Bezbednost Aplikacija
Uvod

Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

Kome je namenjen predmet bezbednost aplikacija?

Administratori Sistema

Programeri

Security Analist – Osobe koje žele da se usavrše na polju bezbednosti informacionih sistema

Šta ćete naučiti?

Na koji način se napadači ponašaju u stvarnom svetu

Koji aspekti treba da budu uključeni za kreiranje bezbednijih aplikacija i sistema

Na koji način detektovati zlonamerno (maliciozno) ponašanje

Sadržaj predmeta

1. Osnove sprovođenja Pen testa

2. Arhitektura web aplikacija

3. Izviđanje i profilisanje web servera

   Tehnike i alati koji se koriste za preuzimanje informacija o tehnologijama koje su upotrebljene za razvoj, hostovanje i podršku ciljne aplikacije.

4. Detektovanje i eksplotacija zasnovana na ubrzgavanju (injection).

   Opisi napada zasnovanih na injektiranju

5. Nedostaci provere identiteta i upravljanja sesijom

   Upoznavanje sa načinima provere identiteta, nedostacima u dizajnu i kako ovi nedostaci mogu da se zloupotreba

6. Pronalaženje i eksplotisanje ranjivosti prenosa i izvršenja skripti (Cross Site Scripting – XSS)

Sadržaj predmeta

7. Napadi na nedostatke na polju kriptografije
   - Koncepti i algoritmi za enkripciju, kodiranje i heširanje
   - Alati za identifikaciju slabih SSL/TLS implementacija
   - Ekplotacija ranjivosti u uobičajnim kriptografskim algoritmima

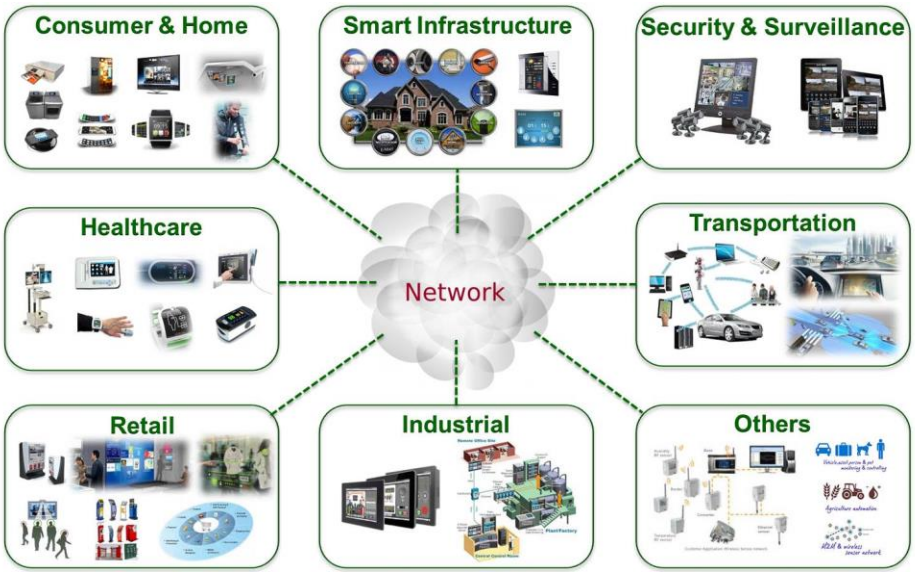
8. Napadi na strani klijenta
   - Upoznavanje sa klijentskim tehnologijama
   - Alati za zaobilaženje bezbedonosnih kontrola koje su implementirane na strani klijenta

9. Upotreba automatizovanih skenera u web aplikacijama

Web aplikacije

Tip aplikacije koji je danas najzastupljeniji u svim kompanijama

Aplikacije za mobilne telefone i IoT uređaji koriste web komponente kroz web servise i interfejse koji su ugrađeni u njih



Potreba za testiranjem web aplikacija

Web serveri i web aplikacije su atraktivne mete za napadače zbog velikog broja web sajtova na Internetu i organizacija koje svoje poslovanje obavljaju online.

Za interakciju sa web aplikacijom dovoljan je samo pretraživač (web browser)

Sajber kriminalci ostvaruju znatne finansijske dobitke eksploatisanjem web aplikacija I instaliranjem zlonamernih programa koji se prosleđuju korisnicima aplikacija

HTTP saobraćaj je dozvoljen od strane firewall-a, napadačima nisu potrebni posebni otvoreni portovi.

HTTP protokol nema ugrađene bezbednosne funkcije, ne obezbeđuje identifikaciju individualnih sesija što znači da je na programeru da ih dizajnira.

Bezbednost se uključuje u fazi projektovanja aplikacije.

Kasnije integrisanje bezbednosti je veoma teško i zahteva prilično prerade koda.

Potreba za zaštitiom od napada u web aplikacijama

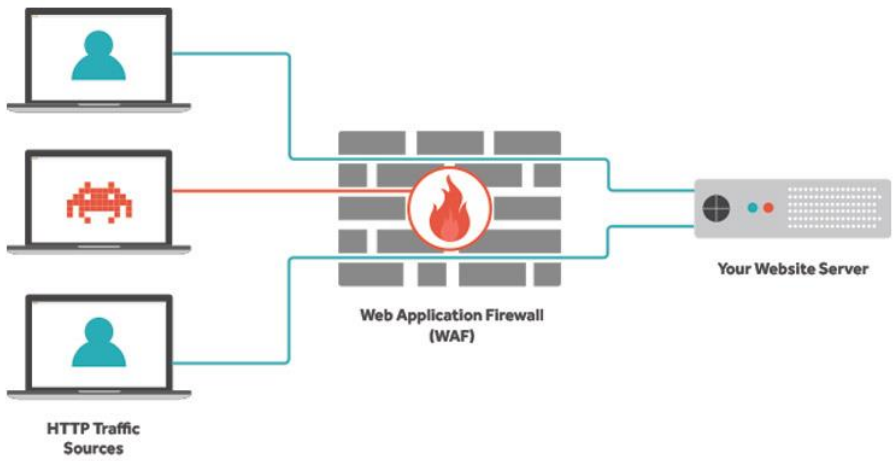
Zaštita podataka klijenata

Gubitak prihoda

Zaštita od prekida poslovanja

Gubitak reputacije

Usklađenost sa zakonima i propisima



Zašto je teško zaštiti računarski sistem

Kod koji sadrži greške u smislu bezbedonosnih propusta i koji se ne pridržava preporuka koje se odnose na bezbednost

Socijalni inženjering – prevarom do poverljivih informacija

- Novac može da se zaradi traženjem i eksplotacijom ranjivih aplikacija
- Market gde mogu da se nađu i kupe informacije o ranjivim aplikacijama
- Market za ukradene podatke i mašine koje su van kontrole vlasnika
- Postoji mnogo načina da se uzme profit od ukradenih podataka ili kompromitovanih mašina

Zašto se napada kompijuterski sistem

Spam

- Slanje sa legitimne IP adrese ima manju verovatnoću da sadržaj bude blokiran

DoS

- Napad na konkurente ili da se traži otkupnina

Inficiranje posetioca malware skriptom

- Jedan inficiran server može da inficira na stotine hiljada klijenata

Krađa podataka

- Krađa poverljivih podataka, brojeva kreditnih kartica, intelektualne svojine