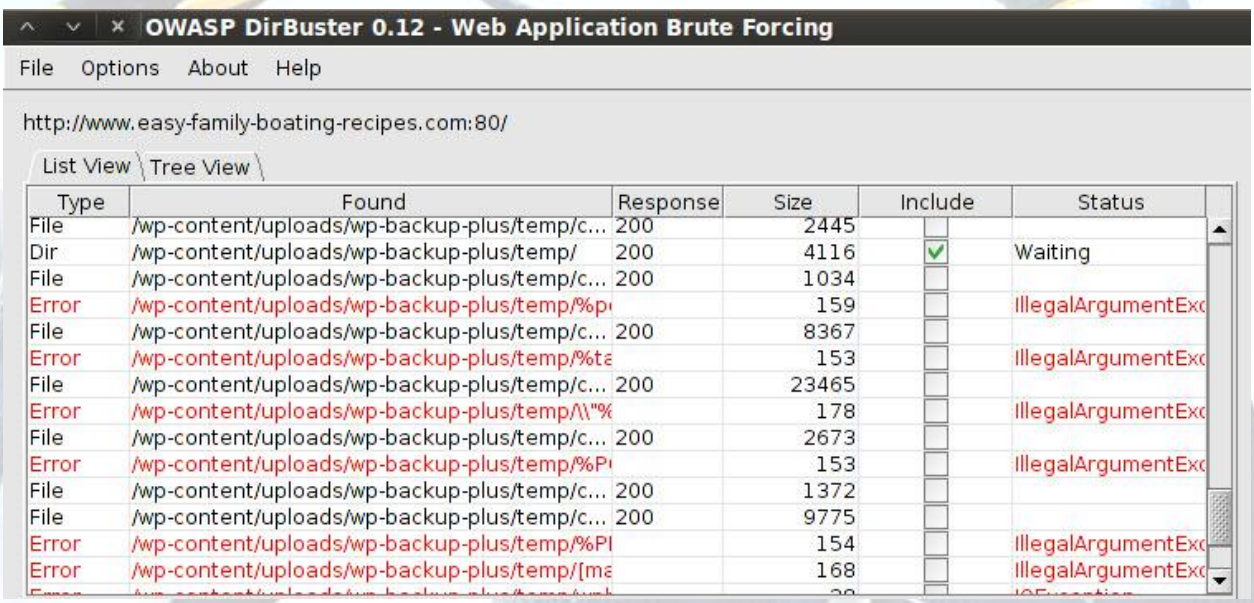




به درخواست هایی که در پروتکل htpp نیست ارور می دهد و ادامه بروت را در اون اسامی ادامه نمی دهد



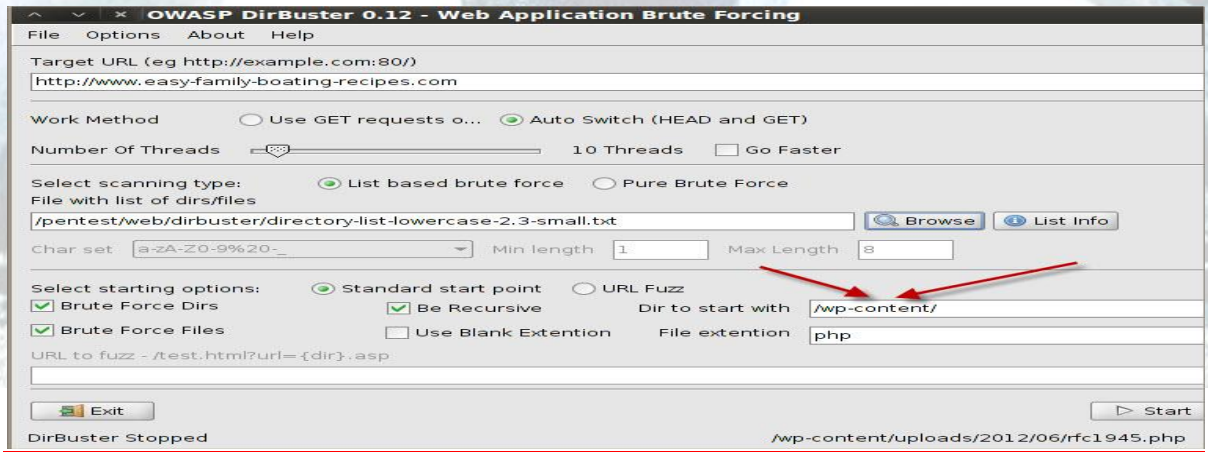
قبل از بروت کردن با توجه به تارگت خودتون که از چه مدیریت محتوایی استفاده میکند میتوانید نام های پوشه ها و فایل هایی که در اون مدیریت محتوا وجود دارد به لیست اضافه کنید و یا لیست جداگانه ای تعریف کنید در تارگت من این قسمت ها پیدا شده



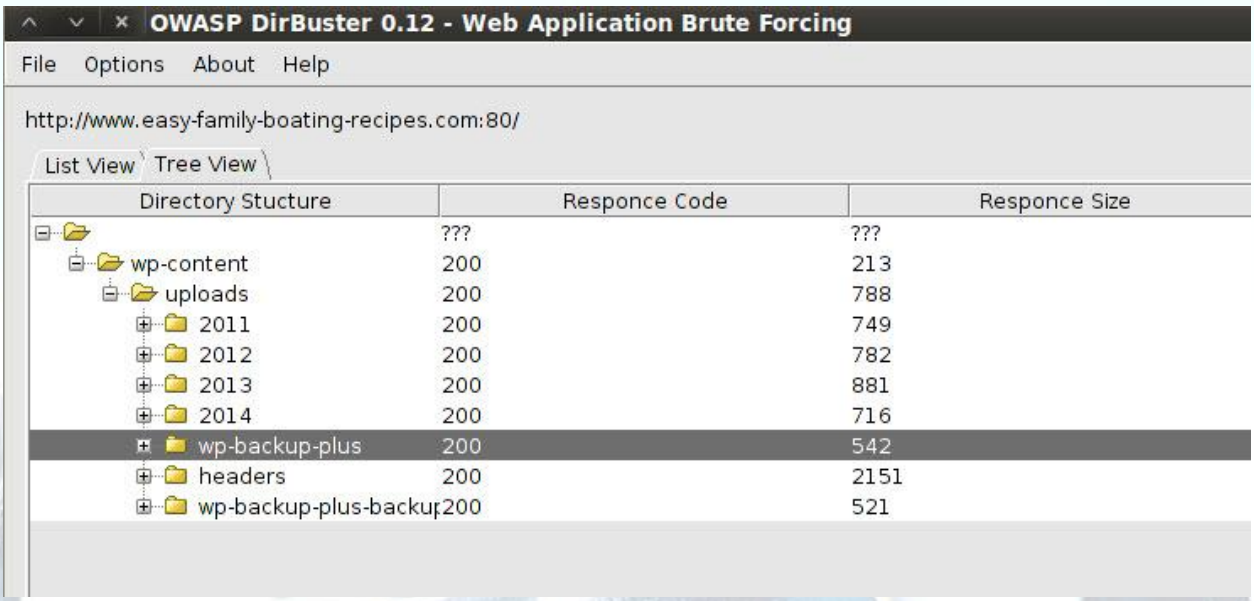
من حمله را متوقف میکنم و wp-content را در قسمت

Dir to start with

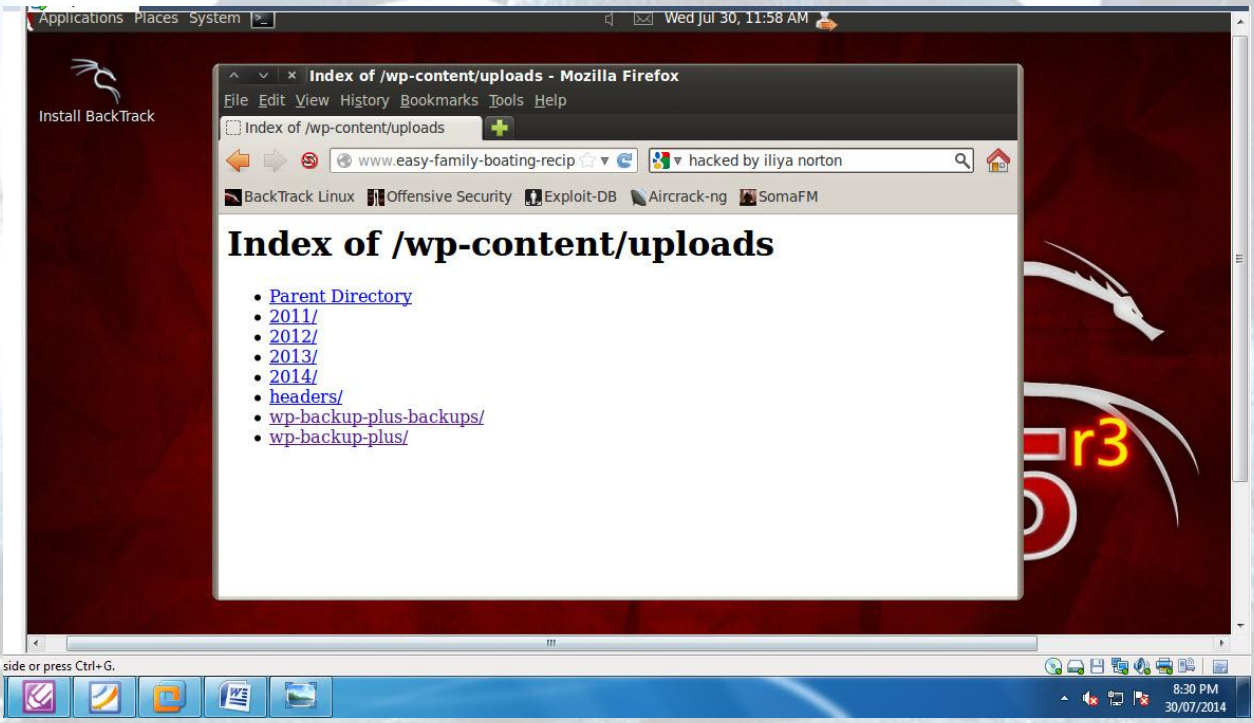
اضافه میکنم تا دایرکتوری وفایل داخل wp-contentرا بروت کند



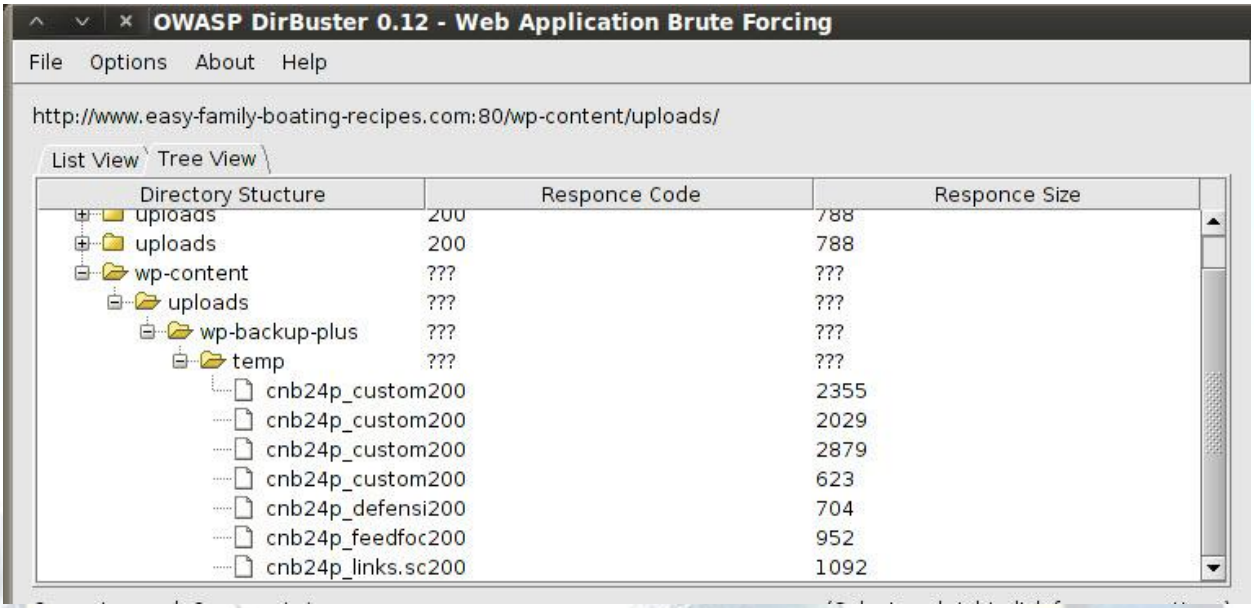
بروت در دایرکتوری wp-content با نتیجه زیر بود



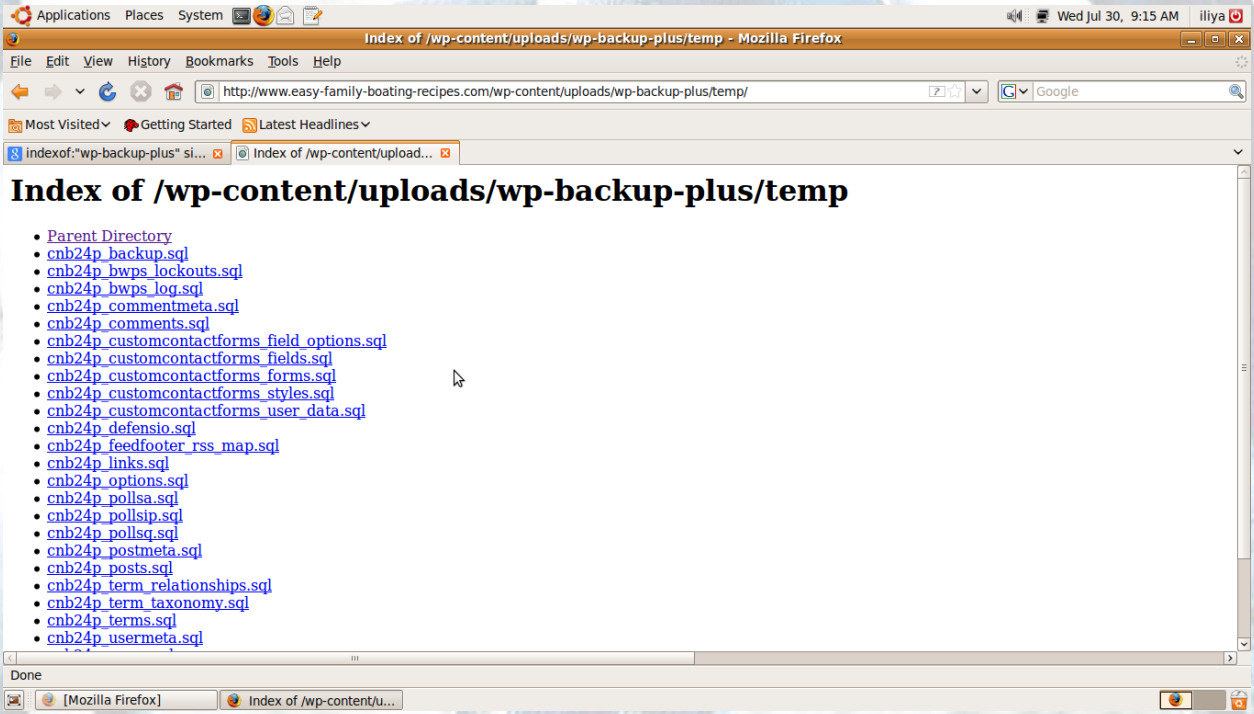
حالا من به ادرس بالا در مرورگر خود می روم تا قسمت ها را ببینم



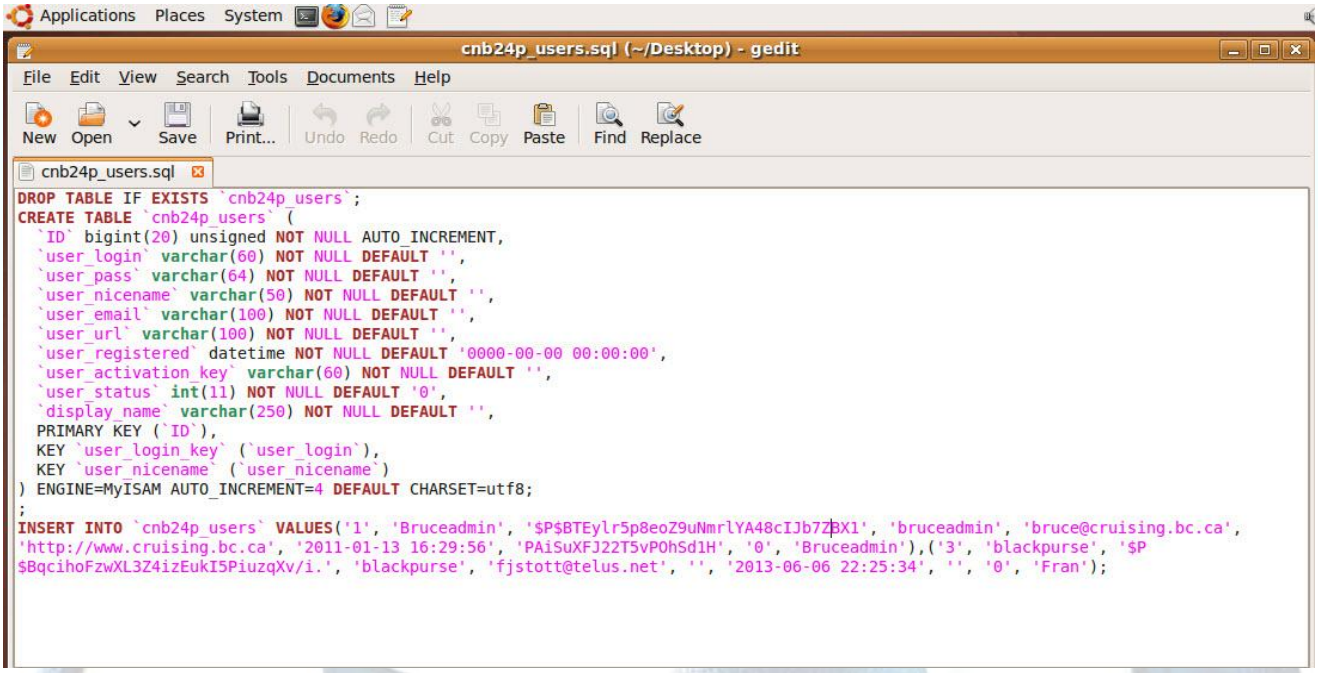
قسمت دیتابیس



و به این ادرس در مرورگر اوبونتو



ما تونستیم با dirbusterبه دیتابیس وب سایت با بروت کردن به فایل cnb24p_users.sql دسترسی پیدا کنیم



User And Password admin

Username : Bruceadmin

Password : PBTEylr5p8eoZ9uNmrlYA48cIJb7ZBX1

با توجه به نیاز خودتون میتوانید بروت کنید این تارگت فقط تست بود تا شما با نرم افزار دایرباستر اشنایی پیدا کنید

امیدوارم لذت برده باشید

کپی برداری با ذکر نام منبع بلا مانع می باشد

با تشکر از mehrdad stryker عزیز جهت همکاری در پایان رساندن مقاله 3> 3>

موفق و موید باشید

ومن الله التوفیق

تابستان 1393