به نام خدا

پروژه: درس توسعه امن نرم افزار

عنوان: پیاده سازی یک ابزار fuzzing وب

در این پروژه قصد داریم برای تشخیص خودکار آسیب پذیری ها در برنامه های تحت وب یک fuzzer بسازیم. ورودی این ابزار یک url از اولین صفحه وب سایت بوده و خروجی آن لیست آسیب پذیری ها در هر صفحه وب سایت است.

برای ساخت این برنامه مراحل زیر لازم است.

۱- Crawling در اولین مرحله لازم است با دریافت url صفحه اول سایت، کلیه url های مرتبط با دامنه وب سایت هدف را استخراج کرد. بدین منظور لازم است با دریافت محتوای http response مربوط به هر صفحه، کلیه لینک های موجود در آن صفحه را استخراج کرده و سپس لینک های مربوط به دامنه وب سایت هدف را visit کرده و به صورت recursive لینک های داخل آن صفحات را نیز استخراج کرد.
۲- پس از استخراج مسیرهای مختلف وب سایت، لازم است برای هر صفحه تگ های form به همراه فیلدهای input به دست آید. در صورت استفاده از زبان پایتون، می توانید برای این کار از کتابخانه beautifulSoup استفاده کنید. همچنین لازم است نحوه ارسال اطلاعات به فرم ها به صورت post یا get را تشخیص دهید.
۳- تزریق خطا: در این مرحله برای تشخیص یک آسیب پذیری داده متناسب با حمله را در فیلد ورودی فرم قرار داده و یک request به صفحه مورد نظر ارسال می کنید.
۴- تشخیص خطا: بر اساس محتوای پاسخی که وب سایت به تقاضای شما می دهد باید بتوانید تشخیص دهید که حمله موفقیت آمیز بوده است یا خیر. در صورت موفق بودن حمله صفحه مورد نظر و رشته حمله باید ثبت شود تا در گزارش نهایی اعلام گردد.

در رابطه با این پروژه نکات زیر را در نظر بگیرید:

- انجام پروژه به صورت دو نفره مجاز است.
- اگرچه از هر زبان برنامه نویسی می توانید استفاده کنید، پیشنهاد می شود که با زبان پایتون پیاده سازی را انجام دهید.

- یکی از چالش هایی که در ابزارهای تست برنامه ها وجود دارد گذشتن از صفحه ورود و مدیریت session کاربر است. این ابزارها معمولا یک نام کاربری و کلمه عبور از تحلیلگر دریافت می کنند تا بتوانند در صفحات login وارد شوند. همچنین ارسال تقاضاهای http را به گونه ای انجام می دهند که session ایجاد شده حفظ شود. از طرفی باید دقت شود که ابزار لینک های مربوط به logout را visit نکند تا session تشکیل شده تمام نشود.
- آزمون و تشخیص آسیب پذیری XSS در این پروژه اجباری است، و در صورت تشخیص سایر آسیب پذیری ها به شما نمره اضافه تعلق می گیرد.