

Računarstvo i društvo

Matematički fakultet
Beograd



Cybersecurity i Etičko hakovanje

profesor: Sana
Stojanović Đurđević

April 2022

Nemanja Lisinac
478/17

Šta je Cybersecurity

Definicija i primena



Pod pojmom cyber security smatramo primenu tehnologija, procesa i pravila kako bi zaštitili sisteme, mreže, uređaje i podatke od hakerskih napada. To se postiže kombinacijom alata koji omogućavaju što veću sigurnost i smanjuju šansu od potencijalnih napada.

Sigurno ste primetili da kada hoćete da resetujete vašu šifru, internet stranica prvo mora da potvrdi vaš identitet i tek nakon dokaza da je to baš vaš nalog, možete promeniti šifru. To je jedna od stvari kojima se bavi cyber security.

FAZE PRIMENE

Kako bi se zaštitili od napada, odnosno pravilno primenili cyber security, ceo proces je podeljen na 5 faza:

- Identifikacija - treba videti koji delovi su rizični
- Zaštita - zaštititi delove koji su rizični
- Detekcija - saznati da se desio sigurnosni probaj
- Reakcija - reagovati na detektovan sigurnosni probaj



Etičko hakovanje

Definicija i tipovi



Prepostavimo da ste napravili aplikaciju i primenili sve mere kako bi je zaštitili.

Ali kako možete biti sigurni da je vaša aplikacija u potpunosti bezbedna i da niko ne može da zaobiđe sistem zaštite?

Moraćete da proverite da li bilo koja od tehnologija ima sigurnosnih propusta u verziji koju ste koristili i da proverite da li mere zaštite u potpunosti funkcionišu.

Upravo tu na scenu stupaju hakeri.

HAKOVANJE UOPŠTENO

Termin haker se koristio za osobe koji su svojim znanjem i veštinama prepravljali sisteme i time povećavali njihovu efikasnost i dozvoljavali im da multi taskuju.

Danas taj termin opisuje programere koji upadaju u sisteme tako što iskorišćavaju bagove i sigurnosne propuste.

Na primer haker može napraviti algoritam koji provaljuje šifre, ometa mreže i slično. Primarni motiv neetičkog hakovanja (blackhat hakere) je pristup informacijama od značaja ili finansijska dobit.





***"Postoje samo dva tipa kompanija:
One koje su već hakovane
i one koje će tek biti"***

Robert Mueller
Direktor FBI



Ali, nema svaki haker lošu nameru. To nas dovodi do sasvim drugačije grupe hakera: Etičke hakere (whitehat hakere).

Etičko hakovanje je autorizovan postupak u kome haker pokušava da zaobiđe zaštitu i identificuje pretnje u sistemima.

Kompanija u čijem je vlasništvu sistem dozvoljava tim hakerima da “testiraju” njihov sistem i da im ukažu na propuste. Samim tim što je to planirano i odobreno čini sam taj proces legalnim.



PROCES ETIČKOG HAKOVANJA

Etički hakeri istražuju sistem ili mrežu i traže slabe tačke koje mogu biti iskorišćene u nekom cyber napadu. Oni sakupljaju i analiziraju informacije kako bi pronašli način da sistem, mreža ili aplikacija budu bezbedni. Tim procesom se poboljšava sigurnost, a kao posledica sistem je otporniji na napade i neki napadi se mogu izbegći.

Oni između ostalog proveravaju:

- Injekcione napade
- Promene u sistemu bezbednosti
- Izloženost osetljivih podataka
- Proboje autentifikacionih protokola
- Komponente sistema i mreža koji mogu da se iskoriste kao pristupna tačka

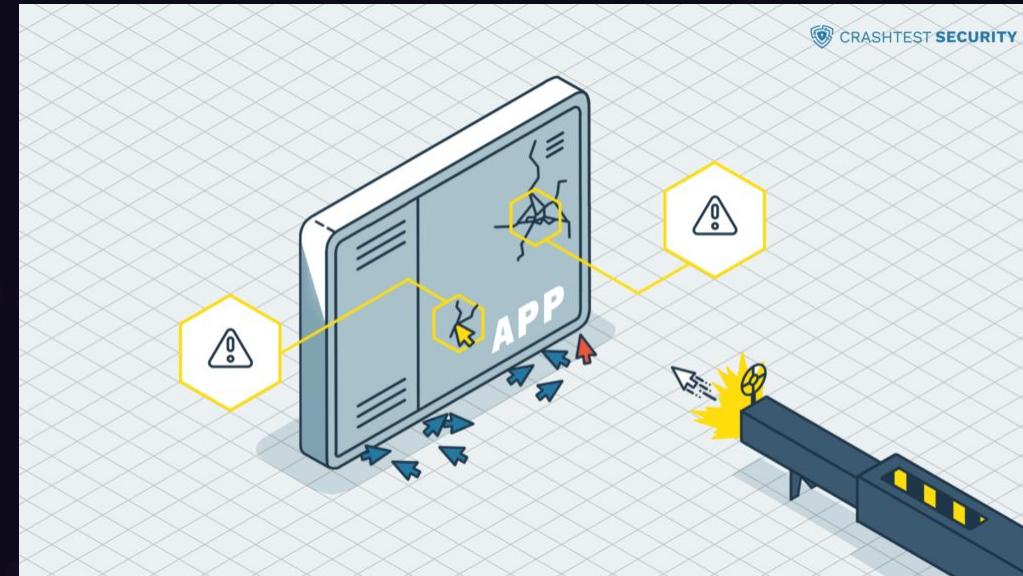
Injekcioni napadi

vrste

Pod injekcijom se smatra iskorišćavanje baga u softveru koji je prouzrokovani nevalidnim podacima, odnosno umetanjem koda koji će se izvršavati umesto nekog validnog unosa i time promeni tok izvršavanja softvera.

U odnosu na mesto "injekcije" delimo ih na sql, xss, nativne (programske, sistemske) i druge.

Smatra se da moguće xss injektovati preko 65% webstranica.



Etičko hakovanje

01

SQL

Structured Query Language

SQL je jezik koji služi za komunikaciju sa bazom podataka.

Napadač će pokušati da manipuliše upitom koji se pošalje bazi podataka i na taj način izvrši umetnute komande.

Pri uspešnom izvršavanju, dobija se odgovor u vidu tabele (osetljivih podataka korisnika, administratora ...)

02

XSS

Cross-Site Scripting

Ako aplikacija u svom ispisu podataka koristi nešto što joj korisnik upiše, otvara se prostor za ovaj tip napada. Kod koji je najčešće u JavaScript-u se ubaci pri ispisu i moguće je da on trajno promeni webstranicu ako ona nema dobru validaciju.

Posledica je sajt koji može da prikuplja podatke od posetioca, menja kolačiće i dr.

03

Nativne

Programske i
sistemske

Ako je napadač upoznat sa kodom i načinom izvršavanja programa ili sistema.

On može da iskoristi to znanje i u delovima koji nisu najbolje obezbeđeni da ubaci svoj kod. Posledice mogu biti od blagih do totalne kontrole u zavisnosti od koda.

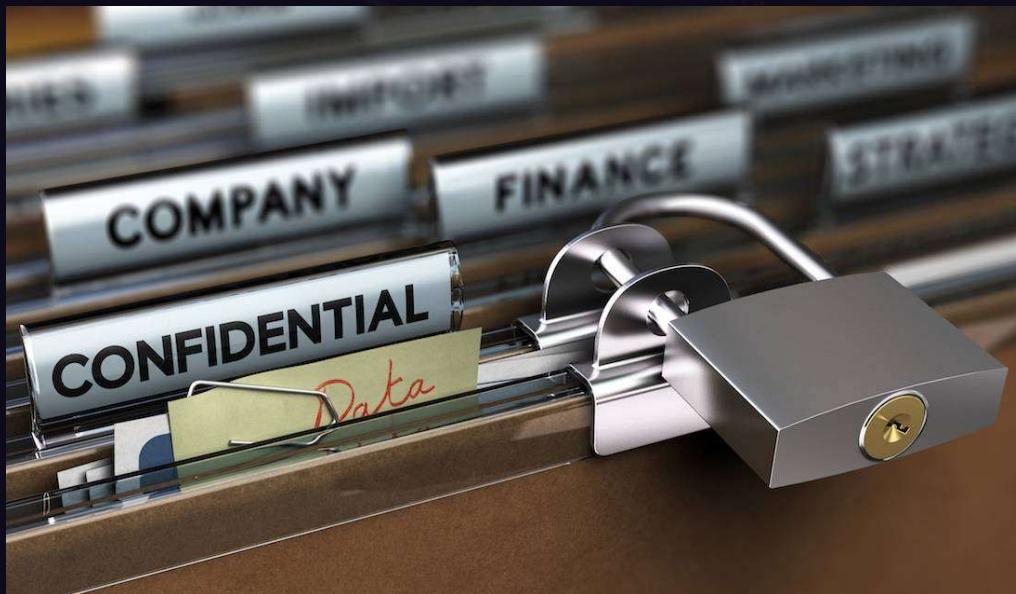
Promene u sistemu bezbednosti

Svaka promena polise koja se tiče bezbednosti mora biti detaljno testirana kako bi se obezbedio siguran rad aplikacije.

Pod promenama u sistemu se smatra bilo šta što menja trenutni tok podataka



IZLOŽENOST OSETLJIVIH PODATAKA



Pod osetljivim podacima, smatraju se svi oni podaci kojima se može identifikovati pojedinac.

Etički haker će u ovom delu videti koliko su dobro čuvani podaci, odnosno koliko je jednostavno do njih doći.

Jedan od načina bezbednog čuvanja podataka je da su podaci enkriptovani nekom metodom gde bi i u slučaju dobijanja tih podataka bilo neophodno dešifrovanje.

Proboj autentifikacionog protokola

Tip protokola koji služi za prenos podataka o autentifikaciji između servera i korisnika.

Kod njega je bitno da:

- Svi učesnici u protokolu znaju kakav je protokol
- Ne sme se odstupati od protokola
- Svaki korak protokola mora biti jasno definisan
- Mora postojati akcija za svaki mogući scenario





KOMPONENTE SISTEMA I MREŽA KOJI MOGU DA SE ISKORISTE KAO PRISTUPNA TAČKA



Pristupna tačka je bilo koja komponenta mreže ili sistema kroz koju svi korisnici moraju proći kako bi razmenili podatke.

U kućnoj varijanti je to switch, ruter i wireless antena i da bi ste pristupili internetu vi morate proći kroz sve te uređaje.

Kod napada na pristupne tačke haker klonira jedan od tih uređaja i predstavlja se kao on.

Postoje razne vrste napada u odnosu na način kloniranja:

Man in the Middle (posrednik), Evil Twin (zli blizanac)...

Algoritam rada etičkog hakera

Izviđanje

reconnaissance



Obeležavanje sistema i
prikupljanje informacija.



Testiranje mreže i uređaja
kako bi se našle kritične
tačke.

Pristup

Gaining Access



Korišćenje kritičnih tačaka
u cilju dobijanja
administratorskih prava

Skeniranje

scanning



Uveravanje da se
sistemu može pristupiti
u budućnosti.

Trajnost

Maintaining
Access

Skrivanje

Clearing Tracks



Brisanje svih tragova
koji su napravljeni
prilikom pristupa
sistemu.



Algoritam



Bezbednost nastavlja da bude velika briga svih tehnoloških kompanija i sve više se daje na značaju zaštiti poverljivih podataka. Ova briga proizilazi iz činjenice da su kritične tačke teške za pronalaženje i da je za pojedine propuste neophodno i do godinu dana za detekciju.

Etičko hakovanje pomaže organizacijama da otkriju te propuste i da ih poprave pre nego što ih neko iskoristi. Kroz kombinaciju automatskih i manualnih testova, etički hakeri dostavljaju detaljan izveštaj bezbednosnih pretnji, efektivnost trenutnih bezbednosnih polisa i generalne savete za kreiranje bezbednih aplikacija.

Pitanja za diskusiju

1. Kako bi ste ocenili važnost etičkog hakovanja u zaštiti bezbednosti softvera

2. Da li smatrate da bi ste mogli da se bavite etičkim hakovanjem ili cybersecurity

3. Da li se slažete sa citatom direktora FBI da se sve može hakovati

Hvala na pažnji