Programowanie Defensywne

Przeglądy bezpieczeństwa projektu

Arkadiusz Chrobot

Katedra Systemów Informatycznych

29 kwietnia 2024

Plan

1. Wprowadzenie
2. Techniki testowania statycznego
3. Przegląd bezpieczeństwa projektu
4. Ocena bezpieczeństwa
5. Kompetencje miękkie w SDR

Wprowadzenie

Weryfikację bezpieczeństwa i zabezpieczeń oprogramowania przeprowadza się przy pomocy testów. Współcześnie wyróżniamy dwa rodzaje testowania [1]:

- statyczne, które można zastosować do każdego *artefaktu* powstającego w ramach tworzenia oprogramowania,
- dynamiczne, polegające na eksperymentalnym uruchamianiu wykonywalnego kodu i badaniu jego zachowania oraz wyników dla określonych danych wejściowych.

Dzisiejszy wykład będzie dotyczył zastosowania tej pierwszej formy testowania do weryfikacji bezpieczeństwa projektu aplikacji. Sprawdzanie bezpieczeństwa jej kodu będzie tematem innego wykładu. Informacje o tego rodzaju testach statycznych dla aplikacji internetowych można znaleźć w [2].

Techniki testowania statycznego

Testowanie statyczne może być przeprowadzone za pomocą kilku różnych metod, które mogą mieć zarówno charakter formalny, jak i nieformalny. Testy te mogą być zautomatyzowane, jak i całkowicie manualne. Do wspomnianych metod zaliczamy [1]:

analizę statyczną analiza artefaktu przy użyciu narzędzi, ale bez uruchamiania takich artefaktów, jak np. kod,

przegląd ocena artefaktu lub stanu projektu (ang. *project*),

przegląd formalny przegląd z udokumentowanymi procedurami i wymaganiami,

przegląd koleżeński (ang. *peer review*) przegląd artefaktów wykonywany przez współpracowników ich twórcy,

inspekcja forma przeglądu koleżeńskiego, ale oparta na udokumentowanej procedurze i formalna,

audyt weryfikacja oparta na obiektywnych kryteriach i nakierowana na sprawdzenie zgodności artefaktów ze standardami, wytycznymi, specyfikacjami, itd.

Przegląd bezpieczeństwa projektu

Przegląd bezpieczeństwa projektu (ang. *Software Design Review*, SDR) jest przeglądem, w ramach którego *recenzenci* oceniają poprawność i wystarczalność zabezpieczeń zastosowanych do ochrony istotnych aktywów w projektowanym oprogramowaniu. Najlepiej, jeśli osoby te są „z zewnątrz" zespołu wytwórczego, ponieważ mogą zachować wtedy obiektywizm. Niemniej jednak powinny one znać projekt oprogramowania, dziedzinę jego zastosowania oraz środowisko w jakim będzie ono zainstalowane i używane.

Przegląd bezpieczeństwa projektu

Korzyści

W przeciwieństwie do testowania dynamicznego przeglądy są mniej kosztowne, można je wdrożyć we wczesnych fazach prac nad oprogramowaniem i pozwalają wykryć defekty, których znalezienie i naprawienie byłoby trudne. Dotyczy to zwłaszcza defektów będących źródłem podatności. Przegląd pozwala spojrzeć na oprogramowanie z kilku różnych perspektyw. Dzięki temu twórcy oprogramowania zaczynają lepiej rozumieć problemy związane z bezpieczeństwem, a recenzenci od bezpieczeństwa poznają dokładniej wymagania narzucane przez dziedzinę zastosowania wytwarzanego oprogramowania i dzięki temu mogą zaproponować bardziej adekwatne zabezpieczenia.

Przegląd bezpieczeństwa projektu

Umiejscowienie SDR w pracach projektowych

Przeglądy bezpieczeństwa projektu wykonywane są cyklicznie w takcie trwania prac nad oprogramowaniem. Zazwyczaj przeprowadza się je po przeglądach funkcjonalnych. W przypadku rozbudowanych systemów lub takich o krytycznym znaczeniu dla bezpieczeństwa wstępne SDR przeprowadza się we wczesnej fazie prac projektowych, aby jak najszybciej zidentyfikować i przeanalizować problemy. We wszystkich projektach przeglądy bezpieczeństwa powinny być wykonywane na *kompletnych i stabilnych* wersjach dokumentów projektowych.

Przegląd bezpieczeństwa projektu

Wymagania

Wyniki przeglądu bezpieczeństwa projektu i jeśli jest to konieczne, również jego przebieg powinny zostać dobrze udokumentowane. Dzięki temu żadna cenna uwaga nie zostanie pominięta.
Z drugiej strony taki przegląd musi bazować na (najlepiej) dobrej dokumentacji projektowej. Jeśli są w niej zawarte nieprecyzyjne lub ogólnikowe informacje na temat wymagań i zastosowanych środków bezpieczeństwa, to powinna ona zostać uzupełniona.

Przebieg SDR

Przegląd bezpieczeństwa projektu składa się z sześciu kroków:

1. analiza projektu i dokumentacji uzupełniającej,
2. uzupełnianie informacji dotyczących projektu,
3. identyfikowanie istotnych z punktu widzenia bezpieczeństwa komponentów,
4. współpraca z projektantem,
5. tworzenie raportu końcowego,
6. weryfikacja nanoszonych zmian.

W przypadku niewielkich projektów wszystkie te kroki można wykonać w trakcie jednej sesji. Z drugiej strony, w przypadku skomplikowanych projektów, pojedynczy krok może wymagać przeprowadzenia wielu sesji. W tym kontekście sesja oznacza pojedyncze spotkanie recenzentów z zespołem wytwórczym lub ich samodzielną pracę.

Przebieg SDR

Analiza projektu

Analiza projektu polega na zapoznaniu się recenzentów z dokumentacją projektową i uzupełniającą, a także z dziedziną zastosowania budowanego oprogramowania, aby proponowane przez nich rozwiązania w zakresie bezpieczeństwa, nie kolidowały z funkcjami systemu, które wynikają choćby z wymagań biznesowych. Jej przebieg może być następujący:

1. zapoznanie się z dokumentacją, celem uzyskania ogólnych informacji o projekcie,
2. przejrzenie projektu z punktu widzenia bezpieczeństwa,
3. tworzenie na bieżąco notatek na temat pomysłów i obserwacji,
4. oznaczenie potencjalnych problemów, jeśli jest jeszcze za wcześnie, aby dokładnie je przeanalizować.

Przebieg SDR

Uzupełnienie informacji dotyczących projektu

W przypadku prostych lub dobrze udokumentowanych projektów ten etap można pominąć. Polega on głównie na zadawaniu pytań projektantom, których celem jest głównie uzyskanie informacji, która nie jest zapisana w dokumentacji projektowej. Realizując ten etap recenzent powinien:

1. upewnić się, że dokumentacja projektowa jest klarowna i kompletna,
2. znaleźć i pomóc uzupełnić braki w dokumentacji,
3. zrozumieć na tyle projekt, aby biegle się w nim poruszać,
4. poznać obawy członków zespołu wytwórczego związane z bezpieczeństwem.

Przebieg SDR

Identyfikacja istotnych komponentów

Bazując na triadzie CIA, złotym standardzie (uwierzytelnienie, autoryzacja i audyt), definicjach aktywów, powierzchni ataku i granicy zaufania, recenzent musi znaleźć i przeanalizować krytyczne z punktu widzenia bezpieczeństwa komponenty. W tym kroku należy:

1. przeanalizować interfejsy, pamięć masową i komunikację,
2. przeprowadzić analizę zaczynając od najbardziej narażonych na atak komponentów, w kierunku najcenniejszych aktywów,
3. ocenić, w jakim stopniu obecny projekt uwzględnia kwestie bezpieczeństwa,
4. jeśli jest to konieczne — wskazać kluczowe zabezpieczenia i spowodować, aby zostały one uznane za kluczowe elementy projektu.

Przebieg SDR

Współpraca z projektantem

Recenzent powinien przedyskutować z projektantem swoje ustalenia i omówić alternatywne rozwiązania. Na tym etapie zachodzi wymiana wiedzy: projektant zaczyna lepiej rozumieć kwestie bezpieczeństwa, a recenzent uwarunkowania projektu. Aby ta współpraca była udana warto:

1. aby recenzent przedstawił perspektywę bezpieczeństwa w kontekście zagrożeń i środków zaradczych,
2. naszkicować scenariusz, który pokaże w jaki sposób zmiana zabezpieczeń może przynieść korzyści w przyszłości,
3. zaproponować więcej niż jedno rozwiązanie znalezionych problemów,
4. ostateczną decyzję zostawić projektantowi, bo to on bezpośrednio odpowiada za bezpieczeństwo tworzonego oprogramowania,
5. udokumentować wymianę pomysłów — co będzie zrealizowane, a co nie.

Przebieg SDR

Tworzenie raportu końcowego

Raport końcowy należy rozpocząć od (wyważonej i obiektywnej) ogólnej oceny stanu bezpieczeństwa w projekcie. Proponowane zmiany należy podzielić na trzy kategorie: *konieczne, wskazane i zalecane*. Treść raportu powinna spełniać następujące warunki:

1. być zorganizowana wokół konkretnych zmian w projekcie,
2. dotyczyć przede wszystkim spraw o najwyższym priorytecie, a w mniejszym stopniu kwestiom mniej istotnym,
3. proponować alternatywne strategie i rozwiązania, ale bez wyręczania projektanta,
4. nadawać priorytety ustaleniom i zaleceniom,
5. poruszać przede wszystkim kwestie związane z bezpieczeństwem, ale również inne uwagi, jeśli mogą one być istotne dla projektanta.

Przebieg SDR

Weryfikacja nanoszonych zmian

Jeśli zaproponowane w raporcie zmiany zostaną uwzględnione w projekcie, to należy zweryfikować, czy zrobiono to poprawnie. Takie sprawdzenie może obejmować nie tylko projekt, ale również implementację (kod). Śledzenie nanoszonych zmian można przeprowadzić przy pomocy odpowiedniego narzędzia (np. Jira, Bugzilla lub inna wersja oprogramowania do śledzenia błędów (ang. *bugtracker*)). Ten etap powinien uwzględniać następujące kwestie:

1. Jeśli zmiany są poważne, to warto współpracować z projektantem, aby były one wprowadzone prawidłowo.
2. Jeśli opinie co do zmian są rozbieżne, to recenzent w raporcie powinien umieścić wszystkie stanowiska, opis niewdrożonych zmian i zaznaczyć, że są to kwestie otwarte, do dalszej dyskusji.

Ocena bezpieczeństwa

Ocena bezpieczeństwa projektu tworzonego oprogramowania w SDR ma podobny charakter do modelowania zagrożeń. W związku z tym można ją oprzeć na tych samych pytaniach pomocniczych, co w przypadku tego procesu:

1. Co opracowujemy?
2. Jakie przeciwności mogą się pojawić?
3. Jak poradzimy sobie z przeciwnościami?
4. Na ile skuteczne działanie podjęliśmy?

Kompetencje miękkie w SDR

W trakcie przeprowadzania przeglądów bezpieczeństwa projektu oprogramowania równie ważne co kwestie techniczne są umiejętności miękkie. Przegląd to wprawdzie pośrednia, ale jednak publiczna ocena pracy zespołu, a nawet poszczególnych jego członków. Aby był skuteczny należy tak nim pokierować, aby nie recenzenci, a twórcy odkrywali problemy związane z bezpieczeństwem w ich projekcie i nawiązywali dialog dotyczący ich rozwiązania.
Kwestie sporne, dla których trudno uzyskać konsensus, należy opisać, poczynając od punktów, co do których obie strony konfliktu się zgadzają i przekazać do decyzji kierownictwu wyższego stopnia.

Bibliografia


Adam Roman. *Testowanie i jakość oprogramowania: modele, techniki, narzędzia*. Warszawa: Polskie Wydawnictwa Naukowe, 2015.


Larry Conklin i Gary Robinson. *OWASP Code Review Guide, Release 2.0*. 2017. URL: https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!