ZI 2021/22

1. Što je površina napada i kako se mjeri/određuje, a kako smanjuje? (4)

To je kolekcija ulaznih točaka programskog proizvoda (API, web servisi, izravan pristup BP, kanali za komunikaciju s resursima – vektori napada). Površina određuje rizik napada - mjera potencijalnog pristupa i udara. Kontrole pristupa smanjuju, mogućnost da se dosegne sustav i broj elemenata koji su vidljivi ili se mogu koristiti. Smanjuje se smanjenjem količine koda koji se izvodi „po viđenju“, zatvaranjem pristupnih točaka.

2. Što je STRIDE i kako se provodi? (6)

Praksa modeliranja definirana SDL-om. Procjena po kategorijama prijetnji: zatvaranje/lažiranje (Spoofing), zlonamjerna izmjena podataka(Tampering), nepriznavanje/poricanje(Repudiation), otkrivanje informacija (Information disclosur), uskraćivanje usluge(Denial of service) i povišenje ovlasti(Elevation of priviledge). Provodi se tako da se sustav raščlanjuje u relevantne komponente pa se onda: procjenjuje osjetljivost na prijetnje svake komponente (analiza dijagramom toka podataka), prijetnje se smanjuju (mitigation) prikladnim svojstvima sigurnosti, ponavlja se (rekurzivno) do zadovoljavajućeg rezultata.

3. Što je DREAD i kada te kako se provodi? (4)

Model procjene rizika, rangiranje rizika za zadanu prijetnju. Damage potential, Reproducibility, Exploitability, Affected users, Discoverability. Provodi se tako da: procijeni se svaka prijetnja po navedenim parametrima, daje se pojedinačno vrijednost 1-10 (najmanje loše do najgore) i ukupan rizik - prosjek 5 pojedinačnih DREAD vrijednosti. Alternativa je jednostavna shema ocjenjivanja nisko, srednje, visoko preslikano u interval 1-3, te se na kraju zbrajaju vrijednosti za zadanu prijetnju i pridjeljuje se rizik. Nakon modeliranja je razrješenje prijetnji, odluka što učiniti. Popraviti, ne učiniti ništa, obavijestiti korisnika, ukloniti rizično svojstvo, …

4. Objasnite postupak inspekcije (uloge i proces) te timski pregled i prohod. (5)

Uloge: Moderator - vodi sastanak, prati probleme, Čitalac - parafrazira kod, nije autor, Zapisničar - evidentira defekte,

Autor - osigurava kontekst koda, objašnjava, popravlja nakon pregleda

Postupak:

Planiranje - autor inicira, moderator ekipira, skupa pripreme inspekcijski paket,

Priprema - recenzenti pregledavaju, koriste kontrolne liste i analitičke alate, označavaju defekte

Sastanak - čitalac prepričava, recenzenti komentiraju i zapitkuju, zapisničar evidentira, tim zaključuje procjenu koda

Prerada - autor popravlja

Kontrola - moderator verificira korektnost promjena, autor prijavljuje kod

Timski pregled: lagana inspekcija, sudjeluju moderator i recenzenti (nisu autori koda), analiziraju se moduli ili manji skupovi klasa, traje 1-2 sata.

Prohod: autor vodi sastanak i objašnjava kod, manje formalni i nedefiniran proces bez metrika i kontrolnih listi.

5. Što je statička analiza i kako se provodi? Ključni problemi, prednosti i nedostaci. (4)

Način provjere ispravnosti softvera bez izvršavanja, obuhvaća sve osim testiranja, koristi se analizator koda, te može biti dio revizije koda. Može se provesti leksičkom analizom, analizom toka podataka, grafom kontrole toka, analizom mrlja.

Ograničenja: pogrešno otkrivanje i pogrešno neprepoznavanje

False Positives - nepostojeći bugovi, nemoć pri složenom kodu ili vanjskom

False Negatives - neprepoznavanje bugova, složenost koda, slabost pravila

Prednosti: potpuna pokrivenost koda, potencijal potvrde izostanka čitavih klasa bugova, hvata bugove različite u odnosu na dinamičku analizu.

Slabosti: visok postotak pogrešnog otkrivanja, teško oblikovanje testa, složenost izgradnje (alata), nedovoljno kada se koriste dodatni okviri ili biblioteke, neimanje cjelokupnog izvornog koda u praksi

6. Objasnite osnovnu ideju i postupke dinamičke analize pročešljavanjem (fuzzing). (3)

Cilj je ubrizgati kvar u aplikaciju, slati neispravne ili nasumične podatke. Slično je regresiji, samo s lošim podacima. Prednosti: jednostavnost, nezavisnost o platformi i jeziku. Nedostaci: primjena na uzak skup povredivosti, dugo traje, složena primjena na tehnologije.
Dumb fuzzing: uz dovoljno manje znanja o cilju i alatima, koriste se pseudoslučajne anomalije ispravnih podataka, što ima za posljedicu potrebu za više analize i redundanciju nalaza. Smart fuzzing: podaci generirani na temelju modela, zahtijeva dubinsko poznavanje cilja i specijaliziranih alata, smišljene anomalije poznavanjem formata, standarda, ... (PDF, RFC), posljedice su manja potreba za analizom i manje dupliciranje nalaza.

7. Navedite i ukratko opišite korake penetracijskog testa. (5)

1. Istraživanje: ispitivač pokušava prikupiti što više informacija., pasivno - javno dostupne informacije, aktivno - istraživački alati
2. Skeniranje: ispitivač skenira otvorene portov korištenjem alata, cilj - enumeracija servisa, verzije enumeriranih servisa i OS, skeniranje ranjivosti automatiziranim alatima
3. Dobivanje pristupa: iskorištavanje ranjivosti, ručno ili alatom, ovisno o dogovoru s vlasnikom, neke ranjivosti se neće iskorištavati
4. Zadržavanje pristupa: ispitivač instalira zloćudne backdoor i rootkit programe za daljnji pristup sustavu, ova i naredna faza se u praksi najčešće ne provode ali predstavljaju scenarij realnog napada
5. Brisanje tragova: ispitivač pokušava izbrisati dnevničke zapise koji bi ukazivali na njihov neovlašteni pristup

8. Objasnite napredni i kvalificirani elektronički potpis. (3)

1. Napredni elektronički potpis: na nedvojben način je povezan s potpisnikom, omogućava identificiranje potpisnika, izrađen je korištenjem podataka za izradu elektroničkog potpisa koje potpisnik
može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom, povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka
2. Kvalificirani elektronički potpis: napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za
izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za
elektroničke potpise

9. Kojom se normom definiraju digitalni certifikati (tj. njihov format)? (1)

X.509

10. Objasnite ulogu vremenskog žiga pri digitalnom potpisivanju. (2)

Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika. Pomoću vremenskog žiga može se dokazati da je potpis napravljen prije isteka valjanosti certifikata.

11. Navedite barem 6 zahtjeva norme PCI-DSS. (3)

Zahtjev 3: Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi.
Zahtjev 9: Maksimalno ograničiti fizički pristup podatcima o vlasniku kartice.
Zahtjev 6: Razvijati i održavati sigurne sustave i aplikacije
Zahtjev 10: Pratiti i nadzirati svaki pristup mrežnim resursima i podatcima o vlasniku kartice.
Zahtjev 11: Redovito provjeravati sigurnost sustava i procesa.
Zahtjev 12: Razviti i održavati odgovarajuću politiku informacijske sigurnosti.

12. Kako se naziva norma koja opisuje kako će format potpisa ili šifriranja ugraditi u SOAP poruku? (1)

WS-Security

13. Što znate o normi ISO/IEC 27001. (4)

Norma za upravljanje informacijskom sigurnošću, sadrži zahtjeve za uspostavljanje, provedbu, održavanje i kontinuirano
poboljšanje sustava upravljanja informacijskom sigurnošću (ISMS). ISO/IEC 27001 osigurava da se organizacija brani ne samo od rizika temeljenih na tehnologiji, već i drugih prijetnji, kao što su slabo informirani zaposlenici ili neučinkoviti postupci.

14. Koja su tri oblika potpisa definirana unutar norme XML Signature? Objasnite ih. (2)

Omotani potpis (Enveloped) – potpis se nalazi unutar dokumenta.

Omotavajući potpis (Enveloping) – potpis omeđuje dokument koji potpisuje.
Odvojeni potpis (Detached) – potpis se nalazi u zasebnom dokumentu, a URI (Universal Resource Identifier) određuje koji dokument potpisuje.