ДРУШТВО МАТЕМАТИЧАРА СРБИЈЕ

АКРЕДИТОВАНИ СЕМИНАР:

345
ДРЖАВНИ СЕМИНАР О НАСТАВИ МАТЕМАТИКЕ И РАЧУНАРСТВА ДРУШТВА МАТЕМАТИЧАРА СРБИЈЕ

Компетенција: К1
Приоритети: 3

ТЕМА:

БЕЗБЕДНОСТ САВРЕМЕНИХ ВЕБ-РЕСУРСА

РЕАЛИЗАТОР СЕМИНАРА:

ВЕЛИМИР РАДЛОВАЧКИ

БЕОГРАД,
09. – 10. 02. 2019.

1. Увод

Доласком интернета у Србију 1996. године, све чешће смо почели да се сусрећемо са терминима World Wide Web, веб сајт, хипер текст, веб хостинг, интернет домен итд. Убрзо су и прве дефиниције ових термина нашле своје место у уџбеницима за рачунарство и информатику и сродне предмете, које се до данас нису мењале. Обично се World Wide Web описује као мноштво веб сајтова који су сачињени од HTML страница међусобно повезаних хипер везама. За имплементацију таквог веба били су неопходни веб сервери који комуницирају са веб прегледачима корисника и на захтем им достављају веб странице сајта, као и сервери за трансфер фајлова помоћу којих су веб дизајнери слали фајлове са својих рачунара на сервере. Овакви описи, дефиниције и системи, најблаже речено, одавно су застарели.

World Wide Web данас чини мноштво комплексних система за управљање садржајима. У позадини тих система налазе се:

- Сервери: Web, DNS, FTP, E-mail, даљински приступ, сервиси за безбедност, складиштење и одржавање, контролни панели, сервиси за конфигурацију наведених сервера итд.
- Сервери база података: MySQL, MariaDB, MongoDB, PostgreSQL, PostGIS, CockroachDB, SQLite, Percona, NoSQL, MS SQL…
- Системи за управљање серверима база података: phpMyAdmin, Adminer, RockMongo, SIDU, SQLiteManager, MyWebSQL, Chive, Vty, phpLiteAdmin…
- Решења заснована на базама података: Hadoop, Hypertable, Stratosphere, OrientDB, ObjectDB, Infinispan, Derby, Cassandra, Neo4j, Couchdb…
- Програмски и описни језици за развој веб садржаја: HTML/CSS, JavaScript, PHP, Java, Python, Perl, Ruby, Golang, ColdFusion, ASP.NET…
- Програмске библиотеке: jQuery, AngularJS, React, Ext JS, Dojo, Vue.js, Meteor, Ember, Backbone, Aurelia, Polymer, Mithril…
- Програмска окружења: Chrome V8, Opera, NodeJS, Couchbase, SpiderMonkey, Nitro…
- Готова решења за управљање садржајима: WordPress, Joomla, Drupal, concrete5, django…
- Додаци за готова решења за управљање садржајима: WooCommerce, Yoast SEO, Jetpack…

Дати списак је више него скроман и служи само као илустрација комплексности система на вебу данас.

2. Веб хостинг и хостинг домена

2.1. Веб хостинг

Веб хостинг сервис је тип интернет хостинг сервиса који омогућује појединцима и организацијама да поставе веб сајт или веб апликацију која ће бити доступна на јавном интернету. Веб хостинг провајдери нуде мноштво услуга које можемо поделити у неколико категорија:

1. Дељени хостинг (Shared Hosting) – један физички ресурс на интернету (нпр. један сервер) деле више независних корисника. Ова категорија представља оптимални однос цене, перформанси, простора на диску и протока за мање захтевне кориснике који, могу одабрати, према својим потребама, пакете услуга чија цена износи од $20 на више на годишњем нивоу.
2. Хостинг виртуалног приватног сервера (Virtual Private Server Hosting) – представља виртуални сервер на интернету намењен напреднијим корисницима који имају потребу за већом количином ресурса. Куповином оваквог пакета добија се потпун приступ серверу чија цена износи од $20 на више на месечном нивоу.

3. Хостинг сервера у облаку (Cloud Server Hosting) – представља виртуални сервер у облаку тј. мрежи синхронизованих рачунара, чија је недоступност сведена на минимум. Цена ове услуге на месечном нивоу слична је цени VPS хостинга.
4. Хостинг наменског сервера (Dedicated Server Hosting) – представља хостинг физичког сервера у дата центру намењеног само једном кориснику. За разлику од претходних услуга, у овој нема дељења ресурса са другим корисница, а цена износи од $40 на више на месечном нивоу.

2.2. Хостинг домена

Под хостингом домена подразумевамо чување записа на јавном интернету који повезује име које човек може лако да запамти са нумеричким, односно алфанумеричким адресама ресурса на интернету. Провајдер хостинга домена може бити иста компанија која нуди услугу веб хостинга, али треба разликовати те две услуге. Постоји више типова домена:

1. Генерички домени највишег нивоа (gTLD – generic Top-Level Domains) међу којима су најпопуларнији: COM, NET, ORG, EDU итд. Ови домени називају се и глобални домени и настали су као скраћенице општих појмова на енглеском језику (commercial, network, organization, education). Цена хостинга генеричких домена највишег нивоа на годишњем нивоу износи око хиљаду динара односно око $10.
2. Национални домен највишег нивоа (енгл. ccTLD – country code Top-Level Domain) је домен који је повезан са одређеном државом или територијом. Одређује на основу међународне ознаке државе са два карактера, који према стандарду ISO 3166-2, садржи искључиво карактере енглеског алфабета (као што је наш .RS домен). Постоје и IDN (Internationalized Domain Name) ccTLD који садрже и карактере који нису део енглеског алфабета (као што је наш .СРБ домен). Цена хостинга националних домена највишег нивоа на годишњем нивоу износи око 2300 динара.
3. Национални домени другог нивоа (енгл. ccSLD – country code Second-Level Domain) регистровани су испод ccTLD-а и од њега је одвојени тачком. Намењени су регистрантима различитих делатности и у Републици Србији подељени у шест категорија: CO.RS, ORG.RS, EDU.RS, AC.RS, GOV.RS и IN.RS. Такође, у оквиру IDN ccSLD у Републици Србији постоји шест категорија намењених истоветним групама: ПР.СРБ, ОРГ.СРБ, ОБР.СРБ, АК.СРБ, УПР.СРБ и ОД.СРБ). Цена хостинга националних домена другог нивоа на годишњем нивоу износи око 850 динара.
4. Персонализовани домени могу бити: TRAVEL, TOURS, PHOTOGRAPHY, NINJA итд. Обично их користе регистранти који желе да нагласе бренд своје делатности. Цена хостинга персонализованих домена највишег нивоа на годишњем нивоу креће се у опсегу од $15 до $50.

Регистроване образовне институције основног и средњег образовања у Републици Србији, уз доказ о регистрацији којег издаје Агенција за привредне регистре, имају право на регистрацију EDU.RS домена. Појединци који немају регистровану организацију могу регистровати свој домен уз генерички домен највишег нивоа, национални домен највишег нивоа или персонализовани домен.

3. Безбедност савремених веб ресурса

Након одабира пакета услуга хостинга ресурса и хостинга домена, корисник у већини случајева добија приступ контролном панелу. Контролни панел за веб хостинг је веб-базирани интерфејс који омогућава корисницима да управљају својим ресурсима и много више од тога. Са неколико кликова мишем корисник може да креира базу података, преузме актуелну „инсталациону“ верзију веб софтвера и инсталира и подеси изузетно комплексне веб сајтове у виду система за управљање садржајима (Content Management System - CMS). Цео процес је интуитиван и не захтева скоро никакво предзнање о веб технологијама.

У тренутку инсталације, овако инсталиран и подешен систем може бити прилично безбедан. Међутим, након инсталације, корисници инсталирају често теме и додатке, понекад и са непоузданих извора, који значајно повећавају простор за експлоатацију могућих сигурносних пропуста. Нередовним ажурирањем система за управљање садржајима, тема и додатака, скоро је сигурно да ће веб сајт постати магнет за малициозне нападаче.

Разлог за избегавање ажурирања често и није неажурност корисника, већ популарно названа закључана верзија (version lock) – ситуација када креатори тема и додатака престану да ажурирају своје теме и додатке, па корисници не могу да ажурирају систем за управљање садржајима, јер инсталирана тема и додаци нису подржани у новој верзији. Овакве ситуације треба избећи по сваку цену.

3.1. Сигурносна заглавља HTTP одговора

Сигурносна заглавља HTTP одговора користе се за повећање сигурности садржаја на вебу. Једном постављена, ова заглавља могу помоћи у ублажавању малициозних напада и експлоатацији сигурносних пропуста. Циљ овог предавања јесте да подигне свест наставника о могућностима имплементације ових заглавља на личним и школским ресурсима на вебу.

Следећи списак садржи HTTP заглавља која могу утицати на безбедност веб садржаја:

- HTTP Strict Transport Security (HSTS)
- Public Key Pinning Extension for HTTP (HPKP)
- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies
- Referrer-Policy
- Expect-CT
- Feature-Policy

3.2. HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) је механизам веб безбедносне политике који помаже приликом заштите веб сајтова од напада на снижавања категорије протокола и отмице колачића. Он дозвољава веб серверима да прогласе да веб прегледачи (или други веб агенти) требају да комуницирају искључиво безбедним HTTPS везама, а никако необезбеђеним HTTP везама. HSTS је IETF стандардни протокол са спецификацијом у RFC-6797 документу. Веб сервер имплементира HSTS политику тако што дозвољава пренос преко HTTPS везе, односно игнорише захтеве за преносом преко HTTP везе.

На пример, следеће подешавање:

```
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

веб прегледачу саопштава параметар `max-age` као време у секундама током које треба да запамти да се датом сајту приступа искључиво путем HTTPS везе; и опционо параметар `includeSubDomains` који говори да ово правило важи и за све поддомене.

3.3. Public Key Pinning Extension for HTTP (HPKP)

HTTP Public Key Pinning (HPKP) је сигурносни механизам који омогућује HTTPS веб сајтовима да избегну малициозне нападаче који користе лажне сигурносне сертификате. Ова безбедносна функција говори прегледачу да повеже одређени криптографски јавни кључ са одређеним веб сервером, чиме се смањује ризик од напада помоћу кривотворених сертификата.

Први пут, када сервер веб сајта преко посебног заглавља јави прегледачу који му јавни кључеви припадају, прегледач чува ове информације током одређеног временског периода. Када поново посети сервер, прегледач очекује да најмање један сертификат у ланцу сертификата садржи јавни кључ којег је сачувао. Ако сервер достави непознати јавни кључ, прегледач треба да прикаже упозорење кориснику.

На пример, следеће подешавање:

```
Public-Key-Pins: pin-sha256="d6qzRu9zOECb90Uez27xWltNsj0e1Md7GkYYkVoZWmM="; pin-
sha256="E9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g="; report-
uri="https://mojsajt.edu.rs/pkp-report"; max-age=10000; includeSubDomains
```

веб прегледачу саопштава: отиске `pin-sha256` енкодираних информација о јавним кључевима субјекта (Subject Public Key Information - SPKI); параметар `max-age` као време у секундама током које прегледач треба да запамти да се датом сајту приступа помоћу датог кључа (кључева); опциони параметар `report-uri` који садржи URL на који се шаљу извештаји о неуспелим валидацијама; и опционо параметар `includeSubDomains` који говори да ово правило важи и за све поддомене.

3.4. X-Frame-Options

Заглавље одговора X-Frame-Options побољшава заштиту веб апликација од такозваних Clickjacking напада. Ова заглавља декларишу правила која веб сервер саопштава прегледачу о томе да ли сме или не сме приказивати садржаје у оквиру других веб страница.

На пример, следеће подешавање:

```
X-Frame-Options: deny
```

веб прегледачу саопштава параметар `deny` да приказ у оквиру није дозвољен; односно уместо тог параметра може се навести параметар `sameorigin` да приказ није дозвољен уколико садржај не долази са истог домена, или параметар `allow-from: imedomena` да приказ јесте дозвољен уколико садржај долази са наведеног домена.

3.5. X-XSS-Protection

Ово заглавље наређује прегледачу да укључи XSS (Cross-site Scripting) филтер.

На пример, следеће подешавање:

```
X-XSS-Protection: 1; mode=block
```

веб прегледачу саопштава параметар `1; mode=block` којим се укључује филтер и блокира приказ садржаја странице. Може се навести и параметар `1` за укључивање филтера и приказ очишћене странице; параметар `1; report=https://mojsajt.edu.rs/reportURI` за укључивање филтера, приказ очишћене странице и пријаве на дату адресу - функционише у Chromium прегледачима; или параметар `0` да се искључи филтер.

3.6. Content-Security-Policy (CSP)

Content Security Policy (CSP) захтева највише пажње приликом подешавања јер може да има велики утицај на начин на који прегледачи приказују странице. Добро подешена CSP може да спречи XSS и injection нападе. Списак параметара и вредности је велик и може се пронаћи на www.w3.org/TR/CSP/.

На пример, следеће подешавање:

```
Content-Security-Policy: script-src 'self'
```

веб прегледачу саопштава параметар `script-src 'self'` којим се дозвољава извршавање скрипти које се налазе на матичном домену, док се извршавање осталих забрањује.

3.7. Остала заглавља HTTP одговора на која треба обратити пажњу

Како током једночасовног предавања временски није могуће обрадити сва заглавља HTTP одговора и њихове опције, треба обратити пажњу на још пет заглавља:

1. **X-Content-Type-Options** - забрањиће прегледачу да интерпретира садржај датотека, MIME-sniffing, на погрешан начин – на пример, датотеку са екстензијом JPEG неће моћи да интерпретира као JavaScript датотеку без обзира на њен садржај. Овај проблем постоји у Microsoft Internet Explorer прегледачу.
2. **X-Permitted-Cross-Domain-Policies** - XML документ који може да дозволи веб клијентима, као што је Adobe Flash Player, да манипулишу подацима ван матичног домена. Више информација на www.adobe.io.
3. **Referrer-Policy** одређује које ће се информације са Referer заглављима слати у захтевима. Више информација на www.w3.org/TR/referrer-policy/.
4. **Expect-CT** заглавље користе сервери како би наредили прегледачу да испита сагласност сигурносног сертификата са Certificate Transparency (пројекат компаније Google). Више информација на www.certificate-transparency.org.
5. **Feature-Policy** заглавља омогућавају веб програмерима да селективно одаберу, односно омогуће или не омогуће функције прегледача и интерфејса за програмирање апликација. Више информација на w3c.github.io/webappsec-feature-policy/.

4. Закључак

Комплексност, а самим тим и проблеми у вези безбедности веб ресурса данас, у значајној мери разликују се у односу на период пре двадесет и више година, када је српски веб почео да се развија. Данас на првом месту треба одабрати пажњу на одабир услуге која треба бити у складу са потребама корисника, а такође, треба се распитати и о историјату пословања хостинг провајдера и услугама у вези безбедности које нуди.

Када се корисник одлучи за хостинг пакет, треба са пажњом да одабере систем за управљање садржајем и са још већом пажњом, теме и додатке за тај систем. Током времена, све одабрано мора редовно да ажурира.

На сваки захтев или проблем, инсталација додатака није решење. Корисник мора обратити пажњу и на перформансе и безбедност веб ресурса, а не само на естетику и функционалност. Треба проверити репутацију програмера или компаније који развијају теме и додатке, испитати да ли постоји подршка, да ли постоје ажурирања (претходне верзије) и да ли су раније постојали сигурносни пропусти.

Након свега наведеног треба приступити примени сигурносних заглавља HTTP одговора. Како је по правилу случај у свету безбедности информационих технологија, тако је и са сигурносним заглављима HTTP одговора – што већи комфор и комплексност то мања безбедност и обрнуто. На кориснику остаје да вага између комфора и безбедности, као и да се информише о последицама које му одлуке у корист комфора могу донети.

Аутор

Велимир Радловачки, професор рачунарске групе предмета у Школском центру „Никола Тесла“ у Вршцу:

- Е-пошта: velimir.radlovacki@gmail.com
- Веб сајт: www.radlovacki.com
- Блог: radlovacki.wordpress.com
- YouTube канал: www.youtube.com/c/VelimirRadlovački
- Друштвене мреже: Facebook, Instagram, LinkedIn, Twitter