

FUNKCIONALNO-BEZBEDNOSNI ASPEKTI VEB 2.0 I VEB 3.0

Gojko Grubor¹
Angelina Njeguš²
Nenad Ristić³

Univerzitet Singidunum
Danijelova 32, Beograd
Tel: +381 11 3093-236

¹e-mail: ggrubor@singidunum.ac.rs

²e-mail: anjegos@singidunum.ac.rs

³e-mail: nristic@sinergija.edu.ba

Rezime – Pored toga što se još uvek razmatra bezbednost najjednostavnijih veb 1.0 aplikacija pa do onih najsloženijih SOA zasnovanih veb 2.0 aplikacija, tržište se već hvata u koštac sa problemima bezbednosti veba najnovije generacije. U radu se razmatraju funkcionalni aspekti generacija veba, maliciozne pretnje za veb lokacije i ističu glavni napadi na veb 2.0 aplikacije.

Abstract - Although still considered the security of a simple Web 1.0 applications or more complex SOA-based Web 2.0 applications, the market is already consider the security problems of the latest generation of the web. The paper discuss the functional aspects of the Web generations, the malicious threats of web sites and highlight the main attacks on Web 2.0 applications.

1. UVOD

Ako se klasičan veb definiše kao meta servis Interneta namenjen „samo za čitanje“¹, onda je najbliža pojednostavljena definicija veb 2.0 - „za čitanje i pisanje“, a veb-3.0 – za „čitanje - pisanje - izvršavanje“. Dakle, prvi veb je dopuštao pretragu i čitanje informacija, sa malo interakcije korisnika i doprinosa sadržaju veba. Tipičan predstavnik u ovoj kategoriji je veb aplikacija potrošačke korpe, prisutna na većini komercijalnih lokacija.

Osnovno obeležje veb 2.0 je interaktivna komunikacija svih učesnika, gde učesnici mogu uticati i na sam sadržaj stranica. Termin koji karakteriše veb 2.0 su: blogovanje (*bloging*), veb zajednice (*Web communities*), hostovanje servisa (*hosted services*), veb aplikacije, sajtovi za društveno umrežavanje (*social-networking*), sajtovi za deljenje videa (*video-sharing*), wiki koncept, *mashups* i druge. Društvene mreže kao što su MySpace, Facebook i dr., zatim blogovi ili web lični dnevници, wiki sajtovi na kojima posetilac može da kreira i ažurira sadržaje (npr. Wikipedia) su obeležili veb 2.0 generaciju.

Najnovija generacija veba je Web 3.0. Za razliku od veba 2.0 koji koristi internet da bi se povezao sa ljudima, veb 3.0 koristi internet kako bi se povezao sa informacijama. Veb 3.0 je kao lični asistent koji poznaje profil svog vlasnika i na osnovu njegovih zahteva krstari vebom

¹ Direktor W3C, Tim Berners-Lee

radi dobijanja željenih informacija. Osnova veb 3.0 je semantički veb koji predstavlja standarde i tehnologije za razvoj veb ontologije. Prema internet terminologiji, ontologija je fajl koji definiše relacije između grupa termina. Na primer, termin „rođak“ se odnosi na porodične odnose između dvoje ljudi koji dele isti skup praroditelja.

Da bi semantički veb bio efektivan, ontologije moraju biti detaljne i sveobuhvatne i pisane u formi metapodataka. Metapodatak je informacija koja je uključena u kôd veb stranice, nevidljiva je za korisnike, ali čitljiva za računare. Izrada ontologija zahteva puno vremena, tako da to predstavlja jednu od glavnih prepreka uvođenja semantičkog veba. Takođe se postavlja pitanje da li će korisnici na njihovim veb stranicama kreirati sveobuhvatne ontologije, da li će ih redovno ažurirati itd. Sa semantičkim vebom ne dobijaju se samo tačniji rezultati pretrage, već se informacije sa različitih izvora mogu i povezivati, mogu se primeniti i elementi poslovne inteligencije, kao što su algoritmi data mining-a i dobiti znanje o određenom domenu. Na primer, ukoliko planirate da odete na godišnji odmor na destinaciju iz vaših snova, ali pod pristupačnom cenom i uslovima putovanja, potrebno je da u vaš veb 3.0 pretraživač otkucate složeniju rečenicu, na osnovu čega softverski agenti semantičkog veba skeniraju i interpretiraju željene informacije. Veb 3.0 pretraživač će se ponašati kao vaš lični asistent, dok pretražujete na vebu on će učiti o vama, vašim interesovanjima, ponašanju itd. Što više koristite veb, više će pretraživač znati o vama, tako da pri postavljanju svakog narednog pitanja ne morate da budete mnogo detaljni. Na primer, možete postaviti sledeće pitanje vašem pretraživaču: „Gde da odem na večeru?“. Pretraživač će konsultovati zapise o vama, šta volite, uzeće u obzir vaše trenutno stanje na računaru, lokaciju gde se trenutno nalazite i dr. podatke i na osnovu toga predložiti vam listu restorana. Međutim, on neće samo izlistati nazive restorana, već njihove lokacije može prikazati i na mapi, koristeći npr. Google Maps program.

Upoređujući veb kroz generacije, može se uvideti sledeće:

- Web 1.0 – gradile su se informacione tehnologije isključivo namenjene korisnicima (npr. kreirali su se veb sajtovi za korisnike). Oblik veb 1.0 je P2W (*People connecting to the Web*)
- Web 2.0 – gradile su se veb aplikacije i alati da bi korisnici mogli sami graditi „IT“ za njihove potrebe (npr. društvene mreže, wiki). Oblik veba 2.0 je P2P (*People connecting to other People*)
- Web 3.0 – veb kao portabilni lični asistent koji kombinuje više različitih aplikacija u jednu i koristi prednosti semantičkog veba, inteligentnih pretraživača, georeferenciranih veb aplikacija i dr. Oblika je W2W (*Web applications connecting to Web applications on behalf of People to enrich online experiences*).

Za nove funkcionalnosti veb 2.0 i veb 3.0 pojavile su se nove, sofisticirane pretnje, za koje tradicionalne mere zaštite IS nisu dovoljne, a najčešće ni adekvatne.

2. FUNKCIONALNI ASPEKTI VEB SERVISA

Veb servis je programski sistem dizajniran da podržava interakciju računar-računar preko Interneta, uobičajeno u formi nekog API-a (*Application Programming Interface*). Danas je na raspolaganju na hiljade veb servisa. Kombinovanjem semantičkog markap jezika i veb servisa, otvara se mogućnost da veb 3.0 aplikacije međusobno komuniciraju direktno i šire

pretražuju informacije kroz jednostavan interfejs. Veb 2.0 za razliku od veba 1.0 ima interfejse koji više liče na desktop aplikacije nego na dokumente.

Web 1.0		Web 2.0		Web 3.0
“najčitaniji read-only veb”		“najrasprostranjeniji read-write veb”		“portabilni lični veb”
45 miliona globalnih korisnika (1996)	>	1 bilion + globalni korisnici (2006)	>	Fokusiran na pojedinca
Fokusiran na kompanije	>	Fokus na zajednice	>	<i>lifestream</i>
<i>Home pages</i>	>	Blogovi	>	Dinamički sadržaj
<i>Posedovanje sadržaja</i>		Deljenje sadržaja		Semantički veb
<i>Britannica Online</i>	>	<i>Wikipedia</i>	>	<i>Widgets, drag & drop mashups</i>
HTML, portali		XML, RSS		Korisničko ponašanje (“me-onomy”)
<i>Web forms</i>		<i>Web applications</i>		iGoogle, NetVibes

Tabela 2 – Poređenje generacija veba

Osnovne tehnike na kojima se zasniva Web 2.0 su:

- veb servisi – web API kojima se pristupa preko mreže da bi se izvršili na udaljenoj mašini koja je zahtevala dati servis
- Ajax (Asynchronous JavaScript And XML) - tehnika za kreiranje interaktivnih veb aplikacija. Cilj ove tehnike je podela stranice na dinamičke delove koji šalju odvojene zahteve i na taj način mogu nezavisno komunicirati sa serverom (serverima)
- Web syndication - forma udruživanja (sindikacije) koji omogućava da se sadržaj veb sajta multiplicira na druge sajtove

Generalno, veb 2.0 servisi su jeftiniji, lakši za razvoj i implementaciju i fleksibilniji od skraćenih i ugrađenih poslovnih softverskih aplikacija. Veb 2.0 aplikacije su dizajnirane na bazi otvorenih standarda i alata kao što su *tagovanje*, *indeksiranje* (bukmarking) i *korisnički generisani sadržaji*, koji omogućavaju nove oblike saradnje za poslovne sisteme. Aplikacije za tabelarne prikaze (*spreadsheets*) se pomeraju na veb i obezbeđuju novu funkcionalnost za komunikaciju i razmenu podataka. Dobar primer su Google-ove veb-bazirane aplikacije za obradu teksta i tabelarne prikaze, kompatibilne sa MS Office ekvivalentima, kao i *Zoho Sheet-ov online spreadsheet* servis kompatibilan sa svim *Excel* dokumentima i API za potpunu (savršenu) integraciju sa brojnim drugim softverskim alatima.

Veb 2.0 servisi pomažu korisnicima da se lakše pronađu i obezbeđuju alate za identifikovanje mreže ljudi koji su najuticajniji u organizacijama (npr., *Workday Human Capital Management* ERP rešenje za upravljanje ljudskim resursima, *Cogentz i dr.*). Tehnologije veb 2.0 (blogovi, *wikipedia* i sajtovi za deljenje video zapisa) omogućile su nove oblike komunikacije poslovnih sistema sa kupcima, kao i pojavu brojnih veb 2.0 alata kao što su:

- *Astoria Software* veb bazirani CMS (*Content Management System*) za koordinaciju svih aspekata proizvodnih procesa;
- *Jadu Intranet 2.0*, veb bazirani CMS koji nudi proizvode za netehničke korisnike, male i srednje organizacije i državne organe;
- *Marqui*, veb bazirani CMS i sistem za upravljanje projektima za kreiranje integrisanih marketinških kampanja;

- *IBM Lotus Connections, Big Blue*-ov softver sa modulima za kreiranje i deljenje profila, blogova, *bookmarks* i statusa projekata;
- *BaseCamp*, set alata za upravljanje projektima koji kombinuje blogove, liste i multimedijske sadržaje i omogućava komunikaciju sa članovima tima;
- *CentralDesktop*, alat za saradnju ne-tehničkih korisnika, lagan za podešavanje sa gotovim templejtima;
- *Salesforce.com*, fleksibiln set veb baziranih alata za CRM (*Customer Relationship Management*) proizvode;
- *Relenta CRM*, baziran na genričkom e-mail klijentu za male i srednje organizacije, koji prati sve komunikacije koje se odnose na prodaju;
- *Microsoft Dynamics CRM Live*, veb bazirana verzija lansirana krajem 2007. i dr.

3. MALICIOZNE PRETNJE ZA VEB LOKACIJE

U toku šest meseci 2009. godine porastao je broj malicioznih veb lokacija za 233% u odnosu na prošlu godinu, a za 671% tokom 2008. godine (u odnosu na 2007.)¹. Od malicioznih veb lokacija u prvoj polovini 2009., 77% su kompromitovane legitimne lokacije. Ovaj visok procenat porasta malicioznih veb lokacija nastao je zbog masovnih napada tipa *SQL injection*, uključujući *Gumblar*, *Beladen* i *Nine Ball* napade. Pokušaji da se zaštite veb 2.0 aplikacije individualnim merama samozaštite, bili su neuspešni.

Pored toga, 69% veb stranica sa problematičnim sadržajem imalo je barem jedan maliciozni link. Isti je slučaj sa 78% novo-otkrivenih veb stranica u prvoj polovini 2009. godine. Veb SOA i dalje su najčešći vektori napada radi krađe podataka. U prvoj polovini 2009. godine preko 57% napada radi krađe podataka izvršeno je preko veb lokacija, od čega je 37% malicioznih veb napada uključivalo kod za krađu podataka. U istom periodu, od svih neželjenih e-mail poruka koje cirkulišu Internetom, 85,6% sadrži linkove za *spam* lokacije i/ili maliciozne veb lokacije. Samo u junu 2009. godine od ukupnog broja *e-mail*-ova sa otkrivenim virusom, porastao je za 600% u odnosu na prethodni mesec. U prvoj polovini 2009. godine 83% veb lokacija imalo je veoma kritične ili urgentne probleme a najmanje 64% veb lokacija trenutno ima velike, kritične ili urgentne bezbednosne probleme². Od 22.000 identifikovanih ranjivosti, skoro 9.000 ostaje otvoreno, dok je glavnina – 13.000 otklonjeno. Samo 36% veb lokacija nije imalo ozbiljnijih ranjivosti, što je za 17% manje od prethodnog izveštaja. Na osnovu ovih istraživanja sve veb lokacije imaju šansu da budu kompromitovane, jer koriste iste tehnologije, a one koje uspevaju da se zaštite preduzimaju interne mere da fiksiraju glavne ranjivosti da smanje verovatnoću štete za svoju reputaciju i klijente.

Nedavni napadi na hiljade veb sajtova, uključujući *Twiter*, *Facebook* i *MySpace* ukazuju da ove platforme imaju ono što hakeri žele ukrasti – korisničke podatke. Takođe su veoma ranjive i ugrožene veb lokacije obrazovnih institucija- 83% sa najmanje jedno ranjivosti, što ne iznenađuje pošto većina obrazovnih institucija ima brojne veb-izložene aplikacije, a nemaju dovoljno resursa posvećenih zaštiti veb servisa.

Najnovije pretnje dolaze u malim skupovima od po nekoliko hiljada kombinovanih malicioznih kodova koji konstantno menjaju svoj potpis na svakom PC kojeg napadnu i ostaju

¹ Websense, godišnji izveštaj

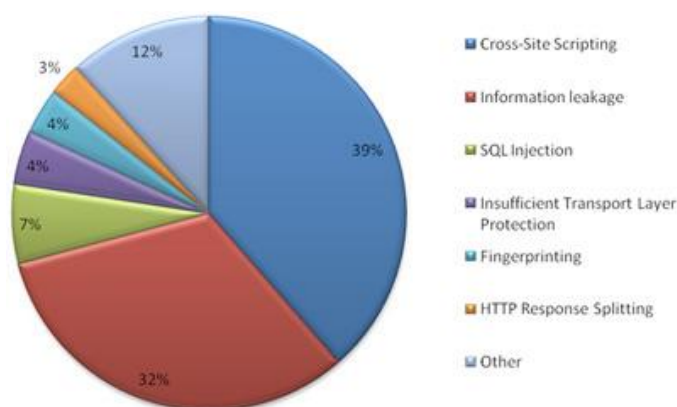
² The WhiteHat Security Website Security Statistics Report, oktobar 2009

skriveni. Dok AVP, *antispy* i drugi slični programi uglavnom reaktivno čiste infekciju posle napada, oni nisu efektivna odbrana za napade nultog-dana na veb aplikacije. Veb 2.0 aplikacije donose mnogo više novih funkcionalnosti i interakcije u realnom vremenu između krajnjih korisnika i veb aplikacija pa ovo povećanje funkcionalnosti automatski otvara više tehničkih mogućnosti za maliciozne napade. Ovo je glavni razlog poslednje poplave hakerskih napada na veb lokacije. Važnu ulogu u bezbednosti veb aplikacija imaju, takođe, krajnji korisnici - posetioци veb lokacija.

Pošto je veb lokacija ranjiva na mobilne kodove (*skriptove*) kroz veb lokacije (*Cross-Site Scripting*), maliciozni napadač može ubaciti specifičan kod u ranjivu aplikaciju koja se automatski izvršava kada korisnik –žrtva pristupi stranici u koju je kod ubačen. Obično veb lokacija izgleda legitimno, a korisnik nije svestan opasnosti. Kada jednom pristupi veb stranici, korisnik podnosi zahtevane podatke veb aplikaciji, kao što su lozinka, detalji za e-bankarstvo ili broj kreditne kartice. Tada napadač može lako ukrasti korisnikov kolačić (*cookies*) i otkriti korisničke podatke, dok je ulogovan na ranjivoj lokaciji. Ako je korisnik administrator veb lokacije, napadač može ukrasti administratorske privilegije za veb aplikacije, odnosno tokom vremena preuzeti punu kontrolu nad veb aplikacijom, ako otkrije druge ranjivosti u veb aplikaciji.

Analizom rezultata WASC¹ statističkog projekta za bezbednost veb aplikacija na uzorku od 12.186 veb aplikacija, otkriveno je 97.554 ranjivosti na različitom nivou rizika od čega, su najvažniji sledeći zaključci, (slika 3):

- Najčešća ranjivost su *Cross-site Scripting*, različiti tipovi curenja informacija, *SQL injection*, deljenje HTTP odgovora (*HTTP response splitting*);



Slika 1.1. Zastupljenost veb napada tokom 2008.godine (WASC)

- Verovatnoća da se otkrije urgentna ili kritična ranjivost u dinamičkoj veb aplikaciji iznosi oko 49% automatskim skeniranjem, a 96% ako se izvrši sveobuhvatna digitalna forenzička analiza (metodom *bele kutije*);
- Za 20% su češće greške administratora, nego projektanata i programera veb lokacije.
- Oko 99% veb aplikacija nije usaglašeno sa standardnim zahtevima (PCI DSS), a 48% veb aplikacija nije usaglašeno sa kriterijumima ASV skeniranja sa PCI DSS.

¹ WASC - Web Application Security Consortium (2008)

- Metod detaljne forenzičke analize *bele kutije* omogućava otkrivanje do 91% ranjivosti, dok automatsko skeniranje može otkriti samo 3 ranjivosti po veb lokaciji;
- U poređenju sa 2007. godinom, broj veb lokacija sa ranjivostima na *SQL Injection* i *Cross-site Scripting* napade, pao je za 13% i 20% respektivno, ali je broj lokacija sa različitim tipovima curenja informacija porastao za 24%. Takođe je verovatnoća kompromitacije hosta veb lokacije automatski porastao sa 7% na 13% u istom periodu.

3.1. Deset glavnih vektora napada na veb 2.0 aplikacije

Pokretačka snaga za razvoj veb 2.0 aplikacija su veb servisi koji jačaju ključne komponente serverske strane i AJAX (*Asynchronous JavaScript + XML*) i RIA (*Rich Internet Application*) klijenti koji poboljšavaju interfejs klijenta u samom pretraživaču. XML značajno utiče na slojeve prezentacije i transportni sloj (HTTP/HTTPS) i u određenoj meri zamenjuje HTML na sloju prezentacije, dok SOAP postaje transportni mehanizam na bazi XML-a.

Na serverskoj strani servisi bazirani na XML-u zamenjuju neke od ključnih funkcionalnosti i obezbeđuju pristup distribuiranim aplikacijama preko interfejsa veb servisa (GET, POST ili SOAP). Sa druge strane RIA, AJAX i veb servisi zahtevaju nove dimenzije zaštite veb aplikacija. Glavnih deset vektora napada na veb lokacije su:

1. **Cross-site scripting u AJAX-u**, gde se maliciozni JavaScript mobilni kod sa određene veb lokacije izvršava na pretraživaču žrtve i kompromituje informacije. Primer je *Yamanner crv* koji je nedavno iskoristio ovu ranjivost na AJAX pozivu Yahoo-ovog mejla. AJAXS je izvršen na klijentskoj strani, dopuštajući napadaču da iskoristi netačno napisani skript. Ova ranjivost postoji u tradicionalnim aplikacijama, ali joj AJAX dodaje novu dimenziju
2. **Zagađivanje XML formata** koji putuje napred-nazad između servera i pretraživača klijenta u brojnim veb 2.0 aplikacijama. Veb aplikacije troše XML blokove koji dolaze od AJAX klijenata. Kako je moguće zagađiti XML, napad može izazvati pad servera i odbijanje izvršavanja servisa (DOS). Napadač takođe može generisati slabo formatiran XML dokument koji može pokvariti logiku, zavisno od *parsing* mehanizma na serveru: SAX ili DOM. Isti mehanizam vektora napada korišćen je uza napad na SOAP poruke, koje nisu ništa drugo nego XML poruke. Ova ranjivost može pomoći napadaču da kompromituje poverljivost informacija.
3. **Maliciozno izvršavanje AJAX koda**. AJAX je grupa međusobno odnosnih tehnika koje se koriste na klijentskoj strani za kreiranje interaktivnih aplikacija. Sa AJAX-om veb aplikacija može asinhrono izvlačiti podatke iz servera u pozadini, ne utičući na displej i ponašanje postojeće lokacije. Upotreba AJAX tehnika dovela je do povećanja interaktivnih, dinamičkih interfejsa na veb lokacijama. Podaci se obično izvlače iz servera pomoću *XMLHttpRequest* objekta. Uprkos imenu, ne zahteva se upotreba *JavaScript*-a i *XML*-a, niti da zahtevi budu asinhroni. AJAX poziv je nečujan i krajnji korisnik ga ne može registrovati. Kada pretraživač šalje poziv sa *XMLHttpRequest* objektom nekoj veb lokaciji sa nje preuzima kolačiće (*cookies*) sa svakim zahtevom, što potencijalno može dovesti do kompromitacije lokacije. Na primer korisnik XY se uloguje posle autentifikacije na veb server svoje banke. Po kompletiranju procesa autentifikacije on preuzima kolačić. Kako veb stranica banke može imati mnogo kritičnih informacija. Kada pretražuje druge veb stranice, dok je još uvek ulogovan na veb stranicu svog bakarskog naloga može stići na veb stranicu napadača, na kojoj je

napadač upisao tihi AJAX pozivni kod, koji pošalje nazad zahtev veb stranici banke korisnika XY bez njegovog znanja, pokupi kritične informacije sa te stranice i pošalje natrag na veb stranicu napadača. Ovaj napad dovodi do proboja sistema zaštite veb servera banke i omogućava krađu brojeva bankarskih računa klijenata.

4. **RSS/ubacivanje atoma** je novi veb 2.0 napad. RSS podržava sve poznate metode za deljenje informacija na veb portalima i veb aplikacijama. Ove metode veb aplikacije koriste i šalju pretraživaču na klijentskoj strani. Napadač može ubaciti bukvalno Java Scripts u RSS format i generisati napade na pretraživač klijenta. Kada krajnji korisnik poseti neku veb stranicu sa RSS formatom i malicioznim skriptom može instalirati maliciozni program ili ukrasti kolačiće sa poverljivim informacijama. Ovo je katastrofalan napad na klijentsku stranu. Još gore je što može mutirati. Kako RSS i ATOM feeds postaju integralni deo veb aplikacija važno je filtrirati određene karatere na serverskoj strani pre slanja podataka krajnjem korisniku.
5. **Skeniranje i listiranje WSDL** (*Web Services Definition Language*) interfejsa za veb servise. U ovom fajlu nalaze se ključne informacije o tehnologijama, izloženim metodama, pozivne obrasce itd. Ovo su vrlo osetljive informacije i mogu pomoći u definisanju korišćenog metoda. Ako se drže otvorenim nepotrebne funkcije ili metodi mogu se izazvati potencijalnu katastrofu za veb servise. Važno je zaštititi WSDL fajl ili mu ograničiti pristup. U realnom scenariju moguće je skeniranjem WSDL otkriti nekoliko ranjivosti.
6. **Validacija klijentske strane u AJAX rutinama** koje koriste veb 2.0 bazirane aplikacije na klijentskoj strani, kao što je validacija tipova podataka, provere sadržaja, polja podataka itd. Moguće je zaobići AJAX bazirane validacije i poslati direktan POST ili GET zahtev aplikacijama, što je glavni izvor za ubacivanje napada na bazi validacije kao što su *SQL injection*, *LDAP injection* itd., koji mogu kompromitovati ključne resurse veb aplikacija.
7. **Ranjivost ruterskih protokola veb servisa** koji dopuštaju da SOAP poruke putuju u specifičnim sekvencama od različitih čvorova na Internetu. Ove čvorove često prolaze šifrovane poruke. Kompromitacija bilo kojeg posrednog čvora može omogućiti pristup SOAP porukama koje putuju između dve krajnje tačke. Ovo može biti ozbiljan bezbednosni proboj za SOAP poruke. Kako veb aplikacije adaptiraju okvire veb servisa, fokus se pomera na ove nove protokole i generiše nove vektore napada.
8. **Manipulacija parametara sa SOAP**. Veb servisi uzimaju informacije i varijable iz SOAP poruka, pa je moguće manipulirati ovim varijablama. Na primer „10“ je jedan od čvorova u SOAP poruci. Napadač može početi manipulaciju ovog čvora i pokušati drugačiju ubacivanje - SQL, LDAP, XPATH komandni šel i otkriti moguće vektore napada da pristupi računaru i internoj mreži. Nekorektna ili nedovoljna validacija ulaza u kodove veb servisa ostavlja aplikacije veb servisa otvorene za kompromitaciju. Ovo je novi vektor napada koji pogađa veb aplikacije koje se pokreću sa veb servisima.
9. **XPATH injektiranje u SOAP poruke**. XPATH je jezik za postavljanje upita za XML dokumente i sličan je SQL saopštenjima gde možemo postaviti određene informacije (parametre) i izvući informacije iz baze podataka. *Parsing* mogućnosti XPATH podržavaju brojni jezici. Veb aplikacije troše veliki broj XML dokumenata i mnogo puta ove aplikacije primaju ulaze od krajnjih korisnika i XPATH saopštenja. Ove sekcije koda su ranjive na XPATH injektiranje. Ako napadač uspešno izvrši XPATH injektiranje, može zaobići autentifikacione mehanizme ili izazvati gubitak poverljivih informacija. postoji nekoliko poznatih tokova u XPATH koje napadač može iskoristiti.

Jedini način da se blokira ovaj vektor napada je da se obezbedi propisan validacija ulaznih parametara pre prenosa vrednosti u XPATH saopštenje.

10. Binarna manipulacija RIA tankog klijenta. Bogate Internet aplikacije–RIA (*Rich Internet Applications*) koriste vrlo bogate karakteristike korisničkog interfejsa kao što su *Flash*, *ActiveX Controls* ili *Applets*, njihovi primarni interfejsi prema veb aplikacijama. Između nekoliko bezbednosnih problema, jedan od glavnih je upravljanje sesijom, pošto se RIA sesija pokreće u pretraživaču koji deli iste sesije. U isto vreme, pošto se cela binarna komponenta daunloduje na lokaciju klijenta, napadač može izvršiti reverzni inženjering binarnog fajla i dekompileirati kod. Moguće je korigovati ovaj binarni zapis i zaobići neku od logika autentifikacionog mehanizma koje se sadrže u kodu. Ovo je još jedan interesantan vektor napada na veb 2.0 okvire.

3.2. Trendovi malicioznih napada na veb lokacije

U 2010. godini očekuje se porast malicioznih napada sa Interneta, sa sofisticiranim tradicionalnim metodima i fokusom na nove platforme (*Windows 7* i *Ubuntu Linux*). Dominiraju sledeće pretnje, [1]:

1. *Maliciozni napad na Windows 7 platforme;*
2. *Iskorišćavanje ranjivosti aplikacija*, kao što su ranjivosti pretraživača za napad na veb aplikacije, što zahteva brže bezbednosne popravke ;
3. *Lažni proizvodi zaštite*, kao što su AVP, *antispyware* i drugi programi koji su naizgled pravi, a u stvari slabi ili nikako štite, daju lažne alarme i pogrešne instrukcije;
4. *Kompromitacija ne-Windows platformi*, kao što je novi *Linux - Ubuntu OS*;
5. *Maliciozni kôdovi za mobilne uređaje*, kao što su smart telefoni sa kojim korisnici pristupaju Internetu, vrše finansijske transakcije, skidaju e-poštu i pretražuju Internet.

U godišnjem izveštaju *Bit9* (16.12.09) pažnja je usmerena na ranjivost aplikacija. Na osnovu rezultata analize NIST baza podataka u izveštaju su objavljene ranjivosti sledećih popularnih aplikacija,:

1. *Adobe Acrobat, Flash Player, Reader i Shockwave* – visoka ranjivost koja dopušta udaljenom napadaču da instalira arbitrarni kod, korumpira memoriju, izvrši DoS napad ili obori aplikaciju;
2. *Apple Quicktime*
3. *Mozilla Firefox*
4. *Opera*
5. *RealPlayer*
6. *Sun Java*
7. *Trillian*.

Sve ove aplikacije zadovoljavaju sledeće opšte kriterijume:

- rade na Windows platformama,
- dobro su poznate, korišćene i često preuzimane sa Interneta na laptop i desktop računare,
- organizacije i vendori proizvoda zaštite ih ne klasifikuju kao maliciozne i
- sadrže najmanje jednu kritičnu ranjivost.

4. ZAKLJUČAK

AJAX, RIA i veb servisi su tri značajna tehnološka vektora za veb 2.0 aplikacije. Ovo su obećavajuće tehnologije koje povećavaju ukupnu efektivnost i efikasnost veb aplikacija. Međutim, sa ovim novim tehnologijama dolaze novi bezbednosni izazovi, koji ako se ignorišu mogu dovesti do katastrofalnih posledica za poslovne sisteme. Pored navedenih deset glavnih napada na veb 2.0 aplikacije u prethodne 2 godine, analitičari predviđaju da će u 2010 godini dominirati 5 tipova napada: na nove Windows platforme, na ranjivosti poznatih aplikacija, sa lažnim proizvodima zaštite, na nove Linux i druge platforme i sa malicioznim kodovima za mobilne uređaje. Rezultati analize bezbednosnih pretnji ukazuju da su, pored tradicionalnih mera zaštite IS, najbolja odbrana od novih vektora napada na veb 2.0 aplikacije, povećanje svesti o potrebi zaštite veb aplikacija, izrada bezbednog kôda i bezbedna implementacija kôda.

5. LITERATURA

- [1] *Lavasoftware Labs Releases 2010 Internet Security Trends*, PR Log - Global Press Release Distribution, decembar 2009.,
- [2] *The WhiteHat Security Website Security Statistics Report*, oktobar 2009.
- [3] *Websense*, godišnji izveštaj, 2008.
- [4] *WASC - Web Application Security Consortium*, izveštaj za 2008.
- [5] *Top Web 2.0 Security Threats*, Industry Report, izveštaj 2009, Secure Enterprise 2.0 Forum, <http://www.secure-enterprise20.org/files/Top%20Web%20%200%20Security%20Threats.pdf>
- [6] White paper, Visual WebGui 'Empty Client' AJAX Security Concept, <http://www.visualwebgui.com/Technology/WhitePapers/tabid/528/articleType/ArticleView/articleId/467/Visual-WebGui-Empty-Client-AJAX-Security-Concept.aspx>
- [7] Requirements of a security framework for the semantic web, <http://ksg.meraka.org.za/~agerber/GerberIASTED2009.pdf>