

INSTITUT ZA MATEMATIKU I INFORMATIKU

Web programiranje - SSL

Profesor

Dr Miladin Stefanović

Asistent

Branko Arsić

Studenti

Katarina Ralević 89/2013

Marko Stojanović 95/2013

SADRŽAJ

<i>Šta je ssl</i>	<i>3</i>
<i>SSL sertifikat</i>	<i>3</i>
<i>Zahtev za izdavanje sertifikata.....</i>	<i>5</i>
<i>Sigurna konekcija.....</i>	<i>5</i>
<i>SSL Ubuntu Apache - Instalacija</i>	<i>6</i>
<i>Kupovina sertifikata</i>	<i>7</i>
<i>Instalacija sertifikata na web server-u</i>	<i>7</i>
<i>Više informacija</i>	<i>8</i>

SSL

ŠTA JE SSL

SSL je akronim za Secure Sockets Layer i predstavlja sigurnosni protokol komunikacije na internetu. Nekada nije bio podržan od strane svih internet browsera, ali danas jeste. Prvu specifikaciju SSL sertifikata napravila je kompanija Netscape 1994. godine, tada tvorci najpopularnijeg browsera na svetu. Nakon nekoliko iteracija, SSL je evoluirao u **TRANSPORT LAYER SECURITY – TLS**, standard koji se danas koristi u aktuelnoj verziji 1.2, a uskoro će početi upotreba i 1.3 standarda. Ipak, ime SSL se zadržalo i danas.

SSL omogućava prenos osetljivih informacija. Svrha je da omogući šifrovanu komunikaciju direktno između korisnika i verifikovane lokacije, što prenos osetljivih informacija čini bezbednim, bez prisluškivanja, ometanja ili falsifikovanja. Najčešći primer korišćenja SSL protokola je **https** koji predstavlja sigurnu verziju **http**-a (secure http) i koristi se za uspostavu zaštićene veze sa nekim web serverom.

Najčešće se koristi za

- ◇ Online transakcije
- ◇ Web forme i login podatke korisnika
- ◇ Email i webmail aplikacije
- ◇ Komunikacije na cloud platformama i virtualizovanim aplikacijama

Podaci koje razmenjuju korisnici i web serveri se najčešće prenose kao običan tekst. Što može da dovede do

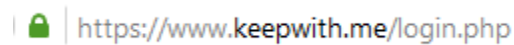
- ◇ Krađe identiteta
- ◇ Bankarskih prevara
- ◇ Zloupotrebe informacija

SSL CERTIFIKAT

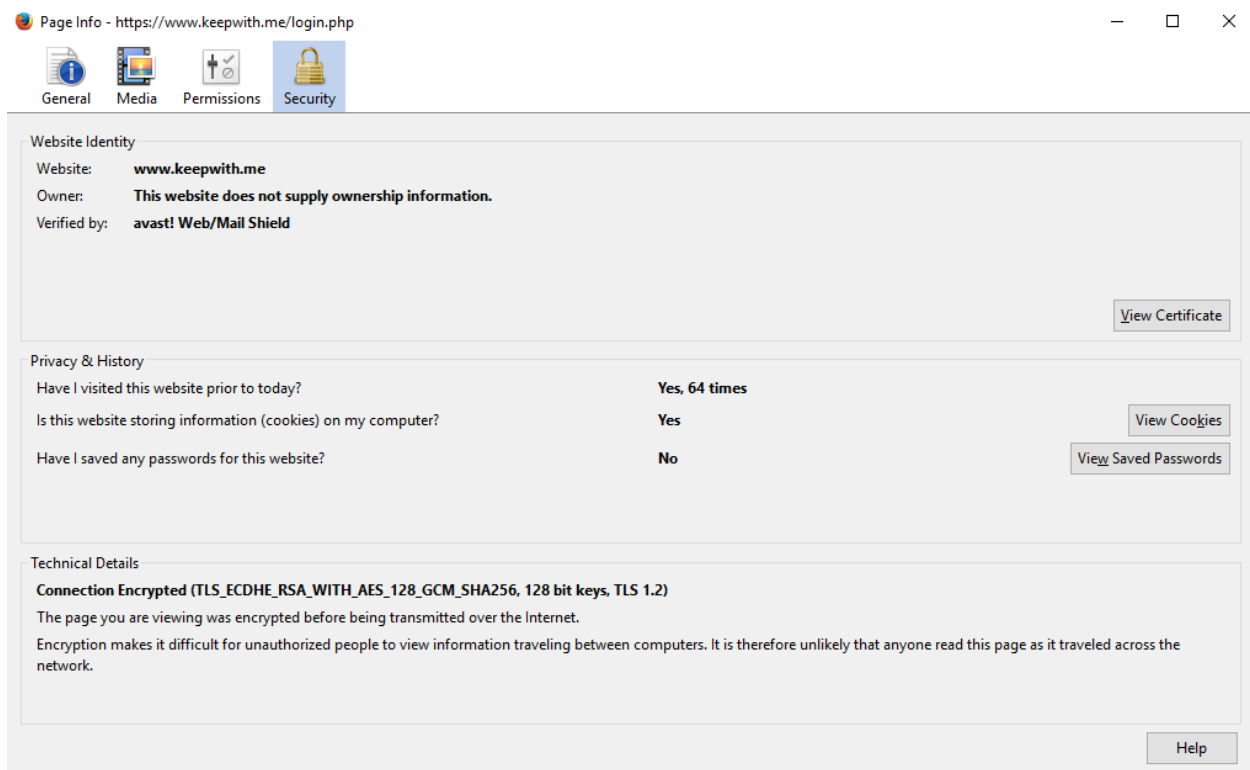
Da bi se zloupotreba informacija sprečila u što većoj meri, koristi se enkripcija. Enkripcija je matematički proces kodiranja i dekodiranja informacija, sam SSL se zasniva na enkriptovanoj bezbednoj vezi.

SSL sertifikat služi kao identifikacioni dokument, u online svetu. Svaki SSL sertifikat je jedinstvena identifikacija za određeni domen i web server. Pouzdanost sertifikata zavisi od pouzdanosti organizacije koja ga je izdala. Sertifikaciona tela (Certificate Authority) na različite načine utvrđuju tačnost informacija koje im pošalju pojedinci ili organizacije. Sertifikaciona tela kao što su Comodo, Symantec, Thawte i GeoTrust, imaju odličnu reputaciju i uživaju poverenje browsera, pa tako i njihove sertifikate smatraju pouzdanim.

SSL sertifikat sadrži verifikovane informacije o sajtu koji štiti. Proširena validacija (Extended Validation) je najviši standard verifikacije i na upadljiv način uverava korisnike u autentičnost i bezbednost sajta. Sve web stranice koje su obezbeđene sa SSL-om imaju **https://** u svojoj URL adresi.



Osim adrese, korisnike sajta u autentičnost uverava i žig poverenja (trust mark, trust seal), koju dobijate sa sertifikatom i koju možete da instalirate na sajt. Klikom na ikonicu katanca, možete dobiti detaljne informacije o SSL sertifikatu, informacije o vlasniku sajta kao i nezavisnom telu koje je sertifikat izdalo.



Broj bitova enkripcije (40-bit, 56-bit, 128-bit, 256-bit) govori o veličini ključa. Kao i duža lozinka, veći ključ ima više mogućih kombinacija. Šta više, 128-bitna enkripcija je jedan trilion puta jača od 40-bitne enkripcije. Kada se uspostavi kriptovana sesija, jačina se određuje na osnovu kapaciteta web browsera, SSL sertifikata, web servera i operativnog sistema na kompjuteru koji pristupa sajtu.

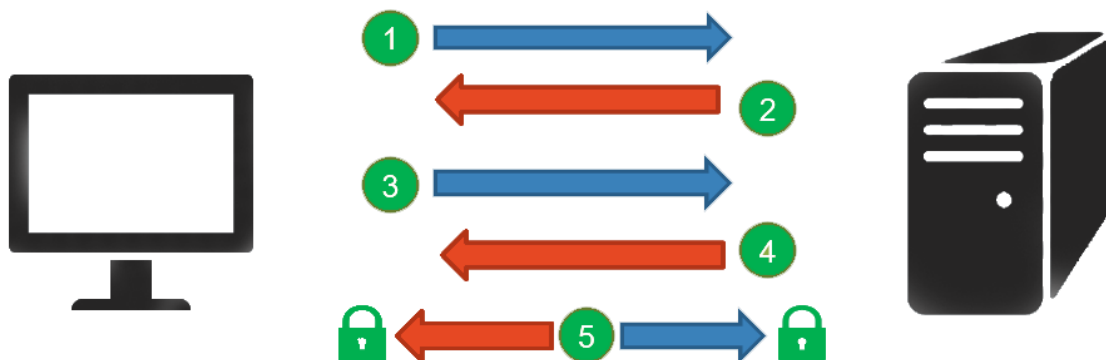
ZAHTEV ZA IZDAVANJE SERTIFIKATA

Dobijanje sertifikata od željenog sertifikacionog tela se sastoji iz više koraka.

- ◇ Zahtev
Kreiranje zahteva za izdavanje sertifikata na vašem serveru, čime dobijate javni i privatni ključ
- ◇ CSR
Slanje podataka, SSL CA (Certificate Authority), koji u sebi sadrže javni ključ. Na osnovu njega se pravi struktura koja odgovara vašem privatnom ključu
- ◇ Instalacija
Kada dobijete željeni SSL sertifikat, potrebno je instaliranje sertifikata na serveru

SIGURNA KONEKCIJA

Klijent je strana koja inicira sigurnu komunikaciju, dok server odgovara na zahtev klijenta. Svrha je da omogući šifrovanu komunikaciju direktno između korisnika i verifikovane lokacije, što prenos osjetljivih informacija čini bezbednim, bez prisluškivanja, ometanja ili falsifikovanja.



1. Klijent se povezuje na webserver koristeći bezbedni https i traži od web server da se identifikuje.
2. Server šalje kopiju SSL sertifikata uključujući i javni ključ.
3. Klijent proverava da li je sertifikat izdat od strane poverljivih sertifikacionih tela i da li je sertifikat povučen, nevažeći i da li se domen poklapa sa sajtom kome želimo da pristupimo. Ukoliko browser utvrdi da je sertifikat validan onda kreira, enkriptuje i šalje serveru simetrični ključ sesije koristeći javni ključ dobijen od servera.
4. Server dekriptuje dobijeni ključ sesije koristeći svoj privatni ključ i šalje potvrdu enkriptovanu sa ključem sesije i tako pokreće enkriptovanu sesiju.
5. Server i klijent sada razmenju podatke enkriptovane sa ključem sesije.

SSL UBUNTU APACHE - INSTALACIJA

Ukoliko koristite Apache za generisanje privatnog ključa i CSR-a možete koristiti openssl. Za generisanje privatnog ključa `example.com.key` i CSR fajla sa nazivom `example.com.csr` pokrenite ovu komandu.

```
openssl req -newkey rsa:2048 -nodes -keyout example.com.key -out example.com.csr
```

Sada unosite osnovne informacije neophodne za pravljenje CSR fajla. Najvažnije polje jeste Common Name koje treba se poklopiti sa imenom domena, npr: `example.com` ili `*.example.com` ukoliko koristimo wildcard.

Name (2 letter code) [AU]: RS

State/Country or Province Name (full name) [Some-State]: Kragujevac

Locality Name (eg, city) []: Kragujevac

Organization Name (eg, company) [Internet Widgits Pty Ltd]: keepwithme

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []: keepwith.me

Email Address []: admin@keepwith.me

KUPOVINA CERTIFIKATA



INSTALACIJA CERTIFIKATA NA WEB SERVER-U

Sledeće komande služe za backup podataka.

```
cd /etc/apache2/sites-available  
cp 000-default.conf 000-default.conf.orig
```

Otvaramo fajl za editovanje.

```
sudo nano 000-default.conf
```

Ovaj konfiguracioni fajl menjamo tako što mu dodajemo sledeći kod:

```
<VirtualHost *:443>  
    DocumentRoot /var/www/html  
    DirectoryIndex index.php  
    ServerName keepwith.me  
    SSLEngine on  
    SSLCertificateFile /home/keepwith_me.crt  
    SSLCertificateKeyFile /home/keepwith.me.key  
    SSLCACertificateFile /home/keepwith_me.ca-bundle  
</VirtualHost>
```

<VirtualHost *:443> - omogućava da server osluškuje port 443: ServerName example.com – domen sa kojim se radi. Ostale linije služe za specifikaciju fajlova sertifikata koje dobijamo kupovinom sertifikata od ovlašćenih sertifikacionih tela.

Sada je server konfigurisan da osluškuje samo https (port 443) pa http zahtevi (port 80) neće biti opsluženi , treba dodati i sledeće komande.

```
<VirtualHost *:80>
    DocumentRoot /var/www/html
    DirectoryIndex index.php
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Za pokretanje ssl modula na apache serveru.

```
sudo a2enmod ssl
```

Komanda za restart apache servera radi pokretanja novog konfiguracionog fajla i omogućavanja SSL-a.

```
sudo service apache2 restart
```

VIŠE INFORMACIJA

Više informacija o SSL-u kao i detaljan tutorijal za DigitalOcean i NameCheap možete pronaći na sledećem linku: [SSL DigitalOcean Tutorial](#)

Github studentima poklanja besplatan hosting, domen kao i SSL sertifikat [Student Developer Pack](#)

Tutorial za MITM napad : [SSLStrip](#)

Operativni sistem za testiranje bezbednosti: [Kali](#)

Korisni programi:

- ◇ [urlsnarf](#) - sniff HTTP zahteva
- ◇ [driftnet](#) - prikazivanje slika sa ostalih uređaja u mreži
- ◇ [ettercap](#) - softver za olakšavanje MITM napada
- ◇ [wireshark](#) - omogućava detaljan pregled i analizu mreže