آزمایشگاه امنیت شبکه

تابع چکیده‌ساز MD۵ و تابع HMAC

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با نحوه بکارگیری توابع چکیده ساز آشنا شویم.

آزمایش ۱-۳: صحت دریافت نرم افزار

- در آزمایش قبلی یک کلید عمومی برای سرور ایجاد کردیم و آن را در اختیار کلاینت قرار دادیم.
- در این آزمایش همین کار را برای کلاینت انجام دهید. یعنی یک کلید عمومی برای کلاینت ایجاد کرده و آن را در اختیار سرور قرار دهید.
- یک برنامه دلخواه بنویسید.
- سمت سرور مقدار MD۵ آنرا در محاسبه کنید.
- مقدار محاسبه شده را با کلید عمومی کلاینت رمز کنید.
- برنامه‌ای که نوشتید همراه با هش رمز شده مرحله‌ی قبل برای کلاینت ارسال کنید.
- در سمت کلاینت MD۵ برنامه دریافت شده از سمت سرور را محاسبه کنید.
- هش ارسال شده از طرف سرور را رمزگشایی و سپس این مقدار را با مقدار محاسبه شده هش نرم افزار دریافت شده مقایسه کنید.
- اگر مقادیر برابر بود برنامه را در سمت کلاینت اجرا کنید.

آزمایش ۲-۳: تداخل در توابع چکیده ساز

- یک برنامه متفاوت با برنامه‌ی قبلی بنویسید.
- این برنامه را طوری بنویسید که علی رغم تفاوت در عملکرد، کد و حتی نام، دارای MD۵ یکسان با برنامه قبلی باشد.
- بقیه مراحل را همانند آزمایش قبلی انجام دهید.

آزمایش ۳-۳: HMAC

- یک برنامه تحت وب بنویسید که شامل یک صفحه با یک فرم ورود کاربران باشد. این فرم شامل دو ورودی برای نام کاربری و کلمه عبور، یک کنترل دکمه برای ارسال اطلاعات به سرور و یک لینک فراموشی کله عبور می‌باشد.
- یک کاربر برای برنامه تعریف کنید.
- فرض کنید کاربر کلمه عبور خود را فراموش کرده و درخواست بازیابی می‌دهد.
- لینک بازیابی را طوری ایجاد کنید که فقط برای ۳ دقیقه معتبر باشد.
- همچنین مکانیزمی به کار ببرید که اگر لینک بیش از یکبار مورد استفاده قرار گرفت، عملیات موفقیت آمیز نباشد.