پاسخ سوال 1 :

وقتی مثلا آدرس google.com را میزنیم ابتدا مرورگر باید آدرس dns را داشته باشد. بنابر این از مراحل زیر dns را میپرسیم تا درصورت داشتن آن خبربدهد.

1. کامپیوتر
2. isp
3. سرور های dns برای دامنه های com

سپس مروگر مطابق قوانین TCP / IP و با استفاده از سرور آپاچی بخش های مختلف سایت را پیکربندی و نمایش میدهد.

پاسخ سوال 2 :

الگوریتم‌های رمزنگاری متقارن

رمزگذاری متقارن یک روش رمزگذاری است که از یک کلید واحد برای encryption (رمزگذاری) و decryption (رمزگشایی) داده‌ها استفاده می‌کند. کلید مخفی می‌تواند یک کلمه، یک شماره یا یک رشته از کارکترها یا اعداد باشد که توسط یک تولید کننده عدد تصادفی ایمن تولید شده است. پیام طبق قوانین الگوریتم رمزگذاری در کلید تغییر می‌کند. اشخاصی که از طریق رمزگذاری متقارن در حال برقراری ارتباط هستند باید کلید را مبادله کنند تا بتوانند اطلاعات را رمزگذاری و رمزگشایی کنند.

رمزنگاری متقارن کاربردهای زیادی در تکنولوژی امروزه دارد. برخی از کارشناسان امنیت تنها الگوریتم‌های نامتقارن را پیشنهاد می‌کنند در صورتی که در بسیاری از موارد کاربردهای این الگوریتم با الگوریتم‌های نامتقارن متفاوت است. برخی از پرکاربردترین و محبوب‌ترین الگوریتم‌های رمزنگاری متقارن عبارتند از:

* AES
* DES
* IDEA

الگوریتم رمزنگاری نامتقارن

رمزنگاری نامتقارن یک نسخه پیشرفته‌تر در رمزنگاری، نسبت به رمزنگاری متقارن است. این روش به رمزنگاری کلید عمومی نیز شهرت دارد زیرا یکی از کاربردهای آن، استفاده در زمانی است که یک کلید عمومی برای قفل مورد نظر تعریف می‌شود. این روش همچنین یکی از روش‌های محبوب است و امنیت سیستم را افزایش می‌دهد.

یکی از معروف‌ترین الگوریتم‌های رمزنگاری نامتقارن، الگوریم RSA است. الگوریتمی که از آن در امضاهای دیجیتال و بخش‌های PGP و SSL استفاده می‌شود.

. پاسخ سوال 3 :

به تبدیل یک عبارت ورودی به یک عبارت خروجی گفته می‌شود که مقدار خروجی قابل تبدیل به مقداراولیه نیست.

هش کردن یک فرایند یک طرفه است که در آن هر نوع داده خروجی درنهایت تبدیل به یک رشته داده خروجی با یک اندازه ثابت می‌شود.

از رمزنگاری بیشتر وقتی که میخواهیم پیام امنی را برای شخص دیگر در آن سوی دنیا بفرستیم ،در این صورت به جای استفاده هش کردن از رمزنگاری استفاده می‌کنیم.

در صورتی که تصمیم گرفتید از encryption استفاده کنید،باید تصمیم بگیرید از الگوریتم متقارن بهتر است استفاده کنید یا الگوریتم نامتقارن.که رمزنگاری متقارن عملکرد بهبود یافته ای را ارائه میدهد و استفاده از آن ساده تر است.

MD5 : یکی از محبوب ترین الگوریتم های تابع hashing است.این الگوریتم یک رشته ۱۶ بیتی را به عنوان خروجی ایجاد میکندکه معمولا به صورت یک رشته ۳۲ عددی نمایش داده می‌شوند.

اخیرا چند مورد آسیب پذیری در این الگوریتم کشف شده است و جداولی برای نگه داری مقادیر مختلفی مانند لیست پسوردهای مختلف به صورت هش شده،منتشر شده اند. که به اشخاص اجازه می‌دهند تا هش های MD5 را بدون saltهای خوبی تولید کنند.

SHA :به طور کلی سه نوع الگوریتم SHA وجود دارد

پاسخ سوال 4 :

متد Get به طور پیش فرض برای ارسال اطلاعات فرم‌ها به سرور استفاده می‌شود. این متد داده‌های یک فرم را برای سرویس دهنده ارسال می‌کند، به این شکل که به انتهای URL یک “نام/مقدار” را اضافه کرده و پارامترها را به کمک query string به سرور می‌فرستد.

مزایا و معایب استفاده از متد GET عبارتند از:

* از آن‌جایی که اطلاعات فرستاده شده با متد GET در URL آدرس صفحه نمایش داده می‌شوند، می‌توانید صفحه را با مقادیر query string مورد نظر خود بوک مارک (Bookmark) کنید.
* متد GET مناسب ارسال اطلاعات حساس و مهمی مثل نام کاربری، رمز عبور، اطلاعات کارت بانکی و… نیست، زیرا اطلاعات به طور کامل در query string آدرس صفحه قابل مشاهده است و اینکه در حافظه مرورگر کاربر به عنوان یک صفحه بازدید شده ذخیره می‌شود.
* متد GET دیتا را در یک متغیر داخل محیط سرور ذخیره می‌کند؛ به همین دلیل طول URL محدود شده و در نتیجه کل داده ارسالی ما محدود می‌شود.

متد POST داده‌ها را به صورت یک پکیج و در ارتباطی جداگانه به سرور ارسال می‌کند. داده‌هایی که به کمک متد POST ارسال می‌شوند، در URL صفحه نمایش داده نمی‌شوند و از لحاظ امنیتی انتخاب بسیار مناسبی هستند.

مزایا و معایب استفاده از متد POST عبارتند از:

* امنیت این روش ارسال اطلاعات بسیار بالا است و اطلاعاتی که کاربر تایپ می‌کند به هیچ عنوان در مرورگر قابل مشاهده نیست، علاوه بر آن، در گزارشات (Logs) سرور هم ذخیره نمی‌شوند.
* از آن‌جایی که اطلاعات ارسال شده‌ی صفحه با متد POST در URL دیده نمی‌شوند، نمی‌توان آن صفحه را در مرورگر Bookmark کرد.
* در متد POST محدودیت بسیار بیشتری برای ارسال اطلاعات وجود دارد. به کمک POST می‌توان داده‌های متنی و باینری (آپلود فایل) را ارسال کرد.