دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

به نام خدا

تمرین عملی سوم درس امنیت کامپیوتر

پیاده‌سازی ابزار ساخت و مدیریت گذرواژه

دکتر حمیدرضا شهریاری

پاییز ۱۴۰۲

نکات مهم:

کد: استفاده از کتابخانه‌های موجود در زبان پایتون مجاز است. برای راحتی و درگیر نبودن با رابط کاربری گرافیکی، از کتابخانه argparse و رابط کاربری کامند لاینی (CLI) استفاده کنید.

گزارش: بخش اصلی ارزشیابی شما گزارش است؛ لذا ارسال کدها بدون گزارش شامل نمره نخواهد بود. گزارش باید شامل اسکرین‌شات از کد و خروجی و نحوه کار ابزارها باشد. همچنین سعی کنید توضیحی کوتاه درباره نحوه پیاده‌سازی و کارکرد توابع و کدها ارائه دهید.

تذکر: هر نوع کپی‌برداری غیرقابل‌قبول بوده و باعث درج نمره‌منفی برای هر دو طرف خواهد بود.

ارسال: فایل گزارش به همراه فایل کدها را به‌صورت یک فایل فشرده درآورده و آن را با فرمت prj3_studentfamilyname_studentnumber.zip در سامانه بارگذاری نمایید.

تأخیر: درمجموع ۱۰ روز تاخیر قابل قبول خواهد بود که هر روز تاخیر منجر به کسر ۵ درصد از نمره تمرین خواهد بود.

** در صورت نیاز می‌توانید سؤالات خود را در خصوص انجام تمرین، از طریق راه‌های ارتباطی زیر از تدریس یار بپرسید.

ایمیل: erf.mohammadi@aut.ac.ir

تعریف تمرین:

تمرین شامل دو بخش است.

بخش اول شامل پیاده‌سازی یک ابزار مدیریت گذرواژه و ساخت گذرواژه‌های پیچیده و امن است.

بخش دوم شامل استفاده از ابزار statsgen برای تحلیل گذرواژه‌های تولید شده توسط ابزار پیاده‌سازی شده است.

بخش ۱:

۱-۱- در تمرین عملی اول دیدید که امنیت گذرواژه رابطه مستقیمی با بزرگی فضای حالات گذرواژه دارد، اما مشگل از جایی شروع می شود که به خاطر سپاری یک گذرواژه با خصوصیات امنیتی خوب مشگل است و اکثر افرار گذرواژه های راحتی را انتخاب میکنند که از نظر امنیتی دارای در برابر حملات مرسوم گذرواژه آسیب پذیر هستند. همچنین اکثر افراد و کاربران در صورت انتخاب یک گذرواژه مناسب با فضای حالات بزرگ، آن را در محلی غیر امن ذخیره می کنند. یکی از راه حل های این چالش استفاده از ابزارهای مدیریت گذرواژه است.

این نوع از ابزارها باید دارای دو خصوصیت کلیدی باشند. اول باید توانایی تولید گذرواژه‌های امن و پیچیده را داشته باشد و دوم اینکه خود ابزار امن باشد.

در این بخش از شما خواسته شده است تا یک ابزار مدیریت گذرواژه را پیاده‌سازی کنید.

خصوصیات ابزار:

۱-ابزار شما باید توانایی این را داشته باشد که یک پسورد ساده که به خاطرسپاری آن برای کاربر آسان است را از کاربر گرفته و سپس از روی آن گذرواژه های پیچیده ای را تولید کند .

**:نکته ۱: برای اینکار میتوایند از توابع رمزنگاری استفاده کنید. برای مثال میتوانید از سیستم رمز AES استفاده کرده و از گذرواژه ساده داده شده توسط کاربر به عنوان متن واضح (ورودی سیستم رمز) و یا کلید سیستم رمز استفاده کنید.

**نکته ۲: غیر از روش رمزنگاری میتوانید از هر روش دیگری که به ذهنتان می رسد برای تولید گذرواژه از گذرواژه ساده داده شده توسط کاربر استفاده کنید اما دقت کنید که گذرواژه های تولید شده باید خواص امنیتی خوبی را دارا باشند. در صورت استفاده از هر روشی لطفا آن را به صورت مفصل در گزارش کار خود شرح دهید.

۲-ابزار شما باید توانایی مدیریت گذرواژه های تولیدی را داشته باشد. به این معنا که درهنگام ساخت گذروژه کاربر یک نام و یک متن به عنوان کامنت را برای گذرواژه ساخته شده انتخاب میکند که این نام نشان دهنده کاربرد آن و کامنت برای توضیح بیشتر برای استفاده آن گذرواژه برای آن شخص است.

برای مثال: کاربر یک گذرواژه با نام پورتال دانشگاهی و یک گذرواژه با نام بانک ملت می‌سازد.

بعد از ساخت این دو گذرواژه کاربر می‌تواند لیست گذرواژه‌های خود را مشاهده کند و با استفاده از نام آن‌ها، مقدار گذرواژه را مشاهده کند و یا آن را حذف کند و یا آن گذرواژه را آپدیت کند (مقدار گذرواژه جدید بسازد).

دقت کنید برای پیاده‌سازی بخش مدیریت گذرواژه‌ها، ابزار شما باید بتواند گذرواژه‌های ساخته شده را درون یک فایل متنی ذخیره کند، و همچنین برای حفظ محرمانگی گذرواژه‌های تولیدی فایل متنی باید به‌صورت رمز شده در سیستم شما ذخیره‌سازی شود.

**نکته ۱:برای سادگی کار، از همان گذرواژه ساده داده شده توسط کاربر به عنوان کلید رمزنگاری برای رمزکردن فایل متنی گذرواژه ها استفاده کنید.

** نکته ۲:تمامی گذرواژه های تولید شده باید از همان گذرواژه ساده داده شده توسط کاربر تولید شوند (تابعی از آن باشند).

**** نکات مهم پیاده‌سازی:**

۱-حتما از قالب دستوری زیر برای پیاده سازی بخش CLI ابزار استفاده کنید.

1-passmanager.py –newpass “user password name ” –c “comment” –key “user simple password”

به‌عنوان‌مثال

Passmanager.py –newpass uniportal -c pass for my aut portal - key 1234

2-passmanager.py –showpass

نشان‌دادن نام پسوردهای ساخته شده و ذخیره شده توسط کاربر

3-passmanager.py –sel “user password name”

نشان‌دادن مقدار گذرواژه و کامنت مربوط به آن

4-passmanager.py –update “user passwrord name”

آپدیت مقدار گذرواژه با مقدار جدید

5-passmanager.py –del “user password name ”

حذف گذرواژه

بخش ۲:

در این بخش از شما خواسته شده است تا با استفاده از ابزار statsgen گذرواژه‌های تولید شده توسط ابزار خود به‌صورت آماری تحلیل کنید. هدف از این کار بررسی این نکته مهم است که ابزار شما تا چه حد توانایی تولید گذرواژه‌هایی با خواص بی‌قاعدگی خوب را داراست. (میزان شباهت گذرواژه‌های تولیدی به یکدیگر موردتوجه است). این خاصیت یک معیار خوب برای بررسی این است که گذرواژه‌های تولیدی توسط ابزار شما تا چه حد در برابر تحلیل‌های آماری مقاوم است.

پیاده‌سازی:

در ابتدا مود کاری جداگانه‌ای را با خصوصیات زیر برای ابزار خود پیاده‌سازی کنید.

۱-در این مود ابزار شما باید تعداد ۱۰۰۰۰ گذرواژه را از روی گذرواژه "0000" بسازد.

۲- گذرواژه های تولیدی را در یک فایل متنی با نام test.txt ذخیره کند. دقت کنید که فقط و فقط پسورد ها در فایل ذخیره شوند و نه چیز دیگری.

به‌عنوان‌مثال:

Qwes

1234

Awdwsad

P@ss0rd

....

....

در مرحله بعدی فایل متنی را به ابزار statsgen داده و از خروجی ابزار عکس بگیرید.

در مورد خروجی‌های تولید شده توسط ابزار statsgen تحقیق کنید و با استفاده از آن بیان کنید که گذرواژه‌های تولید شده توسط ابزار شما دارای چه خصوصیاتی هستند.

**موارد شامل نمره مثبت:

۱-درصورت تولید گذرواژه‌هایی با طول متغیر

۲-درصورت پیاده سازی رابط کاربری گرافیکی برای ابزار خود

موفق باشید