UDC: 007:004.056 Info M str. 12-18

# ISTRAŽIVANJE IZAZOVA I PRIJETNJI OD XSS NAPADA
# EXPLORING CHALLENGES AND THREATS OF XSS ATTACKS

Dragan Korać, PMF, Univerzitet u Banja Luci
Boris Damjanović, BLC, Banja Luka College
Dejan Simić, FON, Univerzitet u Beogradu

**REZIME:** Sa razvojem digitalnih tehnologija, Cross-Site Scripting (XSS) napad se izdvojio kao velika prijetnja za korisnike. Radi prevazilaženja tih izazova, ovaj rad daje preglede i komparaciju osnovnih tipova XSS napada. Komparacija je urađena sa aspekta napadača i korisnika, i zasnovana na tri bazična korisnička prioriteta kao što su zaštita, upotrebljivost i privatnost. Rezultati komparacije ukazuju na svu moć XSS napada i njegovu sposobnost zloupotrebe benefita novih digitalnih tehnologija. Takođe, u ovom radu su diskutovani i dati novi prijedlozi i pravci za redukovanje i ublažavanje od XSS napada. Na kraju, ovaj rad treba da doprinese boljem razumijevanju XSS napada, njegovim prijetnjama i izazovima koji dolaze sa razvojem budućih digitalnih tehnologija.

**KLJUČNE REČI:** XSS napad, informaciona sigurnost, zaštita, personalne informacije

**ABSTRACT:** With development of digital technology, Cross-Site Scripting (XSS) attack is differentiated as a big threat to users. Due to overcome these challenges, this paper gives a review and comparison a basic type of XSS attacks. The comparison is made with aspect of an attacker and a user, and it is based on three a basic users priorities such as security, usability and privacy. The comparison results point out all power XSS attack and it's a capability to misuse benefits of a new digital technologies. Also, in this paper are discussed and given a new proposals and directions to reduce and mitigate of XSS attack. Finally, this paper needs to contribute a better understanding XSS attacks, its threats and challenges that coming with development of the future digital technologies.

**KEY WORDS:** XSS attack, information security, protection, personal information

## I. UVOD

Brzi razvoj digitalnih tehnologija je donio neizbježne promjene u svakodnevnom ljudskom funkcionisanju. Posebno, pandemija COVID-19 je značajno ubrzala primjenu digitalnih tehnologija dajući predvidljiv trend u kojem će, u budućnosti svi subjekti ubrzati tranziciju ka internetu. Takav trend stvara omiljene uslove za napadače donoseći nove prijetnje i izazove po veb aplikacije. Upotreba veb aplikacija u različitim platformama donosi mnoge benefite ali istovremeno donosi posebne izazove u aspektu zaštite. U takvom okruženju, napadačima se otvaraju nove mogućnosti za još efikasniju upotrebu različitih napada kao što su Cross-Site Scripting (XSS), SQL injection, Cross site request forgery (CSRF), [1]. Iz dostupne literature, XSS je izdvojen kao jedan od najčešćih i najopasnijih tipova napada koji obuhvata dvije ili više odvojenih veb aplikacija. Njegova moć se ogleda u tome što isti ima mogućnost da bude izvršen na korisničkoj ili serverskoj strani. Prema tome, mogu se razlikovati tri osnovna tipa XSS napada imenovani Reflektovani, Direktni i Model objektnog dokumenta [2].

Prvi i osnovni problem u aspektu razmatranja XSS napada je "Šta doprinosi uspješnosti i učestalosti XSS napada?" Pojednostavljeno rečeno, šta to XSS napad izdvaja od drugih sajber napada, pa čak i od fizičkog napada? Ovaj problem zahtijeva da bude sagledan kroz prizmu digitalnih tehnologija. Posljednjih godina, digitalne tehnologije su privukle pažnju miliona korisnika, bez geografskih ograničenja, koji mogu da pristupe u bilo koje vrijeme i bilo kog mjesta. Sa druge strane, napadač ima mogućnost da iskoristi bilo koju ranjivost u sistemu bilo ona na hardverskom, softverskom ili mrežnom nivou. Ipak, većina sajber napada se danas dešava kao rezultat iskorišćavanja softverskih ranjivosti uzrokovanih propustima u softveru i nedostacima u dizajnu [3]. Najčešća ranjiva mjesta su softverski programirajući bagovi (na primjer upravljanje memorijom, validacija korisničkog unosa, *race conditions*, privilegija korisničkog pristupa, i sl.), bagovi softverskog dizajna, razvojne greške, itd. [4]. Upravo softverska ranjiva mjesta predstavljaju u ovom radu centralni problem u razmatranju XSS napada jer sajber napadači često koriste softverske bagove da uzrokuju promjene u ponašanju sistema koja su suprotna njegovoj originalnoj namjeni. Sagledavanje ovog problema nije moguće sagledati bez razmatranja korisničkih faktora. Prema Korać i Simić (2019) korisnički faktori kao što su SUAPCPC su definisani kao osnovni korisnički faktori [5]. Pojam SUAPCPC je nastao kao akronim od engleskih riječi i predstavljaju osnovne korisničke prioritete: zaštitu, upotrebljivost, pristupačnost, cijenu, složenost, privatnost i pogodnost.

Osim navedenog, sa razvojem mobilnih tehnologija prijetnje XSS napada postaju još izraženije i kompleksnije. Strahovit razvoj mobilnih tehnologija omogućio je bolju konekciju između veb servisa i korisnika. Ove tehnologije uključuju više uređaja a time i komplikuju problem u aspektu zaštite. Prije svega, pogodnosti koje donose ove tehnologije kao što su na primjer pohranjivanje personalnih informacija, za poslovne svrhe i brzi pristup internetu čine ove korisnike posebno atraktivnom grupom za XSS napade. Drugi problem u aspektu razmatranja XSS napada je usmjeren u razumijevanju XSS napada i njegove ciljne grupe. Postoje različita mišljenja autora, kao što su [2; 6-8] koji smatraju da je XSS napad usmjeren na veb servise dok autori poput [9-12] smatraju da je XSS napad usmjeren na korisničku stranu. Prema tome, suštinski motiv u ovom istraživanju predstavljaju neprekidni kontinuirani izazovi i prijetnje od XSS napada koji traju godinama unazad direktno usmjerenim prema korisnicima. Fokus je stavljen na istraživanju stvarnih prijetnji i izazova od XSS napada, koji dolaze u integraciji sa novim digitalnim tehnologijama.

Doprinosi ovog rada: ovaj rad se bavi prijetnjama i izazovima od XSS napada prvenstveno usmjerenim prema korisnicima. Ono što izdvaja ovaj rad u odnosu na druge radove jeste da su prijetnje i izazovi koji dolaze od XSS napada razmatrani iz napadačeve perspektive. Dakle, ovaj rad se bavi činjenicama koje doprinose cvjetanju i moći XSS napada. Radi realnog sagledavanja tih problema, ovaj rad daje integrisani pregled i komparaciju osnovnih tipova XSS napada zasnovanih na korisničkim prioritetima zaštita, upotrebljivost i privatnost. Ovaj rad predstavlja neka od ozbiljnih otvorenih istraživačkih sajber pitanja suočenih kod postojećih rješenja u zaštiti informacija time otkrivajući novu dimenziju XSS napada. Na kraju, ovaj rad diskutuje o prijedlozima za prevazilaženje ili ublažavanje prijetnji od XSS napada.

Ostatak ovog rada je struktuiran kao sljedeće. Sekcija 2 opisuje prethodne radove dok sekcija 3 definiše osnovne pojmove, definicije i aktere XSS napada. Sekcija 4 predstavlja pregled osnovnih tipova XSS napada. Sekcija 5 daje metode zaštite XSS napada dok sekcija 6 daje komparaciju XSS napada zasnovanu na tri korisnička prioriteta. Sekcija 7 daje diskusiju a sekcija 8 daje zaključke rada.

## II. PRETHODNI RADOVI

Brojni prethodni radovi u dostupnoj literaturi bave se problematikom XSS napada. Ovaj problem nije nov, i bavljenje sa ovim problemom je istorijski dobro-poznato. Postoji mnogo radova koji su pokrivali komparativne preglede i preglede XSS napada iz različitih aspekata. Na primjer, Hydara et al., (2015) su dali komparaciju između podataka i predloženih rješenja povezanih prema XSS napadima [13]. Chen et al., (2019) su dali komparaciju algoritama mašinskog učenja za detekciju XSS napada [14] dok Kazemian et al., (2015) su dali komparaciju algoritama mašinskog učenja za detekciju malicioznih veb strana [15]. Shanmugasundaram (2015) su dali komparaciju istraživačkih radova zasnovanih na prevenciji od XSS napada, i komparaciju različitih XSS alata zasnovanih na diskutovanim ranjivostima i upotrebljivostima alata [16]. Deepa and Thiligam (2016) su dali pregled različitih radova u kojim XSS napad je razmatran i poređen u pogledu drugih sajber napada kao što je *SQL Injection* [17]. U tom istraživanju XSS napad je u manje detalja opisan kao relevntni podproblem, a ne kao centralna tema. Takođe, postoji mnogo radova koji su se u aspektu XSS napada, pored zaštite kao najvažnijim korisničkim prioritetima bavili i drugim korisničkim prioritetima, kao što su upotrebljivost i privatnost. Na primjer, Korać et al., (2020) su pokrivali privatnost faktor u pogledu sajber prijetnji u m-learning sistemima [18] dok Csontos and Heckl (2020) su se bavili korisničkim prioritetom kao što je upotrebljivost u pogledu procjene veb sajtova Mađarske vlade [19]. Wang et al., (2018) su se bavili korisničkim prioritetom kao što je privatnost [20]. U literaturi postoje i podijeljena mišljenja u vezi razumijevanja XSS napada i njegove ciljne grupe. Primjer su [21; 22] koji ukazuju da je veb aplikacija glavni cilj napadača dok autori poput [9; 23] ukazuju da su to korisnici. Međutim, u ovom radu je fokus prijetnji od XSS napada primarno usmjeren prema korisnicima.

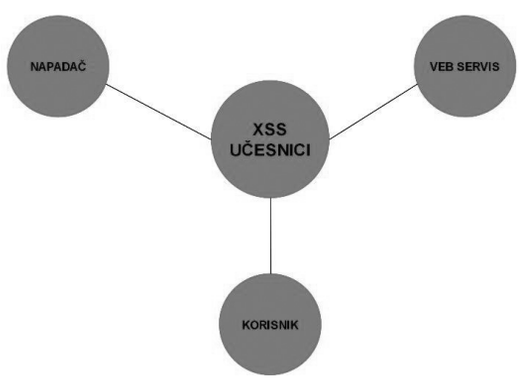
## III. OSNOVNI POJMOVI, DEFINICIJE I AKTERI XSS NAPADA

Prije nego što se opišu osnovni tipovi XSS napada i njihov način funkcionisanja, potrebno je dati najvažnije osnovne definicije termina u okviru ovog istraživanja obuhvatajući pri tome osnovne korisničke prioritete i učesnike uključene u XSS napade. Od osnovnih definicija izdvojene su sljedeće:

- *XSS napad* je tip injekcionog kôda koji omogućava napadaču da posredstvom veb server izvrši maliciozni kôd u korisničkom pretraživaču.
- *Ranjivost* je prema IETF RFC 2828: "slabost u dizajnu ili specifikaciji sistema, implementaciji ili funkcionisanju i upravljanju (konfiguracija) koji mogu biti iskorišćene za kršenje sistemske politike zaštite [24].
- *Softverski bag* je opšti termin korišćen da opiše greške, mane i nedostatke u računarskim programima kao što su unutrašnji operativni sistem, eksterne Ulazno/Izlazne interfejs drajveri i aplikacije [25].
- *Revizor sigurnosti* je subjekat koji pronalazi ranjivosti u izvornom kôdu, identifikuje njihove uzroke i otklonja ih.
- *Zaštita* je definisana kao skup metoda tehnika i aktivnosti koji ima za cilj da spriječi krađu ili odliv korisničkih informacija [5], i predstavlja najvažniji korisnički faktor [26].
- *Upotrebljivost* je preliminarno definisana kao sposobnost da se izvrši optimalna interakcija sa funkcionalnostima Sistema [27].
- *Privatnost* je definisana kao limitirajući faktor u sprečavanju narušavanja korisničke autonomije i slobode [5] tokom pristupanja veb servisima.

Pored gore datih definicija osnovnih pojmova definisani su i učesnici XSS napada. Kao što je to prikazano na slici 1, XSS napad generalno obuhvata tri učesnika i to:

- *Veb servis* je servis koji sadrži bazu podataka u koju se pohranjuju neki od korsničkih unosa uključujući i osjetljive personalne informacije.
- *Žrtva* je korisnik koji koristi uslugu malicioznog veb servisa.
- *Napadač* je maliciozni korisnik veb servisa koji napada veb servere radi ostvarivanja svojih specifičnih ciljeva kao što je krađa korisničkih osjetljivih informacija.




**Slika 1.** *XSS učesnici*

## IV. PREGLED OSNOVNIH TIPOVA XSS NAPADA

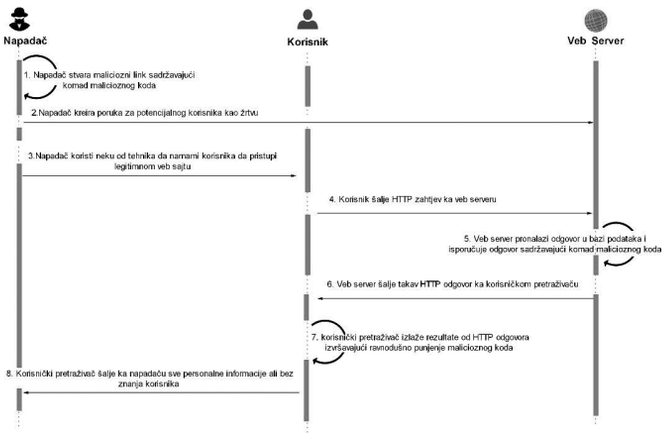
Prije svega, potrebno je istaknuti činjenicu da napadač može da inicira XSS napad putem dve glavne rute (korisnička i serverska). Prva (korisnička) ruta je da napadač upotrebi pretraživač žrtve kao transportno sredstvo putem kog će biti injektiran kôd u veb aplikaciju. Druga (serverska) ruta je da napadač ima mogućnost da maliciozni kôd direktno injektira na server putem HTTP (*engl. Hypertext Transfer Protocol*) zahtjeva. Kao što je u uvodu rada pomenuto, zavisno od načina izvršenja danas je u literaturi prisutna podjela XSS napada na tri osnovna tipa:

- *Nepostojani (engl. Non-persistent)*
- Postojani *(engl. Persistent)*
- *Model objektnog dokumenta (engl. Document Object Model - DOM)*

Da bi se bolje razumijela razlika između ovih osnovnih tipova XSS napada kratki pregled i način njihovog funkcionisanja je ukratko dat.

### *NEPOSTOJANI XSS NAPAD*

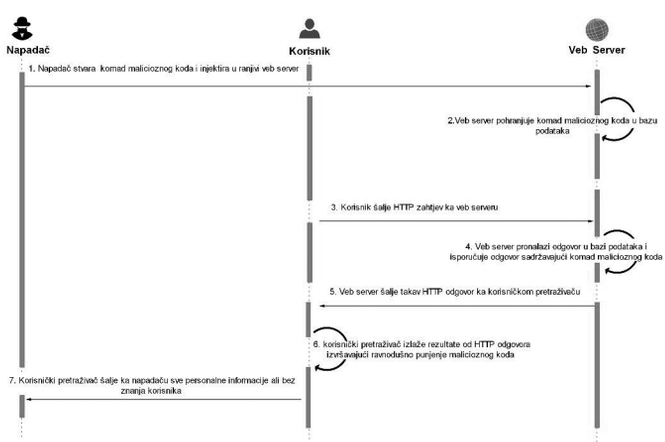
Nepostojani XSS napad karakteriše svojstvo u kome su veb servisi iskorišćeni za injektiranje malicioznog kôda u korisnički veb pretraživač. Dijagram sekvence za nepostojani XSS napad je dat u slici 2. Na tom dijagramu se prikazuju svi neophodni procesi koje napadači koriste za stvaranje i izvršavanje nepostojnog XSS napada. Jasno se može vidjeti redoslijed izvršavanja svih procesa od stvaranja malicioznog linka do završnog procesa u kome se vrši proslijeđivanje korisničkih personalnih informacija ka napadaču. Svojstvo ovog napada karakteriše da napadač pored stvorenog malicioznog linka upućenog prema žrtvi zahtijeva dodatnu upotrebu neke od tehnika kao što je na primjer socijal inženjering. Svrha upotrebe ove tehnike je da namami (inicira) korisnika da pristupi legitimnom veb sajtu. Maliciozni link je realizovan putem malignog *JavaScript* na drugoj veb strani ili kontrolisanom veb serveru. Prilikom korisničkog HTTP zahtjeva korišćen bilo metodom GET ili POST, zahtjev će biti odbijen od servera tako da obuhvata neke ili sve unose. Najčešće, proces odbijanja zahtjeva je u formi poruka o pogrešci, pregledi komentara, pretraživanje rezultata, itd. Po prihvatanju HTTP zahtjeva, korisnički pretraživač izlaže rezultatat HTTP odgovora. Rezultat je punjenje malicioznog kôda i njegovo ravnodušno izvršavanje. Na kraju, slijedi prosleđivanje personalnih informacija ka napadaču bez znanja korisnika. Potrebno je istaknuti da za krađu kredencijala, napadač često koristi ovaj tip XSS napada putem kontrolisanog veb servisa koji je identičan legitimnom veb servisu.




**Slika 2.** *Dijagram sekvence za nepostojani XSS napad.*

### *POSTOJANI XSS NAPAD*

Dijagram sekvence za postojani XSS napad je dat u slici 3. Na tom dijagramu se prikazuju svi neophodni procesi za stvaranje i izvršavanje ovog tipa XSS napada. Na dijagramu je vidljiv redoslijed izvršavanja procesa od stvaranja malicioznog linka do završnog procesa u kome se vrši proslijeđivanje korisničkih personalnih informacija ka napadaču.

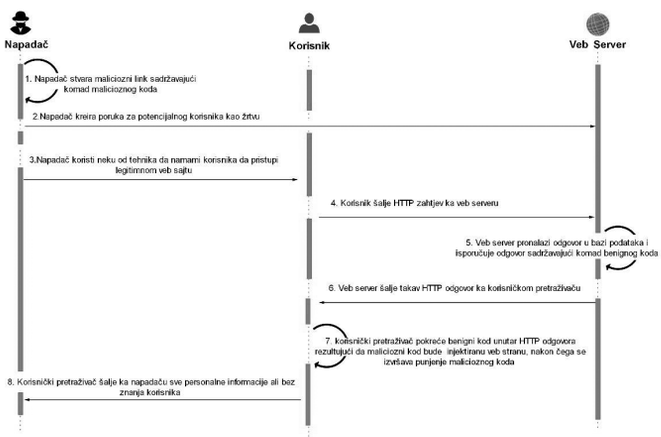



**Slika 3.** *Dijagram sekvence za postojani XSS napad.*

Posebno svojstvo ovog napada koje ga izdvaja od svih drugih tipova XSS napada je usmjereno ka činjenici da je maliciozni kôd injektiran direktno u veb servis. Najčešća su to ranjiva mjesta poput baze podataka, forumi, aplikacije za čet i drugi stringovi. Ovaj tip napada se pokreće kada korisnik posjeti maliciozni veb sajt. Na osnovu korisničkog HTTP zahtjeva, veb servis pronalazi HTTP odgovor u koji je sadržan komad malicioznog kôda. Takav HTTP ogovor se prosljeđuje ka korisničkom pretraživaču koji izlaže rezultate HTTP odgovora i pri tom izvršava punjenje malicioznog kôda. Nakon toga, korisnik bez znanja o tom šalje svoje personalne informacije ka napadaču.

***DOM XSS NAPAD***

Dijagram sekvence za DOM XSS napad je dat u slici 4. Na tom dijagramu se prikazuju procesi koji napadači koriste za stvaranje i izvršavanje ovog tipa XSS napada. Na dijagramu je vidljiv redoslijed izvršavanja svih neophodnih procesa od stvaranja malicioznog linka do završnog procesa u kome se vrši proslijeđivanje korisničkih personalnih informacija ka napadaču. Posebno svojstvo ovog napada koje ga izdvaja među XSS napada je usmjereno ka činjenici da maliciozni kôd kao dio DOM neće biti izvršen na korisničkom pretraživaču sve dok benigni kôd ranjivog veb servisa ne postane izvršiv. Ovaj tip napada može biti izvršiv u formi veb strane ili promjenom DOM okruženja u kojem kôd ostaje isti (benigan). Takođe, posebno svojstvo ovog napada je da DOM struktura veb strane može biti modifikovana samo na korisničkoj strani što ga čini nevidljivom sa veb strane. Ovaj tip napada je alternativa za prethodna oba napada.




**Slika 4.** *Dijagram sekvence za DOM XSS napad.*

## V. METODE ZAŠTITE OD XSS NAPADA

Kako XSS napad može biti izvršen na korisničkoj ili serverskoj strani time i mehanizmi odbrane od XSS napada mogu biti postavljeni na korisničkoj, serverskoj ili na obe strane. U pojmu analiziranja, postoje tri pristupa za zaštitu od XSS napada [10]:

- *Pristup zasnovan na statičkoj analizi*, koji pregleda kôd veb aplikacija uključujući izvorni kôd, binarni kôd, ili prenosivi kôd (*engl. bytecode)* s ciljem posmatranja toka podataka prije nego što program bude izvršen.
- *Pristup zasnovan na dinamičkoj analizi*, koji analizira podatke stečene tokom izvršavanja programa radi otkrivanja ranjivosti. Dinamička analiza je obično izvršena u testirajućem vremenu tokom razvoja nakon što je program stavljen u funkciju.
- *Hibridni pristup* koji kombinuje oba prethodna pristupa.

Može se uočiti da pristup zasnovan na statičkoj analizi spada u preventivne postupke dok pristup zasnovan na dinamičkoj analizi spada u korektivne postupke debagiranja. Treba naglasiti da sve ove procese debagiranja izvode revizori sigurnosti. Takođe, potrebno je istaknuti da danas postoje dvije osnovne metode sprečavanja XSS napada. Da bi se spriječio ovaj tip sajber napada, potrebno je bolje upravljanje sa mjestima na kojima se unose ulazne informacije u sistem. Za veb programere, postoje dva fundamentalna različita unosa upravljanja unosa u aspektu zaštite [28]:

- *Enkodiranje*, koji izbjegava korisnički unos tako da pretraživač interpretira to samo kao podatak, a ne kao kôd.
- *Validacija*, koja filtrira korisnički unos tako da pretraživač interpretira to kao kôd bez malicioznih komandi. Validacija unosa je proces osiguravanja u kojem ulazni podaci slijede određena pravila.

Pored gore navedenog, treba naglasiti da postoje mnoge razvijene tehnike u otkrivanju XSS napada. Primjer je tehnika filtriranje sadržaja koja je korišćena za otkrivanje malicioznih kôdova u veb stranama, tehnika obostrane autentifikacije [29], u kojoj se pored korisničke autentifikacije zahtijeva i serverska autentifikacija. Svakako tu su i dobro poznate tehnike za borbu protiv XSS napada kao što su su tehnika orezivanja (*engl. technique pruning*) [30] i tehnike "prelijevanje" bafera (*engl. buffer overflow*). Tehnike "orezivanja" imaju za cilj da smanje orginalne programske dijelove na ono što se naziva zaštitinim kriškama (*engl. security slices*) koji sadrže zvuk i precizne informacije [30]. Takođe, potrebno je naglasiti da pojedine tehnike kao što je tehnika zamagljivanja [31], mogu biti korišćene od strane napadača za stvaranje malicioznog kôda.

Činjenica je da postojeći razvijeni pristupi i metode kao ublažavajući alati nisu dovoljni da bi otkrili XSS napade [32]. Stoga, posljednjih godina razvijaju se novi koncepti zaštite od XSS napada zasnovani na upotrebi vještačke inteligencije - AI (*engl. artificial intelligence*) tj. proširenoj upotrebi tehnika mašinskog učenja pri otkrivanju sajber napada [33]. Generalno, tehnike klasičnog mašinskog učenja su predstavljene sa niskom stopom detekcije i koje su nesposobne u detektovanju malih mutacija od postojećih malicioznih napada kao što su napadi *zero-day* [34]. Za povećavanje stope detekcije, razvijena su istraživanja od strane [35] koji su predložili detekciju *DeepXSS* zasnovan na tehnikama dekodiranja, generalizacije i tokenizacije. U tim tehnikama korišćeni su *word2vec* za ekstrakciju svojstava od XSS koji je bio dat kao ulaz za modele dubokog učenja (*engl. deep learning*) zasnovanog na LSTM (*engl. Long short-term memory*) za trening.

Pored brojnih gore pomenutih razvijenih različitih rješenja u pogledu zaštite od XSS napada, XSS napad zahtijeva dublje i šire sagledavanje njegovih svojstava iz kojih proističe njegova moć. U ovom radu, suočavanje i analiziranje tog problema je urađeno u narednoj sekciji kroz komparaciju osnovna tri tipa XSS napada.

## VI. POREĐENJE OSNOVNA TRI TIPA XSS NAPADA

Kao što je izloženo u sekciji IV, pregledi osnovna tri tipa XSS napada su elaborirana sa izdvojenim prednostima i nedostacima. Na osnovu tih dobijenih informacija, poređenje XSS

napada je napravljeno u pogledu tri osnovna korisnička faktora: zaštite, upotrebljivosti i privatnosti. Ova tri korisnička faktora su korišćena za komparaciju jer oni u dostupnoj literaturi predstavljaju tri najčešće opisivana kao najvažnija korisnička pioriteta. Dakle, radi se o korisničkim faktorima koji predstavljaju suštinske prioritete u bilo kom mehanizmu zaštite informacija. Ova tri korisnička kriterijuma obuhvataju ključne probleme u svakom od tipova XSS napada koja su izvedena iz napadačevog gledišta. Sagledavanje ovog problema kroz prizmu napadača i korisnika biće moguće da se istinski razumiju razlike među XSS napadima kao ključna svojstva iz kojih proizlazi sveukupna njihova moć napada. Jednostavno rečeno, na taj način biće moguće steći precizniji uvid u svojstva XSS napada u pogledu korisničkih prioriteta odnosno uspješnije definisanje zaštitinih praznina u kojima XSS napad djeluje. Važan izvor za ideju formiranje Tabele 1 je korišćena dostupna literatura kao što je [16; 20; 36; 37]. Takođe, izvor informacija prezentovan u Tabeli 1 predstavlja integrisani pristup za sva relevantna istraživanja do sada, tj. sublimat svih stečenih rezultata iz prethodnih komparativnih istraživanja.

**Table 1** Poređenje osnovna tri tipa XSS napada zasnovani na faktorima zaštite, upotrebljivosti i privatnosti.

| *Faktori* | *Nepostojani XSS* | *DOM XSS* | *Postojani XSS* |
|---|---|---|---|
| ***Zaštita*** | Pasivan napad, opasna prijetnja po korisnike i može biti vidljiv sa veb strane. | Pasivan napad, opasnija prijetnja po korisnike i ne može biti vidljiv sa veb strane. | Aktivan napad, najopasnija prijetnja po korisnike i veb servise i može biti vidljiv sa veb strane. |
| ***Upotrebljivost*** | Daleko najčešći tip napada, dizajniran u obliku koji omogućava pohranjivanje malicioznog kôda u URL ili e-mejlu. Njegovo aktiviranje je posredno putem ranjivog veb servisa. | Relativno neuobičajan tip napada, dizajniran u obliku koji omogućava pohranjivanje malicioznog kôda kao dio DOM i koji se u toj formi nikad ne šalje ka veb servisu, već ka korisničkoj strani. | Opšti tip napada, dizajniran u obliku koji omogućava direktno pohranjivanje malicioznog kôda u veb serveru koji je lokalno izvršen. |
| ***Privatnost*** | Anonimna priroda internet omogućava visok nivo privatnosti za napadače, a veoma nizak nivo privatnosti za korisnike. | Anonimna priroda internet omogućava visok nivo privatnosti za napadače, a veoma nizak nivo privatnosti za korisnike. | Anonimna priroda internet omogućava visok nivo privatnosti za napadače, a veoma nizak nivo privatnosti za korisnike. |

Na osnovu izdvojenih karakteristika datih u Tabeli 1, moguće je uočiti svojstva iz kojih proističe moć XSS napada zasnovanih na tri osnovna korisnička faktora: zaštite, upotrebljivosti i privatnosti. Prije svega, u odnosu na posmatrane korisničke faktore može se primjetiti sličnost svih tipova XSS napada u pogledu prijetnji prema korisnicima gdje svaki tip pod određenim okolnostima ima svoje specifične prednosti i nedostatke u odnosu na druge. Dakle, svaki tip XSS napada predstavlja specifičnu prijetnju prema korisnicima. Nedostaci jednog tipa XSS napada predstavljaju prednost kod drugog tipa XSS napada kod kojeg se javljaju problemi druge prirode. Primjer za to je DOM napad u kome generalno ranjiva mjesta nisu vidljiva sa veb strane što čini veoma pogodnim za zloupotrebu drugih tehnika kao što je *clickjacking.* Sa druge strane, može se primjetiti da postojani XSS napad je aktivni napad jer punjenje malicioznog kôda je direktno izvršeno na veb servisu bez nadgledanja napadača. To podrazumijeva da postoji kontinuirana prijetnja jer svaki korisnik koji posjeti veb sajt biće žrtva, a da tog i nije svjestan. Takođe, zbog jednostavnosti upotrebe nepostojanog XSS napada, upotrebljivost kao korisnički faktor je daleko najzastupljeniji od svih tipova XSS napada. Kada je u pitanju privatnost kao korisnički faktor može se primjetiti da svi tipovi XSS napada omogućavaju izuzetni visok nivo privatnosti što direktno podstiče napadače da upotrebljavaju ovaj napad. Nasuprot tome, sa ovim napadom napadači predstavljaju veliku prijetnju u pogledu privatnosti osjetljivih korisničkih informacija.

## VII. DISKUSIJA

Iz dobijenih rezultata poređenja, moguće je primjetiti da sva tri tipa XSS napada omogućavaju napadačima da pod različitim okolnostima veoma efikasno mogu da ugroze korisnike odnosno njihove personalne informacije. Svaki od XSS napada karakterišu posebna svojstva koja mu omogućavaju da u sistemu korisnik/server iskoriste najmanju prazninu u aspektu zaštite kao što su neodgovarajući korisnički autentifikacioni unosi, slabost u autentifikacionom kôdu, siromašne programerske prakse kodiranja, itd. Posebno je to izraženo sa razvojem novih digitalnih tehnologija čija je primarna svrha usmjerena ka postizanju višeg nivoa korisničkih prioriteta. Međutim, u praksi situacija ukazuje da napadači takve benefite od novih digitalnih tehnolgija takođe koriste u svrhu modifikovanja svojih XSS napada. Primjer za to su upotreba socijalnog inženjeringa koji predstavlja istaknuto svojstvo nepostojanog XSS napada. Dakle, posebna prijetnja po korisnike je da napadač ima sposobnost da izvrši potpunu ili djelimičnu krađu pri iskorišćavanju korisničkog ponašanja ili nekih drugih praznina u aspektu zaštite kao što su identifikacioni i autentifikacioni sistemi. Na ovaj način XSS napadi su sposobni da prežive i idu u korak sa vremenom u kojem postaju još inteligentniji, specifičniji i softificiraniji i mnogo opasniji po korisnike. Svakako, jedna od najozbiljnijih posljedica XSS napada su krađa osjetljivih personalnih informacija sa korisničkih uređaja kao što su e-mejlovi, lozinke za bankovne račune, kontakt brojevi, itd.

Očigledno je da u svim postojećim razvijenim alatima, filterima i tehnikama za u borbu protiv XSS napada postoje određene praznine koje omogućavaju da takvi napadi i dalje predstavljaju veoma opasnu prijetnju po korisnike. Primjer za to je pristup zasnovan na statičkoj analizi koji mogu da otkriju potencijalne ranjivosti u izvornom kôdu ali takođe mogu da generišu mnoga pogrešna upozorenja sa mnogo irelevantnih informacija, čineći njihovo usvajanje nepraktičnim za reviziju u aspektu zaštite. Radi toga, razvoj alata je razmatran kao urgentno pitanje u borbi protiv XSS napada. Ipak, XSS napadi su uspjeli da pronađu praznine i u takvim alatima. Postoje automatizovani skeneri za zaštitu veb aplikacija za provjeravanje ranjivosti od XSS napada kao što su analiza zasnovana na potpisu i analiza zasnovana

na sadržaju za detekciju od XSS napada. Takođe, postoje i veb proksiji kao posrednici između korisnika i veb servera koji su uvedeni da popune transakciju u ime korisnika. Sa druge strane, brojne tehnike su razvijene za borbu protiv XSS napada kao što je tehnika zamagljivanja koju napadači mogu da koriste za zamagljivanje malicioznog kôda kako bi izbjegli sisteme detekcionih napada posebno sisteme zasnovane na potpisu i sisteme zasnovane na analizi. Povrh toga, mnogi filteri su razvijeni u kojem veb pretraživači kao ekstenzija su postavljeni. S druge strane, brzi tehnološki razvoj je uslovio razvoj različitih veb pretraživača i njihovih novijih verzija što otežava da se sanitiziraju korisnički unosi sa serverske strane. Sve ovo ukazuje da je potrebno da se izvrši dodatna sanitizacija korisničkog unosa tj. čišćenja sadržaja u pogledu uklanjanja irelevantnih i opasnih karaktera. Osim navedenog, postoji i preporuka upotrebe TSL (*engl. Transport Layer Security*) kako bi se obezbijedila zaštitna interakcija između korisnika i servera. Nesumnjivo, strašna trka u razvoju veb aplikacija primorava programere da kreiraju veb aplikacije sa mnogim prazninama u aspektu zaštite jer ne ostavljaju dovoljno vremena za temeljne studije u pogledu svih njenih ranjivosti.

Kroz ovu diskusiju može se uvidjeti da uprkos brojnim digitalnim tehnološkim unapređenjima i ogromnim brojem razvijenih rješenja zaštite, XSS napad ostaje i dalje veliki problem za korisnike. Razlog tome je što XSS napad ima skalabilno svojstvo koje mu dozvoljava kako međusobnu integraciju različitih svojstava prisutnih među XSS napadima tako i integraciju sa svojstvima koje donose nove digitalne tehnologije. Dakle, ključno u ovoj diskusiji je da XSS napad ima sposobnost mutacije u kojem svojstva jednog tipa XSS napada mogu da se integrišu sa drugim tipom XSS napada ili sa nekim drugim svojstvima koje donose nove digitalne tehnologije. Sa razvojem digitalnih tehnologija, napadači istražuju njihove jedinstvene karakteristike kako bi na brz i efikasan način došli do novih varijacija ili modifikacija XSS napada kao i većeg broja potencijalnih žrtava. Takve modifikacije XSS napada su u stanju da zaobiđu sva postojeća rješenja zaštite. Razlog je što razvojem novih digitalnih tehnologija, napadač ima mogućnost da, na primjer upotrebom DOM XSS napada zasnovanog na upotrebi socijalnog inženjeringa, potpuno zaobiđu sva rješenja zaštite koja su vidljiva sa veb strane. Dakle, pored tehničkih mjera kao što su enkodiranje i validacija, buduće komparacione studije treba da budu zasnovane na svim SUAPCPC faktorima, da obuhvataju i psihologiju korisnika. Mogućnost mutiranja XSS napada čini ih teškim za otkrivanje a veoma lakim za implementaciju. Sve ovo ukazuje zašto XSS napadi su tako opasni i učestali u sajber prostoru, zašto su postojeća detekciona i preventivna rješenja zaštite ranjiva u suprostavljanju XSS napadima.

Takođe, potrebno je istaknuti da opasnosti od XSS napada su isključivo razmatrani po korisnika. Međutim, rezultati ovog rada ukazuju da snaga i moć XSS napada je mnogo šira i napad može biti upotrebljen protiv vlasnika veb sajtova, protiv programera. Ako se pri tome uzmu obzir rezultati ove studije koji ukazuju da napadač ima potencijalnu mogućnost kombinovanja različitih svojstava od XSS napada stvarajući nove mutacije napada, u tom slučaju razvoj nove studije treba da bude usmjeren na razvoju cjelovite komparativne studije zasnovane na svim SUAPCPC faktorima.

## VIII. ZAKLJUČAK

Na osnovu gore diskutovanog, može se zaključiti da postoje rastući izazovi za kontinuirano pronalaženje boljeg rješenja zaštite u borbi protiv XSS napada. U ovom radu, komparaciona studija je urađena iz ugla napadača i korisnika. Komparaciona studija je bazirana na tri osnovna tipa XSS napada zasnovanih na osnovnim korisničkim prioritetima kao što su zaštita, upotrebljivost i privatnost. Na osnovu dobijenih rezultata, može se zaključiti da napadači upotrebom XSS napada ostvaruju najbolje pogodnosti u pogledu sva tri gore pomenuta korisnička prioriteta, a sve na uštrb korisnika. Ovaj rad pomaže da se dobije jasnija slika nadolazećih izazova i prijetnji XSS napada povezanih ka korisnicima. Nesumnjivo, svojstva XSS napada omogućavaju da ovaj tip napada ima sposobnost mutiranja i zloupotrebe benefita koji dolaze sa razvojem novih digitalnih tehnologija i koji će kao takav u bliskoj budućnosti i dalje predstavljati veliki problem u dijelu zaštite informacija. Dakle, Za razliku od svih prethodnih radova na ovu temu, ovaj rad daje novu dimenziju u aspektu zaštite informacija u kojem se diskutuju moguće varijacije XSS napada koje mogu pratiti razvoj budućih tehnologija kao što su na primjer društveni mediji, pametne mobilne tehnologije, računarstvo u oblaku, i kritična infrastruktura. Takođe, kako su implikacije od XSS napada usmjerene ka korisnicima tako zaključci ovog rada ukazuju da ne postoji tehničko pojedinačno niti kombinovano rješenje sa kojim je moguće da se i sistem apsulutno zaštiti od XSS napada niti će to biti moguće u budućnosti. Za uspješnu borbu protiv XSS napada, takva tehnička rješenja moraju da uzmu u obzir i korisničko ponašanje. Stoga, budući pravci istraživanja o XSS napadima mogu se izdvojiti u formi razvoja nove studije poređenja zasnovane na svim bazičnim korisničkim SUAPCPC prioritetima, u kojima je potrebno razmotriti ne samo tehničke mjere već i aspekte korisničke svijesti. Nesumnjivo, budući radovi treba da bude usmjereni na uzdizanje svijesti o problemu koji nastaju kao posljedica XSS napada i da obezbijedi kontekst za daljnje diskusije među istraživačima i širom društvenom zajednicom.

## REFERENCE

[1] G. P. Bherde and M. A. Pund. 2016. Recent attack prevention techniques in web service applications. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 1174–1180. doi: 10.1109/ICACDOT.2016.7877771.

[2] E., Kirda, C., Kruegel, G., Vigna and N., Jovanovic. 2006. Noxes: a client-side solution for mitigating cross-site scripting attacks. In Proceedings of the 2006 ACM symposium on Applied computing. ACM, 330–337.

[3] S. Liu and B. Cheng, Cyberattacks: “Why, what, who and how”,in:ITPro.,IEEE Computer Society, May/June 2009.

[4] K. Tsipenyuk, B. Chess and G. McGraw, 2005. Seven pernicious kingdoms: A taxonomy of soft waresecurity errors, IEEESecur. Priv. 3(6), 81–84.

[5] D. Korać and D. Simić, 2019. Fishbone Model and Universal Authentication Framework for Evaluation of Multifactor Authentication in Mobile Environment, Computers & Security, 85, 313-332.

[6] Y. Zhou and P. Wang. 2019. An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence. Computers & Security, 82, 261-269.

[7] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar and W. Xiaoxi, 2019. MLPXSS: An Integrated XSS-Based Attack Detection Scheme in Web Applications Using Multilayer Perceptron Technique, in IEEE Access, 7,100567-100580.
[8] G.E., Rodríguez, D.E., Benavides, J., Torres, P., Flores, and W. Fuertes 2018. Cookie Scout: An Analytic Model for Prevention of Cross-Site Scripting (XSS) Using a Cookie Classifier. In: Rocha Á., Guarda T. (eds) Proceedings of the International Conference on Information Technology & Systems (ICITS 2018). ICITS 2018. Advances in Intelligent Systems and Computing, vol 721. Springer, Cham.
[9] Verizon. 2018. 2017 data breach investigations report. (Accessed July 2020). http://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf.
[10] U., Sarmah, D.K., Bhattacharyya and J.K., Kalita. 2018. A Survey of Detection Methods for XSS Attacks, Journal of Network and Computer Applications, 118, 113-143.
[11] J. P. Singh, 2016. Analysis of SQL Injection Detection Techniques, Theoretical and Applied Informatics (TAAI) 28 (1-2), 37–55.
[12] V. Nithya, S. L. Pandian and C. Malarvizhi, 2015. A Survey on Detection and Prevention of Cross-site Scripting Attack, International Journal of Security and Its Applications 9(3), 139–152.
[13] Hydara, I., Sultan, A.B., H. Zulzalil and N. Admodisastro, A. 2015. Current state of research on cross-site scripting (XSS) – A systematic literature review, Information and Software Technology 58, 170–186.
[14] X., Chen, M., Li, Y., Jiang and Y. Sun, 2019. A Comparison of Machine Learning Algorithms for Detecting XSS Attacks. In: Sun X., Pan Z., Bertino E. (eds) Artificial Intelligence and Security. ICAIS 2019. Lecture Notes in Computer Science, vol. 11635. Springer, Cham.
[15] H.B., Kazemian and S. Ahmed, 2015. Comparisons of machine learning techniques for detecting malicious webpages. Expert Syst. Appl. 42(3), 1166–1177.
[16] G. Shanmugasundaram, S. Ravivarman and P. Thangavellu. 2015. A study on removal techniques of cross-site scripting from web applications. In 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 0436–0442. doi: 10.1109/ICCPEIC.2015.7259498.
[17] G. Deepa and P.S. Thilagam, 2016. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, 74, 160-180.
[18] D. Korać, B. Damjanović and D. Simić, 2020. Information Security in M-learning Systems: Challenges and Threats of Using Cookies, 19th International Symposium INFOTEH-JAHORINA 2020.
[19] B., Csontos and I. Heckl, 2020. Accessibility, usability, and security evaluation of Hungarian government websites. Univ Access Inf Soc. https://doi.org/10.1007/s10209-020-00716-9.
[20] R. Wang, G. Xu, X. Zeng, X. Li and Z. Feng, 2018. TT-XSS: A novel taint tracking based dynamic detection framework for DOM Cross-Site Scripting, Journal of Parallel and Distributed Computing, 118(1), 100-106.
[21] B. K., Ayeni, J. B. Sahalu and K. R. Adeyanju, 2018, Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System." Journal of Computer Networks and Communications, vol. 2018, 1-10.
[22] Imperva. 2018. The state of web application vulnerabilities in 2017. (April 2018). https: //www.imperva.com/blog/2017/12/the-state-of-web-application-vulnerabilities-in-2017/.
[23] S. Gupta, S. and B. B. Gupta. 2017. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of System Assurance Engineering and Management, 8, 512–530.
[24] J. D., Howard and Longstaff, T. A. 1998. A Common Language for Computer Security Incidents. Sandia Report # SAND98-8667. Retrieved from https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/1998/988667.pdf (Accessed July 2020).
[25] H. Shahriar and M. Zulkernine, 2012. Mitigating program security vulnerabilities: Approaches and challenges, ACM Comput. Surv. 44 (3), Article No.11.
[26] D. Korać and D. Simić, "Design of Fuzzy Expert System for Evaluation of Contemporary User Authentication Methods Intended for Mobile Devices," Journal of Control Engineering and Applied Informatics, vol. 19(4), pp. 93-100, 2017.
[27] J., Grudin, 1992. Utility and usability: research issues and development contexts. Interacting with Computers, 4(2), 209-217.
[28] Preventing XSS, 2020. available at: https://excess-xss.com/ (Accessed July 2020).
[29] G. Coker, J. Guttman, P. Loscocco, J. Sheehy, B. Sniffen, Attestation: Evidence and trust, in: ICICS'08, 2008, pp.1–18.
[30] J. Thomé, L. K. Shar, D. Bianculli and L. Briand, 2018. Security slicing for auditing common injection vulnerabilities. Journal of Systems and Software, 137, 766-783.
[31] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011.
[32] S. Lekies, K. Kotowicz, S. Groÿ, E. A. V. Nava, and M. Johns, Codereuse attacks for theWeb, in Proc. ACMSIGSAC Conf. Comput. Commun. Secur., Oct./Nov. 2017, pp. 1709-1723.
[33] J. Murphree, Machine learning anomaly detection in large systems, in *Proc. IEEE AUTOTESTCON*, Sep. 2016, pp. 1-9.
[34] A. Abeshu and N. Chilamkurti, 2018. Deep learning: The frontier for distributed attack detection in fog-to-things computing, IEEE Commun. Mag., 56(2), 169-175.
[35] Y. Fang, Y. Li, L. Liu and C. Huang, DeepXSS: Cross site scripting detection based on deep learning, in Proc. Int. Conf. Comput. Artif. Intell., Mar. 2018, pp. 47-51.
[36] J.L. Thames, 2015. Comparing Cross-site Scripting Vulnerabilities. Vulnerability and Exposure Research Team Tripwire, Inc. DOI: 10.13140/RG.2.1.1488.2725
[37] D. Mitropoulos, P. Louridas, M. Polychronakis and A. D. Keromytis, 2019. Defending Against Web Application Attacks: Approaches, Challenges and Implications, in IEEE Transactions on Dependable and Secure Computing, 16 (2), pp. 188-203.

**Dragan Korać**, Univerzitet u Banja Luci, RS, BiH.
**Kontakt:** dragan.korac@pmf.unibl.org
**Oblast interesovanja:** sigurnost, zaštita informacija u računarskim sistemima, e-učenje, mobilne tehnologije, i fazi logika.

**Boris Damjanović**, Banja Luka College, Banja Luka, RS/BiH
**Kontakt:** boris.damjanovic@blc.edu.ba
**Oblast interesovanja:** kriptografija, sigurnost, zaštita informacija u računarskim sistemima, programski jezici i primjenjene informacione tehnologije.

**Dejan Simić**, Univerzitet u Beogradu, Fakultet organizacionih nauka.
**Kontakt:** simić.dejan@fon.bg.ac.rs
**Oblast interesovanja:** zaštita informacija u računarskim sistemima, sigurnost podataka, organizacija i arhitektura računarskih sistema, sistemi elektronskog plaćanja, i primjenjene informacione tehnologije.