**Information disclosure**-predstavlja objavljivanje informacija i omogućava napadaču da dobiju vredne informacije o sistemu. Zbog toga je neophodno uvek razmotriti koje se informacije otkrivaju i da li mogu biti zloupotrebljene od strane zlonamernog korisnika.

Informacije su najvažniji resurs današnjice. Hakerima su neophodne za svaki drugi napad. Dobar deo tehnika se i koristi upravo da bi se informacije nabavile. Kompanije i državne agencije uglavnom i strahuju od mogućnosti objavljivanja osetljivih ili tajnih informacija ( information disclosure). U nekim situacijama napad može biti organizovan sa ciljem špijuniranja i uticaja na komunikaciju, ako se haker umetne kao "osoba u sredini" (*man in the middle*).

**Izlistavanje direktorijuma i objavljivanje informacija**

**Iz**listavanje direktorijuma je funkcija web servera koji prikazuje listu svih fajlova kada nema index fajl, kao što su indek.php i default.asp u određenom direktorijumu sajta. Na primer, kada korisnik zahteva *www.acunetix.com* bez navođenja fajla, web server će obraditi ovaj zahtev i vratiće index fajl za taj direktorijum i stvarni sajt će se pojaviti. Međutim, ako index fajl ne postoji, web server će vratiti listu sadržaja tog direktorijuma. Može se povući paralela između ove funkcionalnosti i komande operativnim sistemima u konzoli komandne linije, kao što su "*ls*" na *Unix* i *Linux* sistemima i "*dir*" na *Windows*-u. Osim toga, treba imati u vidu to da izlistavanje direktorijuma može biti zloupotrebljeno korišćenjem posebnih zahteva.  
  
**Osnovne informacije**

Česta greška koju administratori websajtova obično naprave je da pretpostavljaju da ako nema veze sa brojnim datoteka u direktorijumu, niko ne može da im pristupi. Ovo nije tačno jer mnogi skeneri web ranjivosti kao što su *Acunetix WVS* će otkriti takve direktorijume. Takvo curenje informacija iz fajlova u direktorijumima može dati dovoljno informacija za napadača da osmisli dalje napade na određene mete.  
  
**Primeri napada:**

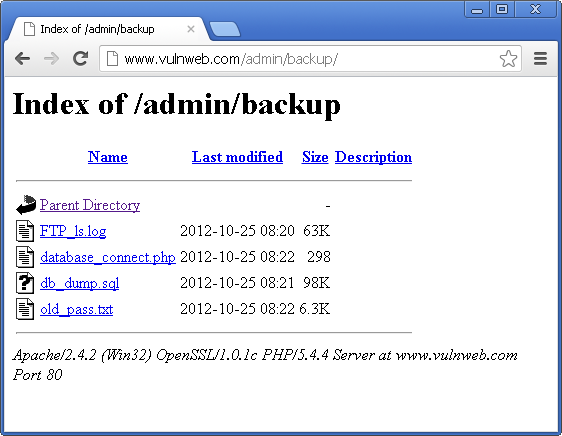
1. Neki web administratori ili nepravilno konfigurišu web server ili ne rade to uopšte i time omogućavaju izlistavanje direktorijuma. Na primer, administratori mogu da konfigurišu složena podešavanja, kako bi se omogućilo izlistavanje direktorijuma za pojedine direktorijume ili pod-direktorijume. Nepravilna konfiguracija ovog zadatka može da dovede do neočekivane i neplanirane mogućnosti izlistavanja direktorijuma koji sadrže osetljive informacije.  
  
2. Čak i ako je izlistavanje direktorijuma onemogućeno na web serveru, napadači bi mogli da otkriju i iskoriste slabosti web servera koji će rezultovati izlistavanje nekih posebnih direktorijuma aplikacija. Na primer, mana starog *Apache Tomcat*-a je bila nepravilno rukovanje *null* bajtovaima(% 00) i karakterima sa kosom crtom( '') što je ostavljalo prostor za napade izlistavanja direktorijuma.  
  
3. Napadači bi mogli da otkriju indekse direktorijuma iz konteksta ili keširanih podataka sadržanih u bazama podataka. Na primer, Google-ova keš baza podataka može da sadrži istorijske podatke o meti, koja je ranije izlistavanja direktorijuma omogućila. Takvi podaci omogućavaju napadaču da dobije informacije koje su potrebne bez da iskoriste ranjivosti.  
  
 **Primer:**

Korisnik šalje web zahtev za *www.vulnweb.com/admin/*. Odgovor sa servera obuhvata sadržaj izlistavanja direktorijuma administratora, kao što se vidi na Slici 1.



*Slika 1*

Iz gornjeg **iz**listavanja direktorijuma možete videti da u */admin* direktorijumu postoji pod-direktorijum pod nazivom *backup*, što može biti dovoljno informacija da napadač izvede napad.



*Slika 2*

Navedeno izlistavanje direktorijuma(Slika 2) prikazuje ceo sadržaj *backup* direktorijuma. To uključuje osetljive informacije kao što su lozinke, podatke baze, *FTP logs* i *PHP* skripti. Očigledno je da ove informacije nisu bile namenjene javnosti, međutim, zbog greške web servera ovo je dovelo do otkrivanja ovih informacija, tako da su sada dostupne javnosti. Osim toga, fajlovi poput ovih, kao što su *FTP logs*, mogu da sadrže druge osetljive informacije kao što su korisnička imena, *IP* adrese, kao i kompletnu strukturu kataloga operativnog sistema korisnika sajta.

**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.