

# ওয়ার্ডপ্রেস সিকিউরিটি

সাইফুল ইসলাম



# ওয়ার্ডপ্রেস সিকিউরিটি

সাইফুল ইসলাম

<http://saifulzone.com>

mail: saifulislam@gmail.com

WordPress Security by [Saiful Islam](#) is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License](#).



### ওয়ার্ডপ্রেস সিকিউরিটি কি ?

ওয়েবে সিকিউরিটি শব্দটা অনেক জটিল , কেউ বলে সিকিউরিটি বলে কিছু নেই আবার কেউ বলে এটার কি দরকার। অভিজ্ঞরা সিকিউরিটি নিয়ে অত টেনসন করেন না , কারন ১০০% সিকিউরিটি বলে কোন কিছু নেই। আপনি আপনার ঘরকে যতই তালা চাবি দিয়ে সিকিউর করেন না কেন চোর একদিন না একদিন ঠিকই ঢুকতে পারবে। ওয়ার্ডপ্রেস বর্তমানে সবচেয়ে বেশি ব্যবহৃত CMS , তো এই CMS এ তৈরি সাইট প্রতিনিয়ত হ্যাক হচ্ছে। তাই বলে ভাববেন না যে ওয়ার্ডপ্রেস এর সিকিউরিটি খুবই খারাপ, আসলে সাইটগুলো হ্যাক হয় বেশ কিছু কারনে যেমনঃ প্লাগিন্স , থীম , পাসওয়ার্ড , হোস্টিং, পিসি ইত্যাদির কারনে।

### প্লাগিন্স কিভাবে সাইটের জন্য হুমকি হয়ে দাড়ায় ?

প্লাগিন কারো সাইটের জন্য হুমকি না , কিন্তু কিছু প্লাগিন যেগুলোতে বাগ থাকে সেগুলো আপনার সাইটের জন্য হুমকি স্বরূপ। এই বাগ যুক্ত প্লাগিন ব্যবহার করা যাবে না , আপনি হয়তো বলতে পারেন প্লাগিনে বাগ আছে কিনা কিভাবে বুঝবো ?

আপনার জন্য রয়েছে এই সাইটটি [http://www.exploit-db.com/search/?action=search&filter\\_page=1&filter\\_description=Wordpress&filter\\_exploit\\_text=Wordpress&filter\\_author=&filter\\_platform=0&filter\\_type=6&filter\\_lang\\_id=0&filter\\_port=&filter\\_osvdb=&filter\\_cve=](http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=Wordpress&filter_exploit_text=Wordpress&filter_author=&filter_platform=0&filter_type=6&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve=) এখানে

ওয়ার্ডপ্রেস এর প্লাগিনের বাগ আর Vulnerabilities লিস্ট আছে , দেখে নিন আপনার প্লাগিন এই লিস্টে আছে কিনা ।

এতক্ষন বেশ আজাইরা প্যাচাল পাড়লাম , এবার মূল বিষয়ে যাচ্ছি। এই বইয়ে আমি যা যা নিয়ে আলোচনা করবঃ

১. সেফ ইন্সটলেশন,
২. ফাইল পারমিসন,
৩. brute force থেকে সাইট বাঁচানো,
৪. .htaccess,
৫. BulletProof Security প্লাগিনের ব্যবহার।

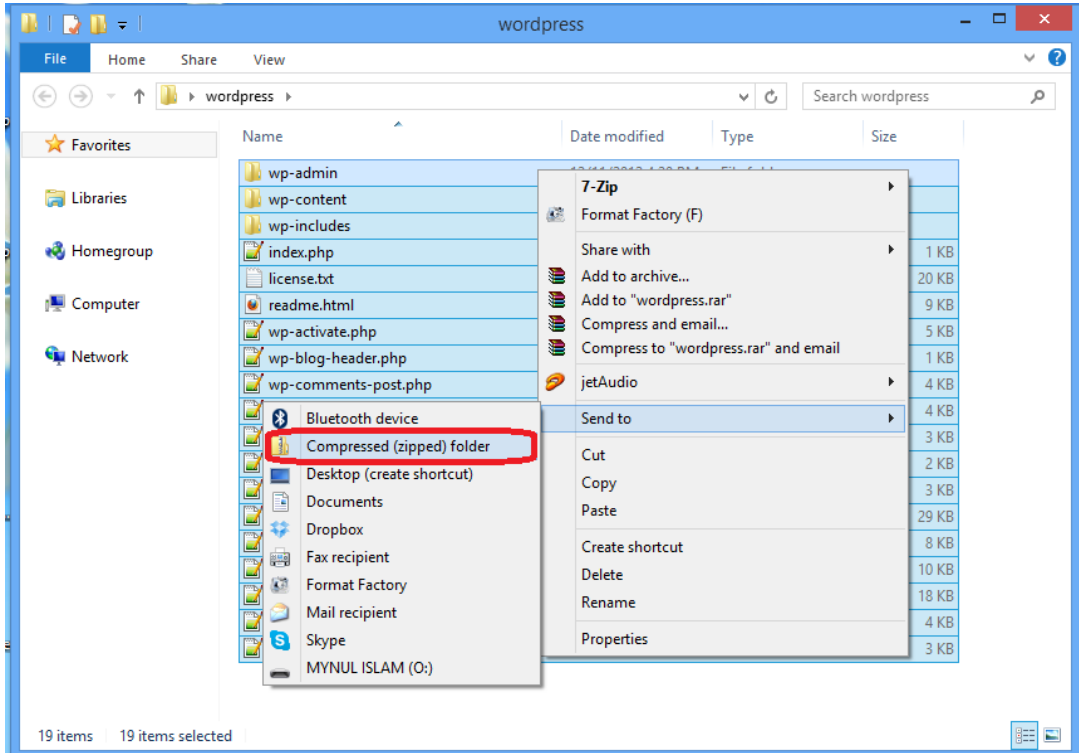
# সেফ ইন্সটলেশন

যা যা করা যাবে নাঃ

১. অটো ইন্সটল স্ক্রিপ্ট ব্যবহার করা যাবে না।
২. ডাটাবেস প্রিফিক্স wp\_ ব্যবহার করা যাবে না।
৩. থার্ডপার্টি সাইট থেকে wordpress নামানো যাবে না।
৪. পুরানো ভার্সন ইন্সটল করা যাবে না।

যেভাবে করতে হবেঃ

১. ইন্সটলেশন সোর্স বানানোঃ প্রথমে আপনি ওয়ার্ডপ্রেস.অরগ থেকে ওয়ার্ডপ্রেস এর লেটেস্ট ভার্সন ডাউনলোড করবেন, তার পর এটা কে আপনার পিসিতে এক্সট্রাক্ট / আনজিপ করবেন। তারপর নিচের মত করে জিপ করুন। এবং যেকোনো নামে সেভ করুন।

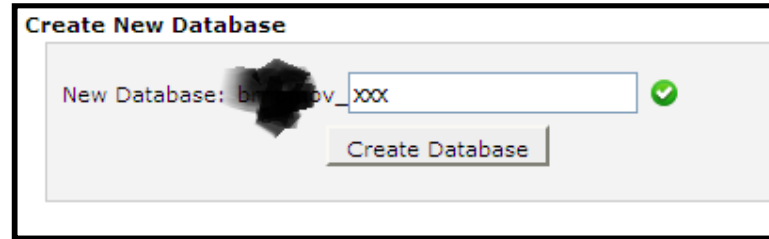


এভাবে ওয়ার্ডপ্রেস জিপ করে সাইটে উঠালে আপনি যে কোনো ডিরেক্টরীতে ওয়ার্ডপ্রেস আনজিপ করতে পারবেন কোন সাব ফোল্ডার ছাড়াই।

## ২. ডাটাবেস ও ডাটাবেস ইউজারঃ

একটা ওয়ার্ডপ্রেস সাইটের মোস্ট ইম্পরট্যান্ট জিনিশ হল ডাটাবেস। অনেকেই ওয়ার্ডপ্রেস ইন্সটল করার সময় অটো ইন্সটলার ব্যবহার করেন এটা পরিহার করতে হবে। ওয়ার্ডপ্রেস ইন্সটলের সময় ম্যনুয়ালি ইন্সটল করা উচিত। ম্যনুয়ালি ইন্সটল করতে হলে আপনাকে একটা ডাটাবেস বানাতে হবে আর একটা ডাটাবেস ইউজার। মনে করুন আপনি একটা ডাটাবেস আর একটা ইউজার বানিয়েছেন, এবার আপনাকে ইউজার কে ডাটাবেস ব্যবহারের অনুমতি দিতে হবে। নিচ্ছে দেখুন ডাটাবেস > ইউজার > ইউজার কে ডাটাবেস ব্যবহারের অনুমতি > কি কি অনুমতি দেয়া হয়েছে তা।

স্টেপ-১ (ডাটাবেস বানানো)

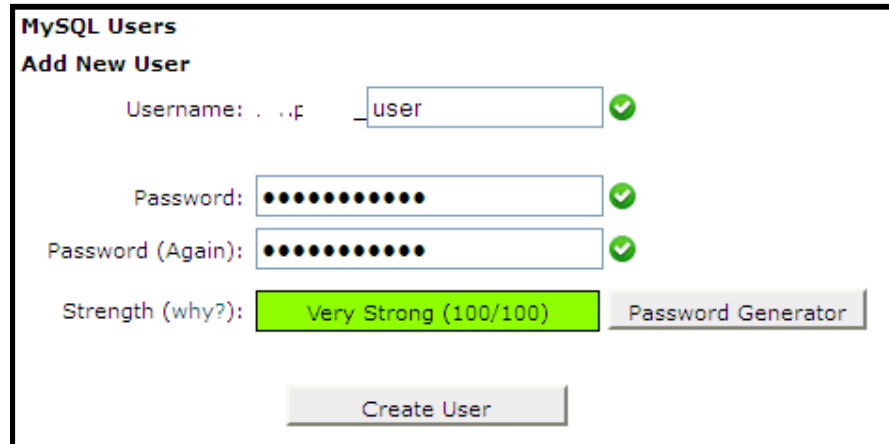


**Create New Database**

New Database: b... v\_XXX ✓

Create Database

স্টেপ-২ (ইউজার বানানো)



**MySQL Users**

**Add New User**

Username: user ✓

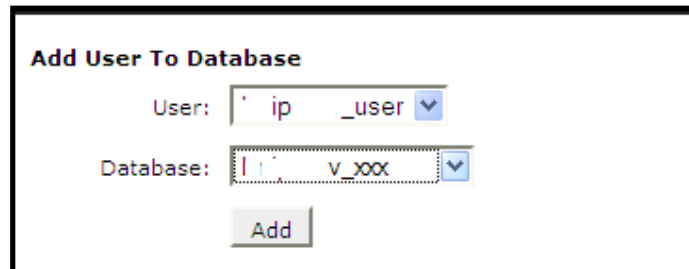
Password: ..... ✓

Password (Again): ..... ✓

Strength (why?): Very Strong (100/100) Password Generator

Create User

স্টেপ-৩ (ইউজার কে ডাটাবেস ব্যবহারের অনুমতি দেওয়া)



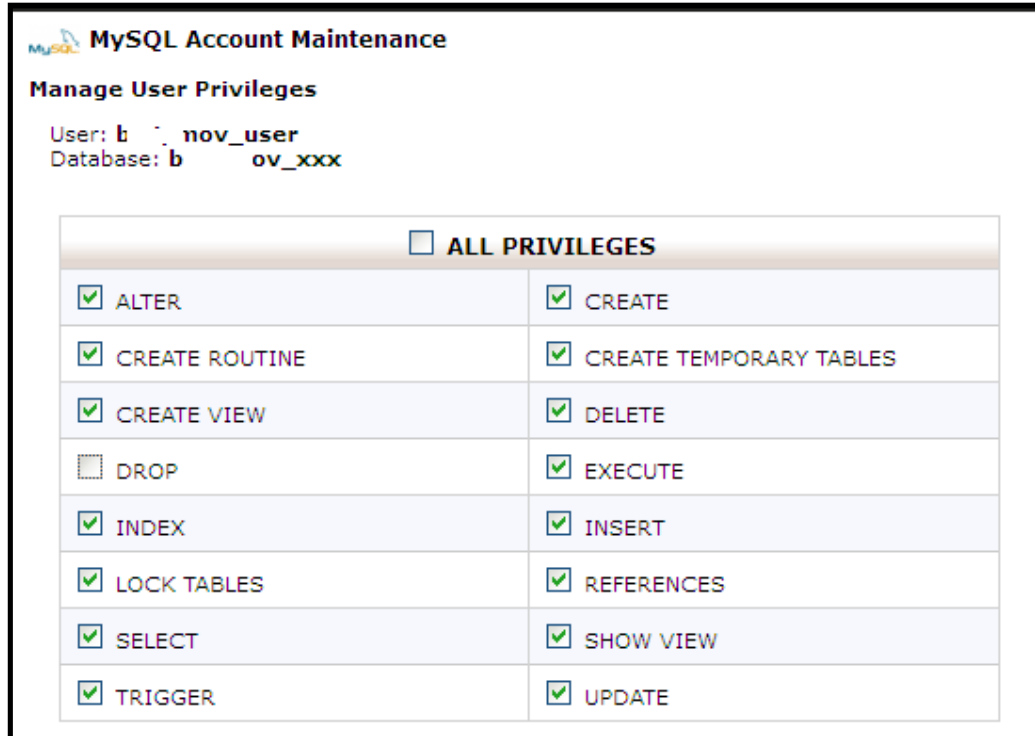
**Add User To Database**

User: ip...\_user ▼

Database: v\_XXX ▼

Add

স্টেপ-৪ (কি কি অনুমতি দেয়া হয়েছে তা ঠিক করে দেওয়া)

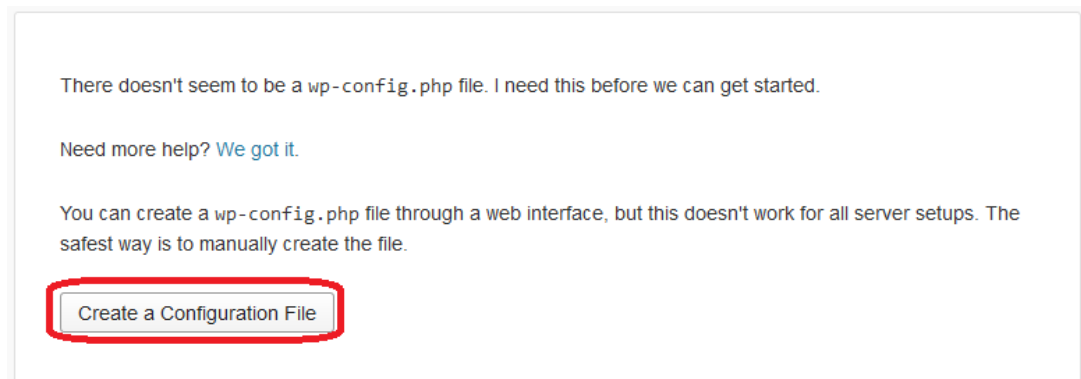


The screenshot shows the 'MySQL Account Maintenance' interface for managing user privileges. The user is 'b...nov\_user' and the database is 'b...ov\_xxx'. A table lists various privileges with checkboxes. The 'DROP' privilege is unchecked, while all others are checked.

<input type="checkbox"/> ALL PRIVILEGES	
<input checked="" type="checkbox"/> ALTER	<input checked="" type="checkbox"/> CREATE
<input checked="" type="checkbox"/> CREATE ROUTINE	<input checked="" type="checkbox"/> CREATE TEMPORARY TABLES
<input checked="" type="checkbox"/> CREATE VIEW	<input checked="" type="checkbox"/> DELETE
<input type="checkbox"/> DROP	<input checked="" type="checkbox"/> EXECUTE
<input checked="" type="checkbox"/> INDEX	<input checked="" type="checkbox"/> INSERT
<input checked="" type="checkbox"/> LOCK TABLES	<input checked="" type="checkbox"/> REFERENCES
<input checked="" type="checkbox"/> SELECT	<input checked="" type="checkbox"/> SHOW VIEW
<input checked="" type="checkbox"/> TRIGGER	<input checked="" type="checkbox"/> UPDATE

এবার আশা যাক মূল কথাতে, ইউজারকে ডাটাবেসে কি কি করার অনুমতি দেওয়া হবে। ইউজারকে ডাটাবেসে সবকিছু করার অনুমতি দেওয়া হবে কেবল ডটা DROP করার অনুমতি ব্যাতিত। কারণ কেউ আপনার সাইটে ঢুকে গেলে সে কনফিগ ফাইল থেকে ডাটাবেস ইনফো নিয়ে ডাটাবেস ডাম্প করে দেবে। সো যদি ইউজারকে ডাম্প করার অনুমতি না দেওয়া হয় তাহলে হ্যাকার অতি তাড়াতাড়ী ডাটাবেস ডাম্প করতে পারবে না। আর কোন হ্যাকারই বসে বসে একটা একটা করে ডাটা ডিলেট করবে না। এতে আপনার ডাটাবেস অনেকটা সিকিউর থাকবে। চাইলে ডিলেট আনচেক করে দিতে পারেন, তবে এটা করে দিলে নিজের কাজ করতে সমস্যা হবে।

**৩.ইন্সটলেশনঃ** ১ম ধাপে বানানো জীপ ফাইলটি সি প্যানেলের ফাইল ম্যানেজার অথবা ftp দিয়ে আপলোড করুন, আপলোড হয়ে গেলে জপফাইলটি আনজিপ করুন। এবার ব্রাউজারে সাইট এর url



The screenshot shows a WordPress installation error message. It states that there is no wp-config.php file and provides a link for more help. A button labeled 'Create a Configuration File' is highlighted with a red rectangle.


There doesn't seem to be a wp-config.php file. I need this before we can get started.

Need more help? [We got it.](#)

You can create a wp-config.php file through a web interface, but this doesn't work for all server setups. The safest way is to manually create the file.

[Create a Configuration File](#)

ওপেন করুন , সেখানে ওয়ার্ডপ্রেস আপনার কাছে ইন্সটলেশন ইনফোর জন্য একটি ফর্ম আসবে।  
ছবির মত করে ইন্সটল করুন।




Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

**If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.**

In all likelihood, these items were supplied to you by your Web Host. If you do not have this information, then you will need to contact them before you can continue. If you're all ready...

Let's go!



Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="এখানে ডাটাবেসের নাম"/>	The name of the database you want to run WP in.
User Name	<input type="text" value="এখানে ডাটাবেস ব্যবহারকারীর নাম"/>	Your MySQL username
Password	<input type="text" value="এখানে ডাটাবেসের পাসওয়ার্ড"/>	...and your MySQL password.
Database Host	<input type="text" value="localhost"/>	এখানে ডাটাবেস হোস্ট , বাই ডিফল্ট এটা localhost থাকে You should be able to get this info from your web host, if localhost does not work.
Table Prefix	<input type="text" value="sytR_iYt"/>	If you want to run multiple WordPress installations in a single database, change this.

এটা ডাটাবেস প্রিফিক্স র্যান্ডম লেটার দিয়ে লিখুন

Submit

এরপর এডমিন লগিন ডিটেইলস দিয়ে সেটাপ কমপ্লিট করুন। অনেকে সাজেসন দিয়ে থাকেন যে সাল্ট জেনারেট করে কনফিগে দিতে , এটার তেমন একটা প্রয়োজন হয় না , কারন ওয়ার্ডপ্রেস ইন্সটলের সময় এটা অটোমেটিক জেনারেট হয়।

## ফাইল পারমিসন

ফাইল পারমিসন একটা ফাইলে / ফোল্ডারে ব্যবহারকারী অথবা মালিক কি করতে পারবে তা ঠিক করে দেয়, মনে করুন আপনার সাইটের একটা পিএইচপি ফাইলে আপনি রাইট এক্সেস পাবলিক করে রাখলেন, সেক্ষেত্রে যেকোনো এক্সটোরনান এপ / স্ক্রিপ্ট দিয়ে আপনার পিএইচপি ফাইলের যায়গায় একটা শেল ডুকিয়ে আপনার সাইটের ১২টা বাজাতে পারবে। তাহলে দাড়াচ্ছে যে ফাইল পারমিসন ফেলনা জিনিশ নয়। সার্ভারে ফাইল পারমিসন গুলো তিন সংখ্যার একটা নাম্বার দিয়ে প্রকাশ করা হয়ে থাকে। আমি এখানে চেষ্টা করব বেসিক জিনিশগুলো দেখাতে।

- **Read**—ভ্যালু- 4 ইউজারকে রিড করার পারমিশন দেবে।
- **Write**—ভ্যালু- 2 ইউজারকে রাইট করার পারমিশন দেবে।
- **eXecute**—ভ্যালু 1 ইউজারকে রিড/রাইট/ডিলেট করার পারমিশন দেবে।

তাহলে খেয়াল করা যাক কিভাবে ফাইলের পারমিশনের নাম্বারটা পাওয়া যায়।

একটা ফাইলের পারমিশন গঠিত হয় ৩ টি সংখ্যার যোগফল পাশাপাশি সাজিয়ে। মনে করুন Owner এর ফাইল পারমিশন গঠিত হয় r+w+x এর যোগফলের মাধ্যমে। খেয়াল করলে দেখতে পারবেন আমরা উপরে উল্লেখিত ভ্যালু গুলো ব্যবহার করেছি পারমিশন দেয়ার জন্য। তাহলে r+w+x এর যোগফল পেলাম ৭ যা আমাদের ফাইল পারমিশনের প্রথম অংশ। এখানে দেখুন রিড (r) এর জন্য ভ্যালু 4, রাইট (w) এর জন্য ভ্যালু 2, এক্সিকিউট(x)এর জন্য ভ্যালু 1। আর যদি পারমিশন না দেন তাহলে ভ্যালু হবে 0।

User / Owner			Group			World		
r	w	x	r	w	x	r	w	x
4	2	1	4	0	1	4	0	1
7			5			5		

একই ভাবে ২য় এবং ৩য় অংশ পেলাম, এবার এদের পাশাপাশি সাজালে পাওয়া যায় 755 যা ফাইলের মালিককে রিড+রাইট+ডিলেট/এক্সিকিউট করার পারমিশন দেয়, গ্রুপ কে রিড+এক্সিকিউট করার পারমিশন এবং ওয়াল্ড/পাবলিক কে কে রিড+এক্সিকিউট করার পারমিশন দেয়।



ওয়ার্ডপ্রেসে কিছু ফাইলের পারমিশনের উপর আপনার সাইটের সিকিউরিটি সামান্য হলেও নির্ভর করে। নিচে সেগুলো দেয়া হল।

ফাইল/ফোল্ডারের নাম	ফাইল/ফোল্ডারের পথ	রিকমেন্ডেড পারমিশন
.htaccess	../.htaccess	404
wp-config.php	../wp-config.php	400
index.php	../index.php	400
wp-blog-header.php	../wp-blog-header.php	400
root folder	../	705
wp-admin/	../wp-admin	705
wp-includes/	../wp-includes	705
wp-content/	../wp-content	705

\*কট ফোল্ডারে ৭০৫ পারমিশন দিনে অনেক সময় সার্ভার রেস্পঞ্জ করে না/এরর/ফরভিডেন দেখায়, যদি এই রকম সমস্যা হয় তবে পারমিশন ৭৫০ করে সমস্যার সমাধান করতে হবে।

এই কাজটি ম্যানুয়ালে করতে অনেকের সমস্যা হয় / করতে পারেন না, তাদের জন্য নিচের স্ক্রিপ্টটি। স্ক্রিপ্টটি সাইটের পাবলিক এইচটিএমএল / httpdocs এ per.php / যেকোনো নামে সেভ করে ব্রাউজার থেকে ২বার ভিজিট করুন, এটি ফাইল পারমিশন ঠিক করে দেবে, কাজ শেষে ফাইলটি ডিলেট করে দিতে হবে।

```
<!DOCTYPE HTML>
<html>
<body>
<head><title>File Permission Changer</title></head>
<?php
/*
Script Name: File Permission Changer
Version: 1.0
Author: Saiful Islam
Author URI: http://saifulzone.com/
License: GPL2
*/
function c_f_p($file,$per){
if (file_exists($file)) {
$c_f=substr(decoct(fileperms("$file")),2);

$per1=octdec($per);
if($per1==$c_f){
@chmod($file, $per1);
$c_f=substr(decoct(fileperms("$file")),2);
echo "<tr><td>$file</td><td><font color='\"#FF0000\"'>$c_f</font></td></tr>";
}
else {echo "<tr><td>$file</td><td><font color='\"#008800\"'>$c_f</font></td></tr>";}
}
}

//echo substr(decoct(fileperms("$xx.php")),2);
echo '<table border="1"><tr><td>File Name</td><td>Status</td></tr>';
c_f_p(".htaccess","0404");
c_f_p("wp-config.php","0400");
c_f_p("index.php","0400");
c_f_p("wp-blog-header.php","0400");
c_f_p("../","705");
c_f_p("wp-admin/","705");
c_f_p("wp-includes/","705");
c_f_p("wp-content/","705");

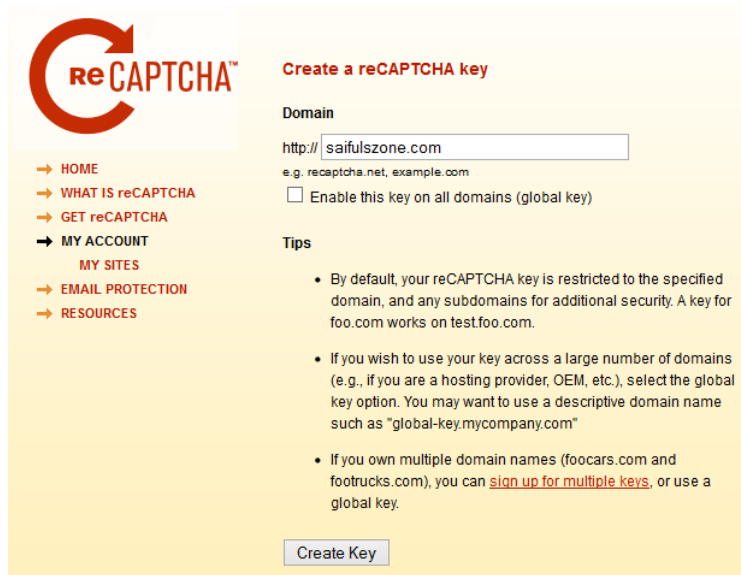
echo '<table>';
?>
</body>
</html>
```

## Brute Force থেকে সাইট বাঁচানো

ওয়েবে brute force ব্যাপারটি এখন আর আগের মত নেই, আগে একটা ছোট স্ক্রিপ্ট দিয়েই কাজ চালানো যেতো, এখন CMS গুলো ৪-৫ বার ভুল ট্রাই করার পর অটোমেটিক IP ব্লক করে থাকে, তাই বলে থেমে নেই brute force কারীরা, তারা প্রক্সি লিস্ট আর ডায়নামিক আইপি + VPN দিয়ে স্ক্রিপ্ট বানিয়ে নিয়েছে, যেগুলো ভুল ট্রাইয়ের পর আইপি চেঞ্জ করে অন্য আইপি থেকে ট্রাই করতে থাকে। এটা প্রতিকার হিসাবে নিচের সিস্টেমটি ব্যবহার করতে পারেন।

১.প্রথমে গুগলের [রিক্যাপাছা](http://www.google.com/recaptcha/captcha) এর সাইটে যেতে হবে, (<http://www.google.com/recaptcha/captcha>) এখানে গুগোল একাউন্ট দিয়ে লগিন করতে হবে।

২.মাই একাউন্টে যেয়ে মাই সাইট এ আপনার সাইটটি এডেড করতে হবে, নিচের মত করে।



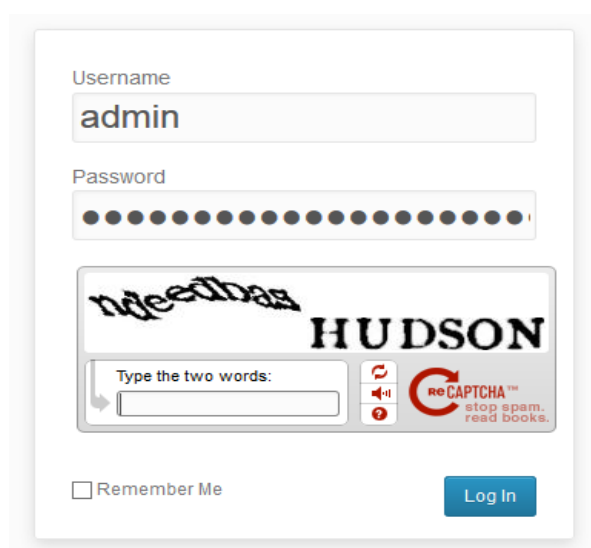
৩.এবার ক্রিয়েট কি চাপলেই আপনার সাইটের জন্য রিক্যাপাচার কি জেনারেট হবে। এখান থেকে ২ টি কি আমাদের লাগবে (পাবলিক আর প্রাইভেট কি)



৪.এবার ওয়ার্ডপ্রেস এ গিয়ে ২ টি প্লাগিন ইন্সটল করতে হবে ( চাইলে প্লাগিন ছাড়াই কাজটি করা যায় , কিন্তু প্লাগিন কিছুটা বাড়তি সুবিদা দিবে) ।

- wp recaptcha (<http://wordpress.org/extend/plugins/wp-recaptcha/>)
- login recaptcha (<http://wordpress.org/extend/plugins/wp-login-recaptcha/>)

৫.এবার reCAPTCHA Options এ গিয়ে প্রাইভেট আর পাবলিক কি দিয়ে সেভ করুন, তাহলে reCAPTCHA API এর সাথে আপনার সাইটের লিঙ্ক হয়ে যাবে , এবার Login reCAPTCHA এর সেটিং এ গিয়ে মন মত থীম সেট করুন । এর পর লগআউট করে লগিন করার চেষ্টা করুন , আপনার লগিন বক্স নিচের মত হয়ে যাবে। যেহেতু বট রিক্যাপাচা এন্ট্রি করতে পারে না সেহেতু সাইট ব্রাউজ থেকে বেছে যাবে। যদিও এটা বাইপাস করা যায় কিন্তু সেটা হিউম্যান করতে পারে বট নয় বট নরমালী ফর্ম সাবমিট আর সাকসেস মেসেজ চেক করতে পারে।

A screenshot of the WordPress login page. It features a 'Username' field with the text 'admin' and a 'Password' field with masked characters. Below the password field is a reCAPTCHA challenge showing the words 'needles' and 'HUDSON'. A text box below the challenge says 'Type the two words:'. To the right of the text box are icons for refreshing, audio, and help. The reCAPTCHA logo and tagline 'stop spam. read books.' are also visible. At the bottom left is a 'Remember Me' checkbox, and at the bottom right is a blue 'Log In' button.

**\*\*User নেম admin রাখবেন না যেন\*\***

# .htaccess

.htaccess একে হাইপারটেক্সট এক্সেস নামে পরিচয় দেয়া হয়ে থাকে। এটা ওয়েব সার্ভারে কনফিগারেশন ফাইল হিসাবেও কাজ করে থাকে, ওয়ার্ডপ্রেস নিজে একটা .htaccess জেনারেট করে থাকে পারমালিঙ্ক, বট এক্সেস... ইত্যাদি সেটিংস নিয়ে।

.htaccess মূলত যেসব কাজ ব্যবহার হয়ে থাকেঃ

- Authorization, authentication
- Rewriting URLs
- Blocking IP
- SSL
- Directory listing
- Customized error responses
- MIME types
- Cache Control

[এই](http://www.javascriptkit.com/howto/htaccess.shtml) সাইটে এর উপর বিস্তারিত টিউটোরিয়াল আছে, শিখে রাখলে পরে অনেক কাজ লাগবে।  
(<http://www.javascriptkit.com/howto/htaccess.shtml>)

# BulletProof Security

এটি একটি প্লাগিন যার কাজ .htaccess কে নিয়ে , এই প্লাগিনটি একটি WP সাইটকে XSS, RFI, CRLF, CSRF, Base64, Code Injection and SQL Injection থেকে প্রোটেক্ট করে থাকে। আর এটাকে ওয়ার্ডপ্রেস এর সবচেয়ে ভালো সিকিউরিটি প্লাগিন বলা যেতে পারে। এই প্লাগিনটা আপনার সাইটে কোন পিএইচপি ফাইলকে ডিরেক্ট এক্সেস করতে বাধা দেবে , যেমনঃ আপনি চাইলেন <http://site.com/wp-content/theme/xx/404.php> এই ঠিকানা ভিজিট করতে কিন্তু এই হতচ্ছাড়া প্লাগিন এই কাজটি করতে দিবে না। তাই কেউ অসৎ উদ্দেশ্যে কোন স্ক্রিপ্ট ডুকালে সেটা সে ডিরেক্ট এক্সেস করতে পারবে না। এছাড়া base64 এনকোড করা কোনো কোড এক্সিকিউট করবে না।

এবার দেখা যাক কিভাবে এই প্লাগিন ব্যবহার করতে হয়,

১. <http://wordpress.org/extend/plugins/bulletproof-security/> এই ঠিকানা থেকে প্লাগিনটি নামিয়ে ইন্সটল করে নিন। এরপর একে এন্টিভ করুন।

২. এবার সাইডবারের BPS Security বাটনে ক্লিক করে সিকিউরিটি মুডে ক্লিক করুন। এবার বুলেটপ্রুপ সিকিউরিটি মুড অন করতে Create default . htaccess File এবং Create secure . htaccess File বাটনে ক্লিক করুন। এতে বুলেটপ্রুফ আপনার ডিফল্ট . htaccess সেটিং তার . htaccess File এ নিয়ে নেবে , যার মধ্যে পারমারলিঙ্ক ,এরর ইত্যাদি থাকবে।

Why Upgrade to BulletProof Security Pro?

BulletProof Security ~ htaccess Core

★★★★★  
Downloaded 497,426 times.  
Please Rate BPS 4.75 Ratings

Security Modes | Security Status | Security Log | System Info | Backup & Restore | Edit/Upload/Download | Custom Code | Maintenance Mode

Help & FAQ | Whats New | My Notes | BPS Pro Features | Website Scanner | Website SEO

BulletProof Security Modes

AutoMagic - Create Your htaccess Master Files [Read Me](#)

Use These AutoMagic Buttons For Your Website For Standard WP Installations

Do Not Use These AutoMagic Buttons For Network / MU Sub-domain Websites Only

Do Not Use These AutoMagic Buttons For Network / MU Sub-domain Websites Only

Create default.htaccess File

Create secure.htaccess File

Create default.htaccess File

Create secure.htaccess File

Create default.htaccess File

Create secure.htaccess File

Activate Security Modes

Activate Website Root Folder .htaccess Security Mode [Read Me](#)

☒ BulletProof Mode [Read Me](#)  
http://demo5.local/.htaccess  
Copies the file secure.htaccess to your root folder and renames the file name to just .htaccess

☐ Default Mode  
http://demo5.local/.htaccess  
CAUTION: Your site will not be protected if you activate Default Mode. ONLY activate Default Mode for Testing and Troubleshooting.

☐ Delete wp-admin htaccess File

[Activate](#)

Activate Website wp-admin Folder .htaccess Security Mode [Read Me](#)

☒ BulletProof Mode [Read Me](#)  
http://demo5.local/wp-admin/.htaccess  
Copies the file wpadmin-secure.htaccess to your /wp-admin folder and renames the file name to just .htaccess

☐ Delete wp-admin htaccess File  
http://demo5.local/wp-admin/.htaccess  
CAUTION: Deletes the .htaccess file in your /wp-admin folder. ONLY delete For testing or BPS removal.

[Activate](#)

Activate Deny All htaccess Folder Protection For The BPS Master htaccess Folder [Read Me](#)

☒ BulletProof Mode [Read Me](#)  
http://demo5.local/wp-content/plugins/bulletproof-security/admin/htaccess/  
Copies the file deny-all.htaccess to the BPS Master htaccess folder and renames the file name to just .htaccess

[Activate](#)

Activate Deny All htaccess Folder Protection For The BPS Backup Folder [Read Me](#)

☒ BulletProof Mode [Read Me](#)  
http://demo5.local/wp-content/tps-backup/  
Copies the file deny-all.htaccess to the BPS Backup folder and renames the file name to just .htaccess

[Activate](#)

BulletProof Security Plugin by [AlPro Website Security](#)

Thank you for creating with WordPress.

Version 3.5.1

৩.এবার Security Status এ ক্লিক করে নিচের চিহ্নিত অংশে দেখুন কোন লাল রঙে লেখা মেসেজ আছে কিনা , যদি থাকে তাহলে সেটা সমাধান করতে চেষ্টা করুন। এবাই ফাইল পারমিশন এর দিকে

নজর দিন রিকমেন্ডেড পারমিশন আর কারেন্ট পারমিশন চেক করে দেখুন , কারেন্ট পারমিশন বদলে রিকমেন্ডেড পারমিশন সেট করুন। এর পর আপনার কাজ শেষ , মানে এই প্লাইগিন নিয়ে আর মাথা না ঘামালেও চলবে।

Why Upgrade to BulletProof Security Pro?

BulletProof Security ~ htaccess Core

Downloaded 497,426 times. Please Rate BPS 470 Ratings

Security Modes **Security Status** Security Log System Info Backup & Restore Edit/Upload/Download Custom Code Maintenance Mode

Help & FAQ Whats New My Notes BPS Pro Features Website Scanner Website SEO

### BulletProof Security Status

Activated BulletProof Security .htaccess Files [Read Me](#)

The htaccess file that is activated in your root folder is:  
BULLETPROOF\_47.8 >>>>>> SECURE .HTACCESS

wp-config.php is htaccess protected by BPS  
php5.ini and php5.ini are htaccess protected by BPS

Deny All protection activated for BPS Master .htaccess folder  
Deny All protection activated for /wp-content/tps-backup folder

The htaccess file that is activated in your wp-admin folder is:  
BULLETPROOF\_47.8 WP-ADMIN SECURE .HTACCESS

File and Folder Permissions - CGI or DSO [Read Me](#)

DSO File and Folder Permissions / Recommendations

File Name	File Path	Recommended Permissions	Current Permissions
.htaccess	./htaccess	644	666
wp-config.php	./wp-config.php	644	666
index.php	./index.php	644	666
wp-blog-header.php	./wp-blog-header.php	644	666
root folder	./	755	777
wp-admin/	./wp-admin	755	777
wp-includes/	./wp-includes	755	777
wp-content/	./wp-content	755	777
wp-content/tps-backup/	./wp-content/tps-backup	755	777

Additional Website Security Measures

- WordPress DB Show Errors Function Is Set To: false
- WordPress Database Errors Are Turned Off
- WordPress Meta Generator Tag Removed
- WordPress Version Is Not Displayed / Not Shown
- The Default Admin username "admin" is not being used
- The WP readme.html file is .htaccess protected
- The WP /wp-admin/install.php file is .htaccess protected

General BulletProof Security File Checks [Read Me](#)

- An .htaccess file was found in your root folder
- An .htaccess file was found in your wp-admin folder
- A default htaccess file was found in the .htaccess folder
- A secure htaccess file was found in the .htaccess folder
- A maintenance htaccess file was found in the .htaccess folder
- A bp-maintenance.php file was found in the .htaccess folder
- A bps-maintenance-values.php file was found in the .htaccess folder
- A wpadmin-secure.htaccess file was found in the .htaccess folder
- Your Current Root .htaccess File is backed up
- Your Current wp-admin .htaccess File is backed up
- Your BPS Master default.htaccess file is backed up
- Your BPS Master secure.htaccess file is backed up
- Your BPS Master wpadmin-secure.htaccess file is backed up
- Your BPS Master maintenance.htaccess file is backed up
- Your BPS Master bp-maintenance.php file is backed up
- Your BPS Master bps-maintenance-values.php file is backed up

BulletProof Security Plugin by [AIToro Website Security](#)

Thank you for creating with WordPress.

Version 3.5.1

এবার একটি অটো ব্যাকাপ স্ক্রিপ্ট চালু করেদিয়ে নিশ্চিন্তে থাকুন। যদিও ১০০% সিকিউর হব না , তবে ৮০%+ সিকিউর হব , বাকিটা হোস্টিং , পাসওয়ার্ড আর স্ক্রিপ্ট এর দুর্বলতা এর উপর ডিপেন্ড করবে।

এছাড়া আরো অনেক ট্রিক / হ্যাক আছে যা এর পরের বইতে ক্লিয়ার করার চেষ্টা করব।

এটা আমার লেখা প্রথম ই-বুক , যদিও আমি নিজে অতবড় সিকিউরিটি এক্সপার্ট না। তবে আশা করি ই-বুকটি আপনাদের উপকারে লাগবে , আর যেকোনো ভুলের জন্য ক্ষমা করবেন। আর ভুল পেলে আমাকে মেইল করুন ([saaifulislam@gmail.com](mailto:saaifulislam@gmail.com)) , যত দ্রুত পারি সমাধান করার চেষ্টা করব।