TEHNIČKO VELEUČILIŠTE U ZAGREBU

Tehničko veleučilište u Zagrebu

Politehnički specijalistički diplomski stručni studij specijalizacija Informatika

Napredne tehnike programiranja web servisa (.open-source)

dr.sc. Alen Šimec, predavač | alen@tvz.hr

TEHNIČKO VELEUČILIŠTE U ZAGREBU
POLYTECHN CUM ZAGRABIENSIS

Sigurnost web aplikacija

Primjena Interneta u poslovnim procesima neprekidno raste

Tvrtke nude svoje usluge putem Internet aplikacija

Korisnici Interneta šalju osobne podatke, brojeve kartica putem web formi ili e-mail poruka, dijele osobne informacija preko društvenih mreža

Sigurnost web aplikacija

Sve češće korisnici kupuju proizvode preko Internet trgovina.

Bankarske transakcije (plaćanje i prijenos sredstava) koje smo prije radili na pošti ili u banci danas možemo napraviti u okruženju svoga doma

Sigurnost web aplikacija

Kako bi se zaštitio informacijski sustav, provjeru ranjivosti web aplikacija nužno je provoditi:

- prilikom kreiranja nove aplikacije,
- nakon svake izmjene u aplikaciji,
- nakon promjene nadležnih osoba (informatičara, specijalista za IT sigurnost ,..) te
- periodički (najmanje jednom godišnje)

Sigurnost web aplikacija

Provjerom se ispituje ranjivost sustava na sljedeće napade:

- SQL injection (ubacivanje SQL upita),
- Cross site scripting (ubacivanje programskog koda),
- CRLF injection (ubacivanje specijalnih znakova),
- Directory Traversal (neovlašteni pristup direktorijima na poslužitelju),
- Authentication Hacking (krađa autentikacijskih podataka)

Sigurnost web aplikacija

Web aplikacija kao usluga sastoji se od nekoliko komponenti:

- baze podataka koja skladišti informacije,
- poslužitelja sadržaja koji korisniku (tj. pregledniku) pruža sadržaj,
- preglednik koji na korisničkoj strani prikazuje sadržaj

Sigurnost web aplikacija

Alati za ispitivanje ranjivosti web aplikacija mogu raditi na dva principa:

- *glass-box* je usporedba ponašanja stranice sa poznatim obrascima ranjivosti. Korisniku su vidljivi procesi i obrasci koji se testiraju.
- *black-box* je nasumično ispitivanje (eng. fuzzying) i generiranje nasumičnih ulaznih i izlaznih parametara za aplikaciju uz praćenje ponašanja aplikacije. Ulazni i izlazni parametri su nečitljivi za korisnika

Sigurnost web aplikacija

Podjela sigurnosnih prijetnji prema Web Security Glossary (www.webappsec.org)

Klasifikaciju sigurnosnih prijetnji je izradila organizacija WebAppSec Consortium

Raspodjela sigurnosnih prijetnji prema WASC

Napadi	Slabosti
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions

Sigurnost web aplikacija

Napadi	Slabosti
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross - Site Scripting	Information Leakage
Cross - Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti - automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation

Sigurnost web aplikacija

Napadi	Slabosti
HTTP Request Smuggling	Insufficient Session Expiration
HTTP Request Splitting	Insufficient Transport Layer Protection
Integer Overflows	Server Misconfiguration
LDAP Injection	
Mail Command Injection	
Null Byte Injection	
OS Commanding	
Path Traversal	
Predictable Resource Location	

Sigurnost web aplikacija

Napadi	
Remote File Inclusion (RFI)	
Routing Detour	
Session Fixation	
SOAP Array Abuse	
SSI Injection	
SQL Injection	
URL Redirector Abuse	
XPath Injection	
XML Attribute Blowup	

Sigurnost web aplikacija

Napadi	
XML External Entities	
XML Entity Expansion	
XML Injection	
XQuery Injection	

Open Web Application Security Project

The Open Web Application Security Project (OWASP) je otvorena zajednica posvećena tome da omogući organizacijama razvijanje, kupnju i održavanje aplikacija koje se mogu smatrati sigurnima.

Suradnici na projektu su razni sigurnosni stručnjaci iz cijelog svijeta koji su podijelili svoje znanje za izradu ovog popisa.

Open Web Application Security Project

Na OWASP -ovom popisu deset najvećih ranjivosti iz 2010. godine su:

- Napad SQL upitom
- Cross-site scripting
- Nesigurne reference na objekte
- Loša autentifikacija i upravljanje sjednicama
- Krivotvorenje zahtjeva na drugom sjedištu

Open Web Application Security Project

Na OWASP -ovom popisu deset najvećih ranjivosti iz 2010. godine su:

- Pogrešno postavljene sigurnosne postavke
- Nesigurna pohrana šifriranih podataka
- Nezaštićeni pristup URL
- Nedovoljna zaštita na transportnom sloju
- Neprovjerena preusmjeravanja i prosljeđivanja

Abuse of Functionality

Ova klasa napada se odnosi na prijetnje koje koriste funkcionalnosti web - aplikacija kako bi nanijele štetu drugoj aplikaciji.

Koristi se nedovoljno zaštićena ispravna funkcionalnost informacijskog sustava

Ovakve prijetnje najčešće su kombinirane s drugim vrstama prijetnji: zlouporaba Send – Mail, zlouporaba funkcionalnosti oporavka zaporke

Brute Force

Napadi živom silom su vrste prijetnji kojima se pokušavaju odrediti nepoznati parametri korištenjem metode pokušaja i promašaja, a kao pomoć se koriste automatizirani procesi koji ispituju mnogo različitih mogućnosti.

Prednost koju koriste napadači je skup korištenih vrijednosti puno manji od statistički mogućih.

Brute Force

Pri napadu živom silom mogu se primjerice, istodobno pogađati korisničko ime i lozinka ili se jedno od njih može fiksirati (ako je poznato), a drugo pogađati.

Napad kod kojeg se fiksira zaporka, a pogađa korisničko ime se naziva obrnuti napad živom silom.

Kod ove vrste napada nije moguće pogoditi podatke specifičnog korisnika, pa se ovaj napad koristi kako bi se nasumično zaključali korisnički računi kod sustava koji nakon nekoliko neuspjelih pokušaja blokiraju korisnički račun.

Buffer Overflow

Napad prekoračenjem kapaciteta (spremnika) mijenjaju tijek izvršavanja programa (programskog odsječka) zauzimanjem memorijskog kapaciteta.

Mogu se koristiti za kontroliranje izvršavanja procesa, rušenje procesa ili mijenjanje internih varijabli sustava

Content Spoofing

Napad mijenjanjem sadržaja predstavlja namjeru napadača da se korisnika uvjeri (zavara) kako je određeni sadržaj koji je prikazan legitiman i da ne dolazi iz drugog izvora.

Primjer je dinamičko učitavanje stranica, dio html koda koji ispisuje okvir u kojem se nalazi druga stranica
<frame src="http://foo.example/file.html">

URL se može definirati:
http://foo.example/page?frame_src=http://attackers.example/spoof.html

Predviđanje korisničinih podataka

Predviđanje korisničkih podataka (engl. Session Prediction) metoda označava prijetnje kod kojih se pogađaju ili otimaju podatci o korisniku koji je spremljen u kolačić (engl. cookie), skriveno polje obrasca ili u URL

Kako bi se napadač predstavio kao korisnik može:

- se spojiti na web aplikaciju i zahtijevati određeni identifikator
- korištenjem kalkulacija izračunati idući identifikator
- zamijeniti trenutni identifikator s izračunatim sljedećim i tako se predstaviti kao korisnik koji se sljedeći ispravno prijavi u sustav.

Napad Cross - Site skriptama

Cross-site scripting (XSS) je vrsta računalne sigurnosne ranjivosti koja se nalazi u Internet aplikacijama.

To je aplikacija koja omogućava ulaz skripte koja se izvršava na klijentskoj strani, odnsno u Internet pregledniku korisnika.

Cross-site scripting je ranjivost koja se može iskoristiti od strane napadača, te zaobići kontrole pristupa računalu.

Provedeno istraživanje od firme Symantec 2007. godine oko 80% svih sigurnosnih propusta bilo je preko XSS

Napad Cross - Site skriptama

Utjecaj XSS-a može biti od manjih smetnji u radu računala do značajnijih sigurnosnih rizika, ovisno o osjetljivosti podataka koji se nalaze na računalu.

Cross-site scripting odnosi se na napadačku tehniku koja iskorištava ranjivost u kodu Internet aplikacija kako bi se omogućilo napadaču slanje zlonamjernih sadržaja krajnjem korisniku, te prikupljanju određenih vrsta podataka od žrtve

Napad Cross - Site skriptama

Programski kod se može pisati u različitim programskim jezicima kao što su HTML, Javascript, VBScript, ActiveX, Java, Flash

Postoje tri različita tipa XSS napada:

- Persistent ili Stored,
- Non-persistent ili Reflected
- DOM-based XSS

Napad Cross - Site skriptama

PERSISTENT OR STORED XSS

radi na principu umetanja koda na žrtvinu stranicu, pri ćemu prikuplja potrebne podatke

U ovoj vrsti napada napadač ne treba osigurati url (internet adresu) do korisnika, zato što Internet stranica zahtjeva od korisnika da unese podatke.

Primjer takvog napada je forum ili društvena mreža Twitter.

Napad Cross - Site skriptama

PERSISTENT OR STORED XSS

Napadač želi preuzeti podatke od korisnika. Šalje kroz formu poruku sa kodom koji se sprema u bazu na serveru.

Kada korisnik posjeti stranicu i zatraži stranicu koja po upitu ispiše podatke iz baze, a među tim podacima je i zlonamjerni kod koji korisniku sa njegovog računala pokupi osobne podatke.

Napad Cross - Site skriptama

PERSISTENT OR STORED XSS

Napadač kroz kod preuzima informacije iz kolačića (eng. Cookie) sa korisnikova računala.

U kolačiću nekada mogu biti zapisane informacije o karticama ili neki drugi povjerljivi podaci.

Napad Cross - Site skriptama

NON-PERSISTENT OR REFLECTED XSS

Najčešće korišteni napad na korisnika.

Napad se događa kada podaci poslani sa Internet stranice, kroz HTTP upit ili kroz HTML formu.

Stranica koja se nalazi na serveru obrađuju upit korisnika i prikazuje rezultate pretraživanja.

Napad Cross - Site skriptama

NON-PERSISTENT OR REFLECTED XSS

Korisnik nije svjestan koji se sve zlonamjerne veze mogu pojaviti kod prikaza stranice, te slučajno ili namjerno kliknuti na hipervezu koja će izvršiti napad na računalo.

Primjer takvog slučaja je ako uzmemo Internet stranicu koja je poznata i od povjerenja korisnika

Napad Cross - Site skriptama

NON-PERSISTENT OR REFLECTED XSS

Stranica ima vezu prema sadržaju koji više ne postoji na stranici.

Napadač može u tom slučaju iskoristiti priliku za ubacivanje svoje skripte unutar url adrese koju će poslati korisniku.

Uz url će staviti obavijest kako bi privukao korisnika da obavezno klikne na link koji vodi na sigurnu stranicu za korisnika i time pokrenuti vlastitu skriptu sa svog servera.

Napad Cross - Site skriptama

NON-PERSISTENT OR REFLECTED XSS

Primjer takvog zlonamjernog url-a: http://www.facebook.com/<scriptsrc="www.xss-napad.org/xss.js"></script>.

Kako Facebook stranica ne prepoznaje url sadržaj, vratit će korisniku da sadržaj ne postoji.

U ovom slučaju aktivirat će se vanjska skripta sa url adrese www.xss-napad.org/xss.js. Korisnik neće znati da je zapravo pokrenuo skriptu sa druge stranice.

Napad Cross - Site skriptama

DOM-based XSS

Ne zahtjeva Internet server za primanje zloćudnog koda XSS-a, kao kod reflected ili stored XSS

U DOM based XSS zlonamjerni kod koristi runtime embedding od podataka napadača sa klijentske strane (client-side) sa stranice koju poslužuje web server.

Ako uzmemo u obzir da HTML stranica može uključiti podatke korisnika kroz internet sučelje sa klijentske strane preko Internet preglednika na korisničkom računalu

Napad Cross - Site skriptama

DOM-based XSS

U slučaju da HTML stranica sadrži Javascript kod koji uključuje lokaciju jedne stranice u drugoj stranici.

Takva url lokacija može sadržavati zlonamjerni kod.

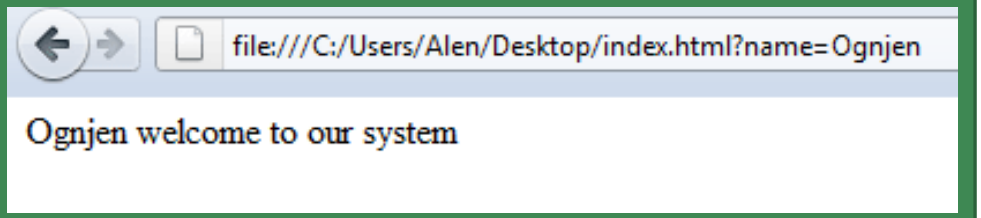
U takvom slučaju napadač može napasti klijentski Internet preglednik.

Napad Cross - Site skriptama

DOM-based XSS

Primjer takvog napada je recimo adresa http://www.sigurna-stranica.com/index.html koja sadrži slijedeći kod:

```
<html><title>(ne)sigurnost na internetu</title>
<head>
<script>
var pos=document.url.indexof("name=")+5;
document.write(document.url.substring(pos,document.url.length));</script>
</head>
<body>
    ovo je (ne)sigurna stranica
</body></html>
```



Napad Cross - Site skriptama

DOM-based XSS

U ovom primjeru Javascript kod uključuje dio od document.URL (lokaciju stranice) u samu stranicu, bez obzira na sigurnost.

Napadač može namamiti korisnika da klikne na link kao što je što će uključiti Javascript zločudni kod.

```
http://www.sigurna-stranica.com/index.html?name=
<script>alert(document.cookie)</script>
```

Napad krivotvorenjem Cross - Site zahtjeva

Krivotvorenje Cross - Site zahtjeva je napad kod kojega posjetitelj stranice koja se predstavlja kao originalna.

Korisnik se prijavljuje na stranicu slanjem HTTP zahtjeva stranici koja je meta napada.

Sva funkcionalnost ovoga napada je skrivena od korisnika i korisnik ne zna da sudjeluje u napadu.

Napad onemogućavanjem opsluživanja

Napad onemogućavanjem normalnog opsluživanja (engl. Denial of Service, DoS) jedna od najpoznatijih tehnka napada na informacijske sustave temeljene na tehnologijama weba.

Onemogućavanje normalnog rada sustava i to tako što se ţeli dovesti računalne resurse (CPU, memoriju, diskovni prostor, ...) do granice normalnog rada, tj. do opterećenja od 100%.

Ispad bilo koje od napadanih komponenti uzrokuje ispad cijelog sustava.

Napad onemogućavanjem opsluživanja

Napadi mogu biti usmjereni na:

- Specifičnog korisnika - napadač se konstatno pokušava logirati kao određeni korisnik, s pogrešnom lozinkom, što će onemogućiti logiranje stvarnom korisniku s tim korisničkim imenom
- Poslužitelja baze podataka - ubrizgava se SQL kod koji kompromitira bazu podataka
- Poslužitelja web aplikacije - koristi se tehnika Buffer Overflow koji će srušiti procese u poslužitelju i dovesti cijeli sustav do ispada

Napad dijeljenjem HTTP zahtjeva

Napad dijeljenjem HTTP zahtjeva (engl. HTTP Request Splitting) prisiljava preglednik da šalje proizvoljni HTTP zahtjev, nameće XSS ili kompromitira memoriju preglednika (cache)

Tehnika se temelji na tome da će umjesto jednog HTTP zahtjeva, slati dva zahtjeva u jednom.

Napad dijeljenjem HTTP odgovora

Napad dijeljenjem HTTP odgovora (engl. HTTP Response Splitting)

Za ovaj napad potrebna su barem 3 sudionika:

- Web poslužitelj koji ima sigurnosnu rupu koja omogućuje ovaj napad
- Meta - cache proxy poslužitelj ili preglednik klijenta koji komunicira s web poslužiteljem
- Napadač koji inicira napad

Napad SQL upitom

Napad SQL upitom (engl. SQL Injection) jedna od najpoznatijih tehnika je ubrizgavanje SQL izraza koji će svojom konstrukcijom ugrozit djelomičnu ili cijelu funkcionalnost sustava.

SQL umetanje je tehnika ubrizgavanja kôda koja iskorištava sigurnosni propust u kôdu web stranice.

Napad SQL upitom

Ranjivost se iskorištava kada se iz korisničkog unosa krivo filtriraju evakuacijski znakovi ugrađeni u SQL naredbe ili kada je unos nepravilno upisan i neočekivano izvršen.

SQL naredbe se tada umeću iz web obrasca u bazu podataka (kao i upiti) kako bi promjenili sadržaj baze podataka ili izvukli iz nje za napadača podatke kao što su brojevi kreditnih kartica ili lozinke.

Napad SQL upitom

SQL umetanje je uglavnom poznat kao napad na web stranice, ali se može koristiti kao napad na bilo koju vrstu SQL baze podataka.

Primjer ove vrste napada SQL izrazom je prikazan u narednom odsječku programskog koda:

```
SELECT * FROM Users WHERE UserId = 105 or 1=1
```

Napad SQL upitom

Ako se kao korisnički podatci unesu sljedeći:
105, 1 ili "=", dobit ćemo upit koji izgleda ovako:

```
SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1
```

Ovaj upit će (zbog usporedbe s "=") uvijek biti točan bez obzira na to jesu li "105" i "1" stvarni podatci ili ne, za sve zapise u tablici.

Napad SQL upitom

Drugi način napada SQL injekcijom odnosi se na spremljene procedure (SQL Injection in Stored Procedures)

Primjer programskog koda i parametara koji mogu kompromitirati sustav (obrisati tablicu o korisnicima)

```
SELECT * FROM Users; DROP TABLE Suppliers
```

Napad SQL upitom

Napadački parametri:

105; DROP TABLE Suppliers

Dobiveni upit:

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE Suppliers
```

Pristup problemu SQL injekcije treba biti sustavan jer se jednim napadom može prouzročiti ogromna šteta, poput prikazanog brisanja podataka iz baze

Top 10 napada na aplikacije

Application vulnerabilities: Closer than you think

http://www.questsys.com

Top 10 Application Vulnerabilities

RANK*	Finding	Percentage of Applications Containing Vulnerability
1	SQL Injection	15%
2	Miscellaneous Logic Flaws	14%
3	Insecure Direct Object Reference	28%
4	Cross-Site Scripting (XSS)	82%
5	Failure to Restrict URL Access	16%
6	Cross-Site Request Forgery	72%
7	Other Injection	7%
8	Insecure File Uploads	10%
9	Insecure Redirects	24%
10	Various Denial of Service	11%

Nastanak i porijeklo prijetnji

Svaka od prijetnji ispravnom funkcioniranju informacijskog sustava uzrokovana je pogreškama u određenim dijelovima razvoja sustava.

Uzrok pojedinih slabosti mogu se podijeliti u 3 skupine:

- Dizajn - pokriva slabosti koje nastaju zbog nepravilnog dizajna samog sustava ili zbog izrade sustava na način koji odstupa od preporučenog ili zahtijevanog.

Nastanak i porijeklo prijetnji

- Implementacija - pokriva slabosti koje nastaju zbog loše implementacije zamisli i tehnologija koje su određene dizajnom.
- Produkcija - pokriva slabosti koje su posljedica loših procedura za puštanje u produkcijski rad ili su posljedica neispravne konfiguracije poslužitelja

Sigurnost web aplikacija

Sva moguća pažnja usmjerena je na sigurnost web aplikacija.

Sigurnost informacijskog sustava obuhvaća:

- Autentifikaciju (Authentication)
- Autorizaciju (Authorization)
- Povjerljivost (Confidentiality)
- Integritet podataka (Data/Message integrity)
- Odgovornost (Accountability)
- Raspoloživost (Availability)
- Neporecivost (Non - repudiation)

Sigurnost web aplikacija

Sigurnost kao pojam obuhvaća:

- fizičku sigurnost,
- tehnološku sigurnost,
- pravila pisanja i procedure.

FIZIČKA SIGURNOST sustava odnosi se na svu elektroničku infrastrukturu koja je vezana za informacijski sustav i pristup navedenoj infrastrukturi.

Sva infrastruktura, od poslužitelja, usmjeritelja i druge opreme, treba biti strateški smještena u prostore u kojima se stalno nadzire pristup. Uz to, prostorije trebaju biti zaštićene od poplava, potresa, požara i drugih pojava koje vode do neželjenih posljedica.

Fizička sigurnost

Poslužitelji na kojima su podaci trebaju imati redundantne sustave koji će osigurati dostupnost samog sustava i podataka.

Za nadzor pristupa poslužiteljima mogu se koristiti nadzorne kamere, čitači kartica ili sustavi za kontrolu pristupa temeljeni na biometriji.

Potrebno je onemogućiti izravno snimanje podataka na prenosive medije s poslužitelja ili je potrebno takve podatke kriptirati. Time će se spriječiti čitanje podataka od strane neovlaštenih osoba, čak i ako su podaci ukradeni

Tehnološka sigurnost

Tehnološka sigurnost je podijeljena u tri područja: sigurnost aplikacija, sigurnost operacijskog sustava i mrežna sigurnost.

Aplikacijska sigurnost odnosi se na sigurnost samog informacijskog sustava. Ovdje se mogu razmatrati sve slabosti koje su nastale u fazama dizajna i implementacije.

Iako su operacijski sustavi najkompleksniji u cijelom lancu sigurnosti, za njih se najčešće brinu njihovi proizvođači.

Obvezno je redovito instalirati zakrpe operacijskog sustava.

Mrežna sigurnost

Mrežna sigurnost se odnosi na osiguranje da mrežom dolaze samo valjani paketi podataka prema informacijskom sustavu

Zlonamjerni paketi najčešće sadrže sekvence bitova koji, nakon što su interpretirani od strane poslužitelja ili aplikacije, izazivaju neočekivano ponašanje komponenti sustava.

Ovakve disfunkcionalnosti mogu izazvati razne oblike neočekivanih stanja na korisničkim računalima, od toga da rade neispravno, do toga da prikupljaju povjerljive informacije i šalju ih napadaču.

Tehnološka sigurnost

Najčešći alati koji sprječavaju dotok neželjenog prometa u mrežu su sigurnosne stijene (engl. Firewall) i sustavi za otkrivanje nedopuštenih upada u mrežu (IDS ili Intrusion Detection Systems)

***IDS** sustavi nadziru mrežni promet i sumnjive aktivnosti i događaje prijavljuju administratoru ili zapisuju u log datoteku. U nekim slučajevima ovi sustavi i reagiraju preventivno na sumnjiva ponašanja blokiranjem korisnika ili izvorišne IP adrese.*

Vrste autentifikacije i SSL protokol

U velikim distribuiranim sustavima zasnovanim na principima računarstva u oblacima i drugi entiteti sustava mogu biti subjekti koje je potrebno autentificirati.

Radi se zapravo o autentifikaciji među računalima. Možemo razmatrati tri vrste provjere autentičnosti:

- Autentifikaciju klijenta - označava skup akcija kojima poslužitelj utvrđuje identitet klijentskog računala
- Autentifikacija poslužitelja - označava skup akcija kojima klijentsko računalo utvrđuje identitet poslužitelja
- Uzajamna autentifikacija - označava skupove akcija kojima klijentsko i poslužiteljsko računalo međusobno utvrđuju identitet drugih strana

Vrste autentifikacije i SSL protokol

U kontekstu ovih vrsta autentifikacije se najčešće govori o protokolu SSL, Secure Socket Layer.

Najkorišteniji standard za osiguranje autentifikacije, povjerljivosti i integriteta poruka i podataka u sustavima koji podržavaju.

SSL u svojim temeljima koristi simetričnu i asimetričnu kriptografiju, kao i elektroničke potpise kako bi osigurao sigurnosne principe.

Vrste autentifikacije i SSL protokol

SSL protokol je dio TLS-a (Transport Layer Security), a prepoznaje se pojavom dodatka "s" izrazu "http" u alatnoj traci preglednika.

Vrste autentifikacije i SSL protokol

Povjerljivost je treće važno svojstvo sigurnosti informacijskih sustava namijenjenih elektroničkom poslovanju, a u općenitom smislu govori da svi podatci koji se razmjenjuju u komunikaciji kao i oni koju su pohranjeni u trajnu ili privremenu memoriju moraju biti zaštićeni od drugih strana.

U štićenju komunikacije koristi se SSL koji radi na principu certifikata koji se nalazi na određenom poslužitelju, a izdan je od strane Central Authority.

Vrste autentifikacije i SSL protokol

Infrastruktura javnog ključa je temelj za uporabu certifikata, a zasniva se na asimetričnoj kriptografiji. PKI se sastoji od:

- Certifikacijskog tijela (CA) koje izdaje, povlači i održava certifikate.
- Registracijskog tijela (RA, Registration Authority) koje provjerava sadržaj certifikata za CA, obavlja identifikaciju i autentifikaciju strana koje se prijavljuju za dobivanje certifikata
- Korisnika PKI koji su vlasnici certifikata
- Klijenata (aplikacije)
- Repozitorija koji održava popise certifikata.

SSL Certifikat - sigurnosna zaštita stranica i podataka

SSL certifikati se koriste prilikom unosa osjetljivih podataka kao što su brojevi kreditnih kartica u web trgovinama ili za zaštitu administracijskih sučelja.

Certifikati služe za enkriptirani prijenos podataka između korisnika i servera

- Rapid SSL (url: https://www.rapidssl.com)
- Verisign (url: http://www.verisign.com)
- Thawte (url: http://www.thawte.com)
- Geotrust (url: https://www.geotrust.com)

Zaključak

Internet aplikacije su najčešće meta neovlaštenih korisnika, te je važno održati sigurnost na što višoj razini.

Određene ranjivosti koje se smatraju propustima niskog sigurnosnog rizika, iskusniji neovlašteni korisnici mogu iskoristi za zlonamjerne radnje.

Nema apsolutne sigurnosti od zlonamjernih napada. Ovo je vrlo dinamično područje gdje se nove ranjivosti otkrivaju jednako brzo kao što se poznate ranjivosti osiguravaju.

Aplikacije ne mogu postići 100 postotnu sigurnost, ali bi trebale postići da je sigurnost povjerljivih podataka s kojima raspolažu na najvišoj mogućoj razini.

TEHNIČKO VELEUČILIŠTE U ZAGREBU
POLYTECHN CUM ZAGRABIENSIS

Sigurnost web aplikacija

Literatura:

1. Šimec, Alen; Staničić, Ognjen; Internet application security; http://bib.irb.hr/prikazi-rad?&lang=en&rad=582394
2. Šilić, Marin; Krolo, Jakov; Delač, Goran; Security Vulnerabilities in Modern Web Browser Architecture; http://bib.irb.hr/prikazi-rad?rad=473776
3. Tomiša, Mario; Mrvac, Nikola; Kozina, Goran; Sigurnost web aplikacija; http://biblio.irb.hr/prikazi-rad?&lang=ENG&rad=511346

Pitanja