Teme:

- root detection
- certificate transparency
  Seminarska:
- uvod - poveš motivacijo, kaj je problem, in kakšno rešitev boš opisal v članku
- sledi pregled sorodnih del (related work) - poglej vse, google scholar, rabiš okoli 20 referenc (zotero, mendeley)
- experimental setup/metodologija - kako si naredil stvari
- analiza - objektivno, našteješ kaj so rezultati; izvedel si eksperiment, to so rezultati
- diskusija - subjektivno opišeš rezultate iz analize, kritična presoja
- zaključek - kritična presoja, recap, povzetek + future work
- na stacku so lokalne spremenljivke, na heapu so podatki

SQL:

- SQL vrivanje - nek svoj stavek damo v dobro nameren stavek

  Tipi
  - Union-based SQL Injection
    - Izvedi osnovni stavek ALI pa ---
  - Error Based SQL Injection
    - Nepravilna izvedba, napaka mi poda del podatkov
  - Blind SQL Injection
    - Brez odziva (težje)
- Time-based blind injection (časovno odvisni):
  - lahko preverimo npr. verzijo baze
- konfiguracije web serverjev, ki jih nujno ne rabimo, so lahko ranljivosti - izklopiš kar ne rabiš
- ni vedno cilj, da dobimo podatke:
  - lahko jih manipuliramo
  - lahko probamo pokvariti stvari, da sistem neha delati (DoS)
- varnostne kopije:
  - običajno append only
  - na magnetni trak, ker je najbolj trajno

Nekompleksni napadi:

- izkoriščanje ranljivosti uporabnika

- rabimo ustrezne omejitve privilegijev
- vedno imamo overhead, ko dodajamo varnostne omejitve:
  - če naredimo stvari, ki imajo prevelik overhead, si bodo probali ljudje olajšati stvari
  - ljudje bodo naredili stvari, ki niso čisto intended way
- trivialni napadi zaradi površnosti ljudi
- za uploadanje appa na Google Play, rabiš key za podpisati app:
  - problem, če daš na git
- odlaganje varnostnih kopij (dump):
  - ostane nekje na eni virtualki nezaščiten

Krog zaupanja:

- ne zaupaj nikomur z ničemer - zero trust model
- če kdo rabi dostop do nečesa, mu daj čim manj dostopa (samo do tistega, kar nujno rabi)

Kje najpogosteje odtekajo podatki:

- interno:
  - vsi imajo dostop do nečesa
  - premalo samozaščite - npr. služben laptop uporabljaš za loadanje crackanih programov
- eksterno:
  - nekdo drug pride in se pretvarja, da nekaj rabi in dobi dostop
  - pozabljeni USB ključki

Vklopljene dodatne konfiguracije:

- ne mislimo na neke default nastavitve, ki bi jih bilo dobro onemogočiti
- izklop možnosti, ki jih ne uporabljamo

Onemogočanje storitve (DoS):

- izvedba kompleksnih poizved (npr. pokaži mi vse račune)
- izvedba mnogih poizvedb:
  - pošiljamo več poizvedb kot jih server lahko prenese
- lahko povzročamo stroške:
  - delamo API klice na plačljive storitve
- včasih stvari počepnejo, brez da imamo veliko število naprav (npr. z enim laptopom lahko crashamo nekaj)
- zelo veliko tvojih podatkov je že na spletu:

    - varnostne kopije morajo biti na varnem mestu in kriptirane
    - uporaba enakih gesel povsod
- papir prenese vse, pomembno je kaj se dejansko dela v praksi

SAP:

- phishing mail s prepočasnim odzivom vodstva
- login page enak legit page-u, ampak na drugi domeni
- stara PHP verzija, manjka sanitacija podatkov