ওয়ার্ডপ্রেসে বানানো ওয়েবসাইট যেভাবে নিরাপদ রাখবেন

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

ওপেন সোর্স ও ইউজার ফ্রেন্ডলি বলে ওয়ার্ডপ্রেস হচ্ছে পৃথিবীর সবচেয়ে জনপ্রিয় কনটেন্ট ম্যানেজমেন্ট সিস্টেম। এর জনপ্রিয়তার আরেক কারণ, এটি এমন একটি সিএমএস, যা দিয়ে আপনি খুব সহজেই তৈরি করতে পারবেন যেকোনো ধরনের ওয়েবসাইট, হোক সেটি ব্লগ, ই-শপ কিংবা লার্নিং ম্যানেজমেন্ট সিস্টেম।

তবে ওপেন সোর্স হওয়ার কারণে এটির সোর্স কোড সবার হাতের নাগালে। তাই ওয়ার্ডপ্রেস সিকিউরিটি বাগগুলো সহজেই খুঁজে নিতে পারে হ্যাকারেরা। তাই ওয়ার্ডপ্রেস ব্যবহার করলে অবশ্যই ওয়ার্ডপ্রেস সিকিউরিটি নিয়ে আপনাকে কিছুটা ভাবতে হবে। নিচের ১০টি পদ্ধতি অনুসরণ করলে এসব সিকিউরিটি বাগ থেকে আপনি মোটামুটি সুরক্ষিত থাকতে পারবেন।

০১ 'admin' নামের ইউজারনেম ব্যবহার করবেন না : এই কাজটি একমাত্র তারাই করে থাকেন, যারা ওয়ার্ডপ্রেস ব্যবহারের ক্ষেত্রে একদম নতুন। কিন্তু কথা হলো পৃথিবীতে বিপুলসংখ্যক সাইটের ইউজারনেম এটিই। এর কারণ, ওয়ার্ডপ্রেসের আগের ভার্সনগুলোতে এটি ডিফল্ট ইউজারনেম হিসেবে থাকত। এটি ব্যবহার করে অনেক হ্যাকার আপনার সাইট হ্যাক করে। প্রতিবছর প্রচুর সাইট হ্যাক হয় শুধু এই ইউজারনেম ব্যবহারের কারণে। সুতরাং, প্রথম সুযোগেই এই ইউজারনেম পরিবর্তন করে নিতে হবে।

০২ লগইন লকডাউন সিস্টেম ব্যবহার করুন : ওয়েবসাইট হ্যাকারদের একটি প্রিয় হ্যাকিং সিস্টেম হচ্ছে brute force (ব্রুট ফোর্স), যেখানে তারা একটি ওয়েবসাইটেই বহুসংখ্যক সম্ভাব্য ইউজারনেম ও পাসওয়ার্ড কম্বিনেশন ব্যবহার করে লগইনের চেষ্টা চালায়। আপনার কাছে এভাবে হ্যাক করা হয়তো অসম্ভব মনে হতে পারে। কিন্তু তাদের কাছে এটি খুবই সোজা। কারণ, এরা এই কাজটি করতে বিভিন্ন সফটওয়্যার ব্যবহার করে, যেগুলো খুব দ্রুত বেশ কিছু (এমনকি ঘণ্টায় কয়েক হাজার) লগইন অ্যাটেম্প চালাতে পারে এবং এ ধরনের পদ্ধতিতে বারবার লগইন চেষ্টা করা যায় ও এ ধরনের যেকোনো সাইট হ্যাক করা যায়। এমনকি ডিকশনারি অ্যাটাক (dictionary attack) (বিশেষ কিছু ইউজার ও পাস কম্বিনেশন, যা পৃথিবীব্যাপী বহুল প্রচলিত) ব্যবহার করে বেশ কিছু সাইট হ্যাক করে ফেলে হ্যাকারেরা। এখন কথা হলো, আপনি কীভাবে বাঁচবেন? খুব সহজ পদ্ধতি অনুসরণ করুন। সাইটে লগইন লিমিট রাখুন। অর্থাৎ কেউ যদি তিনবারের বেশি লগইন হওয়ার চেষ্টা করে, কিন্তু সফল না হয়, তাহলে সে হয়তো পরের বার একটি কেপচা কোড দেখতে পাবে। কিংবা তার আইপি ব্লক হয়ে যাবে। বেশকিছু নির্ভরযোগ্য প্লাগইন আছে, যা দিয়ে আপনি এই কাজটি করতে পারেন।

০৩ ভিজিটরের প্রয়োজন নেই এমন তথ্য লুকিয়ে রাখুন : এমন অনেক তথ্য আছে, যা ওয়ার্ডপ্রেস সাইটে শেয়ার করে, কিন্তু যেগুলো ভিজিটর জানার কোনো প্রয়োজন নেই। এই তথ্যগুলোর মধ্যে বেশ কিছু শেয়ার করা আপনার জন্য বিপজ্জনক। যেমন– ওয়ার্ডপ্রেস ভার্সন। এ ধরনের তথ্যগুলো লুকানোর জন্যও অনেক প্লাগইন আছে।

০৪ 'wp-config.php' ফাইল সরিয়ে নিন : যারা ওয়ার্ডপ্রেস ব্যাক-এন্ড সম্পর্কে অবগত নন, তারা 'wp-confi.php'php-এর সাথে পরিচিত হয়ে নিন। এটি ওয়ার্ডপ্রেস রুট ডিরেক্টরিতে থাকা এমন একটি ফাইল, যেটি আপনার ওয়ার্ডপ্রেস ডিরেক্টরির সাথে ডাটাবেজকে যুক্ত করে। এখানে আপনার ওয়ার্ডপ্রেস-সংশ্লিষ্ট ডাটাবেজের নাম, ইউজারনেম, পাসওয়ার্ড, সার্ভার, টেবিল নেম ইত্যাদি থাকে। মানে এই ফাইলটি যদি কারও হাতে যায়, তবে আপনার সাইটের যেকোনো জায়গায় সে প্রবেশ ও পরিবর্তন করতে পারবে। তাই ওয়ার্ডপ্রেসের রুট ডিরেক্টরি থেকে আপনার 'wp-confi.php'php ফাইলটি সরিয়ে অন্য কোনো ফোল্ডারে নিয়ে যান। এতে ওয়ার্ডপ্রেসের কোনো সমস্যা হবে না। যেখানেই থাকুক ওয়ার্ডপ্রেস এটিকে খুঁজে বের করবে।

০৫ table prefix পরিবর্তন করে দিন : সাধারণভাবে আপনি যখন ওয়ার্ডপ্রেস ইনস্টল করেন, তখন এর টেবিলগুলোর প্রিফিক্স হয় 'wp'। যেটি আপনার 'wp-config.php' ফাইলে উল্লেখ আছে। এটি যেহেতু ওপেন সোর্স, তাই আপনি প্রিফিক্স এভাবে রেখে দিলে হ্যাকার ইতোমধ্যে জানে আপনার টেবিলগুলোর প্রিফিক্স কী। তাই এ থেকে বাঁচতে হলে ওয়ার্ডপ্রেস ইনস্টল করার আগে 'wp-config.php'php থেকে আপনার টেবিল প্রিফিক্স পরিবর্তন করে অন্য কিছু দিন।

০৬ সিক্রেট কী ব্যবহার করুন : আপনি যখন 'wp-config.php' php ফাইলটি খুলবেন, তখন নিচের চারটি লাইন দেখতে পাবেন।

```
define('AUTH_KEY', '');
define('SECURE_AUTH_KEY', '');
define('LOGGED_IN_KEY', '');
define('NONCE_KEY', '');
```

সিক্রেট কীগুলো কাজ করে আপনার পাসওয়ার্ড আরও শক্ত করার জন্য। এখানে ভিজিট করে এই কীগুলো জেনারেট এবং কপি করে নিয়ে আসুন : http://api.wordpress.org/secret-key/1.1/। এবার এগুলো wp-config.php-এ যুক্ত করুন।

আপনার /wp-admin লুকিয়ে রাখুন : wp-admin বা wp-login.php যাই বলুন না কেন, এর নাম পরিবর্তন করার অনেক টুল আছে। ধরুন, একটি প্লাগইন ব্যবহার করে আপনার সাইটের wp-admin পরিবর্তন করে দিলেন mysiteadmin। এখন কেউ যদি yoursite.com/wp-admin-এ যায়, তাহলে সে ৪০৪ এরর পাবে। লগইন হওয়ার জন্য তাকে যেতে হবে yoursite.com/mysiteadmin-এ। সুতরাং, আপনার বা আপনার কোম্পানির সাইটে এ ধরনের পরিবর্তন করতে হ্যাকিংয়ের হাত থেকে রক্ষা করতে পারেন। তবে কমিউনিটি ব্লগে এটি করা যাবে না।

০৭

০৮ প্লাগইন ব্যবহারে হুশিয়ার : যেন-তেন প্লাগইন ব্যবহার করবেন না। বিশেষ করে যেসব ক্ষেত্রে প্লাগইন আপনার বিশেষ ডাটা নিয়ে কাজ করে, যেটি হ্যাক হলে আপনার সাইটে সমস্যা হতে পারে, সে ক্ষেত্রে অবশ্যই এর রিভিউ এবং কতটা নির্ভরযোগ্য তা দেখে নেবেন। লুপ ভেঙে তার মাঝে কিছু যুক্ত করে এ ধরনের প্লাগইন ব্যবহার না করে, সে ক্ষেত্রে ওই সুবিধা ম্যানুয়ালি যুক্ত করাই বুদ্ধিমানের কাজ।

০৯ ০৯. ফ্রি থিম ব্যবহার করা থেকে বিরত থাকুন : অনেকে ফ্রি থিম বা প্রিমিয়াম থিম ফ্রিতে ডাউনলোড করে ব্যবহার করে থাকেন। একান্তই যদি এ কাজটি করতে হয় তাহলে সতর্কতা অবলম্বন করুন। চেক করে নিন এতে কোনো সিকিউরিটি বাগ আছে কি না। অনলাইনে চেক করার অনেক সাইট আছে। তবে চেক করার সাইটগুলো বিশ্বাসযোগ্য কি না তা নিয়ে অনেকের সন্দেহ আছে। কিনে প্রিমিয়াম থিম ব্যবহারের ক্ষেত্রেও অনেক সময় কিছু বাগ থাকে।

১০ ব্যাকআপ রাখুন : নিয়মিত আপনার সাইটের ব্যাকআপ রাখুন। প্রায় সব প্রিমিয়াম থিমেই এখন বিল্টইন অপশনটি দেয়া থাকে। তবে না থাকলে কোনো প্লাগইন ব্যবহার করতে পারেন কিংবা ম্যানুয়ালিও করতে পারেন। তবে তার চেয়ে একটি সিস্টেম ব্যবহার করাই যুক্তিযুক্ত, যেটি আপনার কোনো ওয়েব ব্যাকআপ অ্যাকাউন্টে নির্দিষ্ট সময় পরপর অটো ব্যাকআপ পাঠিয়ে দেবে।

এর বাইরেও অনেক ওয়ার্ডপ্রেস সিকিউরিটি রুল আছে। যেমন– সবসময় সাইটের ওয়ার্ডপ্রেস, থিম, প্লাগইন সবকিছু আপডেট রাখুন। হোস্টিং বাছাই করার সময় সতর্কতা অবলম্বন করুন ইত্যাদি। আর মূল ব্যাপার আপনার সাইটের সিকিউরিটিকে গুরুত্ব দেয়া। আশা করি, আপনার সাইটের সিকিউরিটির ব্যাপারে যথেষ্ট সময় দেবেন কজ

ফিডব্যাক : jabedmorshed@yahoo.com