Validacija podataka

Podaci u upotrebi

- Svaki sistem komunicira sa spoljnim subjektima (korisnicima iz veb čitača ili drugim servisima) i prihava određeni skup ulaznih podataka
- **Za bezbednost sistema je ključno ne praviti nikakve pretpostavke o tome kakvi će biti ulazni podaci !**
- U REST baziranim veb aplikacijama svaki endpoint predstavlja ulaz u sistem
- Najveći broj veb-baziranih napada zasnovan je na konstrukciji malicioznog sadržaja u sklopu korisničkog zahteva

Injection napadi

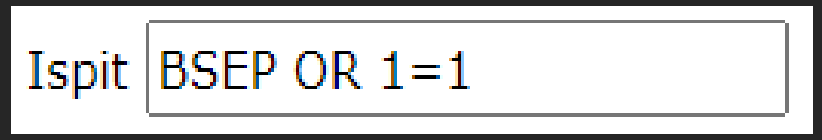
- Omogućavaju slanje malicioznog koda kroz našu aplikaciju do interpretera (operativnog sistema, baze podataka...)
- Svaki interpreter ima neki parser. Injection napadi imaju za cilj da „prevare“ parser da izvrši neki skup podataka kao komandu
- U ovu grupu napada spadaju svi tekstualni napadi koji eksploatišu sintaksu interpretera, poput XPath, LDAP, NoSQL, XML, OS, itd.

SQL injection

- 3. na OWASP TOP 10 listi
- Napad se zasniva na ubrizgavanju SQL koda u podatke koji se šalju bazi podataka (pripada grupi injection napada)
- Uslovi za sprovođenje napada:
  - ❖ Aplikacija koristi SQL bazu podataka
  - ❖ Ima bar jedan endpoint koji prihvata korisničke podatke
  - ❖ Ne postoji zaštita za sprečavanje SQL napada

SQL injection

- 1 = 1 je uvek tačno



  - `SELECT * FROM Ispiti WHERE naziv = 'BSEP' OR 1 = 1;`

- Grupisanje SQL upita

  - `SELECT * FROM Ispiti WHERE naziv = 'BSEP'; DROP TABLE Ocene;`

XML External Entities (XXE) napad

- OWASP TOP 10 – 5. mesto (pripada ***A05:2021-Security Misconfiguration***)
- Tip napada na aplikaciju koja parsira XML dokumente.
- Napad se sprovodi kada XML sadrži referencu ka eksternom entitetu, a parser koji se koristi nije dobro konfigurisan.
- Posledice: otkrivanje poverljivih podataka, denial of service i drugi uticaji na sistem...

Cross Site Scripting

- Pre svega, šta je SOP (*Same Origin Policy*)?
- Ideja je naterati veb pregledač žrtve da izvršava maliciozan JavaScript kod, zaobilazeći SOP
- Nije direktan napad na aplikaciju, već na njene korisnike
- Tri tipa:
  - Reflektovani
  - Snimljeni
  - Bazirani na DOM stablu
- 3. mesto na OWASP TOP 10 listi, u kategoriji Injection napada

Mere zaštite

- *Blacklist* validacija – formira se lista zabranjenih unosa i sve što nije na toj listi prihvata se
  - Kako da unapred predvidimo sve što maliciozan kod može da sadrži?
  - Malicioznih unosa ima mnogo -> problem skalabilnosti
- *Whitelist* validacija – pristup koji je češće u upotrebi
  - Ideja je formirati listu pravila (regularnih izraza) koji definišu kakav unos je dozvoljen
- Character escaping
- Prepared statements
- Input validation – output encoding