ওয়েবসাইটের কিছু সাধারণ নিরাপত্তা সমস্যা ও প্রতিকার

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

ওয়েবসাইট এখন আমাদের জীবনের এক গুরুত্বপূর্ণ অংশ। আমরা ইন্টারনেটে ওয়েবসাইটের মাধ্যমে নিজেদের যোগাযোগ, শিক্ষা থেকে শুরু করে আর্থিকসহ সব ধরনের দৈনন্দিন কাজ করে থাকি। ব্যাপক আকারে আর্থিক লেনদেনের কারণে তা এখন ক্রিমিনালদের জন্য এক চমৎকার টার্গেট। ওয়েবসাইটের ব্যবহার যেহেতু সবার মাঝে ছড়িয়ে গেছে, তাই সবাইকে সতর্ক হতে হবে। তবে সাধারণ জনগণ যেহেতু শুধু ব্যবহারকারী ও তাদের পর্যাপ্ত কারিগরি দক্ষতা নেই। তাই ওয়েবসাইট ডেভেলপারদেরকে এমনভাবে ওয়েবসাইটগুলো ডেভেলপ করতে হবে, যাতে হ্যাকারদের পক্ষে সহজে হ্যাকিং করা বা ওয়েবসাইট ও এর ব্যবহারকারীদের কোনো ক্ষতি করা সম্ভব না হয়। এ লেখায় যারা ওয়েব ডিজাইন করেন বা অ্যাপ্লিকেশন ডেভেলপ করেন, তাদের জন্য এবং যারা তাদের নিজেদের জন্য ওয়েবসাইট তৈরি করবেন, তাদের জন্য সিকিউরিটির কিছু সাধারণ তথ্য দেয়া হলো।

নিরাপত্তা সমস্যা-১ : আপনার হোস্টিংয়ে পিএইচপিতে কি ইস্টার এগ এনাবল্ড? তাহলে দ্রুত বন্ধ করুন।

সমাধান : ইস্টার এগ হলো, যে প্রোগ্রামিং ল্যাঙ্গুয়েজের মাধ্যমে ওয়েবসাইটটি ডেভেলপ করা হয়েছে, তা লিঙ্কের মধ্যে এক্সটেনশন আকারে দেখা। পিএইচপিতে বাই ডিফল্ট ইস্টার এগ এনাবল্ড করা থাকে। ফলে হ্যাকেরেরা জানতে পারে কোন ওয়েবসাইট কী ল্যাঙ্গুয়েজ দিয়ে ডেভেলপ করা হয়েছে। সুতরাং এটিকে ডিজ্যাবল করতে হবে।

নিরাপত্তা সমস্যা-২ : পিএইচপি সেটিংসে 'গ্লোবাল রেজিস্টার' অন না থাকলে স্ক্রিপ্ট কাজ করে না, স্ক্রিপ্ট ফেলে দেন।

সমাধান : রিকোড করুন, গ্লোবাল রেজিস্টার সাইটকে হ্যাকারের হাতে তুলে দেয়ার জন্য একটি যথেষ্ট শক্তিশালী প্রক্রিয়া।

নিরাপত্তা সমস্যা-৩ : অ্যানোনিমাস এফটিপি ইউজার অ্যাকাউন্ট প্রয়োজন ছাড়াই খুলে রেখেছেন?

সমাধান : প্রয়োজন না থাকলে অ্যানোনিমাস এফটিপি ইউজার অ্যাকাউন্ট এখনই বন্ধ করুন। আর প্রয়োজন থাকলে মেইন সাইট ছাড়া আরেকটি অ্যাকাউন্টে হোস্ট করুন।

নিরাপত্তা সমস্যা-৪ : পিএইচপি ইনফো ফাইল (phpinfo()) সার্ভারে আপ করে রেখেছেন?

সমাধান : তবে এখনই ফাইলটি মুছে দিন, নয়ত হ্যাকার আপনার হোস্টিং সার্ভারের ডিটেইলস জেনে যাবে।

নিরাপত্তা সমস্যা-৫ : অ্যাপাচি ভার্সন কী লেটেস্ট?

সমাধান : লেটেস্ট অ্যাপাচি ভার্সন ইনস্টল করুন। নয়তো ড্যানিয়েল অ্যাটাকসহ অনেক ধরনের অ্যাপ্যাচি বেজ অ্যাটাক হতে পারে।

নিরাপত্তা সমস্যা-৬ : আপনার সাইটে এসএসএল সার্টিফিকেট ব্যবহার করেছেন? তবে ওপেন এসএসএলের ভার্সন কত?

সমাধান : লেটেস্ট ওপেন এসএসএল ইনস্টল করুন। কমপক্ষে ভার্সন ১। নয়ত ড্যানিয়েল অ্যাটাকের শিকার হতে পারেন।

নিরাপত্তা সমস্যা-৭ : ডিরেক্টরি (ইউনিক্স) বা ফোল্ডারের (উইন্ডোজ) বা ফাইলের পাবলিক অ্যাক্সেস পারমিশন কি 'রাইটেবল' দেয়া আছে?

সমাধান : সবার আগে যদি কোনো রাইট পারমিশন থাকে, তবে তা বন্ধ করুন। ইউনিক্সে ০৭৭৭ থাকলে ডিরেক্টরির জন্য ০৭৫৫ করে দিন। ফাইলের জন্য ০৬৪৪ করে দিন, যদি সিজিআই স্ক্রিপ্ট হয়ে থাকে এবং এক্সেকিউটেবল হয়ে থাকে তবে প্রয়োজনে ০৬৬৬ করে দিন। তবে সচরাচর CGI-BIN/CGI-SYS/SCGI-BIN etc ডিরেক্টরিতে এক্সেকিউটেবল স্ক্রিপ্ট (পার্ল, পাইথন) রান করে থাকে। আর উইন্ডোজের জন্য ইউজার গ্রুপ সেটিং থেকে পারমিশন চেক করুন এবং প্রয়োজনে রিসেট করুন। আপনার সাইটের ফাইল ফোল্ডারের ব্যাপারে নিশ্চিত না হলে একটার পর একটা ফাইল/ফোল্ডার চেক করে দেখুন। এফটিপি ক্লায়েন্ট দিয়ে লগইন করলে ফাইল পারমিশন দেখাবে।

নিরাপত্তা সমস্যা-৮ : ফাইল ব্রাউজিং সমস্যা? আপনার ওয়েবসাইটের ইমেজ, সিএসএস (এসেট, রিসোর্স ফোল্ডার) ভিজিট করলে সব ফাইল লিস্ট আকারে দেখা যায়?

সমাধান : ব্ল্যাঙ্ক ইনডেক্স ফাইল আপলোড করুন, যাতে করে example.com/images/ ভিজিট করলে ফাইল লিস্ট দেখা না যায়। আপনি .htaccess দিয়েও ফোল্ডার অ্যাক্সেস

(বাকি অংশ ৫৬ পৃষ্ঠায়)

ওয়েব অ্যাপ্লিকেশন লেভেল সিকিউরিটি

০৪. যে ওয়েবসাইটটি বা ওয়েব অ্যাপ্লিকেশনটি আছে তার ভালনারেবিলিটি চেক করা। বিশেষ করে SQL Injection, Cross Site Scripting, Cross Site Request Forgery, File Inclusion, Remote code Executation, Web Backdore, Remote File upload এ ধরনের ভালনারেবিলিটি চেক ও ফিক্স করা। যারা এসব বিষয়ে একেবারে নতুন তারা ভালো Vulnerability Scanner-এর সাহায্য নিতে পারেন।

০৫. ওয়েবসাইটটি যদি কোনো ফ্রেমওয়ার্কের ওপর ভিত্তি করে তৈরি করা হয় (যেমন WordPress, Joomla, PunBB, MyBB), তবে তা দ্রুত লেটেস্ট ভার্সনে আপগ্রেড করা ও কোনো সিকিউরিটি প্যাচ থাকলে তা ইনস্টল করা। CMS-এর সব প্লাগইন চেক করা এবং ওই গুলোর কোনো ভালনারেবিলিটি আছে কি না তা দেখা এবং এর Exploit আছে কি না, তা চেক করা। Exploit থাকলে তা ফিক্স করা অথবা ওই প্লাগইন বাদ দেয়া। CMS-এর Congif File-এ Cpanel থেকে Chmod 640 or 600 করে দিন।

০৬. অ্যাডমিন ও সিপ্যানেলের (সার্ভার অ্যাডমিনিস্ট্রেশন) পাসওয়ার্ড পরিবর্তন ও শক্তিশালী করা। Password minimum 12 Character করা এবং সংখ্যা, নাম্বার, ছোট এবং বড় হাতের লেটারের মিশ্রণ করা।

০৭. সব ধরনের ফাইলের বিশেষ করে কনফিগারেশন ফাইলের রাইট (write) অ্যাক্সেস না দেয়া। কোনো ড্রাইভেও রাইট (write) অ্যাক্সেস না দেয়া। Directory Listing বন্ধ করা এবং Directory Bruteforcing বন্ধ করা। কাজের প্রয়োজনে দিতে হলেও কাজ শেষ হলে সেই অ্যাক্সেস রিভোক করা।

প্রতিকার

০৮. নিয়মিত সাইটের ব্যাকআপ রাখা। ব্যাকআপ ফাইল নিরাপদ জায়গায় ও নিরাপদভাবে রাখা, যাতে ডিরেক্টরি ব্রাউজিংয়ের মাধ্যমে তা পাওয়া সম্ভব না হয়। সবচেয়ে ভালো Offline-এ অথবা Public_html Directory-এর বাইরে রাখা।

০৯. দুর্ভাগ্যবশত সাইটটি হ্যাক হলে সাইটের সব কনটেন্ট ডিলিট করে দিতে হবে। তারপর ব্যাকআপ থেকে পুরো সাইটটি আবার চালাতে হবে। কোনোভাবেই শুধু ডিফেসমেন্ট করা পেজটি রিপ্লেস করে সন্তুষ্ট থাকা যাবে না। কারণ হ্যাকারেরা অন্য ডিরেক্টরিতে কোনো ম্যালিশাস (খারাপ) কোড রেখে দিতে পারে এবং সাথে সাথে অ্যাডমিন ও সিপ্যানেলের পাসওয়ার্ড পরিবর্তন করতে হবে।

১০. সাইট কীভাবে হ্যাক হলো তা Detect করতে হবে। এর জন্য Server লগ Follow করতে পারেন এবং সেভাবে সাইটকে পুরো Patch করতে হবে, যাতে আবার হ্যাক না হয়।

ওয়েবসাইটের কিছু সাধারণ নিরাপত্তা সমস্যা ও প্রতিকার

(৭১ পৃষ্ঠার পর)

রেস্ট্রিক্ট করতে পারেন।

নিরাপত্তা সমস্যা-৯ : আপনার স্ক্রিপ্টের কুকি সেটিং কী নিরাপদ?

সমাধান : সাইটওয়াইজ/অ্যাপ্লিকেশন ওয়াইজ কুকি সেট করুন। আনডিফাইন্ড কুকি মানে আপনার গোপন তথ্যে অন্যের অনুপ্রবেশ।

নিরাপত্তা সমস্যা-১০ : এফটিপি/কন্ট্রোল প্যানেলের পাসওয়ার্ড কি ডিকশনারি ওয়ার্ড/আপনার সাথে সংশ্লিষ্ট?

সমাধান : আপনি পাসওয়ার্ড দ্রুত পরিবর্তন করুন এবং সিস্টেমের অটোজেনারেটেড পাসওয়ার্ড ব্যবহার করুন।

নিরাপত্তা সমস্যা-১১ : আপনার হোস্টিং সার্ভারের ডিএনএসের কোথাও দুর্বলতা নেই তো?

সমাধান : না জেনে থাকলে হোস্টিং প্রোভাইডারের কাছ থেকে বিস্তারিত জেনে নিন। ডিএনএস জোন ফাইল নেটওয়ার্ক হ্যাকারদের একটি অন্যতম প্রধান অস্ত্র।

নিরাপত্তা সমস্যা-১২ : আপনার হোস্টিং সার্ভারে কোনো টেস্ট অ্যাকাউন্ট এনাবল্ড করা নেই তো?

সমাধান : না জেনে থাকলে হোস্টিং প্রোভাইডারের কাছ থেকে বিস্তারিত জেনে নিন। ব্রুট ফোর্স ডিফেন্সের সফটওয়্যার থাকলে এনাবল্ড করে নিন।

ওপরে উল্লিখিত সাধারণ সমস্যা ছাড়াও সবসময় নিচে বর্ণিত নিরাপত্তা টিপগুলো অনুসরণ করলে ওয়েবসাইটকে আরও বেশি নিরাপদ রাখা সম্ভব।

ওয়েবের সিকিউরিটি বাড়ানোর ১০ টিপ

০১. প্রথমেই ওয়েবসাইটটি যে ওয়েব সার্ভারে আছে, তাতে কোনো ভালনারেবিলিটি আছে কি না, তা পরীক্ষা করতে হবে। কোনো ত্রুটি পাওয়া গেলে তা ফিক্স করতে হবে। যত দ্রুত সম্ভব লেটেস্ট ওয়েব সার্ভারে আপগ্রেড করা। সম্ভব হলে আপারেটিং সিস্টেমেরও লেটেস্ট ভার্সনে আপগ্রেড করা। লিনআক্স সার্ভারে হলে এর কার্নেল নিয়মিত আপগ্রেড করতে হবে এবং সিস্টেমের জন্য কোনো সিকিউরিটি প্যাচ থাকলে তা ইনস্টল করতে হবে।

০২. সার্ভারের ফায়ারওয়ালটি চেক ও শক্তিশালী করা। নেটওয়ার্ক এবং অ্যাপ্লিকেশন ২ লেভেলে এ ফায়ারওয়াল ব্যবহার করা। সার্ভারে DDoS Protection ব্যবহার করা।

০৩. সার্ভারের অব্যবহৃত পোর্টগুলো এবং সার্ভিসগুলো বন্ধ করে রাখা এবং নিয়মিত সার্ভিসের সফটওয়্যার আপগ্রেড করা। ভালো IDS/IPS আর Webproxy সেটআপ দেয়া কজ

ফিডব্যাক : jabedmorshed@yahoo.com