آیا می خواهید به صورت امن تر به توسعه ی نرم افزار بپردازید؟ این کار ممکن است یک قدم دشوار باشد اما فقط یادگیری مبانی در بهبود امنیت نرم افزاری که شما توسعه داده اید بسیار موثر خواهد بود. مبانی ها از ۸۰ %حمله های امنیتی جلوگیری می کند. در پست امروز من ۵ راه برای اینکه بتوانید از همین امروز به توسعه ی نرم افزار بپردازید را به اشتراک می گذارم .

همه ی ورودی های کاربر را اعتبارسنجی کنید

یکی از اشتباهات امنیتی که بارها و بارها توسعه دهندگان مرتکب می شوند نادیده گرفتن اعتبارسنجی ورودی های کاربر است. حتی اگر درحال ساخت یک سیستم backendکه کاربران محدود و مشخصی دارد، هستید نادیده گرفتن این اصل سیستم شما را برای حمله های گسترده باز خواهد گذاشت .برای مثال یک حمله کننده ی بیرونی می تواند به شبکه ی شما دسترسی پیدا کند و سپس موفق به دسترسی گواهی نامه های یک کاربر شود و سپس با اعتبارسنجی ضعیف ورودی ها

در دسترسی به بخش های گسترده تر سیستم موفق شود. قانونی که میگوییم یک قانون ساده برای به خاطر سپردن است و به هر توسعه دهنده کمک بزرگی می کند: هیچگاه به ورودی های هیچ کاربری اعتماد نکنید. اگر شما فرض کنید هرکاربری که از اپلیکیشن شما استفاده می کند قصد حمله به شما دارد بطور خودکار درباره ی اعتبارسنجی هر قطعه ای که کاربر وارد می کند، فکر خواهید کرد تا امنیت اپلیکیشن خود را بالا ببرید. اگر می خواهید کاربر فقط عدد صحیح وارد کند، بررسی کنید که فقط عدد صحیح وارد می کند. اگر شما یک متن را میپذیرید، از هرچیزی که می تواند باعث آسیب شود، مانند تگ های HTML، جلوگیری کنید. اکثر زبان ها توابع از پیش ساخته شده ی دردسترسی برای اعتبارسنجی و تمیز ورودی های کاربر دارند. از آن ها استفاده کنید.

از حمله های اسکریپت های CROSS-SITEجلوگیری کنید

فقط اعتبارسنجی ورودی های کاربر طبق اصول کافی نیست بلکه باید خروجی ها را نیز قبل از چاپ کردن آن ها روی سیستم اعتبارسنجی کنید. در پروژه های بزرگتر، روی سیستم هایی کار می کنید که چندین توسعه دهنده روی آن کار می کنند. ممکن است یک توسعه دهنده ی دیگر درجایی یک مورد از اعتبارسنجی ورودی های کاربر را فراموش کند که همین باعث آسیب پذیری آنچه در پایگاه داده ذخیره می شود، می باشد. حال اگر شما داده ها را چاپ کنید در نمایش اطلاعات غیر مرتبط ریسک کرده اید.به عنوان یک مثال از حمله های XSSیک وب اپلیکیشن را فرض کنید. فرض کنید که اپلیکیشن نام کاربر را می خواهد و یک توسعه دهنده ی دیگر اعتبارسنجی صحیح بودن آن را فراموش کرده باشد و شما در قسمت خودتان همان نام را در صفحه ی پروفایل چاپ کنید. یک کاربر ممکن است نام کاربری خود را "Ryan " وارد کند حال صفحه ی پروفایل شما این نام کاربری نادرست که شامل فایل جاوااسکریپت است را، نشان خواهد داد. این فایل جاوااسکریپت نمی تواند کاری برای نشان ندادن cookiهای صفحه ی پروفایل به بازدیدکنندگان انجام دهد و دسترسی حمله کنندگان به اکانت هایی که نباید دسترسی داشته باشند و نرم افزارهای مخرب روی دستگاه بازدیدکننده نصب کنند، تضمین نمی کند.

پیاده سازی اقدامات امنیتی درطول توسعه نه در انتها

قبلا درباره ی چگونگی پیاده سازی امنیت در انتهای اینکه چرخه ی توسعه ی نرم افزار پاسخ دهد و با هزینه ی بالاتر، صحبت کرده ایم این کار باعث می شود موارد مهم زیادی درنظر گرفته نشود و توسعه ی یک سیستم امن دشوار شود اگر شما می خواهید یک توسعه دهنده ی نرم افزار امن شوید باید به امنیت نرم افزار در تمام مراحل توسعه ی نرم افزار از طراحی تا به انتها فکر کنید . همانطور که کار می کنید درباره ی راه هایی که حمله کنندگان می توانند از آنچه شما درحال انجام هستید استفاده کنند، فکر کنید و از آن ها جلوگیری کنید. کدزنی به صورت امن نسبت به کدزنی به صورت ناامن زمان زیادی را از شما نمی گیرد اما پیداکردن و اصلاح یک خط کدی که به صورت ناامن نوشته شده است بعد ها خیلی وقت گیر خواهد بود.

به تمام سیستم فکر کنید نه فقط قسمت های شخصی خودتان

همانطور که وب اپلیکیشن را می سازید بجای اینکه فقط به جنبه هایی از سیستم که به شما مربوط می شود فکر کنید به تمام سیستم فکر کنید. به خاطر داشته باشید که اگر کامپوننت شما بطور امن برنامه نویسی شده باشد به این معنی نیست که کامپوننت های دیگر نیز بطور امن برنامه نویسی شده اند وقتی که افزونگی ممکن است کامپوننت های مختلف را با یکدیگر ترکیب کنید. به این فکر کنید که چه خطا های امنیتی در کامپوننت های دیگر می تواند روی کامپوننت شما و همچنین روی تمام اپلیکیشن تاثیر بگذارد.

از یک منبع ذخیره سازی امن برای ذخیره ی رمزعبور و داده های مهم استفاده کنید

پس از اینکه در رمزعبور ها نفوذی انجام شود اهمیت این موضوع مشخص می شود. اطمینان حاصل کنید زمانی که رمزعبور ها را ذخیره می کنید آن ها هش کنید نه اینکه رمزنگاری کنید با اینکار برای هر رمزعبوری که ذخیره می کنید یک نوع کد کردن منحصر بفرد خواهید داشت بنابراین مواردی از قبیل سرنخ های رمزعبور نمی تواند منجر شود تا افراد به همه ی رمزعبور ها دسترسی پیدا کنند و متوجه شوند معمول ترین رمزعبور ها چه مواردی هستند و چه کاربرانی از رمزعبور های مشخصی استفاده می کنند. اگر شما اطلاعات مهم نظیر کد بیمه،جزئیات حساب بانکی یا اطلاعات کارت اعتباری را ذخیره می کنید، رمزنگاری مناسب مورد نیاز است. سعی نکنید تا از

رمزنگاری که خودتان آن را توسعه داده اید استفاده کنید بلکه از الگوریتم های رمزنگاری اصلی که توسعه و تست شده اند استفاده کنید. به خاطر داشته باشید که کسی از خرید استاندارد های صنعتی و رمزنگاری های نظامی ضرر نمی کند بلکه کسانی که از رمزنگاری های خودشان استفاده می کنند ضرر می کنند. نیاز به یادآوری نیست که چرا چرخ اختراع شد. درحال حاضر الگوریتم های رمزنگاری و هش عالی وجود دارد بنابراین صرف زمان روی توسعه ی الگوریتم هایی که کارا نیستند فقط وقت تلف کردن است .در این مقاله پنج راه برای اینکه بطور امن برنامه نویسی کنید و زمان شما هدر نرود را بررسی کردیم.