



# ওয়ার্ডপ্রেসের নিরাপত্তা

প্রথম সংস্করণ - ১৩/০৪/২০১৩

দ্বিতীয় সংস্করণ - ১৩/০৩/২০১৪

প্রকাশক - বিডিটেকজোন.কম

লেখক

ফয়সাল শাহী

[www.shahi.info](http://www.shahi.info)

কপিরাইট

ফয়সাল শাহী ও [বিডিটেকজোন](#)

বইটি একেবারেই ফ্রী ও বিনামূল্যে বিতরণ যোগ্য।

তবে বইটির কোন অংশ পরিবর্তন করে প্রকাশ করা যাবে না।



# শুরূর আগে

ওয়ার্ডপ্রেস একটি ওপেন সোর্স কনটেন্ট ম্যানেজমেন্ট সিস্টেম হওয়ার কারণে ওয়ার্ডপ্রেস হ্যাকারদের কাছে একটি বড় টার্গেট হয়ে দাঁড়ায়। সম্প্রতি এক গবেষণায় দেখা যায় যে পুরো ইন্টারনেট দুনিয়ার ১৭% থেকে ২০% সাইটই হল ওয়ার্ডপ্রেস সাইট! যা এক কথায় অবিশ্বাস্য। আর এই কারণেও ওয়ার্ডপ্রেস হ্যাকারদের একটি বড় লক্ষ বস্তু। তবে কিছু পদ্ধতি অনুসরণ করলে ওয়ার্ডপ্রেস সাইট হ্যাকিং রোধ করা যায়।



হ্যাকিং রোধে যা করতে হবে, কিছু নিয়ম কানুন মেনে চললে হ্যাকিং থেকে অনেকটাই রক্ষা পাওয়া যায়, তবে কোন সাইটই ১০০ভাগ নিরাপদ নয়। আর কেউ চ্যালেঞ্জ করে বলতেও পারবেন না যে আমার সাইটটি হ্যাকিং করা সম্ভব নয়। অ্যাপল, সনির মত আরও অনেক নামি দামি সাইটও হ্যাকিং এর শিকার হয়েছে। আর তাই বলে আমাদের ওয়েবসাইট তৈরি করা বন্ধ করে দিতে হবে? না, হ্যাকিং এর শিকার যাতে না হয় সেই সব বেবস্থা নিয়ে আমাদের এই জগতে প্রবেশ করতে হবে। কিভাবে ওয়ার্ডপ্রেস সাইট হ্যাকিং থেকে বাঁচানো যায় অর্থাৎ ওয়ার্ডপ্রেস সাইটকে কিভাবে সিকিউরিটি দেওয়া যায় এই সবই আলোচনা করা হবে এই ইবুকে।

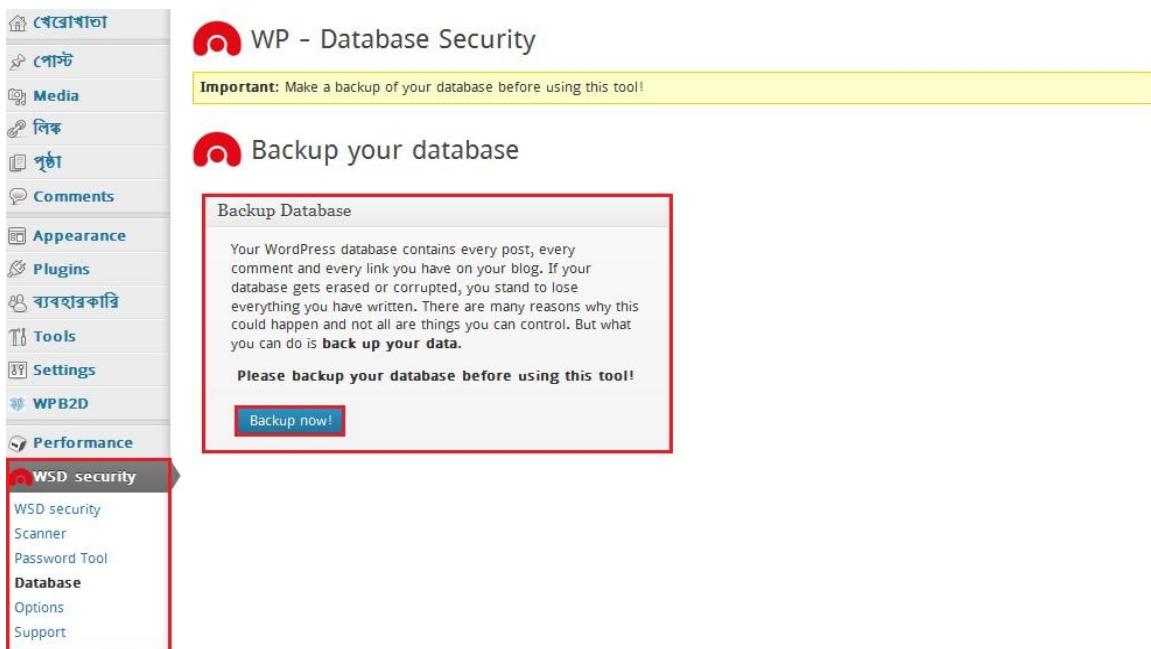
মানুষ মাত্রই ভুল, এই বইয়ে বানানগত কিছু ভুল থাকতে পারে। আশা করি ভুল ক্ষমা সুন্দর দৃষ্টিতে দেখবেন। আপনার দৃষ্টিতে কোন ভুল পড়লে আমাকে দয়া করে জানিয়ে দিবেন, ধন্যবাদ।

[www.facebook.com/mfshahi](http://www.facebook.com/mfshahi)

# ব্যাকআপ

ওয়ার্ডপ্রেস সাইটের নিরাপত্তার জন্য সর্ব প্রথম আপনার উচিত আপনার সাইট নিয়মিত ব্যাকআপ করে রাখা। ব্যাকআপ করার জন্য বাবহার করতে পারেন **WP Security Scan** এই প্লাগিনটি। এই প্লাগিনটি দ্বারা ডাটাবেস ব্যাকআপ করা ছাড়াও ওয়ার্ডপ্রেস সাইটের সিকিউরিটি বিষয়ক বিভিন্ন সমস্যার সমাধান করা যায়। এই প্লাগিনটি দ্বারা ব্যাকআপ নিতে চাইলে নিচের ছবির মত করে ডাটাবেস সেকশনে গিয়ে “Backup Now” বাটনে ক্লিক করুন।

<http://www.websitedefender.com/news/free-wordpress-security-scan-plugin/>



এছাড়াও ওয়ার্ডপ্রেস সাইট ব্যাকআপ করার কিছু জনপ্রিয় প্লাগিন নিচে দেওয়া হল

**BackUpWordPress** - <http://wordpress.org/extend/plugins/backupwordpress/>

**Backup to Dropbox** - <http://wordpress.org/extend/plugins/wp-db-backup/>

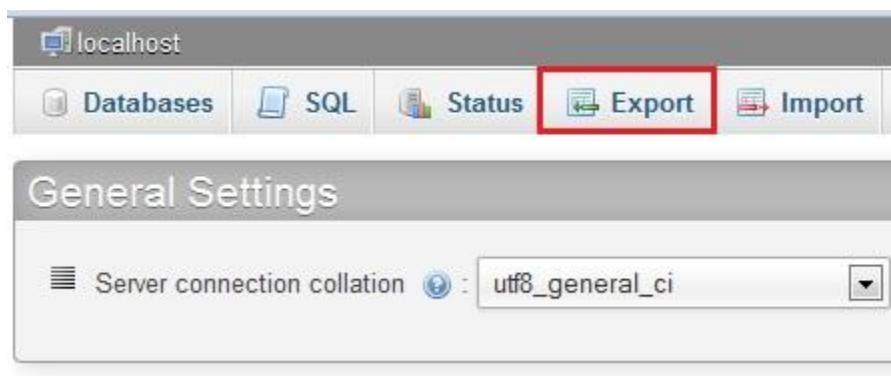
**BP-DB-Backup** - <http://wordpress.org/extend/plugins/wp-db-backup/>

**Goole Drive for WordPress** - <http://wordpress.org/extend/plugins/wp-google-drive/>

আপনি চাইলে কন্ট্রোল প্যানেল থেকেও ব্যাকআপ নিতে পারেন। এর জন্য প্রথমেই আপনার সাইটের কন্ট্রোল প্যানেলে লগিন করুন।



তারপর, পিএইচপিমাইএডমিনে ক্লিক করতে হবে।





## Exporting databases from the current server

### Export Method:

- Quick - display only the minimal options
- Custom - display all possible options



তারপর এক্সপোর্ট বাটনে ক্লিক করে SQL ফরম্যাটে ফাইলটি সেভ করে নিন। শুধু মাত্র ডাটাবেস ব্যাকআপ করলে আপনার সাইটের কোন সমস্যা হলে ডাটাবেসটি রিষ্ট্রেট করলে আপনি শুধু আপনার সাইটের পোস্ট গুলো পাবেন। কিন্তু আপনি আপনার সাইটের থিম, প্লাগিন, ইমেজ গুলো মিস করবেন। আর যদি পুরো সাইটের সবকিছু পেতে চান তাহলে

The screenshot shows a 'File Manager' interface with various tools at the top: Backups, Backup Wizard, File Manager (highlighted with a red box), Legacy File Manager, Disk Space Usage, and Web Disk.

**File Manager Directory Selection**

**Directory Selection**

Please select a directory to open:

- Home Directory
- Web Root (public\_html/www)
- Public FTP Root (public\_ftp)
- Document Root for: [dropdown menu]

Show Hidden Files (dotfiles).

Skip this question, and always open this directory in the future when opening File Manager.

**Go**

|      | Name                               | Size     | Last Modified (Central As) |
|------|------------------------------------|----------|----------------------------|
| 📁    | .smileys                           | 4 KB     | Dec 27, 2012 4:10 PM       |
| 📁    | cgi-bin                            | 4 KB     | Oct 23, 2012 7:11 PM       |
| 📁    | wp-admin                           | 4 KB     | Jan 29, 2013 4:46 PM       |
| 📁    | wp-content                         |          | Yesterday 8:15 PM          |
| 📁    | wp-includes                        |          | Mar 16, 2013 10:14 AM      |
| 📄    | .htaccess                          |          | Yesterday 7:39 PM          |
| PHP  | .wysiwygPro_preview                |          | Dec 27, 2012 4:10 PM       |
| 📄    | error_log                          |          | Mar 16, 2013 12:32 PM      |
| ICO  | favicon.ico                        |          | Oct 31, 2012 4:18 PM       |
| IMG  | google1448f42359461                |          | Jan 11, 2013 11:46 AM      |
| PHP  | index.php                          |          | Jan 11, 2013 3:16 PM       |
| TXT  | license.txt                        |          | Jan 11, 2013 3:16 PM       |
| HTML | readme.html                        | 8.96 KB  | Jan 29, 2013 4:46 PM       |
| XML  | sitemap.xml                        | 17.72 KB | Today 9:12 AM              |
| ZIP  | sitemap.xml.gz                     | 1.88 KB  | Today 9:12 AM              |
| TXT  | softver.txt                        | 5 bytes  | Oct 29, 2012 12:03 PM      |
| IMG  | statscrop_a6c0dcf10b4e727a86455811 | 32 bytes | Mar 15, 2013 3:47 PM       |

A context menu is open over the 'favicon.ico' file, listing options: Move, Copy, Rename, Change Permissions, Delete, Compress (highlighted with a red box), Password Protect, Leech Protect, and Manage Indices.

সিপ্যানেলের ফাইল ম্যানেজারে ক্লিক করে সাইটের সব গুলো ফাইল জিপ করে ডাউনলোড করে নিন।

# সাইট ব্যাকআপের সময় আমরা যেই ভুলগুলো করে থাকি

হ্যাকিং এর এই যুগে সাইট ব্যাকআপ করে না থাকার কোন উপায় নেই। সাইট ব্যাকআপ করার প্রয়োজনীয়তা নিয়ে নতুন করে বলার কিছু নেই। আপনাদের কাছে কিছু বিষয় তুলে ধরবো যেসব কিছু জিনিষ সাইট ব্যাকআপ করার সময় বেশিরভাগ লোকেরাই ভুল করে থাকে। আশা করি সাইট ব্যাকআপ করার সময় আপনারা এই ভুল গুলো থেকে বিরত থাকবেন।



## নিয়মিত ব্যাকআপ না করা

সাইট ব্যাকআপ করার ক্ষেত্রে যেই সমস্যাটি সবচাইতে বেশি ভোগায় তা হল নিয়মিত ব্যাকআপ না করা। আপনি যদি নিয়মিত ব্যাকআপ না করেন তাহলে আপনি আপনার সাইটের মহামূল্যবান অনেক কিছু হারাতে পারেন। তাই আমি আপনাকে রেকমেন্ড করবো ১০/১৫ দিনে একবার করে হলেও সাইট ব্যাকআপ করার জন্য।

## সম্পূর্ণ সাইট ব্যাকআপ না নেওয়া

অনেকই সাইট ব্যাকআপ করার সময় শুধু ডাটাবেস ব্যাকআপ করে থাকে। আপনার উচিত পুরো সাইট ব্যাকআপ করা। আপনি যদি শুধু ডাটাবেস ব্যাকআপ করে থাকেন তবে, আপনি আপনার সাইটের পোস্ট গুলো ঠিকই ফিরে পাবেন তবে আপনি আপনার সাইটের ফটো, থিম, প্লাগিন সহ আরও অনেক কিছু মিস করবেন। তাই আমি আপনাকে রেকমেন্ড করবো পুরো সাইট ব্যাকআপ করার জন্য।

## শুধু অনলাইনে ব্যাকআপ রাখা

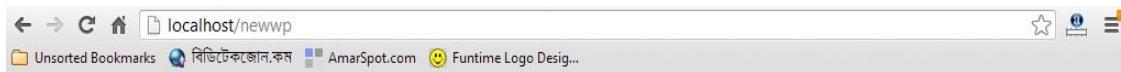
আরেকটি মজার বিষয় হল, অনেক সাইট ব্যাকআপ করে নিজের সার্ভারে রাখে!! সাইট হ্যাক হলে হ্যাকার কি আপনার ব্যাকআপ ফাইল রেখে দিবে?? অনেলাইনে ব্যাকআপ ফাইল রাখার জন্য আপনি mediafire, google drive, copy, sky drive, box, dropbox এই সাইট গুলো ব্যবহার করতে পারেন। আর অবশ্যই আপনার সাইটটি অফলাইনে অর্থাৎ আপনার কম্পিউটারেও ব্যাকআপ করবেন। তাহলেই অনলাইনে ব্যাকআপ ফাইল গুলো যদি কোন কারনে ডিলিটও হয়ে যায় তাহলে সমস্যা হবে না।

## ব্যাকআপ ফাইল চেক না করা

সাইট ব্যাকআপ করার পর সময় পেলে অবশ্যই আপনার সাইটের ব্যাকআপ ফাইল গুলো ব্যবহার করে দেখবেন। ব্যাকআপ ফাইল চেক না করে শুধু ব্যাকআপ করার কোন মানেই হয় না। তাই আমি আপনাকে রেকম্যানেজ করবো যখনই সাইট ব্যাকআপ করবেন তখনই বা সুযোগ পেলে ব্যাকআপ ফাইল গুলো ব্যবহার করে দেখবেন কাজ করছে কিনা।

# রিস্টোর করুন আপনার ওয়ার্ডপ্রেস সাইট

এখন আমরা দেখাবো কিভাবে ওয়ার্ডপ্রেস সাইট রিস্টোর করা যায়। ওয়ার্ডপ্রেস সাইট রিস্টোর করার পূর্বে আপনার কাছে আপনার [সাইটের ব্যাকআপ](#) থাকতে হবে। রিস্টোর করার কাজটি হবে এমন, নতুন একটি ওয়ার্ডপ্রেস ইনস্টল করে তাতে আপনার আগের ব্যাকআপ করা ডাটাবেসটি আপলোড করা। আর ইমেজ ও অন্যান্য ফাইল থাকলে তা wp-content ফোল্ডারে প্লেস করা।



## Object not found!

The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again.

If you think this is a server error, please contact the [webmaster](#).

## Error 404

localhost  
03/27/13 12:09:41  
Apache/2.2.11 (Win32) DAV/2 mod\_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9

কিভাবে ওয়ার্ডপ্রেস সাইট ব্যাকআপ করতে হয় না জানলে [এখানে](#) দেখুন। আপনার সাইটের রুট ফোল্ডারে ওয়ার্ডপ্রেসের সর্বশেষ ভার্শনটি আপলোড করুন এবং ফাইল গুলো আনজিপ করে নিন। এবার phpmyadmin থেকে একটি ডাটাবেস তৈরি করে নিন। আপনার ব্যাকআপ কৃত ডাটাবেসটি নতুন ডাটাবেসে আপলোড করুন।

phpMyAdmin

Server: localhost Database: newwp

Structure SQL Search Query Export Import Designer Operations Privileges Drop

File to import

Location of the text file: Choose File No file chosen (Max: 65,536 KiB)

Character set of the file: utf8

Imported file compression will be automatically detected from: None, gzip, zip

Partial import

Allow the interruption of an import in case the script detects it is close to the PHP timeout limit. This might be good way to import large files, however it can break transactions.

Number of records (queries) to skip from start: 0

Format of imported file

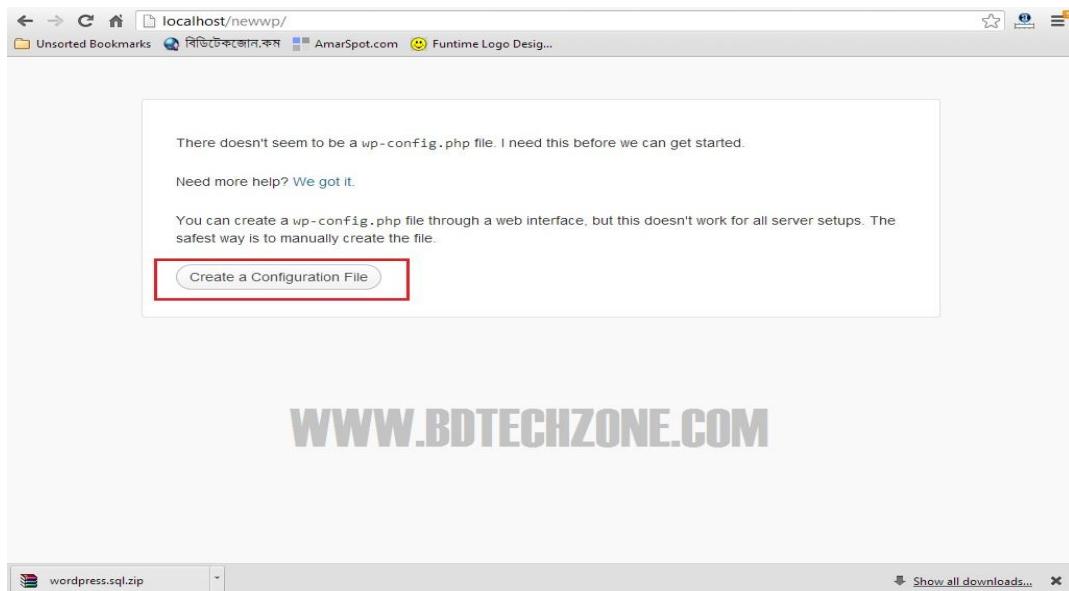
SQL Options

SQL compatibility mode: NONE

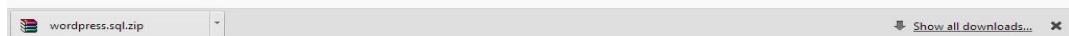
Go

Open new phpMyAdmin window

আপলোড করা হয়ে গেলে আপনার সাইটটি ভিজিট করুন। এবার নিচের মত একটি পেজ দেখেতে পাবেন। (ডাটাবেস আপডেট চাইলে আপডেট করে নিন)



WWW.BDTECHZONE.COM



এবার যথারীতি ওয়ার্ডপ্রেস ইনস্টল করুন।

A screenshot of the WordPress database setup form. The title is 'WORDPRESS'. It asks for database connection details:

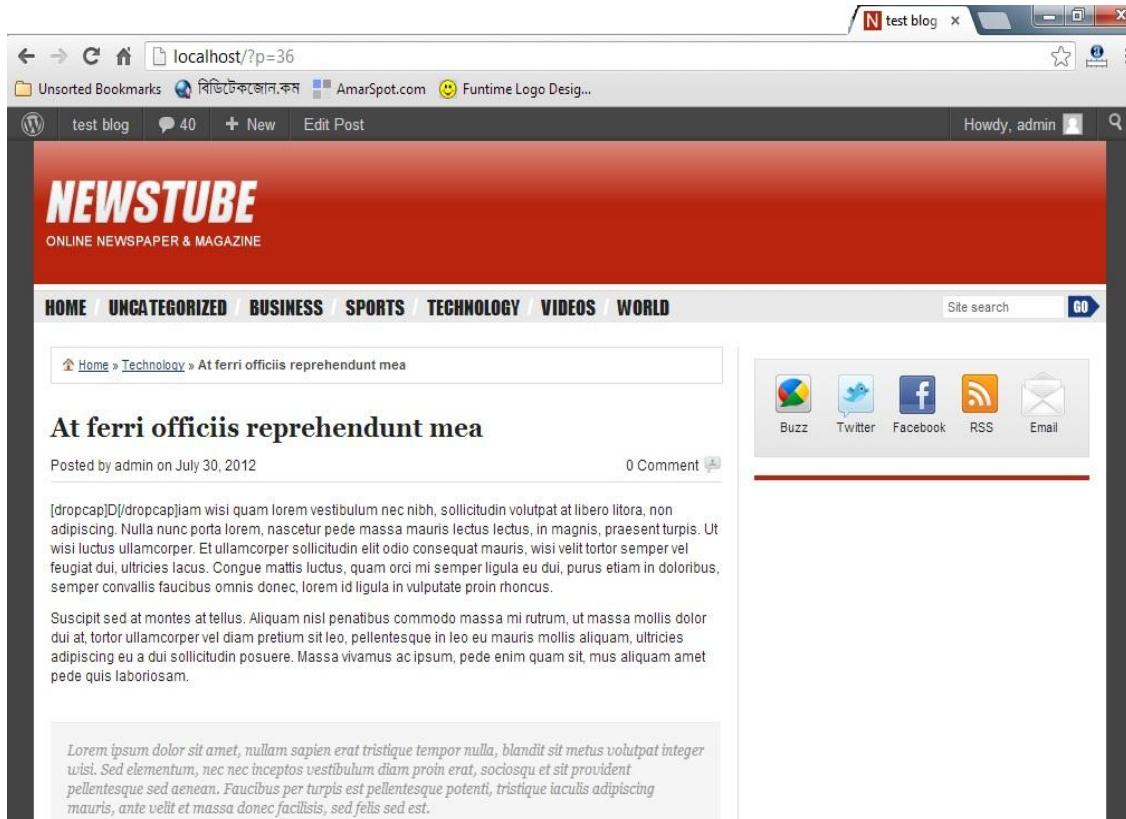
- Database Name:** newwp (highlighted with a yellow box)
- User Name:** root
- Password:** (empty field)
- Database Host:** localhost
- Table Prefix:** wp\_ (highlighted with a yellow box)

Below the fields are descriptions:

- The database name you want to run WP in.
- Your MySQL username.
- ...and your MySQL password.
- You should be able to get this info from your web host, if localhost does not work.
- If you want to run multiple WordPress installations in a single database, change this.

A red box highlights the 'Submit' button at the bottom.

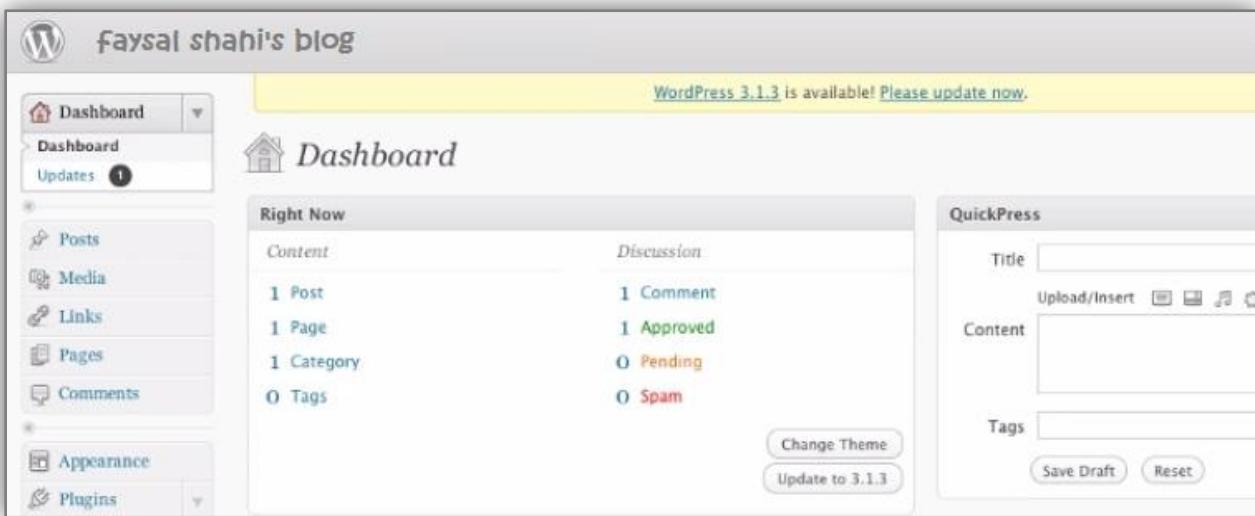
ইনস্টল করার ক্ষেত্রে আপনার কাঞ্চিত ডাটাবেস নাম দিন। ইনস্টল করা হয়ে গেলে আপনার সাইটটি এবার সচল হয়ে যাবে। প্রয়োজনে wp-config.php ফাইলটি আপনার কাঞ্চিত ডাটা দ্বারা ফিলআপ করুন।



**নোট:** এভাবে ওয়ার্ডপ্রেস সাইট রিস্টোর করলে আপনি শুধু আপনার সাইটের পোস্ট গুলো ফিরে পাবেন। আপনি যদি আপনার সাইটের ফটো, থিম, প্লাগইন গুলোও ফিরে পেতে চান তাহলে আপনাকে আগে খেকেই আপনার সাইটের ফটো, থিম, প্লাগইন গুলো ব্যাকআপ করে রাখতে হবে। যদি আপনার ফাইল গুলো ব্যাকআপ করা খেকে তবে ফাইল গুলো wp-content ফোল্ডারে রিপ্লেস করে দিন।

**বিশেষ নোট:** ওয়ার্ডপ্রেস রিস্টোর করার পর অবশ্যই আপনি আপনার নতুন সাইটের সেটিংস থেকে আপনার সাইটের অ্যাড্রেসটি দেখিয়ে দিতে হবে। আর আপনার ডাটাবেসের wp\_options টেবিলটি থেকেও আপনার সাইট অ্যাড্রেসটি পরিবর্তন করুন।

# ওয়ার্ডপ্রেস আপডেট



যখনই ওয়ার্ডপ্রেসের কোন ভার্সনে সিকিউরিটি রিলেটেড\* কোন সমস্যা পাওয়া যায় তখন ওয়ার্ডপ্রেস টিম ওয়ার্ডপ্রেসের নতুন একটি ভার্সন প্রকাশ করে। লেটেস্ট ভার্সনের ওয়ার্ডপ্রেস ব্যবহার করলে আপনার সাইট অনেকটাই সিকিউর হয়ে যাবে। নতুন কোন ভার্সন রিলিজ হলে উপরের ছবির মত আপনার সাইটের ডেশবোর্ডের একেবারে উপরে একটি নোটিশ দেখতে পাবেন। নতুন ভার্সনে আপডেট করতে “Please update now” বাটনে ক্লিক করুন।

তবে সাইট ওয়ার্ডপ্রেস আপডেট করার পূর্বেই সাইটের একটি ব্যাকআপ নিয়ে নিবেন। যদি কোন কারনে আপডেট হতে সমস্যা হয় তাহলে আপনি সাইট আবার রিকভার করতে পারবেন।

## থিম ও প্লাগইন আপডেট

একই ভাবে যখন কোন থিম ও প্লাগইন পাওয়া যাবে সাথে সাথে তা আপডেট করে নিন।

# পাসওয়ার্ড

---

যেই ধরনের সাইট হোক না কেন, সাইটকে নিরাপদ রাখার জন্য অবশ্যই একটি কঠিন পাসওয়ার্ড ব্যবহার করবেন। এমন কোন পাস্ওয়ার্ড ব্যবহার করবেন না যা আপনার পছন্দের কোন কিছু। তাহলে সোশ্যাল ইঞ্জিনিয়ারিং করে আপনার পাসওয়ার্ড হ্যাক করা সম্ভব।

- Ex: rockST4R19!@

কঠিন পাসওয়ার্ড তৈরি করতে দেখুন

<http://strongpasswordgenerator.com>

# এডমিন ইউজার

কখনই ডিফল্ট ভাবে তৈরি কৃত admin ইউজারটি ব্যবহার করবেন না। এটি ওয়ার্ডপ্রেস সাইটের জন্য খুব বড় রিস্ক। নতুন ওয়ার্ডপ্রেস স্টার্টআপ দেওয়ার সময় admin না ব্যাবহার করে অন্য কোন ইউজারনেম দিন। আর যদি আগে থেকেই ওয়ার্ডপ্রেস দেওয়া থাকে তবে ওয়ার্ডপ্রেসের ইউজার

| ব্যবহারকারী | নাম              | ইমেইল                      | ভূমিকা      | পোস্ট | Login statistics        |
|-------------|------------------|----------------------------|-------------|-------|-------------------------|
| AHS         | Anamul Hoque     | anam.sifat10@yahoo.com     | Contributor | 6     | No login data available |
| alamin_bds  |                  | alamin_bds@yahoo.com       | Contributor | 0     | 6 days পূর্বে           |
| DH          |                  | rezabdt@yahoo.com          | Contributor | 0     | No login data available |
| faysal      |                  | mahirfaysalshahi@gmail.com | Contributor | 0     | 6 days পূর্বে           |
| mahmudsumon | মাহমুদ সুমন      | mahmudsumon1989@gmail.com  | Contributor | 2     | No login data available |
| Mdmushfiq   |                  | nahidahmed21@yahoo.com     | Contributor | 1     | No login data available |
| mkhtanvir   | এম কে এইচ তানভীর | mkhtanvirbd@yahoo.com      | Contributor | 2     | No login data available |
| nayem       | kamran hossain   | jhon.ornob@gmail.com       | Author      | 0     | 6 days পূর্বে           |

ট্যাব থেকে নতুন একটি ইউজার তৈরি করে তাকে এডমিন রোল দিয়ে ডিফল্ট admin ইউজারকে ডিলেট করে দিন। নতুন ইউজারনেম নেমটি একটু কঠিন থেকে নির্বাচন করুন।

এই পদ্ধতি কঠিন মনে হলে ব্যবহার করুন - <http://wordpress.org/extend/plugins/admin-username-changer/>

- যেমনঃ Myn4m3

আপনার সাইটের রেজিস্টার অপশন যদি সকলের জন্য উন্মুক্ত হয় তবে সেটিংস ট্যাবে গিয়ে ডিফল্ট রোল Contributor (কন্ট্রিবিউটর) করে দিন।

# প্রিফিক্স

ডিফল্ট ভাবে সব ওয়ার্ডপ্রেস সাইটের ডাটাবেস টেবিল প্রিফিক্স wp\_ দেওয়া থাকে।  
ডিফল্ট ডাটাবেস প্রিফিক্স ব্যাবহার করার জন্য যেকোনো সময় আপনার সাইট হ্যাক হতে পারে।  
নতুন সাইট ইনস্টল করার সময় খুব সহজেই ডাটাবেস প্রিফিক্স সেট করা যায় করা যায়।

The screenshot shows the WordPress database configuration screen. At the top is the classic WordPress logo. Below it, a message says: "Below you should enter your database connection details. If you're not sure about these, contact your host." The form contains five input fields:

- Database Name:** bdtechzone (with a descriptive note: "The name of the database you want to run WP in.")
- User Name:** root (with a descriptive note: "Your MySQL username")
- Password:** BDTECHZONE (with a descriptive note: "...and your MySQL password.")
- Database Host:** localhost (with a descriptive note: "You should be able to get this info from your web host, if localhost does not work.")
- Table Prefix:** wp\_cust0m\_ (with a descriptive note: "If you want to run multiple WordPress installations in a single database, change this.")

At the bottom left is a "Submit" button.

নতুন সাইট ইনস্টল করার সময় ডাটাবেস প্রিফিক্স বক্সে আপনার পছন্দ মত প্রিফিক্স দিয়ে সাবমিট বাটনে ক্লিক করলেই খেল খতম!

তবে পুরাতন সাইটের ডাটাবেস প্রিফিক্স পরিবর্তন করার নিয়ম একটু ভিন্ন। এই জন্য **WP Security Scan** প্লাগইনটি ইনস্টল করুন।

<http://wordpress.org/extend/plugins/wp-security-scan/>



প্লাগইনটি ইনস্টল করা হয়ে গেলে ডাটাবেস অপশনে ক্লিক করুন। তারপর আপনার পছন্দ কৃত প্রিফিক্সটি বক্সে লিখে স্টার্ট রিনেম বাটনে ক্লিক করলেই কোন ঝামেলা ছাড়াই আপনার সাইটের ডাটাবেস প্রিফিক্স পরিবর্তন হয়ে যাবে।

# Wp-Config ও .htaccess ফাইলের নিরাপত্তা

---

ওয়ার্ডপ্রেস সাইটের প্রান হল wp-config.php ফাইলটি। ওয়ার্ডপ্রেস সাইটের অনেক প্রয়োজনীয় তথ্য থাকে wp-config ফাইলে। অনুরূপ ভাবে ওয়ার্ডপ্রেস সাইটের .htaccess ফাইলটিও অনেক মূল্যবান। এখন আমরা দেখাবো কিভাবে wp-config ও .htaccess ফাইল সুরক্ষিত রাখা যায়। .htaccess ফাইল দ্বারা সহজেই এই কাজটি করা যায়।

এই জন্য আপনার সাইটের রুটের .htaccess ফাইলটি খুলুন ও নিচের লিখা গুলো পেস্ট করুন।

```
# PROTECT WP-CONFIG
<Files wp-config.php>
Order Allow,Deny
Deny from all
</Files>
```

```
# PROTECT .htaccess
<Files .htaccess>
Order Allow,Deny
Deny from all
</Files>
```

পেস্ট করা হয়ে গেলে .htaccess ফাইলটি সেভ করে নিন, তাহলেই আপনার Wp-Config ও .htaccess ফাইল সিকিউর হয়ে যাবে।

# কাস্টম চাবি তৈরি করা

আপনার ওয়ার্ডপ্রেস সাইটকে আরও নিরাপদ করতে আপনার উচিত একটি কাস্টম চাবি অর্থাৎ কী তৈরি করে নেওয়া। কাস্টম চাবি তৈরি করতে এখানে যানঃ

<https://api.wordpress.org/secret-key/1.1/salt/>

উপরের লিঙ্কটিতে গেলে আপনি কিছু কোড পাবেন, এবার সব কোড গুলো কপি করে আপনার ওয়ার্ডপ্রেস সাইটের wp-config.php ফাইলের এই অংশে পেস্ট করুন।

```
/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key API}.
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         ' (wmT}ff(1b39R>4U3bX3`N^Dc~C.]y{Vol&Do0cx~9>I=)GJg53Hf^pB:Ut-83z{');
define('SECURE_AUTH_KEY',  ']i6tWIezfzX~[ 96Bt(jYzyL&Ft4&4mU| ^vy]p0,_K# JiLpK=G.|mBHe2[0a.');
define('LOGGED_IN_KEY',    ' G yj56Ew5INS!zaqGwYu|;BsJ4L-x6XOX<c0`Mn7X(NBZp<rS10.owzYT2%`x`_9');
define('NONCE_KEY',        ''sUf6g[g f{nl(.HYgl+`|HM8)fnxJC>G<i;uQu:@k;8?L,rGM;ZMYMx-<tVFtw');
define('AUTH_SALT',        'Uy)/v8~T!5R]Q0:0ncT9=z@uk0Az4)y||4?a~dAt1(gWG-)57=e ipgSM7JM_@H0');
define('SECURE_AUTH_SALT', '7p#cW@+/<m`m^C W_q490=9>J z3Mr=H-`1A-aG6Dd9{/,0Y^0iU,&kXJdZv63LN');
define('LOGGED_IN_SALT',   '(m.E>s@Ai=uMsy/qol<ZE0tK:[j>yz-AWA fAi!]G-pTYT?<IQfw 8m:`GzfIviX');
define('NONCE_SALT',       '&-Vzh&` (~UxS 6V%?&{<%J|%p@kM)5i4W_e5[F0LuidQe=g+*t].!5?1]Qy]U1');

/**#@-*/
```

এবং সর্বশেষ Wp-config.php ফাইলটি সেভ করুন।

# ডিরেকটরি লিস্টিং বন্ধ করুন

ওয়ার্ডপ্রেস সাইটের নিরাপত্তার আরেকটা প্রয়োজনীয় বিষয় হল ডিরেকটরি লিস্টিং। একটি সাইট হ্যাক করার আগে একজন হ্যাকার সর্বপ্রথম এটিই দেখে। ডিরেকটরি লিস্টিং চালু আছে কিনা জানার জন্য দেখুন

<http://yoursite.com/wp-content/uploads>

ডিরেকটরি লিস্টিং যদি চালু থাকে, তবে একজন হ্যাকার আপনার সাইটে কি কি ফাইল আছে তা খুব সহজেই বুঝতে পারবে।

| Name                              | Last modified     | Size | Description |
|-----------------------------------|-------------------|------|-------------|
| <a href="#">Parent Directory</a>  |                   | -    |             |
| <a href="#">? wp-config.php</a>   | 06-Jun-2011 11:48 | 3.0K |             |
| <a href="#">? wp-load.php</a>     | 06-Jun-2011 11:49 | 2.4K |             |
| <a href="#">? wp-login.php</a>    | 06-Jun-2011 11:49 | 27K  |             |
| <a href="#">? wp-mail.php</a>     | 06-Jun-2011 11:49 | 7.6K |             |
| <a href="#">? wp-pass.php</a>     | 06-Jun-2011 11:49 | 494  |             |
| <a href="#">? wp-rdf.php</a>      | 06-Jun-2011 11:49 | 224  |             |
| <a href="#">? wp-register.php</a> | 06-Jun-2011 11:49 | 334  |             |

Apache/2.2.3 (CentOS) Server at bluefeed.net Port 80

ডিরেকটরি লিস্টিং বন্ধ করার জন্য আপনার সাইটের .htaccess ফাইলে নিচের কোডটি লিখে সেভ করুন।

```
# disable directory browsing
Options All -Indexes
```

## Forbidden

You don't have permission to access /directory/ on this server.

*Apache/2.2.3 (CentOS) Server at bluefeed.net Port 80*

আপনি চাইলে এই কাজটি সিপ্যানেল দিয়েও করতে পারেন। এই জন্য সিপ্যানেলের Index Manager থেকে No Indexing সিলেষ্ট করে সেভ করুন।

# মুচুন ওয়ার্ডপ্রেসের ভার্সন নাম্বার

কোন সিকিউরিটি সমস্যা দেখা গেলেই ওয়ার্ডপ্রেস চিম ওয়ার্ডপ্রেসের নতুন ভার্সন বের হয়। তবে কোন সিকিউরিটি সমস্যা দেখা গেলেই হ্যাকাররা তার সুযোগ নেয়। তাই আপনার উচিত আপনি ওয়ার্ডপ্রেসের কোন ভার্সন ব্যবহার করছেন তা ভিজিটর থেকে লুকিয়ে রাখা। কিভাবে ওয়ার্ডপ্রেস সাইটের ভার্সন নাম্বার লুকিয়ে রাখা যায়? এর জন্য আপনার সাইটের যেই থিমটি একটিভ আছে সেই থিমের functions.php ফাইলের একদম নিচে উল্লেখিত কোডটুকু পেস্ট করে সেভ করুন।

```
// remove version number from head & feeds
function disable_version() { return ""; }
add_filter('the_generator','disable_version');
remove_action('wp_head', 'wp_generator');
```



তাহলেই আপনার সাইটের হোমপেজ ও ফীড থেকে ওয়ার্ডপ্রেস ভার্সন নাম্বার লুকানো থাকবে। এতে করে কোন একটি ওয়ার্ডপ্রেস ভার্সনে যদি কোন সমস্যা থেকে থাকে তাহলেও আপনার সাইটের কোন সমস্যা হবে না। কারণ কেউই জানতে পারবে না আপনি ওয়ার্ডপ্রেসের কোন ভার্সনটি ব্যবহার করছেন।

# হটলিঙ্কিং বন্ধ করুন

এখন আমরা দেখাবো কিভাবে সাইটের ফাইল হটলিঙ্কিং বন্ধ করে সাইটের ব্যান্ডউইডথ বাঁচানো যায়। প্রথমেই জেনে রাখা দরকার যে ফাইল হটলিঙ্ক আসলে কি জিনিস? ফাইল হটলিঙ্কিং দ্বারা বুঝায় যে, কোন সাইট তাদের সার্ভারে কোন ফাইল আপলোড না করেই অন্য কোন সাইট থেকে লিঙ্কিং করে ব্যবহার করাকে। এতে করে তাদের সাইটের ব্যান্ডউইডথ কম খরচ হবে। আপনার সাইটের ফাইল যদি অন্য কোন সাইট হটলিঙ্ক করে, তাহলে আপনার সাইট ভিজিট না করা সত্ত্বেও আপনার সাইটের অনেক ব্যান্ডউইডথ খরচ হয়ে যাবে। তাহলে কিভাবে বন্ধ করবেন হটলিঙ্কিং?



প্রথমেই আপনার সাইটের .htaccess ফাইলটি ওপেন করে নিচের কোডটুকু পেস্ট করুন।

```
# HOTLINK PROTECTION - by BDTECHZONE LLC
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{HTTP_REFERER} !$  

RewriteCond %{REQUEST_FILENAME} -f  

RewriteCond %{REQUEST_FILENAME} \.(gif|jpe?g?|png)$ [NC]
RewriteCond %{HTTP_REFERER} !^https?:\/\/([^.]+\.)?bdtechzone\. [NC]
RewriteRule \.(gif|jpe?g?|png)$ - [F,NC,L]

</IfModule>
```

এবার ৭ম লাইনের bdtechzone এর স্থানে আপনার আপনার ডোমেইন নেম লিখুন, শুধুমাত্র ডোমেইন নেম লিখুন ডোমেইনের এক্সটেনশন নয়। যদি আপনার সাইটের নাম amarspot.com হয় তবে শুধু মাত্র amarspot লিখুন। এবার .htaccess ফাইলটি সেভ করুন, তাহলেই আপনার সাইটের হটলিঙ্কিং বন্ধ হয়ে যাবে। আপনার সাইট ছাড়া অন্য কোন সাইট আপনার ফাইল ব্যবহার করতে পারবে না।

এই কাজটি আপনি সিপ্যানেল দ্বারাও করতে পারেন। এর জন্য সিপ্যানেলের সিকিউরিটি ট্যাব  
থেকে HotLink Protection এ ক্লিক করুন। তারপর যেসব সাইটকে হটলিঙ্কের অনুমতি দিবেন  
সেসব সাইটের নাম লিখে সাবমিট বাটনে ক্লিক করুন। তবে .htaccess ফাইল দ্বারা হটলিঙ্কিং বন্ধ  
করা আপনার কাছে সিপ্যানেল থেকে সহজ মনে হবে।

---

# বন্ধ করুন অটোমেটিক স্পাম

স্পাম কথাটি শুনলেই কেমন জানি লাগে। অনেক ইউজার আছে যারা আপনার সাইট ভিজিট করবে আর স্পাম করে চলে যাবে। তবে অটোমেটিক স্পামের কাছে এসব কিছুই নয়। বিভিন্ন বট ব্যবহার করে তারা কয়েক মিনিটেই আপনার সাইটে হাজার হাজার স্পাম করতে পারে। আসুন জেনে নেই



কিভাবে এই অটোমেটিক স্পাম বন্ধ করা যায়? প্রথমেই আপনার ওয়ার্ডপ্রেস সাইটের রুট ফোল্ডারে প্রবেশ করে .htaccess ফাইলটি ওপেন করে নিচের কোডটুকু পেস্ট করুন।

```
# BLOCK NO-REFERRER SPAM - by BDTechZone
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
RewriteCond %{HTTP_REFERER} !.*bdtechzone.com.* [NC]
RewriteCond %{REQUEST_URI} /wp\-comments\-\post\.php [NC]
RewriteRule .* - [F,NC,L]
</IfModule>
```

এবার শুষ্ঠি লাইনের bdtechzone.com এর স্থানে আপনার ডোমেইন নেম লিখে সেভ করুন,  
তাহলেই আপনার সাইট অটোমেটিক স্পাম থেকে মুক্তি পাবে।

- অটোমেটিক স্পাম বন্ধ হয়েছে কিনা দেখতে [botsvsbrowsers.com](http://botsvsbrowsers.com) এ  
গিয়ে <http://www.yourdomain.com/wp-comments-post.php> লিখে সেভ রিকোয়েস্ট বাটনে  
ক্লিক করুন।

<http://www.botsvsbrowsers.com/SimulateUserAgent.asp>

The screenshot shows the 'botsvsbrowsers.com' tool interface. At the top, there are fields for 'Request Type' (set to 'POST') and 'Preview Resolution' (Width: 800 pixels, Height: 600 pixels). Below these are fields for 'URL' (containing 'http://www.bdtechzone.com/wp-comments-post.php') and a 'Send Request' button. Under 'Site Preview', detailed request headers are listed: Method: POST, Request Status: 404 : Not Found, Content-Length: bytes (~k), Content-Type: text/html; charset=UTF-8, and Server: nginx admin. A note below states 'Proxy access not allowed'.

অটোমেটিক স্পাম বন্ধ হয়ে গেলে উপরের মত ছবি দেখতে পাবেন।

# খারাপ বট এক্সেস বন্ধ করুন

---

বিভিন্ন বট দ্বারা আজকাল প্রায়ই ওয়ার্ডপ্রেস সাইট আক্রমণ করা হয়। ওয়ার্ডপ্রেস সাইটকে নিরাপদ রাখতে অবশ্যই এই বট এক্সেস বন্ধ রাখা উচিত। তাহলে কিভাবে খুব সহজেই খারাপ বট এক্সেস বন্ধ করা যায়? এর জন্য আপনার ওয়ার্ডপ্রেস সাইটের রুট ফোল্ডারের .htaccess ফাইলটি ওপেন করে নিচের কোডটুকু পেস্ট করুন।

```
# BLOCK BAD BOTS
```

```
<IfModule mod_setenvif.c>
```

```
SetEnvIfNoCase User-Agent ^$ keep_out
```

```
SetEnvIfNoCase User-Agent (casper|cmsworldmap|diavol|dotbot) keep_out
```

```
SetEnvIfNoCase User-Agent (flickr|ja_archiver|jakarta|kmccrew) keep_out
```

```
SetEnvIfNoCase User-Agent (libwww|planetetwork|pycurl|skygrid) keep_out
```

```
SetEnvIfNoCase User-Agent (purebot|comodo|feedfinder) keep_out
```

```
<Limit GET POST PUT>
```

```
Order Allow,Deny
```

```
Allow from all
```

```
Deny from env=keep_out
```

```
</Limit>
```

```
</IfModule>
```

সর্বশেষে .htaccess ফাইলটি সেভ করুন। তাহলেই আপনার ওয়ার্ডপ্রেস সাইটটি খারাপ বট এক্সেস থেকে বন্ধ হয়ে যাবে।

# ফায়ারওয়াল

---

এই সামান্য কিছু কোড আপনার সাইটকে করে তুলবে অনেক নিরাপদ। খারাপ ইউজার এজেন্ট , খারাপ আই.পি সহ আনওয়ান্টেড ইউজারের অ্যাক্সেস আপনার সাইট থেকে বন্ধ করে দেওয়া হবে এই কোড দ্বারা। এর জন্য প্রথমেই আপনার সাইটের রুট ফোল্ডারের .htaccess ফাইলটি ওপেন করে নিচের কোডটুকু পেস্ট করুন।

```
# 5G FIREWALL

# 5G:[QUERY STRINGS]
<IfModule mod_rewrite.c>

RewriteEngine On

RewriteBase /

RewriteCond %{QUERY_STRING} (environ|localhost|mosconfig|scanner) [NC,OR]

RewriteCond %{QUERY_STRING} (menu|mod|path|tag)\=\.?/? [NC,OR]

RewriteCond %{QUERY_STRING} boot\.ini [NC,OR]

RewriteCond %{QUERY_STRING} echo.*kae [NC,OR]

RewriteCond %{QUERY_STRING} etc/passwd [NC,OR]

RewriteCond %{QUERY_STRING} \=\\%27$ [NC,OR]

RewriteCond %{QUERY_STRING} \=\\\$ [NC,OR]

RewriteCond %{QUERY_STRING} \.\./ [NC,OR]

RewriteCond %{QUERY_STRING} \: [NC,OR]

RewriteCond %{QUERY_STRING} \\ [NC,OR]

RewriteCond %{QUERY_STRING} \\] [NC]

RewriteRule .* - [F]

</IfModule>

# 5G:[USER AGENTS]
<IfModule mod_setenvif.c>
```

```
SetEnvIfNoCase User-Agent ^$ keep_out
SetEnvIfNoCase User-Agent (casper|cmsworldmap|diavol|dotbot)  keep_out
SetEnvIfNoCase User-Agent (flickylia_archiver|jakarta|kmccrew) keep_out
SetEnvIfNoCase User-Agent (libwww|planetnetwork|pycurl|skygrid)  keep_out
<Limit GET POST PUT>
Order Allow,Deny
Allow from all
Deny from env=keep_out
</Limit>
</IfModule>
```

```
# 5G:[REQUEST STRINGS]
<IfModule mod_alias.c>
RedirectMatch 403 (https?|ftp|php)\://
RedirectMatch 403 /(cgi|https?|ima|ucp)/
RedirectMatch 403 (=\\'|=\\%27|\\'/?|).css\()$ 
RedirectMatch 403 (,|//|)+|/,|{\0}\|\(\.\.\.|+|+|\\)
RedirectMatch 403 \.(cgi|asp|aspx|cfg|dll|exe|jsp|mdb|sql|ini|rar)$
RedirectMatch 403 /(contac|fpw|install|pingserver|register)\.php
RedirectMatch 403 (base64|crossdomain|localhost|wwwroot)
RedirectMatch 403 (eval\(|\_\_vti\_|\\(null\)|echo.*kae)
RedirectMatch 403 \.well-known/host\.-meta
RedirectMatch 403 /function\.\.array\.-rand
RedirectMatch 403 \)\;\$\((this)\)\.html\(
RedirectMatch 403 proc/self/environ
RedirectMatch 403 msnbot\.htm\)\.\_
RedirectMatch 403 /ref\.\.outcontrol
RedirectMatch 403 com\_\_cropimage
RedirectMatch 403 indonesia\.\.htm
```

```
RedirectMatch 403 \{$itemURL\}
```

```
RedirectMatch 403 function()\()
```

```
RedirectMatch 403 labels.rdf
```

```
</IfModule>
```

```
# 5G:[BAD IPS]
```

```
<Limit GET POST PUT>
```

```
Order Allow,Deny
```

```
Allow from all
```

```
Deny from 184.56.246.23
```

```
Deny from 195.10.218.132
```

```
Deny from 208.91.57.65
```

```
Deny from 209.190.3.218
```

```
Deny from 64.15.156.15
```

```
Deny from 86.175.86.170
```

```
Deny from 91.121.
```

```
Deny from 41.206.13.3
```

```
Deny from 207.177.225.66
```

```
Deny from 137.82.182.121
```

```
Deny from 79.125.81.232
```

```
Deny from 24.66.27.191
```

```
Deny from 216.40.231.210
```

```
Deny from 151.42.146.98
```

```
Deny from 77.191.130.244
```

```
Deny from 115.79.13.174
```

```
Deny from 84.189.184.170
```

```
</Limit>
```

কোন এডিট করার ঝামেলা নেই, এবার .htaccess ফাইলটি সেভ করুন। তাহলেই আপনার সাইটটি একটি ভার্চুয়াল ফায়ারওয়াল দ্বারা নিরাপদ হয়ে যাবে। কোড দেখতে সমস্যা হলে দেখুন

[www.bdtechzone.com/wp-security/1107](http://www.bdtechzone.com/wp-security/1107)

যেহেতু ফায়ারওয়ালের কোডটি অনেক বড় তাই এই কোড গুলো ইবুকে ভেঙ্গে তথা করাপ্টেড হয়ে যেতে পারে তাই এই কোডটি উপরের লিঙ্কটি ভিজিট করে কপি করুন।

# বন্ধ করুন প্রক্সি এক্সেস

---

আজকাল প্রক্সি সাইট দিয়ে অনেক ওয়ার্ডপ্রেস সাইট অ্যাটাক করা হয়। তাই আমাদের সকলের উচিত যে এই প্রক্সি এক্সেস বন্ধ করা। তাই এখন আমরা দেখাবো কিভাবে সাইটে প্রক্সি এক্সেস বন্ধ করতে হয়। এর জন্য প্রথমেই নিচের কোডটুকু আপনার সাইটের রুটের .htaccess ফাইলে নিচের কোডটুকু পেস্ট করুন। এবার .htaccess ফাইলটি সেভ করুন।

```
# BLOCK PROXY VISITS

<IfModule mod_rewrite.c>

RewriteEngine on

RewriteCond %{HTTP:VIA}      !^$ [OR]
RewriteCond %{HTTP:FORWARDED} !^$ [OR]
RewriteCond %{HTTP:USERAGENT_VIA} !^$ [OR]
RewriteCond %{HTTP:X_FORWARDED_FOR} !^$ [OR]
RewriteCond %{HTTP:PROXY_CONNECTION} !^$ [OR]
RewriteCond %{HTTP:XPROXY_CONNECTION} !^$ [OR]
RewriteCond %{HTTP:HTTP_PC_REMOTE_ADDR} !^$ [OR]
RewriteCond %{HTTP:HTTP_CLIENT_IP}   !^$

RewriteRule .* - [F]

</IfModule>
```

তারপর নিচের কোডটুকু আপনি যেই থিম ব্যবহার করছেন তার header.php এর সর্ব উপরে  
পেস্ট করুন।

```
<?php if(@fsockopen($_SERVER['REMOTE_ADDR'], 80, $errstr, $errno, 1)) die("Proxy access  
not allowed"); ?>
```

এবং সর্বশেষে header.php ফাইলটি সেভ করুন।

প্রক্ষি এক্সেস বন্ধ হয়েছে কিনা দেখতে [inCloak](#) গিয়ে আপনার সাইটের এড্রেস লিখে এন্টার চাপুন।  
যদি সঠিক ভাবে বন্ধ হয়ে থাকে তাহলে Proxy access not allowed লিখা উঠবে।

<https://incloak.com>

# বন্ধ করুন SQL injection

---

ওয়ার্ডপ্রেস ইউজারদের কাছে এক আতঙ্কের নাম হল SQL injection. এর দ্বারা অনেক বড় বড় সাইটও হ্যাক হচ্ছে। তাই ওয়ার্ডপ্রেস সাইট সিকিউর করতে আপনাকে অবশ্যই SQL injection বন্ধ করতে হবে। এখন আপনাদের দেখাবো কিভাবে খুব সহজেই SQL injection বন্ধ করা যায়। প্রথমেই আপনার রুট ফোল্ডারের .htaccess ফাইলটি ওপেন করে নিচের কোডটুকু পেস্ট করুন।

```
# protect from sql injection

Options +FollowSymLinks

RewriteEngine On

RewriteCond %{QUERY_STRING} (\<|\%3C).*script.*(\>|\%3E) [NC,OR]

RewriteCond %{QUERY_STRING} GLOBALS(=|[|%\{0-9A-Z\}{0,2}) [OR]

RewriteCond %{QUERY_STRING} _REQUEST(=|[|%\{0-9A-Z\}{0,2})

RewriteRule ^(.*)$ index.php [F,L]
```

এবার .htaccess ফাইলটি সেভ করুন।

ব্যাস, তাহলেই আপনার সাইট SQL injection থেকে নিরাপদ হয়ে যাবে। যদিও খুব সহজ কাজ, তবুও এটি আপনার সাইটকে অনেক সিকিউর করে তুলবে।

# স্পন্সর

---



[আমারস্পট.কম](http://www.amarspot.com) নিয়ে এলো আপনাদের জন্য হাজার হাজার ইবুক সমাহার

ডাউনলোড করতে এখনই ভিজিট করুন

[www.amarspot.com/ebook](http://www.amarspot.com/ebook)

# থিম ও প্লাগিন নিরপত্তা

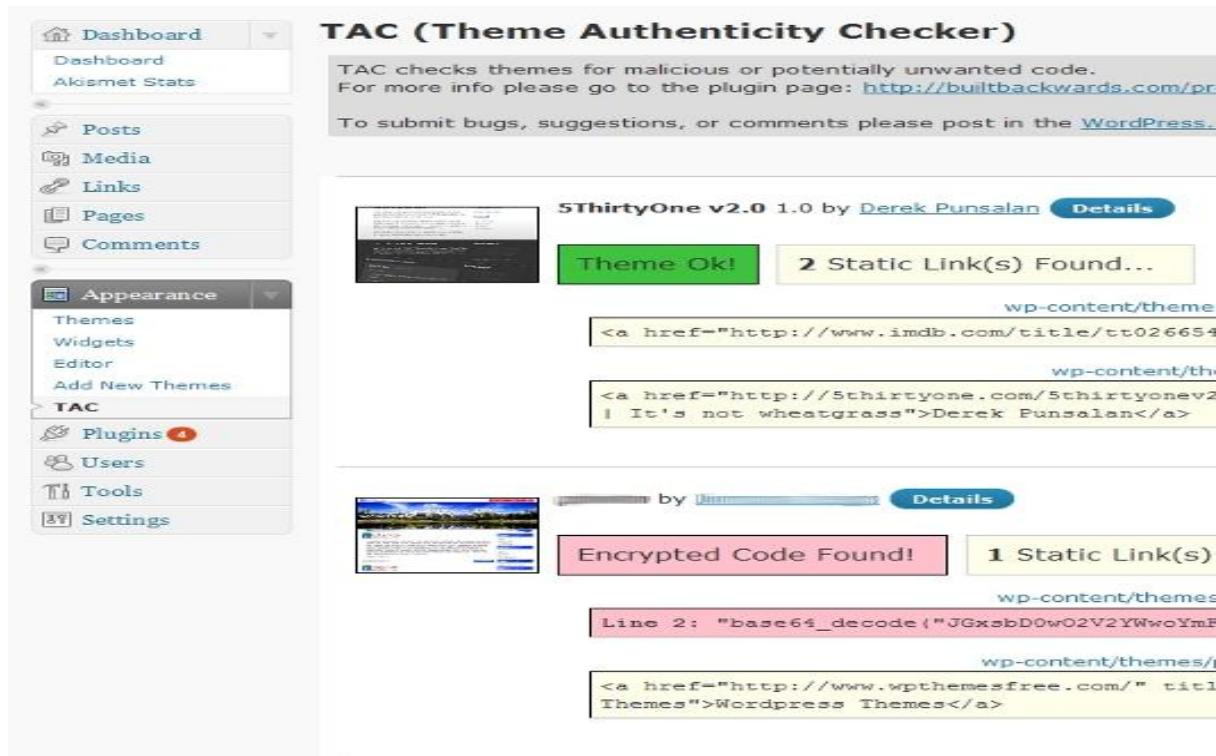
থিম ও প্লাগিন ব্যবহার করার জন্য [wordpress.org](http://wordpress.org) এর থিম ও প্লাগইন ডিরেক্টরি ব্যবহার করুন।

<http://wordpress.org/extend/themes/>

<http://wordpress.org/extend/plugins/>

তবে কখনো প্রিমিয়াম থিম ও প্লাগইন ফ্রীতে ডাউনলোড করে ব্যবহার করবেন না। এসব থিম ও প্লাগিন আপনার সাইটের অনেক ক্ষতি করতে পারে। আর যেকোনো থিম ব্যবহার করার আগে নিচের প্লাগিনটি দিয়ে থিমটি চেক করে নিন। যদি কোন খারাপ কোড পেয়ে যান তবে তা রিমুভ করে নিন।

<http://wordpress.org/extend/plugins/tac/>



# পারমালিঙ্ক

কখনো ওয়ার্ডপ্রেসে ডিফল্ট পারমালিঙ্ক ?p=123 ব্যবহার করবেন না। এটি থেকে বিরত থাকুন।

The screenshot shows the 'Permalink Settings' page in WordPress. At the top, there's a note about the benefits of using permalinks over query strings. Below that, the 'Common Settings' section lists several options:

- ডিফল্ট (Default): <http://www.bdtechzone.com/?p=123>
- Day and name: <http://www.bdtechzone.com/2013/04/14/sample-post/>
- Month and name: <http://www.bdtechzone.com/2013/04/sample-post/>
- সংখ্যাসূচক (Numeric): <http://www.bdtechzone.com/archives/123>
- Post name** (highlighted with a red border): <http://www.bdtechzone.com/sample-post/>
- Custom Structure: [%postname%](http://www.bdtechzone.com)

Below this, there's a 'Custom' section for categories and tags:

If you like, you may enter custom structures for your category and tag URLs here. For example, using `topics` as your category base would make your category links like <http://example.org/topics/uncategorized/>. If you leave these blank the defaults will be used.

বিভাগ ভিত্তি: [empty input field]

ট্যাগ ভিত্তি: [empty input field]

**পরিবর্তন সংরক্ষণ কর** (button highlighted with a red border)

এই ক্ষেত্রে সেটিংস ট্যাব থেকে পারমালিঙ্কে যান। post name এ ক্লিক করে সেভ করুন।

# মনিটর করুন আপনার ওয়ার্ডপ্রেস সাইট

হ্যাকারদের দ্বারা প্রায়ই ওয়ার্ডপ্রেস সাইট আক্রমণ করা হয়। তাই আমি রেকমেন্ড করবো সবসময় ওয়ার্ডপ্রেস আপনার সাইটের উপর নজর রাখার জন্য। ওয়ার্ডপ্রেস সাইট মনিটর করার জন্য এখন আমি আপনাদেরকে একটি প্লাগিনের সাথে পরিচয় করিয়ে দেব।

## প্লাগিন ইনস্টল

এর জন্য প্রথমেই আপনাকে ThreeWP Activity Monitor প্লাগিনটি ইনস্টল করতে হবে। প্লাগিনটি ইনস্টল করতে [এখানে](#) ক্লিক করুন। ইনস্টল করা হয়ে গেলে প্লাগিনটি একটিভ করে নিন।

<http://wordpress.org/extend/plugins/threewp-activity-monitor/>

## কার্যপ্রণালী

|  |                        |  |
|--|------------------------|--|
|  | 2013-04-30<br>14:38:58 | marsxxzaa tried to log in to <a href="#">বিডিটেকজোন.কম</a><br>Password tried qjuc5cS2aa<br>IP ks3318954.kimsufi.com   5.135.165.147<br>User agent Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2) Gecko/20100308 Ubuntu/10.04 (lucid) Firefox/3.6 GTB7.1 |
|  | 2013-04-30<br>01:02:51 | marsxxzaa tried to log in to <a href="#">বিডিটেকজোন.কম</a><br>Password tried qjuc5cS2aa<br>IP ks3318954.kimsufi.com   5.135.165.147<br>User agent Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.2a1pre) Gecko/20110324 Firefox/4.2a1pre                    |
|  | 2013-04-30<br>00:02:38 | marsxxzaa tried to log in to <a href="#">বিডিটেকজোন.কম</a><br>Password tried qjuc5cS2aa<br>IP ks3318954.kimsufi.com   5.135.165.147<br>User agent Mozilla/5.0 (X11; Linux i686 on x86_64; rv:12.0) Gecko/20100101 Firefox/12.0                             |
|  | 2013-04-29<br>21:37:32 | nayem logged in to <a href="#">বিডিটেকজোন.কম</a><br>IP<br>User agent Mozilla/5.0 (Windows NT 6.1; rv:21.0)   |
|  | 2013-04-29<br>20:47:18 | marsxxzaa tried to log in to <a href="#">বিডিটেকজোন.কম</a><br>Password tried qjuc5cS2aa<br>IP ks3318954.kimsufi.com   5.135.165.147<br>User agent Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; ko; rv:1.9.1b2) Gecko/20081201 Firefox/3.1b2             |

## চিত্রঃ বিডিটেকজোনের একটিভিটি

আপনার সাইটের একটিভিটি দেখতে Dashboard থেকে Activity Monitor ট্যাবে ক্লিক করুন।

নোটঃ একটিভিটি ষ্টোর হতে ২৪ঘণ্টা সময় দিন।

# লগিন পেজে এরর বার্তা প্রদর্শন বন্ধ করুন

যখন আপনার ওয়ার্ডপ্রেস সাইটে কেউ প্রবেশ করতে চেষ্টা করে ফেইল করে তখন ইউজার একটি এরর ম্যাসেজ দেখতে পায়। আর এই এরর ম্যাসেজ দ্বারা হ্যাকাররা আপনার সাইট হ্যাক করার পথা পেয়ে যায়। চলুন কথা না বাড়িয়ে দেখে নেই কিভাবে ওয়ার্ডপ্রেস সাইটের লগিন পেজ থেকে এরর বার্তা প্রদর্শন বন্ধ করা যায়।



এর জন্য প্রথমেই আপনার ওয়ার্ডপ্রেস সাইটে ব্যবহারিত থিমের functions.php ফাইল ওপেন করে শেষের ?> ট্যাগের আগের লাইনে নিচের কোডটুকু পেস্ট করুন।

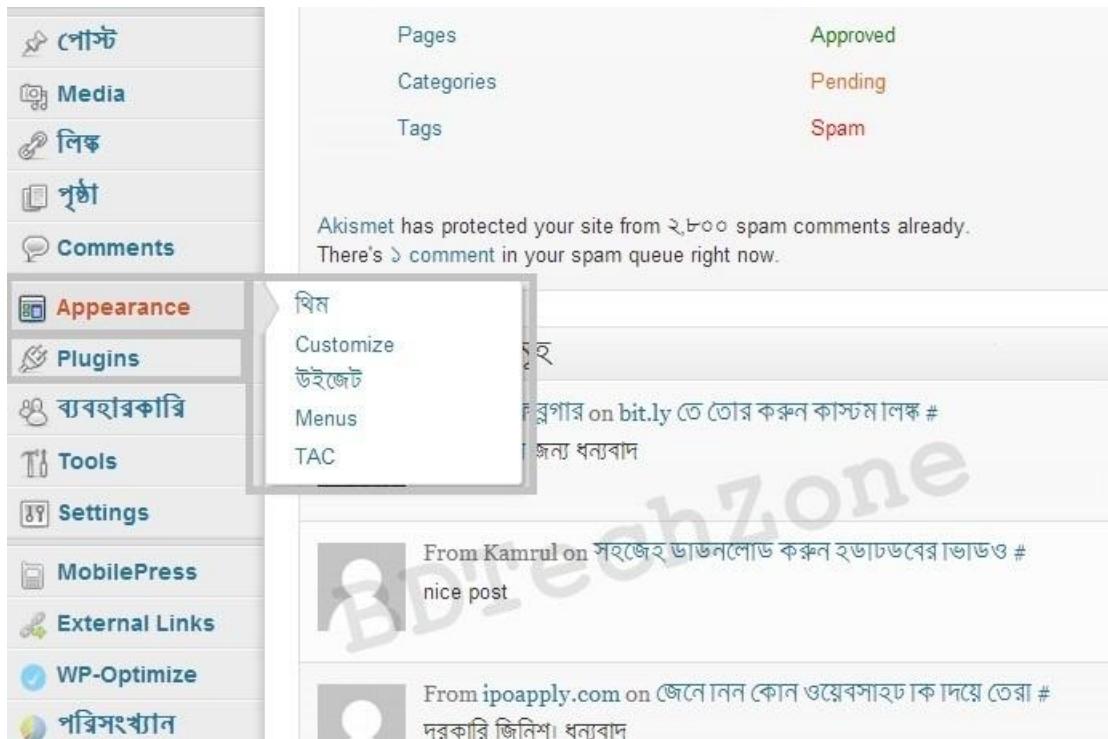
```
add_filter('login_errors',create_function('$a', "return null;"));
```

সর্বশেষ functions.php ফাইলটি সেভ করুন তাহলেই আপনার সাইটের লগিন পেজে এরর ম্যাসেজ প্রদর্শন বন্ধ হয়ে যাবে।

এরর ম্যাসেজ প্রদর্শন বন্ধ হয়েছে কিনা জানতে আপনার সাইটের লগিন পেজে গিয়ে ভুল ইউজারনেম ও পাসওয়ার্ড দিয়ে লগিন করতে চেষ্টা করুন।

# থিম ও প্লাগিন এডিট অপশন বন্ধ করুন

আপনার ওয়ার্ডপ্রেস সাইটের ডেশবোর্ড অর্থাৎ এডমিন প্যানেলে যদি কোন হ্যাকার তুকে পড়ে তখন কি করবেন? ভেবে দেখেছেন, কি হবে আপনার সাইটের? হ্যাকার যদি আপনার সাইটের থিম ও প্লাগিন গুলো এডিট করে কোড নষ্ট করে দেয় তাহলে আপনার অনেক সমস্যায় পড়তে হবে।



ছবিতে দেখতে পাচ্ছেন থিম এডিট অপশন দেখেছে না

নোট: ডেশবোর্ড থেকে থিম ও প্লাগিন এডিট করার অপশন রিমুভ করলেও আপনি আপনার সাইটের সিপ্যানেল থেকে থিম ও প্লাগিন এডিট করতে পারেবন।

## থিম ও প্লাগিন এডিট অপশন বন্ধ করবেন

```
/*
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */

/* This file has been intentionally blanked by the developer. */
if (defined('DISALLOW_FILE_EDIT')) {
    die('Sorry, but you do not have permission to edit this file.');
}

/** This tells the WordPress where to look for things. */
require __DIR__ . '/wp-config.php';

define('DISALLOW_FILE_EDIT', true);
```



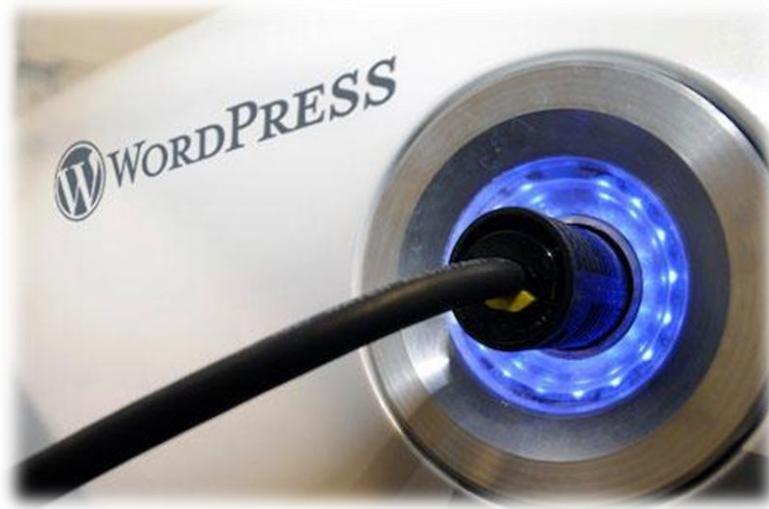
জাস্ট আপনার সাইটের wp-config.php ফাইলে নিচের কোডটুকু অ্যাড করে ফাইলটি সেভ করুন, তাহলেই আপনার সাইটের এডমিন প্যানেল থেকে থিম ও প্লাগিন এডিট অপশন বন্ধ হয়ে যাবে।

```
define('DISALLOW_FILE_EDIT', true);
```

**সিকিউরিটি টিপস:** আপনার সাইটের সি প্যানেল ও ওয়ার্ডপ্রেস এডমিন প্যানেলের পাসওয়ার্ড কখনো এক রাখবেন না।

# কিছু প্রয়োজনীয় সিকিউরিটি প্লাগিন

এখন আপনাদের সামনে কিছু ওয়ার্ডপ্রেস সিকিউরিটি প্লাগিন নিয়ে এলাম, আশা করি এসব প্লাগিন আপনার সাইটের উপকারে আসবে। প্লাগিনগুলো সম্পর্কে তেমন কিছু বললাম না, প্লাগিনগুলো সাইটে ইনস্টল করলেই এদের কাজ বুঝতে পারবেন। প্লাগিনগুলো লাইভ সাইটে ব্যাবহার করার পূর্বে লোকাল সার্ভারে ব্যাবহার করে দেখবেন। তবে একসাথেই সব গুলো প্লাগিন ব্যাবহার করবেন না, যেই প্লাগিনগুলো আপনার ভালো মনে হবে সেই গুলোই ব্যাবহার করুন। মনে রাখবেন বেশি প্লাগিন ব্যবহার করলে আপনার সাইট স্লো হয়ে যেতে পারে।



|   |   |
|---|---|
| 1. <a href="#">AntiVirus</a>                    | 2. <a href="#">Sucuri Security</a>            |
| 3. <a href="#">Limit Login Attempts</a>         | 4. <a href="#">WP-DB-Backup</a>               |
| 5. <a href="#">ThreeWP Activity Monitor</a>     | 6. <a href="#">AskApache Password Protect</a> |
| 7. <a href="#">Wordfence Security</a>           | 8. <a href="#">Better WP Security</a>         |
| 9. <a href="#">WP Security Scan</a>             | 10. <a href="#">Bad Behavior</a>              |
| 11. <a href="#">Block Bad Queries</a>           | 12. <a href="#">Exploit Scanner</a>           |
| 13. <a href="#">BulletProof Security</a>        | 14. <a href="#">WordPress Firewall 2</a>      |
| 15. <a href="#">WordPress File Monitor Plus</a> |   |

# শেষের আগে

---

এই ইবুকে ওয়ার্ডপ্রেস সিকিউরিটির অনেক কিছু নিয়ে আলোচনা করলাম। আশা করি এসব আপনাদের কাজে আসবে। আমরা নিয়মিত ওয়ার্ডপ্রেস সিকিউরিটি নিয়ে লিখে থাকি, আমাদের ব্লগ [বিডিটেকজোন.কমে](http://www.bdtechzone.com/viditechzone) চাইলে ঘুরে আসতে পারেন।

[www.bdtechzone.com/wp-security](http://www.bdtechzone.com/wp-security)

যারা এখনো ওয়ার্ডপ্রেস নিয়ে কাজ করতে পারেন না, তারা দেখতে পারেন আমাদের বেসিক ওয়ার্ডপ্রেস টিউটোরিয়াল

[www.bdtechzone.com/wp-tutorial](http://www.bdtechzone.com/wp-tutorial)

ওয়ার্ডপ্রেসের এডভাঞ্চ টিপস ও ট্রিক জানতে আমারদের এডভাঞ্চ ওয়ার্ডপ্রেস টিউটোরিয়ালও দেখতে পারেন। আশা করি আপনারা উপকৃত হবেন।

[www.bdtechzone.com/tutorial/1143](http://www.bdtechzone.com/tutorial/1143)

- এই ইবুকে ব্যবহার কৃত বিভিন্ন কোড গুলো দেখতে সমস্যা হলে বা যদি কোন কারণে কোড করাপটেড হয়ে যায় তাহলে কোড দেখতে নিচের লিঙ্কটির সাহায্য নিন

[www.bdtechzone.com/tutorial/782](http://www.bdtechzone.com/tutorial/782)

পরবর্তী ইবুকের জন্য আমাদের সাথেই থাকুন, ধন্যবাদ।

সমাপ্ত