**تمرین اول**

**محمدعرفان هومانفر**

**قابلیت بهره برداری Exploitability**

قابلیت بهره برداری نشان میده که به چه آسونی یک آسیب پذیری تو سیستم میتونه توسط هکرها و افراد بیرونی مورد استفاده بگیرد تا اعمال غیرمجاز روی نرم افزار انجام بشود.

این قابلیت به موارد زیادی از جمله به اینکه به چه آسانی یک نقص تو سیستم پیدا میشه، به چه مقدار ابزار و دانش نیاز است برای اینکه از این نقص استفاده بشود و چه مقدار دسترسی به فرد غیرمجاز توسط این نقص داده میشود.

درواقع این مورد نشان دهنده به چه آسانی یک آسیب پذیری توسط یک فرد غیرمجاز میتونه مورد سواستفاده قرار بگیرد با پیشبینی کردن این حالت ها

**مثال ۱)**

بررسی داده های ورودی کاربر و اعتبارسنجی آن ها میتونه این تضمین رو به ما بده که ورودی کاربر مطابق با درخواست ما است و کاربر مخرب نتواند با وارد کردن ورودی های اشتباه موجب نفوذ به سیستم و انجام مواردی مانند SQL Injection شوند

**مثال ۲)**

با مشخص کردن حد و مرز حافظه ها از سرریز حافظه جلوگیری میکنیم تا افراد مخرب با گذشتن از حد و مرز حافظه کد های مخرب قابل اجرا را وارد برنامه نکنند و باعث اجرا ناخواسته این کد ها و آسیب به برنامه و سیستم اجرا کننده برنامه شود

**مثال ۳)**

استفاده از تکنیک (ASLR) ، این تکنیک موارد را در حافظه به صورت رندوم و نامشخص قرار میدهد ، به صورت نامشخص قرار گرفتن موارد در حافظه سبب میشود که افراد مخرب نتوانند به سادگی محل قرارگیری اطلاعات در حافظه را پیدا کنند و به اطلاعات کاربر یا نرم افزار دسترسی داشته باشند

**مثال ۴)**

استفاده از تکنیک های رمزگذاری شده مورداطمینان باعث میشود که افراد مخرب نتوانند به راحتی اطلاعات را رمزگشایی کنند ، معمولا تکنیک های رمزگزاری هایی که توسط خود کاربران ابداع میشوند یا تکنیک های رمزگذاری قدیمی و از کارافتاده ریسک رمزگشایی شدن اطلاعات توسط هکرها و افراد غیرمجاز را افزایش میدهد .

**مثال ۵)**

با درخواست از کاربر برای وارد کردن رمز عبور پیچیده تر باعث میشویم که فرد مخرب نتواند به سادگی، با امتحان کردن حالت های ممکن رمزعبور کاربر را پیدا کرده و به اکانت کاربر نفوذ کند

2dee4ede-cc59-46d5-a304-2c2f5f51e368.png

**حریم خصوصی Privacy**

حریم خصوصی به حق و انتظار افراد برای کنترل دسترسی به اطلاعات شخصی اشان دارد، این شامل توانایی حفظ محرمانگی اطلاعات کاربران با جلوگیری دسترسی افراد غیرمربوط به اطلاعات کاربر است، در دنیای دیجیتال حریم خصوصی نشان دهنده این است که اطلاعات کاربران چگونه ذخیره و نگهداری میشوند و چه افرادی به اطلاعات کاربران دسترسی دارند

به عبارت دیگه حریم خصوصی به توانایی این که کاربران بدانند چه کسانی به اطلاعات اون ها دسترسی دارند و اطلاعات کاربران توسط افرادی که قابل اطمینان نیستند استفاده نمیشود

**مثال ۱)**

شبکه های اجتماعی مانند فیسبوک، توییتر، اینستاگرام و .. حجم زیادی از اطلاعات شخصی کاربران از جمله تصاویر ، موقعیت مکانی، پیام های رد و بدل شده را نگه داری میکنند حریم خصوصی به این معناست که کاربران بدانند و توانایی کنترل این که چه کسانی توانایی دیدن پست ها ، اطلاعات پروفایل آن ها را دارد و اطلاعات آن ها با افراد سوم شخص از جمله کمپانی های تبلیغاتی ، دولت ها و ... درمیان گذاشته میشود.

برای مثال رسوایی فیسبوک که از اطلاعات میلیون ها کاربر برای موارد سیاسی استفاده کرد یکی از موارد قابل توجه نقص حریم خصوصی توسط شرکت ها میباشد.

همچنین استفاده از اطلاعات کاربران و وبسایت ها برای آموزش مدل های هوش مصنوعی یکی دیگه از موارد نقص حریم خصوصی توسط شرکت هایی از جمله گوگل میباشد.

**مثال ۲)**

رمزگزاری END-END یکی از موارد حفظ حریم خصوصی هست که پیامرسان هایی از جمله telegram و singnal از آن استفاده میکنند ، در این رمزگذاری به کاربر این اطمینان داده میشود که تنها ارسال کننده و گیرنده پیام توانایی خواندن محتوا پیام را دارد و حتی صاحبان این پیام رسان ها با دسترسی به دیتابیس ها توانایی دیدن محتوای پیام های کاربران را ندارند.

**مثال ۳)**

کوکی ردیابی (tracking cookie) ، اطلاعات کوچکی هستند که وبسایت ها برروی مرورگر شما قرار میدهند تا عادت های شما تو جستجو رو ذخیره کنند ، این موارد معمولا برای این نشون دادن تبلیغات های شخصی سازی شده استفاده میشود که یکی از موارد نقص حریم خصوصی هست زیرا که کاربران معمولا خبرندارند که درحال ردیابی شدن هستند

دربعضی از کشور ها وبسایت ها موظفند قبل از قرار دادن این کوکی ها از کاربر ها اجازه بخواهند به همین دلیل درخیلی از وبسایت از شما درخواست قبول کردن کوکی هنگام ورود به وبسایت میکنند

**مثال ۴)**

تلفن های همراه مکررا درحال اشتراک گذاری موقعیت مکانی کاربران با برنامه ها هستند ، با وجود اینکه بعضی از این ردیابی ها برای اپلیکیشن های مانند نقشه کاربردی هستند بعضی از برنامه ها با دخیره سازی و اشتراک گذاری موقعیت مکانی شما با کمپانی های تبلیغاتی و دولت ها میتواند باعث نقص حریم خصوصی شود

برای مثال درسال 2020 مشخص که کمپانی data broker با فروش موقعیت مکانی کاربران با کمپانی های تبلیغاتی بدون دانش کاربر موجب نقص حریم خصوصی کاربرانش شده

**مثال ۵)**

فناوری تشخیص چهره با پیشرفت تکنولوژي به سرعت درحال افزایش است ، با اینکه این فناوری در موارد امنیتی خیلی کاربردی است اما درمورد نظارت بیش از حد میتواند موجب نقص حریم خصوصی افراد شود

2dee4ede-cc59-46d5-a304-2c2f5f51e368.png

**بهینه سازی حافظه Memory Optimization**

بهینه سازی حافظه اشاره به مدیریت درست منابع و استفاده درست از سخت افزار است تا به صورت بهینه از منابعمون استفاده کنیم. هدف این است که برنامه به صورت روان اجرا شود و مقدار مصرف رم مدیریت شود تا از کم اومدن رم جلوگیری کنیم و بهینه بودن نرم افزار را افزایش دهیم ، این مورد در نرم افزار هایی که نیاز به پردازش های زیادی دارند بسیار مهم تر میباشد

**مثال ۱)**

عدم ساخت object ها و متغییر های زیاد ، در اپلیکیشن ها بهتر است که بجای ساخت متغییر های جدید از متغییر هایی که قبلا ساخته شده استفاده کنیم ، این عمل باعث میشود که استفاده از مموری کاهش یابد و مقدار کار garbage collector ها کاهش یابد .

**مثال ۲)**

استفاده از ساختمان داده و متغییر های درست و یا از پیش تعریف شده توسط زبان میتواند کمک انبوهی به کاهش استفاده از حافظه شود ، برای مثال در زبان هایی مثل ++C و java استفاده از متغییر هایی که قبلا ساخته شده مانند int, str حافظه کمتری نسبت به ساخت object های جدید دارد یا برای مثال ساختمان داده ای مانند لیست حافظه کمتری نسبت به linked list میگیرد

**مثال ۳)**

کش کردن درست داده ها و استفاده بهینه از کش درموارد زیادی میتواند استفاده از رم را کاهش دهد ، با کش کردن موارد مورد نیاز ، مراجعه برنامه به دیتابیس کاهش می یابد و سبب کاهش نیاز استفاده از رم میشود

**مثال ۴)**

در زبان برنامه نویسی پایتون استفاده از دیتاست هایی که Immutable مانند تاپل که مقدار مموری کمتری استفاده میکنند نسبت به لیست ها باعث میشود که میزان استفاده از رم کاهش یابد ، این مورد دیتاست به دلیل غیرقابل تغییر بودن میتوانند به رم کمک کنند ، استفاده درست از آن ها درجا هایی که مورد نیاز است به برنامه ما کمک میکند.

**مثال ۵)**

استفاده از متود Zero-copy networking در برنامه نویسی نتورک این اجازه میدهد که داده ها به صورت مستقیم با بافر جابجا شود و دیگر نیازی به کپی شدن دیتا در کرنل و فضای کاربر نیست که بسیار از استفاده سخت افزاری مموری را کاهش میدهد ، در برنامه هایی که حجم زیادی رد و بدل در نتورک وجود دارد این تکنیک بسیار ثمربخش میتونه واقع بشه.