**Information disclosure**

**Primeri za našu aplikaciju:**

* Napadač se može otići na određen URL naše web aplikacije i dobiti listu direktorijuma i tako steći uvid u strukturu naše web aplikacije
* Napadač se može otići na određen URL naše web aplikacije i dobiti listu direktorijuma pri čemu se među njima nalazi i fajl *backup*naše web aplikacije.
* Napadač se može otići na određen URL naše web aplikacije i dobiti listu direktorijuma pri čemu se među njima nalazi i *log*  fajl.
* Može doći do SQL Injection-a prilikom unosa(popunjavanje određene forme, npr. logovanja, pretrage itd.)
* Napadač može saznati određene informacije putem grešaka koje dobija(prilikom prijave na sistem dobija informaciju da je dobro uneo email, ali ne i lozinku)

**Kako bi ove probleme trebalo rešiti?**

Kako bi se izbegao ovaj napad, neophodno je pravilno konfigurisanje web servera od strane administratora, kao i onemogućiti izlistavanja svih fajlova u folderu ukoliko ne postoji index stranica što bi bila direktna posledica prethodno navedenog problema. Dakle, index stranica mora postojati. Pored toga, prilikom svakog unosa od strane korisnika neophodno je validirati taj unos kako ne bismo imali SQL Injection (ukoliko je neophodan unos email adrese, omogućiti unos samo u tom formatu, ukoliko je neophodan unos npr. određenog broja onemogućiti unos svih ostalih karaktera osim cifara). Takođe, trebalo bi voditi računa o načinu obaveštavanja putem grešaka(prilikom prijave na sistem, ukoliko se pogrešno unese email ili lozinka ili i jedno i drugo, ispisati istu grešku-npr. “Neuspešna prijava na sistem.”). Naravno, pored svega navedenog, neophodno je korišćenje pouzdanog web servera koji nema ovakve propuste.