**Week-01 OWASP Rating Methodology**

**Agenda:**

1. Forklar begreberne ”threat agents” og ”vulnerability”
2. Forklar hvordan sikkerhedsrisici bliver udregnet i OWASP (*Risk = likelihood x impact*)
3. Forklar hvordan en firewall er med til at mindske OWASP sikkerhedsrisici
4. Gennemgå opsætning af firewall

**Explain the two sets of Factors**

**Threat agents** har magten til at agere, udsætte, udføre, transmittere eller understøtte en trussel. De bedømmes ud fra følgende faktorer.

* 1. Skill level: Hvor teknologisk erfaren er gruppen.
     + Security penetrations færdigheder (9)
     + Netværk og programmerings færdigheder (6)
     + Avanceret computer bruger (5)
     + Nogle tekniske færdigheder (3)
     + Ingen tekniske færdigheder (1)
  2. Motive: Hvor motiverede er gruppen på at finde og udnytte fundne svagheder.
     + Lav eller ingen gevinst (1)
     + Mulig gevinst (4)
     + Høj gevinst (9)
  3. Opportunity: Hvilke ressourcer eller muligheder kræves der for at finde og udnytte disse svagheder.
     + Fuld adgang eller dyre ressourcer kræves (0)
     + Special adgang eller ressourcer kræves (4)
     + Begrænset adgang eller ressourcer kræves (7)
     + Ingen adgang eller ressourcer kræves (9)
  4. Size: Hvor er stor er gruppen.
     + Udviklere (2)
     + Systemadministratorer (2)
     + Intranet brugere – folk der har login adgang til interne systemer (4)

Eksempler på en threat agent: hackere, organiseret kriminalitet, ”insiders” (inkludere systemadministratorer og udviklere), terrorister og national stater.

**Vulnerability,** estimere sandsynligheden for at den specifikke svaghed involveret, kan blive opdaget og udnyttet.

1. Ease of discovery: Hvor let er det for gruppen at opdage/finde denne svaghed.
   * + Praktisktalt umuligt (1)
     + Svært (3)
     + Let (7)
     + Automatiserede værktøjer tilgængelig (9)
2. Ease of exploit: Hvor nemt er det for gruppen, faktisk at udnytte denne svaghed.
   * + Teoretisk (1)
     + Svært (3)
     + Let (5)
     + Automatiserede værktøjer tilgængelig (9)
3. Awareness: Hvor velkendt er denne svaghed for gruppen.
   * + Ukendt (f.eks zero day, ukendt for både gruppen og ofret) (1)
     + Skjult (4)
     + Åbenlyst (6)
     + Offentligt kendt (f.eks. tomcat default bruger) (9)
4. Intrusion detection: Hvor sandsynlig er det at detektere en udnyttelse?
   * + Aktiv detektering i applikationen (1)
     + Logget og revideret (3)
     + Logget uden revidering (8)
     + Ikke logget (9)

Eksempler på svagheder: OWASP A1 – A10

**Give some examples of how you can change those parameters - for example for MySQL servers**

* 1. Sæt en Firewall op, for at styre den ind- og udadgående trafik. Firewall kan sættes op til logging.
  2. Logging skal holdes usynlig for brugere og eventuelle hackere.
  3. Advarsler og fejl skal genere klare og forstålige logbeskeder.
  4. Logging af applikationen og API’er skal monitorers, for mistænkelig aktivitet.
  5. Logging skal ikke kun gemmes lokalt.
  6. Sørge for at loginforsøg og andre vigtige transaktioner bliver logget effektiv og gemmes til senere analyser.

**Explain how security risks are rated in OWASP**

Et billede, der indeholder gade, bærbar computer, side, by

Automatisk genereret beskrivelse

Risk = likelihood x impact

**Beregne likelihood**

Vulnerability på en risiko beregnes ud fra de ovenstående faktorer og gennemsnittet beregnes. Det samme gøres for threat agents. Bagefter findes gennemsnittet af disse to resultater. Gennemsnittet udgør likelihood.

Likelihood = (VF + TAF) / 2

**Beregne impact**

Technical impact på en risiko beregnes ud fra faktorerne og gennemsnittet beregnes. Det samme gøres for business impact. Bagefter findes gennemsnittet af disse to resultater. Gennemsnittet udgør impact.

Impact = (TIF+ BIF) / 2

**Alle tal fra skalaen (1-9) kan omskrives til low, medium eller high.**

**Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse**

**Link til at udregne risiko:**

https://www.owasp-risk-rating.com/

**Argue whether OWASP gives the complete picture of security risks on an application**

Modellen tager kun højde for de kendte svagheder, men ikke for de svagheder der er ukendte. Den kan derfor ikke give et komplet billede af alle de risici der findes. Dog er det muligt at medregne faktorer der er specifikke for en individuel applikation, og de behøves ikke nødvendigvis at indgå i den generelle model, f.eks. kunne en faktor være dødsfald.

At ”business impact” og ”threat agents”, i modellen, er uspecificerede gør modellen mere generel, og kan udfyldes af hver enkel applikation.

OWASP er en non-profit organisation, som kun har til formål at øge sikkerheden på internettet. Dette taler for en øget troværdighed af modellen.