ই-কমার্স সাইটের নিরাপত্তা ইস্যু

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

সম্প্রতি ই-কমার্স সাইটের সংখ্যা যেমন বেড়েছে, তেমনি বেড়েছে ই-কমার্স সাইটগুলোতে বিভিন্ন আক্রমণের ঘটনা। এর মধ্যে কিছু আক্রমণ অনলাইন পেমেন্ট বিষয়ক, আবার কিছু আক্রমণ সাধারণ ওয়েবের নিরাপত্তা দুর্বলতাকেন্দ্রিক। সাধারণ ওয়েবের নিরাপত্তার দুর্বলতার মধ্যে আছে এসকিউএল ইনজেকশন, ক্রসসাইট স্ক্রিপটিং, ইনফরমেশন ডিসক্লোজার, পাথ ডিসক্লোজার ও বাফার ওভার ফ্লো। আর পেমেন্ট বিষয়ক আক্রমণের মধ্যে রয়েছে পেমেন্ট ম্যানিপুলেশন ও ভুয়া ক্রেডিট কার্ড ব্যবহার ইত্যাদি।

এ ধরনের আক্রমণ করে ই-কমার্স সাইটের বিভিন্ন ধরনের ক্ষতি করা সম্ভব, তার কনফেডেনশিয়ালিটি কম্প্রোমাইজ করা সম্ভব এবং সবচেয়ে বাজে ক্ষেত্রে ওয়েবসাইট বন্ধ করে দেয়াও সম্ভব।

ই-কমার্স সাইটে বিভিন্ন কারণে সিকিউরিটি সমস্যা হতে পারে। এজন্য কোনো একটি বিশেষ টেকনোলজি দায়ী এমন নাও হতে পারে। কেননা এটি অনেকগুলো টেকনোলজির সমন্বয়। ফলে শুধু কোনো একটি বিশেষ প্রযুক্তির কারণেও ই-কমার্স সাইটে সমস্যা হতে পারে। তবে সিকিউরিটি সমস্যার অন্যতম মূল কারণ হলো ওয়েবসাইট ডেভেলপাররা সিকিউরড প্রোগ্রামিং টেকনিক সম্পর্কে তেমন জানেন না। তাই এরা কোনো ওয়েব অ্যাপ্লিকেশন ডেভেলপ করার সময় সিকিউরিটির বিষয়টি তেমন লক্ষ রাখেন না বা লক্ষ রাখতে পারেন না। ডিজাইনের সময় সিকিউরিটির বিষয়টি উপেক্ষা করার আরো একটি অন্যতম কারণ হলো ডেডলাইন। ডেভেলপারদের সবসময় কঠিন ডেডলাইনের মধ্যে কাজ করতে হয়।

অনেক সময় দেখা যায়, ই-কমার্স সাইটগুলোতে ১২৮ বিট এসএসএল সার্টিফিকেট দেখানো হয় সাইটটি যে সিকিউরড তা প্রমাণ করার জন্য। কিন্তু শুধু এসএসএল সার্টিফিকেট দিয়েই একটি ই-কমার্স সাইটের সিকিউরিটি দেয়া সম্ভব নয়। এখানে ই-কমার্স সাইটের বিভিন্ন সিকিউরিটি ভলনারিবিলিটি নিয়ে আলোচনা করা হলো।

এসকিউএল ইনজেকশন

এসকিউএল ইনজেকশন হলো এসকিউএল কমান্ড/কোয়ারি, যা ব্যবহারকারীর দেয়া তথ্যের সাথে এমনভাবে যুক্ত হয় যাতে এটি অ্যাকসেস কন্ট্রোল সিস্টেমকে বাইপাস করে ডাটাবেজের তথ্য সংযোজন, বিয়োজন বা প্রদর্শন করতে পারে। এই আক্রমণের মাধ্যমে হ্যাকার ডাটাবেজে থাকা যেকোনো তথ্য চুরি করতে পারে। এটা হতে পারে ব্যক্তিগত তথ্য, ক্রেডিট কার্ড নম্বর অথবা অন্য কোনো সংবেদনশীল তথ্য।

/** Example of SQL Injection **/

উপরোল্লিখিত এইচটিএমএল স্নিপেটটিতে একটি বেসিক অথেনটিকেশন মেথড দেখানো হয়েছে। ব্যবহারকারীর কোডেনশিয়াল (ইউজার নেম ও পাসওয়ার্ড) Login_Account.php ফাইলের মাধ্যমে দেয়া হয়। ঠিকমতো ইনপুট ভ্যালিডেশন করা না হলে এ ধরনের ভলনারিবিলিটি বা ত্রুটিকে ব্যবহার করে ম্যালিশাস এসকিউএল স্টেটমেন্টের (যেমন Select * from LOGIN where username='john_smith' and password = ' ' or 1=1;) মাধ্যমে অথেনটিকেশন মেথডকে বাইপাস করা সম্ভব।

এসকিউএল ইনজেকশন পদ্ধতি বিভিন্ন ডাটাবেজ টাইপের ওপর ভিত্তি করে বিভিন্ন হতে পারে। উদাহরণস্বরূপ, ওরাকল ডাটাবেজে প্রধানত UNION কিওয়ার্ডের মাধ্যমে আক্রমণ করা হয়। অন্যদিকে MS SQL সার্ভার লোকাল সিস্টেমের প্রিভেলেজ নিয়ে রান করে এবং 'xp_cmdshell'-এর প্রসিডিউর এক্সিকিউট করতে পারে, যেটা যেকোনো সিস্টেম লেভেল কমান্ড এক্সিকিউট করতে পারে।

```
<form method="post" action="Login_Account.php">
<input type="text" name="username">
<input type="password" name="password">
</form>
```

চিত্র-১ : অ্যাক্সিস প্রক্সির মাধ্যমে প্রাইজ মডিফাই

```
int main (int argc, char const *argv[])
{
char buffer1[5] = "VXYZ";
char buffer2[5] = "PQRS";
strcpy(buffer2, argv[1]);
printf("buffer1: %s, buffer2: %s\n", buffer1, buffer2);
return 0;
}
```

চিত্র-২ : ই-মেইলের মধ্যমে ভুল লিঙ্ক প্রেরণ

বাফার ওভার ফ্লো

বাফার ওভার ফ্লো হয় যখন কোনো একটি প্রোগ্রামের ইনপুট তার বরাদ্দ করা মেমরির চেয়ে বেশি জায়গায় লিখতে পারে। কোনো একজন হ্যাকার বাফার ওভার ফ্লো ব্যবহার করে পুরো প্রোগ্রামের কন্ট্রোল নিতে পারে বা প্রোগ্রামটি ক্র্যাশ করিয়ে দিতে পারে। C ও C++ ল্যাঙ্গুয়েজ সাধারণত বাফার ওভার ফ্লোতে বেশি আক্রান্ত হয়। জাভাতে অ্যারে বাউন্স ফাংশনালিটির কারণে সরাসরি মেমরি অ্যাকসেস করা যায় না। তাই জাভা সাধারণত বাফার ওভার ফ্লো-তে কম আক্রান্ত হয়।

/** Example of Buffer Overflow **/

এই উদাহরণে আরগুমেন্টটি বাফার ২-তে কোনো ধরনের চেকিং ছাড়াই কপি করা হয়েছে। এ নিরাপত্তা ত্রুটিটি বাফার ওভার ফ্লোর মাধ্যমে এক্সপ্লোয়েট করা সম্ভব।

ক্রস সাইট স্ক্রিপটিং

ক্রস সাইট স্ক্রিপটিং সমস্যাগুলো সাধারণত ওয়েবসাইটগুলোতে পাওয়া যায়। এর মাধ্যমে হ্যাকারেরা সাধারণত ম্যালিশাস ডাটা পাঠায়। এর ফলে এরা অ্যাকসেস কন্ট্রোল সিস্টেমকে বাইপাস করতে সক্ষম হয়। এতে আক্রান্তের ওয়েব ব্রাউজারে ম্যালিশাস ডাটা দেখা যায়। অনেক সময় স্থায়ীভাবেও ম্যালিশাস ডাটা কোনো ওয়েবসাইটে স্টোর করা যায়। এ ধরনের আক্রমণের মাধ্যমে হ্যাকারেরা ওয়েবসাইট ডিফেস, কুকি চুরি, গুরুত্বপূর্ণ তথ্য চুরি বা ফিশিং অ্যাটাক করে থাকে।

/** Example of Cross-Site Scripting **/

এই উদাহরণে কোডটি ইউজারের নাম নিয়ে তাকে অভ্যর্থনা জানায়। কিন্তু কোনো ধরনের ইনপুট ভ্যালিডেশন না থাকায় এই ত্রুটির মাধ্যমে ক্রস সাইট স্ক্রিপটিং করা সম্ভব।

অনিরাপদভাবে সরাসরি অবজেক্ট রেফারেন্সিং

অনেক সময় প্রোগ্রামাররা সঠিক অথরাইজেশন ব্যবহার না করে কোনো একটি রিসোর্সের যেমন ইউআরএল, ফরম্যাট প্যারামিটার বা ডাটাবেজ রেকর্ডকে প্রোগ্রামের ভেতরের অন্য কোনো মডিউলে ব্যবহার করেন। এতে একজন হামলার যার ওই রিসোর্সের ওপর অথারাইজেশন নেই, সেও ওই রিসোর্সটি ব্যবহার করতে পারে এবং ম্যানিপুলেট করতে পারে।

/** Example of Insecure Direct Object Reference **/

http://www.abc.com/resources/account ▸

s/information/getinfo.jsp?padeId=hel...

এই ধরনের ইউআরএল দিয়ে রিসোর্স অ্যাকসেস করার ক্ষেত্রে যদি সঠিক অথরাইজেশন ব্যবহার করা না হয়, তবে হ্যাকাররা ডিরেক্টরি ব্রাউজিংয়ের মাধ্যমে অন্য ফোল্ডারের ডাটা অ্যাকসেস করতে পারে, যা তাদের অ্যাকসেস করতে পারার কথা নয়।

সঠিকভাবে এরর হ্যান্ডেল না করা

যদি সঠিকভাবে এরর হ্যান্ডেল করা না হয়, তবে অনেক সময় অনেক গুরুত্বপূর্ণ সেনসেটিভ তথ্য প্রকাশ পেয়ে যেতে পারে। এ ধরনের তথ্য হ্যাকারেরা ব্যবহার করে থাকে তাদের হামলার মেথড ঠিক করার সময়। ভুলভাবে এরর হ্যান্ডেলিংয়ের ফলে সিস্টেম ক্র্যাশ, টার্মিনেট অথবা রিস্টার্ট হয়ে যেতে পারে। প্রায় প্রত্যেক জনপ্রিয় প্রোগ্রামিং ল্যাঙ্গুয়েজের এক্সসেপশন হ্যান্ডেলিংয়ের ম্যাকানিজম আছে, যা দিয়ে অনাকাঙ্ক্ষিত ডাটা বের হয়ে যাওয়া থেকে প্রোগ্রামকে রক্ষা করা সম্ভব।

/** Example of Improper Error handling and information Leakage **/

404 Not Found

Not Found

The requested URL /abc/xyz_help/ was not found on this server

Apache/ 2.2.3(Debian) PHP/5.2.0-8+etch13 mod_ssl/2.2.3 OpenSSL/0.9.8c server at abc.pqr.de port 80

এই উদাহরণে এরর ম্যাসেজটি ওয়েব সার্ভার, অপারেটিং সিস্টেম, পোর্ট নম্বর, পিএইচপি ভার্সনসহ অন্যান্য তথ্য প্রকাশ করে দিচ্ছে।

প্রাইজ ম্যানিপুলেশন

এই ভলনারিবিলিটি ব্যবহার করে অনলাইন শপিং সাইটগুলোর ক্ষেত্রেই বড় ধরনের আক্রমণ ঘটে থাকে। এই ধরনের আক্রমণে আক্রমণকারী পরিশোধ করা টাকার পরিমাণ পরিবর্তন করতে পারে। একজন আক্রমণকারী কোনো প্রক্সি যেমন অ্যাক্লিস ব্যবহার করে পেঅ্যাবল অ্যামাউন্ট মডিফাই করে যখন এই তথ্য ব্যবহারকারীর ব্রাউজার থেকে ওয়েব সার্ভারে যায়। এখানে চিত্রের মাধ্যমে এ ধরনের একটি আক্রমণ দেখানো হয়েছে।

ফাইনাল পেঅ্যাবল প্রাইসকে (currency=Rs&amount=879.00) মডিফাই করে আক্রমণকারী তার মনমতো সংখ্যা বসিয়ে দিতে পারে। এই তথ্য ই-কমার্স সাইট থেকে পেমেন্ট গেটওয়েতে যাবে। ফলে ই-কমার্স সাইট স্বত্বাধিকারীর বড় ধরনের আর্থিক ক্ষতির সম্ভাবনা রয়েছে।

ফিশিং অ্যাটাক

ই-কমার্স ওয়েবসাইট অ্যাকসেস করার জন্য ব্যবহারকারীকে ইউজারনেম ও পাসওয়ার্ড ব্যবহার করতে হয়। এখন যদি কেউ তার ইউজারনেম ও পাসওয়ার্ড চুরি করতে পারে তবে সে ওই ব্যবহারকারীর সব তথ্য জেনে যেতে পারবে বা পরিবর্তন করতে পারবে।

মাছকে ধোঁকা দিয়েই আমরা মাছ ধরি অর্থাৎ আমাদের বড়শিতে গেঁথে দেয়া খাদ্য মাছ খেতে আসে। তারপর সে নিজেই আমাদের খাদ্যে পরিণত হয়ে যায়। এই Fishing-এর মতো আপনিও Phisher/Hacker-এর Phishing জালে আটকা পড়ে যেতে পারেন। Phishing ব্যাপারটি এমনই। কমপিউটার ব্যবহারকারীকে ধোঁকা দিয়ে ব্যবহারকারীর সব তথ্য Phisher নিয়ে নেবে। কিভাবে ঘটতে পারে ব্যাপারটি?

০১. ব্যবহারকারী যেসব ওয়েবসাইট ব্যবহার করেন, সেরকম কোনো একটি ওয়েবসাইটের হুবহু একটি লগইন পেজ পাঠানো হয় ব্যবহারকারীকে। সাধারণত এটি ই-মেইলের মাধ্যমে হয়ে থাকে।

০২. ই-মেইলের মাধ্যমে একজন হ্যাকার একটি ফেক লিঙ্ক দিয়ে থাকে। ব্যবহারকারী সেই লিঙ্কে ক্লিক করলে সেই ফেক ওয়েবসাইটে যাবে। এখন যদি ব্যবহারকারী সেখানে তার ইউজারনেম ও পাসওয়ার্ড দেন তবে তা ওই সাইটে না গিয়ে সেই ফেক ওয়েবসাইটের মাধ্যমে হ্যাকারের কাছে চলে যাবে।

০৩. তারপর হ্যাকার ব্যবহারকারীকে জানায় তার ইউজারনেম ও পাসওয়ার্ডটি ভুল। কিন্তু প্রকৃতপক্ষে সে ইউজারের ইউজারনেম ও পাসওয়ার্ডটি নিজের কমপিউটার বা সার্ভারে কপি করে রাখে এবং পরে তা ব্যবহার করে ব্যবহারকারীর অ্যাকাউন্টের কর্তৃত্ব নিয়ে নেয়।

দুর্বল অথেনটিকেশন ও অথরাইজেশন পদ্ধতি

যেসব অথেনটিকেশন পদ্ধতিতে একাধিকবার ভুল লগইনের ব্যাপারে কোনো ধরনের নিরাপত্তা ব্যবস্থা নেয়া হয় না সেসব সাইটে বিভিন্ন হ্যাকিং টুল যেমন বুটাস ব্যবহার করে আক্রমণ করা হয়ে থাকে। আবার যদি ই-কমার্স সাইটে HTTPS প্রটোকল ব্যবহার করা না হয় তবে আক্রমণকারী সহজেই স্নিপিং অ্যাটাকের মাধ্যমে ব্যবহারকারী বা ক্রেতার ইউজারনেম ও পাসওয়ার্ড চুরি করতে পারে।

প্রতিকার ও প্রতিরোধ

প্রথম কথা হলো ই-কমার্স সাইট তৈরি করার সময় ডিজাইন ফেস থেকেই সিকিউরিটির বিষয়টি মাথায় রাখা উচিত। ডিজাইন ফেসে বিস্তারিত রিস্ক অ্যাসেসমেন্ট করাটা খুবই গুরুত্বপূর্ণ। এখানে একজন নিরাপত্তা বিশেষজ্ঞকে ওয়েববাইটের অ্যাসেট, তৎসংশ্লিষ্ট ঝুঁকি ও তার কাউন্টার মেজার নিয়ে বিস্তারিত পরিকল্পনা করতে হবে। প্রতিটি বিষয়কে তার গুরুত্বানুযায়ী ভাগ করতে হবে ও সে অনুযায়ী ব্যবস্থা নিতে হবে। পাল্টা ব্যবস্থার মধ্যে থাকবে স্ট্রিক্ট ইনপুট ভ্যালিডেশন, ৩ টায়ার মডুলার আর্কিটেকচার, ওপেন সোর্স ক্রিপটোগ্রাফিক স্ট্যান্ডার্ড এবং নিরাপদ কোডিং অভ্যাস।

শেষ কথা

উপরে উল্লিখিত ব্যবস্থাগুলো সঠিকভাবে প্রয়োগ করলে আশা করা যায়, ই-কমার্স সাইটগুলো আরো অনেক বেশি নিরাপদ হবে। তবে ওয়েব বা ইন্টারনেট দুনিয়ার শতভাগ সিকিউরড সিস্টেম বলে কিছু নেই। তাই সব ধরনের নিরাপত্তা ব্যবস্থা নেয়ার পরও সাইটটি হ্যাকিংয়ের কবলে পড়তে পারে। তাই কোনো ই-কমার্স সাইট হ্যাকিংয়ের কবলে পড়লে, তা কিভাবে আবার ফাংশনাল করতে হয় সে সম্পর্কে ই-কমার্স সাইটের অ্যাডমিনের স্বচ্ছ ধারণা থাকতে হবে।

রেফারেন্স ও গুরুত্বপূর্ণ রিসোর্স

01. SQL injection and Oracle, Pete Finnigan http://www.securityfocus.com/infocus/1644
02. Advanced SQL injection, Chris Anley http://www.nextgenss.com/papers/advanced_sql_injection.pdf
03. News article on SQL Injection vulnerability at Guess.com http://www.securityfocus.com/news/346
04. Jeremiah Jacks at work again, this time at PetCo.com http://www.securityfocus.com/news/7581
05. Achilles can be downloaded from http://achilles.mavensecurity.com/
06. CERT Advisory Malicious HTML HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA-2000-02.html
07. Definition of 'phishing' http://www.webopedia.com/TERM/p/phishing.html
08. Brutus can be downloaded from http://www.hoobie.net/brutus/
09. Brute-Force Exploitation of Web Application Session IDs, David Endler http://www.idefense.com/application/poi/researchreports/display
10. Secure Programming for Linux and Unix HOWTO, David Wheeler, www.dwheeler.com/secure-programs
11. OWASP Guide http://www.owasp.org কজ

ফিডব্যাক : jabedmorshed@yahoo.com