بنام خدا

موضوع : پاسخ سوالات بخش web

۱. به زبان خود بیان کنید وقتی از طریق مرورگر به آدرس سایتی درخواست میزنید محتوای این سایت چگونه نمایش داده میشود؟

پاسخ : هنگامی که ما URL رادر مرورگر وارد میکنیم مرروگر URLرا به سه قسمت تقسیم میکند : پروتکل (HTTP) ، نام سرویس دهنده(نام سایت) ، نام فایل(فایل HTML سایت) تقسیم میکند.

مرورگر نام سرویس دهنده را به DNS میدهد تا DNS آدرس IP را به مرورگر برگرداند (مراحل جستجوی DNS : مرورگر از رایانه میپرسد ، رایانه از اراِه دهنده خدمات خود (ISP) میپرسد ، آن هم ازسرورهای ROOT DNS جهان میپرسد وسپس ROOT DNSجستجو را به ریجستری ترجمه .ORG , .IR , .COM ,... میسپارد وسپس آدرس IP را به مرورگر میرساند)

سپس براساس پروتکل HTTP مرروگر یک در خواست GET را به سرویس دهنده ارسال میکند وسپس سرویس دهنده فایل متنی HTML مربوط به آن صفحه WEB را به مرورگر باز میگرداند.

۲. چند الگوریتم رمزنگاری در وب راتوضیح دهید

الگوریتم رمز نگاری سزار:

یکی از ساده ترین و مبتدیانه ترین روش های رمزنگاری است. در این روش شما کاراکتر ها را جلو و عقب می کنید. برای مثال حرفa b c ، b b dو همینطور تا y b aو z b b تبدیل می شود. این روش یکی از ساده ترین روش های رمز نگاری است که چندین سال است که روش هک آن نیز ازائه شده و الگوریتم خیلی مطمئنی نیست! نام این مدل رمزنگاری به این خاطر سزار شد زیرا سزار در دوران امپراطوری رم از این روش برای رمزنگاری پیام های خود استفاده می کرد.

الگوریتم رمزنگاری بلاک چین :

Block Chain یکی از جدید ترین و بروزترین انواع روش های رمزنگاری است که در محافظت از اطلاعات در ارز های دیجیتال مقل بیت کوین، ترون و ارز های دیجی تال دیگر از آن استفاده می شود. هنوز هیچ اطلاعاتی درباره طرز کار یا نحوه رمزنگاری اطلاعات در این روش وجود ندارد. در حال حاضر تلگرام نیز برای ارسال پیام ها و رسانه های مختلف، از این الگوریتم استفاده می کند.

بلاک چین به این شکل توصیف می شود که شما تعداد زیادی مکعب کوچک ۱ در ۱ در ۱ سانتی متر را تصور کنید که با فاصله یک سانتی متری از یکدیگر چیده شده اند و یک دیوار بزرگ را درست کرده اند. اطلاعات به صورت هزاران، میلیون ها یا میلیارد ها تکه کوچک وارد این مکعب ها می شوند از آنها به مقصد مکعب بعدی خارج می شوند. هر کدام از یک مسیر جدا حرکت می کنند و در آخر، به مقصد می رسند.

۳. Hash چیست و چه تفاوتی بارمز نگاری دارد؟چند الگوریتم هش را نام ببرید(به همراه یک مثال)

Hashing چیست؟

Hash یک رشته یا اعداد تولید شده از رشته‌ای متنی است. رشته یا عدد حاصل شده طول ثابتی دارد و با تغییرات کوچک در ورودی بسیار گسترده است. الگوریتم‌های hashing بسیار خوبی طراحی شده‌اند، به طوری که برگرداندن hash به رشته متنی اصلی غیرممکن است.

تفاوآن با رمزنگاری چیست؟

تفاوت اصلی بین رمزنگاری و hashing این است که در رمز نگاری اگر شما کلید درست را داشته باشید، رشته‌های رمزگشایی شده را می‌توان به فرم اولیه تبدیل کرد.اما در hashing برگرداندن رشته متنی تقریبا غیرممکن است (یعنی تا به حال کسی آن را انجام نداده)

انواع الگوریتم های hashing :

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.

مثال:

```php
<?php
$password = 'hello';

$password_hash = md5($password); // hashing

echo $password_hash; // result = 5d41402abc4b2a76b9719d911017c592
```

SHA : به طور کلی سه نوع الگوریتم SHA وجود دارد:

SHA-0 : که این الگوریتم به دلیل آسیب پذیری خیلی به ندرت مورد استفاده قرار می‌گیرد.

SHA-1 : خطاها و آسیب پذیری SHA-0 در این نسخه اصلاح شده اند و بیشترین استفاده را در بین الگوریتم های SHA دارد،و یک مقدار هش ۲۰ بیتی تولید می‌کند.

SHA-2 : شامل یک مجموعه ۶ عضوی از الگوریتم های hashing است و قدرتمندترین نوع SHA هااست

۱. تفاوت GET و POST در HTML چیست؟

GET و POST دو متد برای ارسال اطلاعات کاربر به وب سرور می باشند.به لحاظ امنیتی متد POST امنیت بیشتری دارد و به همین علت این دو متد تفاوت هایی دارند.

Get : اطلاعات کاربر از طریق URL منتقل می شود و اگر هر فرمی را ثبت کنید، اطلاعات URL برای هر کاربری قابل مشاهده می باشد. سپس اطلاعاتی که شما ارسال می کنید، در URL قابل مشاهده می باشند، و این اصلا امن نیست. یک محدودیت متد Get این است که فقط مجاز به انتقال ۱۰۲۴ کاراکتر می باشیم.

Post : در این متد اطلاعات از طریق http headers ارسال می شوند بنابراین با استفاده از پروتکل امن http داده ها امنیت بیشتری دارند.با استفاده از این متد می توان تعداد زیادی از داده ها و داده های باینری را انتقال داد وهیچ محدودیتی وجود ندارد.