Jose Lorenzo V. Villanueva SE-21 EntJava1 2/25/16

Ang RFC 2109 o mas kilala bilang “HTTP State Management Mechanism” ay naglalaman ng impormasyon tungkol sa kapamaraanan upang gumawa ng sesyon sa pamamagitan ng HTTP request at responses. Meron pinakikilalang bagong pang-ulo ito ay ang Cookie at Set-Cookie na naglalaman ng impormasyon tungkol sa serbidor at sa taga-gamit. Nung kapanahunan na ginawa ang dokumento na ito, ang mga serbidor ng HTTP ay di naiuugnay sa mga nakaraang hiling ng kliyente sa mga susunod nitong kahilingan. Ang sesyon ay ginagamit para malagay ang pagpapalitan ng impormasyon ng kliyente at serbidor sa isang malaking konteksto kung saan maaring maalala ng serbidor ang mga nakaraang kahilingan ng kliyente at magkaroon ng pagpapatuloy na daloy ng impormasyon. Ang sesyon ay may iba’t ibang uri pero meron itong mga sumusunod na katangian: Ang sesyon ay may simula at katapusan, ito ay maiksi ang buhay, ang tagagamit o serbidor ay maaring matigil ang isang sesyon at ang huli ay ito ay di direkta sa pagbibigay ng impormasyon.

Ang orihinal na serbidor ay maaring magsimula ng isang sesyon, para magawa ito, nagpapadala sya ng isang Set-Cookie na isang pang-ulong tugon sa kliyente. Ang gumagamit naman ay magbabalik ng isang hiling na Cookie sa serbidor pag gusto pa nito ipagpatuloy ang sesyon. Ang orihinal na serbidor ay malalaman kung ang kasalukuyang estado ng sesyon. Dahil dito maaari itong magpadala ng Set-Cookie na tugon na may pareho or ibang impormasyon. Ang orihinal na serbidor ay maaring tapusin ang sesyon sa pamamagitan ng pagpapadala ng Set-Cookie na ang pangulo ay may Max-Age na 0.

Ang Set-Cookie ay may kanyang sariling sintaktiko pero ang pinakamahalaga dito ay ang pangalan at halaga nito. Ang pangalan ay dapat nagsisimula sa $ na simbolo at dapat di gamitin sa ibang bagay. Ang halaga naman ay di alam ang ibig sabihin ng taga-gamit at kahit anung ipadala ng orihinal na serbidor, pero maari parin makita ng kahit sinong titingin sa Set-Cookie na pang-ulo.

Ang cache ay lugar kung saan tinatago ang mga datos upang kopyahin para mas madaling gamitin. Kung gagamitin ito ng orihinal na serbidor dapat alam nya ang possible pagtatago ng Set-Cookie ng pang-ulo sa cache. Ang cookie na ginagamit lang ng isang tao ay dapat hindi ilagay sa cache, pag madaming tao naman ang gagamit ay maari itong ilagay sa cache.

Ang kliyente o taong tagamit ay meron din kanyang papel sa pagpapapilitan nila ng serbidor. Siya ang nagtatago ng impormasyon galling sa Set-Cookie na tugon. Para sa segurida maaring tangihan ng taga-gamit ang cookie kung hindi ito sumusunod sa tamang batayan.

Para pamahalaan ang mga cookies may mga bagay na dapat tandaan, kapag ang taga-gamit ay nakatanggap ng Set-Cookie na may kapangalan sa mga cookies na nakatago at kapareho ng Domain at Path na katangian, ang pinakabagong cookies ay papatungan ang lumang cookies, ngunit kung ang halaga nila pareho sa Max-Age ay 0 pareho silang itatapon. Sa paggamit ng cookies ay meron limitasyon sa dami at sa laki na pedeng itago at ito ay ang mga sumusunod, dapat ay di bababa sa 300 cookies, 4096 bytes kada cookie, at 20 cookies kada pangalan ng domain. Kapag sa di inaasahang kadahilanan ay kulang sa espayo sa cookies, ang naidagdag ay dapat tanggalin. Ang mga aplikasyon ay dapat gumamit ng mas konti at mas maliit na cookies at dapat kaya nilang hawakan ang pagkawala ng cookies. Ang taga-gamit ay maaring itakda ang pinakamadaming bilang ng cookies na pedeng mula sa isang domain o ang laki ng isang cookie dahil maaring ang isang di mabuting serbidor ay bahain ang taga-gamit ng napakadaming cookies or malaking cookies para matanggal ang mga dating cookies, mas kilala ang paraang ito biliang Denial of Service Attack.

Sa pagpapadala ng kahilingan sa orihinal na serbidor, ang taga-gamit ay nagpapadala ng cookie na pang-ulong hiling sa orihinal na serbidor batay sa request-host, request-URI at edad ng cookies. May mga kapamaraanan para malaman kung saan ipapadala ang mga cookies at ito ay ang pagtingin sa URL kapag tinutok ang daga or mouse at ang isa pang paraan ay ang pagtingin sa HTML na pinanggalingan ng dokumento. Kapag natapos na ang isang sesyon ay dapat maaring tanggalin ng taga-gamit ang lahat ng katayuang impormasyon o kaya naman tanungin kung dapat pa bang panatilihin ang impormasyon, pero dapat ay hindi. Kapag sinangayunan ng taga-gamit ay mananatili ito.

May mga isyu sa seguridad sa paggamit ng cookies kung saan pinapadala sila bilang blankong teksto sa Internet dahil dito maari silang gamitan ng packet sniffing kung saan kahit sino ay maari silang salisihan mula sa Internet at sa computer. Maari makuha ang login cookie ng taga-gamit para tularan ang sesyon na kanyang pinagkuhanan. Hindi malalaman ng orihinal na serbidor ang pinagkaiba ng orihinal na tagagamit at tsaka nung kumopya. Ang tawag sa atakeng ito ay session hijacking. Ngunit may prebensyon para dito, ito ay ang pagpapadala ng cookies sa pamamagitan ng SSL na nageencrypt ng datos bago it ipadala sa Internet. Ang isa pang paraan ay ang patunayan uli ng tagagamit na sya ang orihinal na tagagamit bago gumawa ng isa pang aktibidad.

Meron pang iba ibang uri ng atake na pedeng gawin tulad Cookie Stealing, Cross –Site Scripting o XSS, at Cross Site Forgery. Ang pinakamagandang gawin para di maging biktima sa mga kapamaraanang ito ay maging listo sa mga isyu sa seguridad at mga bagong paraan para mapigilan ang ganitong atake, higit sa lahat wag basta basta maglagay ng sensitibong impormasyon sa website na hindi tayo sigurado.

Ang RFC 2109 ay lipas na at pinalitan na ng RFC 2965 nung Oktubre 2000 ayon sa Internet Official Protocol Standards.