জুমলা দিয়ে তৈরি ওয়েবসাইটের নিরাপত্তা

জাবেদ মোর্শেদ

ইদানীং বিভিন্ন সাইবার আক্রমণের পরিপ্রেক্ষিতে ওয়েবসাইট অ্যাডমিনিস্ট্রেটর ও ডেভেলপারদের মধ্যে ভীতি এবং একই সাথে সচেতনতা বেড়েছে। জনপ্রিয় কনটেন্ট ম্যানেজমেন্ট সিস্টেম জুমলা (http://www.joomla.org/) এবং জুমলা দিয়ে তৈরি বিভিন্ন ওয়েবসাইটের নিরাপত্তার দিক নিয়ে আলোচনা করা হয়েছে এ লেখায়। জুমলাকে বেছে নেয়ার কারণ হলো বাংলাদেশে বহু ওয়েবসাইট জুমলা দিয়ে তৈরি। এর মধ্যে আছে আমাদের জাতীয় ওয়েব পোর্টাল, মন্ত্রণালয়ের ওয়েবসাইট, জেলা বাতায়ন, এয়ারটেলের ওয়েবসাইট ইত্যাদি।

জুমলা সাইটের নিরাপত্তা নিয়ে আলোচনা করার আগে ওয়েব নিরাপত্তা বিষয়ক বিভিন্ন ধারণা নিয়ে সংক্ষিপ্ত আলোচনা করা উচিত, যাতে পাঠকের জন্য বুঝতে সুবিধা হয়। একই সাথে বলে রাখা ভালো, কোনো সাইটের নিরাপত্তার মাত্রা হলো নিরাপত্তা ব্যবস্থার মধ্যে সবচেয়ে দুর্বল দিকটি ভাঙতে একজন হ্যাকারের যে পরিমাণ সময়, অর্থ আর মেধার প্রয়োজন ঠিক ততটুকুই। সুতরাং একটি ওয়েবসাইটের নিরাপত্তা নিশ্চিত করতে হলে একজন সাইট অ্যাডমিনিস্ট্রেটরের সব ধরনের আক্রমণ (যেমন : এসকিউএল ইনজেকশন, ক্রস সাইট স্ক্রিপ্টিং) ও তার প্রতিকার সম্পর্কে ধারণা থাকা প্রয়োজন।

ওয়েব নিরাপত্তা

এসকিউএল ইনজেকশন : এসকিউএল ইনজেকশন সাধারণত ওয়েবসাইট আক্রমণের জন্য ব্যবহার করা হয়। এর মাধ্যমে সাইটের কোনো ওয়েব ফর্মে (যেমন : অ্যাডমিন লগইন পেজ) এসকিউএল স্টেটমেন্ট লেখা হয়। এর মাধ্যমে হ্যাকার সাইটের গোপন তথ্য চুরি করতে পারে বা অথেনটিকেশন ভায়োলেট করতে পারে। যেমন : কোনো সাইটের ইউজারনেম admin, এখন খারাপভাবে ডিজাইন করা সেই সাইটে যদি ইউজারনেম admin এবং পাসওয়ার্ডের জায়গায় যদি 'or'1'='1' ব্যবহার করা হয় তবে তা আমাকে সাইটিতে admin হিসেবে লগইন করাবে। এরকম আরও অনেক ধরনের এসকিউএল স্টেটমেন্ট লেখা সম্ভব, যা দিয়ে সাইটের নিরাপত্তা বিঘ্নিত হতে পারে।

প্রতিকার : যেকোনো এসকিউএল স্টেটমেন্ট রান করানোর আগে তা চেক করে নিতে হবে। পিএইচপি ফাংশন mysql_real_escape_string() এ ব্যাপারে ব্যবহার করা হয়। নিম্নলিখিত কোড এসকিউএল ইনজেকশন চেক করার কাজে ব্যবহার হয়।

```
$query = sprintf("SELECT * FROM 'Users' WHERE UserName='%s' AND Password='%s'",
mysql_real_escape_string($Username),
mysql_real_escape_string($Password));
mysql_query($query);
```

সুতরাং যখনই কোনো এসকিউএল স্টেটমেন্ট রান করানো হবে তখন ইসকেপ ক্যারেক্টারগুলো বাদ দিয়ে দিতে হবে।

ক্রস সাইট স্ক্রিপ্টিং : ক্রস সাইট স্ক্রিপ্টিং দিয়ে একজন হ্যাকার তার ভিকটিমের ওয়েবসাইটের ব্রাউজের সাইড স্ক্রিপ্টেরের মধ্যে নিজের কোনো স্ক্রিপ্ট ঢুকিয়ে দিয়ে থাকে। যখন একজন ভিজিটর ওই সাইটে ভিজিট করেন তখন স্ক্রিপ্টটি স্বয়ংক্রিয়ভাবে ভিজিটরের ব্রাউজারে ডাউনলোড হয়। এই আক্রমণের মাধ্যমে একজন হ্যাকার কোনো ইউজারের সেশন ও কুকি চুরি করে থাকে। এর মাধ্যমে হ্যাকার নিজে কোনো ভ্যালিড ইউজার হিসেবে ইম্পারসোনেট করতে পারে।

প্রতিকার : ০১. HTML ভ্যালিডেশন করতে হবে। HTML Purifier দিয়ে সাইটটি বা এক্সটেনশনটি ভ্যালিড করে নিতে হবে। ০২. কুকিভিত্তিক অথেনটিকেশন পরিহার করা। ০৩. সাইটে কোনো ধরনের থার্ড পার্টি স্ক্রিপ্ট এমবেড বা এক্সিকিউশন বন্ধ করা; যাতে কেউ সাইটের কমেন্ট বক্সে কোনো কোড পেস্ট করতে না পারে।

দুর্বল পাসওয়ার্ড : মনে হয় না এই বিষয় নিয়ে বিস্তারিত বলার তেমন কিছু আছে। নিচের লিস্ট থেকে দেখে নিতে পারেন খারাপ পাসওয়ার্ডের নমুনা।

http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

এর মধ্যে আপনার পাসওয়ার্ডটি যেনো না থাকে সে ব্যাপারে খেয়াল রাখুন। আপনার পাসওয়ার্ডের স্ট্রেন্থ কেমন তা চেক করে নিতে পারেন এই সাইট থেকে http://www.passwordmeter.com/

প্রতিকার : সবসময় কঠিন ও জানকমন পাসওয়ার্ড ব্যবহার করুন। পাসওয়ার্ড তৈরিতে স্পেশাল কী ব্যবহার করুন। যেমন : @, #, $ । সাথে ক্যাপস লক ব্যবহার করতে পারেন। আরেকটা ভালো অপশন হতে পারে বাংলাতে পাসওয়ার্ড। যেমন : কারখানা-Karkhana, বিশ্ববিদ্যালয়-Bishobiddalo, শিক্ষা-Shikha।

ফাইল পারমিশন : অ্যাপাচি সার্ভারে কোনো ফাইলে সাধারণত তিন ধরনের পারমিশন থাকে। ফাইলটিকে পড়া, ফাইলটিতে লেখা, ফাইলটি এক্সিকিউট করা (শেল বা এক্সিকিউটেবল ফাইলের জন্য, ডাটা ফাইলের জন্য প্রজোয্য নয়)। মালিকানা থাকে তিন ধরনের : ফাইল ওনার (যে ফাইলটি তৈরি করেন), গ্রুপ ওনার (যে গ্রুপে থাকেন), পাবলিক (সবাই)। যদি কোনো ফাইলের পাবলিক রাইট দেয়া থাকে তাহলে যে কোনো হ্যাকার ফাইলটি রিরাইট করতে পারে।

প্রতিকার : কোনো সময়ই কোনো ফাইলের পাবলিক রাইট পারমিশন দেয়া যাবে না।

জুমলা সাইটের নিরাপত্তা চেক লিস্ট : একজন জুমলা অ্যাডমিনিস্ট্রেটরের সাইটের নিরাপত্তার স্বার্থে নিম্নলিখিত বিষয়গুলোর প্রতি নজর রাখা উচিত।

০১. ভালো মানের একটি ওয়েব হোস্টিং : সাইট হোস্টিংয়ের জন্য সবচেয়ে ভালো ভালো মানের ডেডিকেটেড সার্ভার ব্যবহার করা। কিন্তু সার্ভার অনেক দামি হওয়ায় অনেক সময় ডেডিকেটেড সার্ভার কেনা সম্ভব হয় না। তাই যদি ডেডিকেটেড সার্ভার ব্যবহার না করেন তাহলে দেখে নিতে হবে ওই শেয়ার্ড সার্ভারে কোনো হাই ট্রাফিক বা পর্নো সাইট আছে কি না। যদি থাকে তাহলে অবশ্যই তা পরিহার করুন। http://www.robtex.com/dns/ সাইটের মাধ্যমে দেখে নিতে পারেন শেয়ার্ড সার্ভারে আর কোন কোন ওয়েবসাইট হোস্ট করা হয়েছে।

০২. নিয়মিত ব্যাকআপ নেয়া : নিয়মিত সাইটের ব্যাকআপ নিতে হবে। যাতে কোনো কারণে যদি সাইটটি হ্যাকিংয়ের শিকার হয় তাহলে যেনো সাইটিকে আগের অবস্থায় ফিরিয়ে আনা যায়। তবে মনে রাখতে হবে, কোনো অবস্থায়ই ব্যাকআপ কপি সার্ভারে রাখা যাবে না। কারণ এতে ব্যাকআপ কপিটি সহজেই হ্যাকাররা নষ্ট বা খারাপ কাজে ব্যবহার করতে পারে।

০৩. সার্ভার সম্পর্কিত সেটিং ঠিক করা : অ্যাপাচি সম্পর্কিত নিরাপত্তা : htaccess ফাইলের মাধ্যমে আমরা ফাইল বা ডিরেক্টরির নিরাপত্তা দিতে পারি। জুমলা প্যাকেজে htaccess.txtটি থাকে। ফাইলটি .htaccess নামে সেভ করতে হবে। .htaccess ফাইলের মাধ্যমে আমরা ডিরেক্টরিতে পাসওয়ার্ড দিতে পারি। এই ফাইলটি ব্যবহার করে কোন কোন বিশেষ আইপি অ্যাড্রেস থেকে শুধু অ্যাডমিনিস্ট্রেটিভ কাজ করা যাবে তাও বলে দেয়া যায়। এ ক্ষেত্রে বাকি কোনো আইপি অ্যাড্রেস থেকে অ্যাডমিনিস্ট্রেটিভ কাজ করা যাবে না।

ওয়েব সার্ভারের mod_security ও mod_rewrite কনফিগার অন করে দিতে হবে। যদি শেয়ার্ড সার্ভার ব্যবহার করেন, তাহলে হোস্টিং প্রোভাইডারের সাথে কথা বলে নিতে হবে, যাতে তারা এই দুটি সেটিং অন করেন।

ফাইল ফোল্ডার পারমিশন : জুমলা সোর্স ▸

কোডে নিম্নলিখিত পারমিশন দিতে হবে।

- DocumentRoot directory: 750 (e.g. public_html)
- Files: 644
- Directories: 755

কোনো অবস্থাতেই কোনো ফাইল বা ফোল্ডারে ৭৫৫ বা পাবলিক রাইট পারমিশন দেয়া যাবে না। ফাইল পারমিশন সম্পর্কে বিস্তারিত জানতে ব্রাউজ করুন http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s1-acctsgrps-rhlspec.html সাইটে।

পিএইচপি সেটিং : প্রথমে php.ini ফাইলটি সার্ভার থেকে দেখে php সেটিং সম্পর্কে ধারণা নিতে হবে। আপনার সার্ভারের রুট ডিরেক্টরিতে নিম্নলিখিত কোডটি একটি ফাইলে সেভ করে রান করে php সেটিং দেখে নিতে পারেন। ফাইলের extentionটি অবশ্যই .php হতে হবে (যেমন : test.php)।

```
<? php
Phpinfo ();
?>
```

নিম্নলিখিত বিষয়গুলো এই ফাইল থেকে দেখে নিতে হবে।

```
disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open
magic_quotes_gpc = 1
safe_mode = 0
register_globals = 0
allow_url_fopen = 0
```

যদি উপরোক্ত সেটিংগুলো এরকম না থাকে তাহলে php.ini ফাইলটি এডিট করতে হবে। শেয়ার্ড সার্ভারে php.ini ফাইটি এডিট করা সম্ভব নয়। তবে বেশিরভাগ শেয়ার্ড সার্ভার নিজস্ব php.ini সাপোর্ট করে। সে ক্ষেত্রে হোস্টিং প্রোভাইডারের কাছ থেকে php.ini ফাইলটি চেয়ে নিয়ে যথাযথ এডিট করে রুট ডিরেক্টরি ও অ্যাডমিনিস্ট্রেটর ডিরেক্টরিতে রাখতে হবে।

০৪. **জুমলার সেটআপ সম্পর্কিত নিরাপত্তা :** প্রথমত, জুমলা প্যাকেজটি জুমলা ওয়েবসাইট (www.joomla.org) থেকে ডাউনলোড করতে হবে। যতদূর সম্ভব সর্বশেষ সংস্করণটি ব্যবহার করতে হবে। পুরনো ভার্সন ব্যবহার করলে অবশ্যই কোনো সিকিউরিটি প্যাচ আছে কি না তা জুমলা সাইট থেকে দেখে নিতে হবে। জুমলা প্যাকেজটি ভারনারেবল কি না তা MD5 হ্যাকিংয়ের মাধ্যমে পরীক্ষা করা যেতে পারে।

সেটআপের সময় ডাটাবেজ প্রিফিক্স হিসেবে ডিফল্ট jos থাকে। নিরাপত্তার স্বার্থে অন্য কিছু দেয়া উচিত, যাতে কোনো হ্যাকার প্রিফিক্স সম্পর্কে ধারণা করতে না পারে।

সেটআপের পর কোনোভাবেই যাতে configuration.php ফাইলটিতে পাবলিক রাইট অ্যাকসেস না থাকে। সম্ভব হলে ফাইলটি অন্য কোনো ডিরেক্টরিতে রাখা যেতে পারে।

জুমলা সাইট সেটআপ দেয়ার আগে নিম্নের লিঙ্কটি ভিজিট করে সিকিউরিটি সম্পর্কে ধারণা নেয়া উচিত যেকোনো সাইট অ্যাডমিনিস্ট্রেটরের।

http://docs.joomla.org/Security_Checklist_1_-_Getting_Started

০৫. **নিয়মিত সাইটের কনফিগারেশন ও লগ চেক করা :** নিয়মিত সাইটের কনফিগারেশনগুলো দেখতে হবে যাতে কোনো সেটিং পরিবর্তন হলে ধরা পড়বে। সাইট অ্যাডমিনিস্ট্রেটর হিসেবে নিয়মিত বিরতিতে লগ ফাইলটি দেখতে হবে। কোনো অপ্রত্যাশিত ইভেন্ট চোখে পড়লে তা ভালো করে চেক করে প্রয়োজনীয় ব্যবস্থা নিতে হবে।

০৬. **উন্নতমানের পাসওয়ার্ড ব্যবহার করা :** আমাদেরকে অবশ্যই কঠিন কোনো পাসওয়ার্ড ব্যবহার করতে হবে।

জুমলা সাইটের ভাষ্য অনুযায়ী, ৫০ শতাংশ পর্যন্ত হ্যাকিং কমিয়ে ফেলা যায়, যদি অ্যাডমিন ইউজার নেমটি ব্যবহার না করা হয়। জুমলা ইনস্টল করার সময় অ্যাডমিন ইউজারটি তৈরি হয়। জুমলা ইনস্টল করার পরপরই একটি নতুন সুপার অ্যাডমিনিস্ট্রেটর তৈরি করে অ্যাডমিন ইউজারটি ডিজ্যাবল বা এডিট করতে হয়। সাইটে সাধারণত একের অধিক সুপার অ্যাডমিনিস্ট্রেটর না রাখা ভালো। ইনস্টলের পর সব অপ্রয়োজনীয় ফাইল সরিয়ে ফেলতে হবে।

০৭. **লাইভ সাইটে কোনো কিছু যোগ করার আগে :** তা লোকাল সাইটে পরীক্ষা করে নিতে হবে : কোনো নতুন ফিচার সাইটে যোগ করার আগে তা ঠিকমতো পরীক্ষা করে নিতে হবে। কোনো সিকিউরিটি হোল আছে কি না তা দেখে নিতে হবে। লাইভ সাইট থেকে সিকিউরিটি বাগ খোঁজা বোকামি হবে। কারণ হ্যাকাররাও সিকিউরিটি হোল বের করে সাইটের ক্ষতি করতে পারে। সিকিউরিটির ব্যাপারে নিশ্চিত হয়েই শুধু সেই কোড লাইভ সার্ভারে আপলোড করা উচিত। কোডটি নিম্নলিখিত টেস্টে করা উচিত

* এসকিউএল ইনজেকশন
* ক্রস সাইট স্ক্রিপ্টিং
* ফাইল পারমিশন

০৮. **থার্ড পার্টি কোনো এক্সটেনশন ইনস্টল করার আগে :** সতর্কতা অবলম্বন করতে হবে : যেকোনো থার্ড পার্টি কোনো এক্সটেনশন ইনস্টল করার আগে তার রিভিউটি পড়ে নিতে হবে। বিশেষ করে এক্সটেনশনটির কোনো ভালনারিবিলিটি আছে কি না তা দেখতে হবে। সবসময় জনপ্রিয় এক্সটেনশন ব্যবহার করলে এ ধরনের আক্রমণ থেকে রক্ষা পাওয়া সম্ভব।

০৯. **গুগল হ্যাকিং থেকে নিরাপত্তা :** গুগলের মাধ্যমে আমরা কোনো কাঙ্ক্ষিত ওয়েবসাইট খুঁজে বের করি। এ সুবিধা দেয়ার জন্য গুগল সবসময় বিভিন্ন ওয়েবসাইট ক্রল করতে থাকে। গুগল সাধারণত ব্যাপকভাবে পাওয়া যায় এমন ডাটা বা ডকুমেন্ট ক্রল করে। সুতরাং আমদের গোপনীয় ফাইল বা ফোল্ডার যাতে গুগল ক্রল বা ইন্ডেক্স করতে না পারে সেজন্য robot.txt ফাইলে বলে দিতে হবে। robot.txt ফাইলটি রুট ডিরেক্টরিতে থাকে। একটি robot.txt ফাইলে সাধারণত নিম্নলিখিত কনফিগারেশন থাকে বাই ডিফল্ট।

```
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Disallow: /xmlrpc/
```

কোনো ডিরেক্টরিকে ক্রল বা ইনডেক্সিংয়ের বাইরে রাখতে চাইলে এখানে লিখে দিতে হবে। গুগল হ্যাকিং থেকে নিরাপদ থাকার জন্য সবসময় অপ্রয়োজনীয় ফাইল সার্ভার থেকে সরিয়ে ফেলতে হবে।

১০. **গে-বাল কনফিগারেশন ফাইল সেটিং :** গে-বাল কনফিগারেশনের সার্ভার ট্যাবের ক্যাশ ও সেশন সেটিংয়ে অবশ্যই সংক্ষিপ্ত সময় দিতে হবে। আবার খুব কমও দেয়া উচি নয়, তাহলে কম সময়েই সেশন আউট হয়ে যাবে। ফলে বারবার সাইটে লগইন করতে হবে কাজ করার জন্য।

১১. **সাইট হ্যাক হলে সম্পূর্ণ সাইটটি আবার ব্যাকআপ থেকে কনফিগার করতে হবে :** সম্ভাব্য সব ধরনের সতর্কতামূলক ব্যবস্থা নেয়ার পরও দেখা যায় কোনো সাইট হ্যাক হতে পারে। কারণ কেউই কোনো ওয়েবসাইটের শতভাগ নিরাপত্তা নিশ্চিত করতে পারে না। কোনো সাইট হ্যাক হলে নিম্নলিখিত ব্যবস্থা নিতে হবে।

- প্রথমে লগ ফাইলটি পরীক্ষা করে দেখতে হবে কি কি ফাইলের ক্ষতি সাধিত হয়েছে।
- পুরো সাইটটি ব্যাকআপ থেকে পুরোপুরি নতুন করে ইনস্টল করা হলো সবচেয়ে উত্তম।
- কোনোভাবেই শুধু index.php ফাইলটি নতুন করে আপলোড করে কাজ শেষ করা যাবে না। কারণ হ্যাকাররা অন্য ফোল্ডারে খারাপ কোনো স্ক্রিপ্ট আপলোড করতে পারে।
- ডাটাবেজের ইন্টিগ্রিটি ঠিক আছে কি না তা দেখতে হবে। যদি কোনো ডাটাবেজ এন্ট্রি পরিবর্তন হয় তাহলে তা যথাযথভাবে ঠিক করতে হবে। সবচেয়ে ভালো হয় যদি পুরো ডাটাবেজটি ব্যাকআপ থেকে আবার ইমপোর্ট করা হয়।
- লগ এবং অন্যান্য ইনফরমেশন থেকে হ্যাকিংয়ের কারণ চিহ্নিত করতে হবে এবং তা ফিক্স করতে হবে।
- সাইটের অ্যাডমিনিস্ট্রেটিভ পাসওয়ার্ডটি পরিবর্তন করতে হবে।

১২. **নিয়মিত জুমলা সিকিউরিটি ফোরাম ভিজিট করা :** জুমলার সিকিউরিটির জন্য আলাদা একটি ফোরাম আছে। নিয়মিত ফোরামটিতে চোখ রাখতে হবে, যাতে জুমলার সর্বশেষ বাগ বা ভারনাবিলিটি সম্পর্কে আপডেট থাকা যায়। তা ছাড়া এখান থেকে সিকিউরিটি প্যাচ সম্পর্কেও জানা যাবে। সিকিউরিটি নিয়ে কোনো সমস্যা বা প্রশ্ন থাকলে এখান থেকে সহজেই সমাধান পাওয়া সম্ভব। সিকিউরিটি ফোরামের ঠিকানা হলো : http://forum.joomla.org/viewforum.php?f=432

ফিডব্যাক : jabedmorshed@gmail.com