Napadi na softverske sisteme i mehanizmi zaštite

Čedomir Dimić, Jana Milutinović, Miloš Samardžija

Matematički fakultet

maj 2017.

Pregled

Uvod

- Bezbednost sistema je jedna od najsloženijih tema u modernom računarstvu.

Uvod

- Bezbednost sistema je jedna od najsloženijih tema u modernom računarstvu.
- Povrede bezbednosti snose ogromne posledice najčešće u vidu novca.

Uvod

- Bezbednost sistema je jedna od najsloženijih tema u modernom računarstvu.
- Povrede bezbednosti snose ogromne posledice najčešće u vidu novca.
- Stoga, veoma važan zadatak organizacije je da dobro zaštiti poverljive informacije kako one ne bi bile ukradene ili zloupotrebljene.

Uvod

- Bezbednost sistema je jedna od najsloženijih tema u modernom računarstvu.
- Povrede bezbednosti snose ogromne posledice najčešće u vidu novca.
- Stoga, veoma važan zadatak organizacije je da dobro zaštiti poverljive informacije kako one ne bi bile ukradene ili zloupotrebljene.

Definicija

Sigurnost softvera obuhvata razvoj i implementaciju softvera tako da se on zaštiti od zlonamernih napada i drugih bezbednosnih rizika, ali da istovremeno može da nastavi neometano da radi i pored tih rizika pritom zadržavajući sve predviđene funkcionalnosti.

CIA model

- Kao 3 najvažnija aspekta sigurnosti softvera se smatraju poverljivost, integritet i raspoloživost podataka.

CIA model

- Kao 3 najvažnija aspekta sigurnosti softvera se smatraju poverljivost, integritet i raspoloživost podataka.
- Mere koje se preduzimaju da bi se obezbedila poverljivost su napravljene tako da se onemogući da se osetljive informacije nađu u pogrešnim rukama.

CIA model

- Kao 3 najvažnija aspekta sigurnosti softvera se smatraju poverljivost, integritet i raspoloživost podataka.
- Mere koje se preduzimaju da bi se obezbedila poverljivost su napravljene tako da se onemogući da se osetljive informacije nađu u pogrešnim rukama.
- Integritet uključuje održavanje konzistentnosti, preciznosti i pouzdanosti podataka tokom njihovog čitavog životnog ciklusa.

CIA model

- Kao 3 najvažnija aspekta sigurnosti softvera se smatraju poverljivost, integritet i raspoloživost podataka.
- Mere koje se preduzimaju da bi se obezbedila poverljivost su napravljene tako da se onemogući da se osetljive informacije nađu u pogrešnim rukama.
- Integritet uključuje održavanje konzistentnosti, preciznosti i pouzdanosti podataka tokom njihovog čitavog životnog ciklusa.
- Raspoloživost se postiže održavanjem hardvera, preduzimanjem potrebnih popravki hardvera odmah kada za tim postoji potreba i održavanjem korektnog funkcionisanja operativnog sistema.

Mehanizmi zaštite sistema

- Osnovni mehanizmi zaštite na Internetu su: zaštitni zid(eng.firewall),antivirusni programi i šifrovanje podataka.

Mehanizmi zaštite sistema

- Osnovni mehanizmi zaštite na Internetu su: zaštitni zid(eng.firewall),antivirusni programi i šifrovanje podataka.
- Zaštitni zid je mrežni sistem zaštite koji se koristi za praćenje i kontrolisanje dolazećeg i odlazećeg mrežnog saobraćaja.

Mehanizmi zaštite sistema

- Osnovni mehanizmi zaštite na Internetu su: zaštitni zid(eng.firewall),antivirusni programi i šifrovanje podataka.
- Zaštitni zid je mrežni sistem zaštite koji se koristi za praćenje i kontrolisanje dolazećeg i odlazećeg mrežnog saobraćaja.
- Antivirusni programi sprečavaju da na računar dospe zlonamerni softver(eng. malware) ili ga uklanjaju po dospeću na računar.

Mehanizmi zaštite sistema

- Osnovni mehanizmi zaštite na Internetu su: zaštitni zid(eng.firewall),antivirusni programi i šifrovanje podataka.
- Zaštitni zid je mrežni sistem zaštite koji se koristi za praćenje i kontrolisanje dolazećeg i odlazećeg mrežnog saobraćaja.
- Antivirusni programi sprečavaju da na računar dospe zlonamerni softver(eng. malware) ili ga uklanjaju po dospeću na računar.
- U savremenom poslovanju mora postojati mehanizam koji obezbeđuje: zaštitu tajnosti informacija (sprečavanje otkrivanja njihovog sadržaja), integritet informacija (sprečavanje neovlašćene izmene informacija) i autentičnost informacija (definisanje i proveru identiteta pošiljaoca).

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.
- Bezbednost se odnosi na sprečavanje neželjenog ponašanja.

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.
- Bezbednost se odnosi na sprečavanje neželjenog ponašanja.
- Problemi u dizajnu i implementaciji potencijalno mogu da učine aplikaciju ranjivom.

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.
- Bezbednost se odnosi na sprečavanje neželjenog ponašanja.
- Problemi u dizajnu i implementaciji potencijalno mogu da učine aplikaciju ranjivom.
- Pojava bagova je neizbežna.

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.
- Bezbednost se odnosi na sprečavanje neželjenog ponašanja.
- Problemi u dizajnu i implementaciji potencijalno mogu da učine aplikaciju ranjivom.
- Pojava bagova je neizbežna.
- Hakeri aktivno rade na pronalaženju bagova, koje kasnije mogu da iskoriste u svoje svrhe.

Napadi

- Programeri se uglavnom fokusiraju na korektnost softvera, odnosno na postizanje željenog ponašanja softvera.
- Bezbednost se odnosi na sprečavanje neželjenog ponašanja.
- Problemi u dizajnu i implementaciji potencijalno mogu da učine aplikaciju ranjivom.
- Pojava bagova je neizbežna.
- Hakeri aktivno rade na pronalaženju bagova, koje kasnije mogu da iskoriste u svoje svrhe.
- Potrebno je eliminisati sve propuste u dizajnu i implementaciji, ili barem otežati ili u potpunosti onemogućiti njihovo iskorišćavanje.

Najčešći napadi

- Prekoračenje bafera
  - Bag koji pogađa programe pisane na programskom jeziku nižeg nivoa (uglavnom C i C++)

Najčešći napadi

- Prekoračenje bafera
  - Bag koji pogađa programe pisane na programskom jeziku nižeg nivoa (uglavnom C i C++)
  - Pisanjem izvan granica bafera se može izazvati
    - oštećenje podataka

Najčešći napadi

- Prekoračenje bafera
  - Bag koji pogađa programe pisane na programskom jeziku nižeg nivoa (uglavnom C i C++)
  - Pisanjem izvan granica bafera se može izazvati
    - oštećenje podataka
    - nasilno zatvaranje programa

Najčešći napadi

- Prekoračenje bafera
  - Bag koji pogađa programe pisane na programskom jeziku nižeg nivoa (uglavnom C i C++)
  - Pisanjem izvan granica bafera se može izazvati
    - oštećenje podataka
    - nasilno zatvaranje programa
    - izvršavanje zlonamernog koda

Najčešći napadi

- Prekoračenje bafera
  - Bag koji pogađa programe pisane na programskom jeziku nižeg nivoa (uglavnom C i C++)
  - Pisanjem izvan granica bafera se može izazvati
    - oštećenje podataka
    - nasilno zatvaranje programa
    - izvršavanje zlonamernog koda
  - Pored ovog napada, postoje i varijacije
    - prekoračenje hipa (eng. *heap overflow*)
    - prekoračenje celog broja (eng. *integer overflow*)
    - prekoračenje čitanjem (eng. *read overflow*)

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka
    - dodaje, modifikuje i briše zapise

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka
    - dodaje, modifikuje i briše zapise
  - Prevencija napada se vrši upotrebom pripremljenih upita (eng. *prepared statements*).

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka
    - dodaje, modifikuje i briše zapise
  - Prevencija napada se vrši upotrebom pripremljenih upita (eng. *prepared statements*).
- Krađa sesije
  - Predstavlja jedan od načina zloupotrebe kolačića (eng. *cookies*).

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka
    - dodaje, modifikuje i briše zapise
  - Prevencija napada se vrši upotrebom pripremljenih upita (eng. *prepared statements*).
- Krađa sesije
  - Predstavlja jedan od načina zloupotrebe kolačića (eng. *cookies*).
  - Krađom identifikacionog kolačića, napadač se predstavlja kao autentikovan korisnik, i izvršava zlonamerne akcije u njegovo ime.

Najčešći napadi

- Podmetanje SQL upita
  - Napad omogućava izvršavanje zlonamernih SQL upita.
  - Ranjivi su delovi aplikacije u kojima korisnički unos direktno učestvuje u upitu, bez prethodne obrade.
  - Iskorišćavanjem ovog propusta, napadač može da:
    - zaobiđe mehanizme autentikacije i autorizacije
    - pročita sadržaj baze podataka
    - dodaje, modifikuje i briše zapise
  - Prevencija napada se vrši upotrebom pripremljenih upita (eng. *prepared statements*).
- Krađa sesije
  - Predstavlja jedan od načina zloupotrebe kolačića (eng. *cookies*).
  - Krađom identifikacionog kolačića, napadač se predstavlja kao autentikovan korisnik, i izvršava zlonamerne akcije u njegovo ime.
  - Napad se može sprečiti instalacijom dodataka za pregledače isključivo iz proverenih izvora, korišćenjem bezbedne veze, upotrebom skrivenih kolačića...

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.
  - Korisnički unos se tretira kao validan kod od strane JavaScript interpretera.

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.
  - Korisnički unos se tretira kao validan kod od strane JavaScript interpretera.
  - Postoje:
    - **postojani XSS** (eng. *persistent XSS*), gde maliciozni kod potiče iz baze podataka

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.
  - Korisnički unos se tretira kao validan kod od strane JavaScript interpretera.
  - Postoje:
    - **postojani XSS** (eng. *persistent XSS*), gde maliciozni kod potiče iz baze podataka
    - **reflektovani XSS** (eng. *reflected XSS*), gde maliciozni kod potiče iz zahteva žrtve (npr. URL)

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.
  - Korisnički unos se tretira kao validan kod od strane JavaScript interpretera.
  - Postoje:
    - **postojani XSS** (eng. *persistent XSS*), gde maliciozni kod potiče iz baze podataka
    - **reflektovani XSS** (eng. *reflected XSS*), gde maliciozni kod potiče iz zahteva žrtve (npr. URL)
    - **DOM-zasnovani XSS** (eng. *DOM-based XSS*), gde je ranjivost na klijentskoj strani

Najčešći napadi

- CSRF (eng. *cross-site request forgery*)
  - Zlonamerna osoba ne mora da bude autentikovana da bi izvršila prevaru, već korisnike navodi da sami izvrše nepoželjnu akciju.
  - Mete napada su zahtevi koji vrše izmenu stanja aplikacije.
  - Napad se sprečava upotrebom CSRF tokena.
- XSS (eng. *cross-site scripting*)
  - Napad zasnovan na umetanju koda.
  - Korisnički unos se tretira kao validan kod od strane JavaScript interpretera.
  - Postoje:
    - **postojani XSS** (eng. *persistent XSS*), gde maliciozni kod potiče iz baze podataka
    - **reflektovani XSS** (eng. *reflected XSS*), gde maliciozni kod potiče iz zahteva žrtve (npr. URL)
    - **DOM-zasnovani XSS** (eng. *DOM-based XSS*), gde je ranjivost na klijentskoj strani
  - Prevencija se vrši enkodiranjem korisničkog unosa, i izbegavanjem umetanja unosa direktno u script tagove, u atribute za rukovaoce događajima (event handlers), ili u CSS.

Bezbednost i Veb serveri

- Veb server (eng. *Web Server*) je računar koji je odgovoran za preuzimanje i opsluživanje Veb stranica koje zahteva klijent

Bezbednost i Veb serveri

- Veb server (eng. *Web Server*) je računar koji je odgovoran za preuzimanje i opsluživanje Veb stranica koje zahteva klijent
- VS obrađuje klijentske zahteve preko HTTP mrežnog protokola čiji je zadatak da distribuira informacije na Internetu

Bezbednost i Veb serveri

- Veb server (eng. *Web Server*) je računar koji je odgovoran za preuzimanje i opsluživanje Veb stranica koje zahteva klijent
- VS obrađuje klijentske zahteve preko HTTP mrežnog protokola čiji je zadatak da distribuira informacije na Internetu
- Povezan je na Internet, te korisnici mogu da pristupe podacima koje server skladišti sa bilo kog mesta na Internetu, što može imati za posledicu pokušaje neovlašćenog pristupa i zloupotrebu podataka

Bezbednost i Veb serveri

- Veb server (eng. *Web Server*) je računar koji je odgovoran za preuzimanje i opsluživanje Veb stranica koje zahteva klijent
- VS obrađuje klijentske zahteve preko HTTP mrežnog protokola čiji je zadatak da distribuira informacije na Internetu
- Povezan je na Internet, te korisnici mogu da pristupe podacima koje server skladišti sa bilo kog mesta na Internetu, što može imati za posledicu pokušaje neovlašćenog pristupa i zloupotrebu podataka
- Apache Web Server, Internet Information Server (IIS) , lighttpd , Sun Java System Web Server, Jigsaw Server

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija
  - Kontrola **pristupa** - štiti se integritet podataka

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija
  - Kontrola **pristupa** - štiti se integritet podataka
  - Obavezna dobra kontrola pristupa konfiguracijskih fajlova

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija
  - Kontrola **pristupa** - štiti se integritet podataka
  - Obavezna dobra kontrola pristupa konfiguracijskih fajlova
  - Kontrola pristupa smanjuje mogucnost otkrivanja osetljivih informacija koje ne smeju biti javno izložene

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija
  - Kontrola **pristupa** - štiti se integritet podataka
  - Obavezna dobra kontrola pristupa konfiguracijskih fajlova
  - Kontrola pristupa smanjuje mogucnost otkrivanja osetljivih informacija koje ne smeju biti javno izložene
  - Dobra kontrola pristupa će ograničiti korišćcenje resursa u slučaju napada

Bezbednosni propusti pri implementaciji Veb servera

- Kontrola pristupa
  - **Kontrolom pristupa** (eng. *Access Control*) reguliše se ko ima mogućnost pretraživanja i izvršavanja (CGI skripti) na serveru
  - Kontrola **čitanja** - štiti se poverljivost informacija
  - Kontrola **pristupa** - štiti se integritet podataka
  - Obavezna dobra kontrola pristupa konfiguracijskih fajlova
  - Kontrola pristupa smanjuje mogucnost otkrivanja osetljivih informacija koje ne smeju biti javno izložene
  - Dobra kontrola pristupa će ograničiti korišćcenje resursa u slučaju napada
  - Primarni uređaji za kontrolu pristupa su ruter i zaštitni zid

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku
  - Oprez: Korisnicki ulazni podaci mogu biti komande koje se automatski izvršavaju čime mogu da nanesu štetu host mašini i ugroze sigurnost servera

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku
  - Oprez: Korisnicki ulazni podaci mogu biti komande koje se automatski izvršavaju čime mogu da nanesu štetu host mašini i ugroze sigurnost servera
- Mehanizmi logovanja
  - **Logovi** su dnevnici u kojima se cuvaju podaci o tome ko je i kada modifikovao, dodavao i pristupao serverskim komponenatama

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku
  - Oprez: Korisnicki ulazni podaci mogu biti komande koje se automatski izvršavaju čime mogu da nanesu štetu host mašini i ugroze sigurnost servera
- Mehanizmi logovanja
  - **Logovi** su dnevnici u kojima se cuvaju podaci o tome ko je i kada modifikovao, dodavao i pristupao serverskim komponenatama
  - Logovi su često i jedini pokazatelji sumnjivih aktivnosti

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku
  - Oprez: Korisnicki ulazni podaci mogu biti komande koje se automatski izvršavaju čime mogu da nanesu štetu host mašini i ugroze sigurnost servera
- Mehanizmi logovanja
  - **Logovi** su dnevnici u kojima se cuvaju podaci o tome ko je i kada modifikovao, dodavao i pristupao serverskim komponenatama
  - Logovi su često i jedini pokazatelji sumnjivih aktivnosti
  - Dodatno - mehanizmi alarmiranja

Bezbednosni propusti pri implementaciji Veb servera

- Bagovi u CGI skriptama
  - **CGI** (eng. *Common Gateway Interface*) skripte su programi koji se na Veb serverima izvršavaju u realnom vremenu i čija je uloga da rukuju ulaznim podacima korisnika, pristupaju bazi i vraćaju informacije korisniku
  - Oprez: Korisnicki ulazni podaci mogu biti komande koje se automatski izvršavaju čime mogu da nanesu štetu host mašini i ugroze sigurnost servera
- Mehanizmi logovanja
  - **Logovi** su dnevnici u kojima se cuvaju podaci o tome ko je i kada modifikovao, dodavao i pristupao serverskim komponenatama
  - Logovi su često i jedini pokazatelji sumnjivih aktivnosti
  - Dodatno - mehanizmi alarmiranja
  - praviti i rezervne kopije (eng. *backup*) logova

Zaključak

- I pored svih mehanizama zaštite koji postoje, softver nikada ne može biti u potpunosti bezbedan
- S obzirom da su napadi na softverske sisteme učestaliji, mehanizmi zaštite se konstantno unapređuju
- Ovaj rad može predstavljati dobar uvod u detaljnije izučavanje pojedinih aspakata bezbednosti softvera koji su prikazani

Literatura

Software Security
College Park University of Maryland.
https://www.coursera.org/learn/software-security

Guidelines on Securing Public Web Server
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

Avoiding the top 10 software security design flaws
IEEE Computer Society
www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf