فاز دوم پروژه درس مبانی امنیت اطلاعات

نویسنده : ارشیا مخلص (9922762275) , ملیکا اسکافی (4012086(

<< توضیحات فاز اول در README.md>>

قسمت اول :

**شناسایی دارایی ها** و **ارزش گذاری آنها** :

ما چند قسمت داریم که برای ما با ارزش هستند :

* **اطلاعات کاربر ها** 
  + نام کاربری
    - ارزش آن پایین است و باید تا حد زیادی بقیه از آن اطلاع داشته باشند
  + رمز
    - ارزش رمز بسیار بالا است چون بدین گونه افراد دیگر میتوانند به جای شما وارد حساب شما بشوند و کنترل حساب شما را بدست بگیرند.
  + گروه هایی که در آنها عضو هستند
    - ارزش این داده بالا است چون افراد نمیخواهند که بقیه بدانند که آنها متعلق به چه گروهی هستند
  + کلید خصوصی
    - ارزش آن بسیار بالا است چون با این داده افراد دیگر میتوانند به جای شما به بقیه پیام بدهند یا کار های دیگری مانند اضافه کردن یا کم کردن از گروه و تغییر نقش دیگران را نیز انجام بدهند
  + کلید عمومی
    - ارزش پایینی دارد چون باید در دسترس همگان باشد
  + محرمانگی نقش
    - ارزش آن پایین است چون دانستن نقش توسط بقیه شاید خیلی مایه نگرانی نباشد
  + تمامیت نقش
    - ارزش آن بالا است چون اگر نقش شما را پایین تر بیاورند بعضی کار ها را نمیتوانید انجام دهید
* **اطلاعات مربوط به گروه ها** 
  + پورت مخصوص گروه
    - ارزش آن بالا است چون در صورت دانستن آن پورت بقیه نفوذ گر ها میتوانند به آن پیام بدهند و اگر کلید خصوصی یک کاربر را داشته باشند میتوانند برای آن گروه پیام بفرستند
  + کاربر های موجود در گروه
    - این لیست ارزش بالایی دارد چون در صورت داشتن این لیست محرمانگی اطلاعات کاربران نقض میشود
  + پیام های موجود در گروه
    - این داده ارزش بسیار بالایی دارد چون کل کارهایی که ما در حال انجام هستیم برای حفظ محرمانگی این پیام ها است و اگر کسی محرمانگی آنها را نقض بکند با اینکه ما کل **پیام** ها را بدون رمز بفرستیم هیچ تفاوتی ندارد.
    - این داده ارزش بسیار بالایی دارد و ستون و بدنه ی علت استفاده از رمزنگاری ها و ... برای ایجاد امنیت برای پیام ها میباشد.
* **اطلاعات مربوط به چت شخصی**
  + پیام های رد و بدل شده
    - این پیام نیز مانند دو مورد آخر ارزش بالایی دارد
* **سرور**
  + در دسترس بودن سرور
    - این منبع نیز از اهمیت بسیار بالایی برخوردار است به حدی که اگر سرور در دسترس نباشد انگار که هیچ برنامه ای وجود ندارد

تشخیص آسیب پذیری ها :

ابتدا برای منابعی که ارزش بسیار بالایی دارند خطرات را بررسی میکنیم

* رمز
* کلید خصوصی
* پیام ها
* سرور

سپس منابعی که ارزش بالایی دارند را مشخص میکنیم:

* گروه هایی که کاربرها در آن عضو هستند
* تمامیت نقش ها
* پورت مخصوص گروه

سپس منابعی که ارزش پایینی دارند را مشخص میکنیم:

* نام کاربری
* محرمانگی نقش
* کلید عمومی

**اقدامات لازم برای رفع آسیب پذیری:**

* در این قسمت ما به خاطر کم بودن وقت صرفا توضیح میدهیم که چه کار هایی باید انجام بدهیم چون بیشتر این کارها جنبه ی کد نوشتن دارند تا جنبه ی مفهومی
* در قسمت های زیادی ما پیام را به صورت فالش میفرستیم که میتوانیم آنها را با کلید عمومی طرف مقابل رمزنگاری کنیم و برای شخص مقابل بفرستیم و وقتی برای شخص مقابل فرستادیم او با کلید خصوصی خود پیام را باز کند تا محرمانگی پیام حفظ شود
  + در قسمت های زیر پیام ها نیاز به رمزنگاری دارند
    - موقعsignup, login فرستادن اطلاعات کاربر مانند رمز و ایمیل و ... به صورت فالش
    - هر بار که یک پیام را امضا میکنیم بهتر است آنرا رمز نگاری کنیم و بعد برای شخص مقابل بفرستیم
    - در قسمت add\_permissions زمانی که میخواهیم که نام کاربر تغییر نقش یافته و خود نقش را بفرستیم بهتر است آنرا رمزنگاری و امضا بکنیم
    - گاهی أوقات پیام هایی مانند “permission denied” یا "invalid signature" را به صورت فالش میفرستیم میتوانیم آنها را نیز رمز کنیم ولی خیلی نیاز نیست
* برخی اوقات نیز باید یک پیام را امضا کنید و برای شخص مقابل بفرستید تا شخص مقابل مطمئن شود که شما دارید پیام را میفرستید و شما را verify بکند که برای این کار باید ابتدا یک پیام را امضا کنید و پیام را به صورت فالش یا رمز شده به شخص مقابل بفرستید و اگر پیام امضا شده و پیام فرستاده شده به صورت فالش ارزیابی شدند و هویت شخص مقابل تایید شد مطمئن میشویم که پیام را شخص مورد نظر فرستاده است ( این پیام میتواند اسم کاربر مقابل باشد تا نخواهد که یک پیام دیگر به صورت فالش برای کاربر مقابل بفرستیم)
  + قسمت هایی که نیاز به امضا دارند
    - زمانی که میخواهیم آیدی گروه و پیام را بفرستیم تا بگوییم که پیام مورد نظر در گروه مورد نظر گذاشته شود باید یک امضا هم روی نام کاربری خود بزنیم و نام کاربری خود را به صورت رمز شده به سمت سرور برای تشخیص هویت خودمان بفرستیم
    - در بقیه قسمت امضا رعایت شده است

با تشکر

ملیکا اسکافی و ارشیا مخلص