

№ 14 ТӘЖІРИБЕЛІК ЖҰМЫС

Тақырыбы: HTTPS ПАЙДАЛАНУ

HTTP хаттамасы – Web-сервер мен клиент арасында мәліметтерді жіберудің негізгі, әрі аса қарапайым тәсілі. Web және HTTP пайда болмай тұрып, Интернетте файлдарды жіберу үшін енгізу/шығару (input/output, I/O) хаттамасы ретінде көбінесе FTP қолданылды.

HTTP – бұл URL-мен жұмыс істейтін және гипермәтін/гипермедиа орталарына арналған тұтас, әрі шапшаң енгізу/шығару хаттамасы. FTP-ге қарағанда, бұл күйсіз хаттама және оның бірнеше бұйрығы (тәсілі) ғана бар. MIME-ді қолданғанының арқасында, HTTP мәліметтердің көптеген пішімдеріне және түрлі енгізу/шығару міндеттеріне бейімделеді.

HTTP – сұрау/жауап үлгісін іске асыратын клиент-серверлік хаттама. HTTP-клиент, немесе пайдаланушылық агент (әдетте бұл Web-браузер), HTTP-серверге URL көмегімен қосылады да, қорды сұратады, мысалы HTML-күжатты.

HTTPS (Hypertext Transport Protocol Secure) – бұл сайт пен пайдаланушы құрылғысы арасында деректер алмасудың құпиялылығын қамтамасыз ететін хаттама. Ақпараттың қауіпсіздігі қорғаудың 3 деңгейі бар SSL/TLS криптографиялық хаттамаларын пайдалану есебінен қамтамасыз етіледі:

- 1) деректерді шифрлау. Оларды ұстап алудан құтылуға мүмкіндік береді.
- 2) деректердің сақталуы. Деректерді кез келген өзгерту тіркеледі.
- 3) аутентификация. Пайдаланушыны қайта бағыттаудан қорғайды.

Қорғалған деректерді беру хаттамасын міндетті түрде пайдалану интернетте төлемдер жүргізуге қатысты барлық ақпаратты талап етеді: кез келген тәсілмен (жеке төлем картасы, онлайн төлемдер жүйесі және т.б.) интернет-дүкендерде тауарларды төлеу, интернет-банкинг арқылы қызметтерді төлеу, онлайн сервистерде (казино, online-курстар және т.б.) төлемдерді жүргізу және т.б.

HTTPS протоколының жұмысы пайдаланушының компьютері мен сервердің ортақ құпия кілтті таңдайтынына негізделген. Бұл кілт бірегей және әрбір сеанс үшін жасалады. Оны жасау мүмкін емес деп саналады, өйткені онда 100-ден астам таңба бар. Деректерді үшінші тұлғаларға ұстап алмау үшін сандық сертификат пайдаланылады – бұл серверді анықтайтын электрондық құжат. Сайттың (сервердің) әрбір иесі пайдаланушымен қорғалған байланыс орнату үшін осындай сертификат болуы тиіс.

Бұл электрондық құжатта иесінің деректері мен қолы көрсетіледі.
Сертификат көмегімен сіз растайсыз:

- ол берілген адам шын мәнінде бар;
- ол сертификатта көрсетілген сервердің (сайттың) иесі болып табылады.

HTTPS протоколы бойынша қосылуды орнату кезінде браузердің бірінші жасайтын нәрсесі, бұл сертификаттың түпнұсқалығын тексеру және тек сәтті жауап берген жағдайда ғана деректерді алмасу басталады.