# 1.HTTP request কি?

**Answer:**এটি একটি নেটওয়ার্ক প্রোটোকল যা প্রধানত ইন্টারনেটে HTML (Hyper-Text Markup Language) ডেটাকে আদান প্রদান করার জন্য ব্যবহার করা হয়। এই প্রোটোকলটিতে বেশকিছু নিয়ম থাকে যার ওপর ভিত্তি করে কোনও ওয়েব ব্রাউজার এবং সার্ভারের মধ্যে তথ্য আদান প্রদান করা হয়।

**2.HTTP request** এর মেথডগুলো কি কি এবং সেগুলো কখন ব্যবহৃত হয়? উদাহরণ সহ HTTP request এর অংশগুলো কি কি?

## HTTP Methods :

* GET (প্রাপ্ত করুন): এই মেথডটি একটি সহজ HTTP রিকোয়েস্ট প্রেরণ করে যা নির্দিষ্ট রিসোর্সের তথ্য অনুরোধ করে।
* POST (পোস্ট করুন): এই মেথডটি নতুন ডেটা সার্ভারে প্রেরণ করে, যাতে সার্ভার নতুন ডেটা স্থানান্তর করতে পারে।
* PUT (আপডেট করুন): এই মেথডটি একটি রিসোর্স সার্ভারে আপডেট করতে ব্যবহৃত হয়।
* HEAD (শিরোনাম প্রাপ্ত করুন): এই মেথডটি শুধুমাত্র রিসোর্সের শিরোনাম এবং হেডার তথ্য প্রাপ্ত করার জন্য ব্যবহৃত হয়, কিন্তু রিসোর্সের কোনও বডি ডেটা প্রাপ্ত করা হয় না।
* DELETE (মুছে ফেলুন): এই মেথডটি একটি রিসোর্স মুছে ফেলতে ব্যবহৃত হয়।
* PATCH (প্যাচ দিন): এই মেথডটি একটি রিসোর্সে ছোট পরিবর্তন প্রয়োজন হলে ব্যবহৃত হয়।
* OPTIONS (বিকল্পগুলি প্রাপ্ত করুন): এই মেথডটি সার্ভার থেকে বর্তমান রিসোর্সে যে বিকল্পগুলি প্রয়োজন আছে তা জানার জন্য ব্যবহৃত হয়।
* CONNECT (সংযুক্ত করুন): এই মেথডটি একটি প্রক্সি সার্ভারের সাথে সুরক্ষিত সংযোগ স্থাপন করতে ব্যবহৃত হয়।
* TRACE (ট্রেস করুন): এই মেথডটি একটি রিসোর্সের রিকোয়েস্ট পাঠানোর পর উত্তর পেতে ব্যবহৃত হয়, যা রিকোয়েস্টের পথের ট্রেসের মাধ্যমে সাহায্য করে।

**3.HTTP request headers কি এবং সিকিউরিটির জন্য কেন গুরুত্বপূর্ণ?**

যে কোনো ওয়েবসাইটের নিরাপত্তা নিশ্চিত করণে HTTP Security Headers খুবই গুরুত্বপূর্ণ। এটি ওয়েবসাইটকে হ্যাকারদের বিভিন্ন আক্রমণ থেকে সুরক্ষা প্রদান করে।

যখন কোনো ভিজিটর বা হ্যাকার কোনো ওয়েবসাইটের পেজ এক্সেস করতে চায়, তখন ব্রাউজার প্রথমেই ওয়েব সার্ভারে একটি রিকোয়েস্ট পাঠায়।

তারপর উক্ত রিকোয়েস্টের ভিত্তিতে সার্ভার ওয়েব পেজের Meta ডেটা, স্ট্যাটাস Error কোড, Cache রুলস ইত্যাদি ধারণ করে স্বয়ংক্রিয় ভাবে তার উপযুক্ত HTTP Response Headers এর মাধ্যমে রেসপন্স করে।

এটি মূলত ব্যবহারকারীর ব্রাউজারকে বলে দেয় কাঙ্খিত ওয়েব পেজটি ব্রাউজারে কিভাবে প্রদর্শন করবে। কোনো ওয়েবসাইটে যদি Headers Security না থাকে তবে সেই ওয়েবসাইটে যে কোনো ধরণের [সাইবার ক্রাইম](https://www.itnirman.com/%e0%a6%b8%e0%a6%be%e0%a6%87%e0%a6%ac%e0%a6%be%e0%a6%b0-%e0%a6%95%e0%a7%8d%e0%a6%b0%e0%a6%be%e0%a6%87%e0%a6%ae/) হতে পারে।

বিশেষ করে নতুন ওয়েবসাইট মালিকেরা বেশিরভাগ ক্ষেত্রে হ্যাকিংয়ের শিকার হয়ে থাকে। কেননা, নতুন ওয়েবসাইট গুলোর Header এর HTTP Security খুব ভালো থাকে না।

হ্যাকারেরা এই সুযোগকে কাজে লাগিয়ে XSS, কোড ইনজেকশন, ক্লিকজ্যাকিং ইত্যাদি পদ্ধতি ব্যবহার করে বিভিন্ন ওয়েবসাইটে সাইবার আক্রমণ করে।

আপনি যদি একজন ওয়েব মাস্টার বা ওয়েবসাইটের owner (মালিক) হয়ে থাকেন, তবে আপনার ওয়েবসাইটের নিরাপত্তা প্রদানে HTTP Security Headers নিশ্চিত করা আবশ্যক।

4.উদাহরণ সহ HTTP request এর অংশগুলো কি কি?

* HTTP Method (অপারেশন প্রকার): এটি ব্যবহারকারীর ইচ্ছা অনুযায়ী সার্ভারে কী প্রকারের অপারেশন সম্পাদন করা আবশ্যক তা নির্দেশ করে। উদাহরণস্বরূপ GET, POST, PUT, DELETE, ইত্যাদি।
* URI (Uniform Resource Identifier): রিকোয়েস্টে সেলেক্ট করতে চান যে রিসোর্সের উপর অপারেশন চালাতে হবে তা নির্দেশ করে। উদাহরণস্বরূপ, "<https://www.example.com/api/users>".
* HTTP Version: যে HTTP সংস্করণ ব্যবহার হচ্ছে তা নির্দেশ করে। উদাহরণস্বরূপ, "HTTP/1.1" বা "HTTP/2".
* Headers (হেডার): অতিরিক্ত নির্দিষ্ট তথ্য যেগুলি রিকোয়েস্ট বা রিস্পন্সের সাথে প্রেরণ হয়। হেডার মেটা-ডেটা সরঞ্জাম যা ব্যবহারকারীর সংজ্ঞায়িত করতে ব্যবহৃত হয়। উদাহরণস্বরূপ, "Content-Type: application/json", "Authorization: Bearer <token>", ইত্যাদি।
* Request Body (রিকোয়েস্ট বডি): এটি মুখ্যভাবে POST বা PUT মেথডে ব্যবহার হয়, এবং তথ্য এবং ডেটা পরিবর্তন করতে ব্যবহৃত হয়। এটি JSON, XML, বা অন্যান্য ডেটা ফরম্যাট হতে পারে।

এই উদাহরণ হল একটি সাধারণ GET রিকোয়েস্টের উদাহরণ:

GET /api/users HTTP/1.1

Host: www.example.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Accept: application/json