Nedelcea Monica – Anul 4, AC, IS

Temă 1 DATC

HTTP Authentication reprezintă procesul prin care un utilizator este identificat ca fiind aceptat pentru a accesa o resursă. Cele mai utilizate moduri de autentificare a utilizatorului oferite de protocolul HTTP sunt: **Basic Authentication** și **Digest Authentication**. Cele două metode de autentificare se realizează printr-un proces format din patru etape:

1. Browser-ul trimite o cerere HTTP către serverul web.
2. Dacă several web vede că resursa solicitată are nevoie de autentificare pentru acces, atunci trimite codul de stare 401 neautorizat împreună cu WWW-Authenticate.
3. Browser-ul solicită numele de utilizator și parola printr-o casetă de dialog. După introducerea acestora browser-ul le trimite serverului web utilizând antetul de autorizare.
4. Dacă acreditările sunt corecte, serverul web răspunde prin trimiterea codului de stare 200 și a antetului de autentificare.

HTTP Basic Authentication (BA) este o metodă prin care clientul (browser-ul) trimite numele utilizatorului și parola ca text codificat cu Base64, fără a fi criptate, fapt pentru care BA este utilizată împreună cu HTTPS pentru a asigura confidențialitatea. Antetele de autentificare:

- WWW-Authenticate este antetul atribuit unui domeniu (realm). Browser-ul salvează acreditărie pentru toate domeniile. De fiecare dată când browser-ul primește un răspuns WWW-Authenticate cu un domeniu deja salvat (de exemplu: *WWW-Authenticate: realm=”videos”*), acesta va trimite automat acreditările fără acordul utilizatorului.
- Authorization este antetul prin care browser-ul trimite serverului web numele utilizatorului și parola separate prin două puncte și codificate cu Base64. De exemplu: nume de utilizator – “*Aladdin*” și parola “*OpenSesame*” sunt concatenate “*Aladdin:OpenSesame*”, apoi în urma codificării rezultă șirul de caractere “*QWxhZGRpbjpPcGVuU2VzYW1*l”.
- Authentication-Info (optional) folosit de unele severe web pentru a trimite informații despre sesiune și despre următoarele cereri de autentificare.

HTTP Digest Autentication este o metodă prin care un server web poate negocia acreditările cu un browser web, fapt care poate fi folosit pentru a confirma identitatea unui utilizator înainte de a trimite informații de o importanță ridicată. Metoda aplică o funcție hash asupra numelui de utilizator și a parolei înainte de a le trimite. Antetele de autentificare sunt:

- WWW-Authenticate conține următoarele directive: **realm**(la fel ca la BA), **qop** (opțională, reprezintă calitatea protecției), **nonce** (valoare unică generată pentru fiecare răspuns de 401, având un timp de expirare și o limită a numărului de utilizări), **stale** (opțională, este setată pe true dacă clientul a folosit un nonce nevalid), **domain** (opțională, este o listă de URI-uri, care indică că toate adresele URL au aceleași acreditări cu adresa URL solicitată) ,**opaque** (opțională, este un șir de date specificate de server, care ar trebui să fie returnate de client nemodificate), **algorithm** (opțională, poate avea valorile “*MD5*” sau “*MD5-sess*”).
- Authorization conține următoarele directive: **username** (introdus de utilizator), **realm**, **nonce** (ambele asigurate de server), **uri** (ale resuselor care trebuie accesate), **qop** (selectarea unei valorii ca “auth, auth-int”) , **nc** (valoarea în hexa a numărului ce cereri pe care clientul le-a trimis; trebuie specifcată dacă qop este trimisă în câmpul antetului WWW-Authenticate și nu trebuie speificată în caz contrar), **cnonce** (valoare unică, generată de client), **response**(acreditările sunt reluate și atribuite acestei directive).
- Authentication-Info este trimis de server, dacă autentificarea a avut succes.