Tworzenie aplikacji webowych

Mariusz Żynel
mariusz@math.uwb.edu.pl
http://math.uwb.edu.pl/~mariusz

Uniwersytet w Białymstoku

2023/2024

Autentykacja, autoryzacja, kontrola dostępu

Autentykacja Sprawdzenie, czy użytkownik jest tym za kogo się podaje. Zwykle tożsamość użytkownika ustala się na podstawie jego nazwy i hasła.

Autoryzacja Poprzedzona jest autentykacją. Określenie, czy dany użytkownik ma uprawnienia do żądanego zasobu. Różni użytkownicy mogę mieć odmienne prawa do tego samego zasobu.

Kontrola dostępu Oparta wyłącznie na autentykacji to autoryzacja. Zwykle zawiera wiele innych kryteriów, np.: adres IP, rodzaj przeglądarki, porę dnia itp.

Basic Authentication

- Mechanizm autentykacji na poziomie HTTP
- Mechanizm wbudowany do serwera Apache
- Użytkownik jest identyfikowany na podstawie jego nazwy i hasła
- Aby ułatwić zarządzania możliwe jest grupowanie użytkowników
- Zakodowane hasła przechowywane są w plikach na serwerze
- Nazwa użytkownika i hasło przesyłane są jako tekst w kodzie Base64
- Łatwo można odczytać przekazywane siecią hasło

Basic Authentication - konfiguracja

- Tworzymy plik z hasłami i dodajemy użytkownika

```
math$ htpasswd -c /export/home/mariusz/.pwipasswd admin
New password:
Re-type new password:
Adding password for user admin
```

- Hasła w utworzonym pliku są zakodowane

```
math$ cat /export/home/mariusz/.pwipasswd
admin:$apr1$UAw6kljz$cZQb9O5cC4AXEUrT11ahk0
```

- W chronionym katalogu tworzymy plik `.htaccess`

```
AuthType Basic
AuthName "Programowanie w Internecie"
AuthUserFile /export/home/mariusz/.pwipasswd
require user admin
satisfy all
```

Basic Authentication - jak to działa?

- Żądanie klienta

```
GET /~mariusz/pwi/sekret/ HTTP/1.1
Host: math.uwb.edu.pl
User-Agent: Mozilla/5.0 (X11; SunOS i86pc; rv:45.0) Gecko/20100101
```

- Odpowiedź serwera (tylko nagłówki)

```
HTTP/1.1 401 Unauthorized
Date: Wed, 13 Mar 2019 08:12:22 GMT
Server: Apache/2.4.29 (Unix) PHP/5.6.35 OpenSSL/1.0.2n
WWW-Authenticate: Basic realm="Programowanie w Internecie"
```

- Kolejne żądanie klienta

```
GET /~mariusz/pwi/sekret/ HTTP/1.1
Host: math.uwb.edu.pl
User-Agent: Mozilla/5.0 (X11; SunOS i86pc; rv:45.0) Gecko/20100101
Authorization: Basic YWRtaW46YWJjMTIz
```

Digest Authentication

- Mechanizm autentykacji na poziomie HTTP
- Mechanizm wbudowany do serwera Apache
- Użytkownik jest identyfikowany na podstawie jego nazwy i hasła
- Aby ułatwić zarządzania możliwe jest grupowanie użytkowników
- Zakodowane hasła przechowywane są w plikach na serwerze
- Nazwa użytkownika i hasło przesyłane są jako MD5 hash
- Odczytanie przekazywanego siecią hasła jest niemożliwe

Digest Authentication - konfiguracja

- Tworzymy plik z hasłami i dodajemy użytkownika

```
math$ htdigest -c /export/home/mariusz/.pwidigest \
                    "Programowanie w Internecie" admin
Adding password for admin in realm PWI.
New password:
Re-type new password:
```

- Hasła w utworzonym pliku są zakodowane

```
math$ cat /export/home/mariusz/.pwidigest
admin:PWI:2d4d40bb69aeb7b37ce02178c0a5e1d4
```

- W chronionym katalogu tworzymy plik `.htaccess`

```
AuthType Digest
AuthName "Programowanie w Internecie"
AuthUserFile /export/home/mariusz/.pwidigest
require user admin
satisfy all
```

Digest Authentication - jak to działa?

- Żądanie klienta

```
GET /~mariusz/pwi/sekret/ HTTP/1.1
Host: math.uwb.edu.pl
User-Agent: Mozilla/5.0 (X11; SunOS i86pc; rv:45.0) Gecko/20100101
```

- Odpowiedź serwera (tylko nagłówki)

```
HTTP/1.1 401 Unauthorized
Date: Wed, 13 Mar 2019 09:03:53 GMT
Server: Apache/2.4.29 (Unix) PHP/5.6.35 OpenSSL/1.0.2n
WWW-Authenticate: Digest realm="Programowanie w Internecie",
    nonce="5f7AFfaDBQA=df1b8a23925ca52c5325c1f63274e9f40dfe7b79",
    algorithm=MD5, qop="auth"
```

- Kolejne żądanie klienta

```
GET /~mariusz/pwi/sekret/ HTTP/1.1
Host: math.uwb.edu.pl
User-Agent: Mozilla/5.0 (X11; SunOS i86pc; rv:45.0) Gecko/20100101
Authorization: Digest username="admin", realm="Programowanie w Internecie",
    nonce="5f7AFfaDBQA=df1b8a23925ca52c5325c1f63274e9f40dfe7b79",
    uri="/~mariusz/pwi/sekret/", algorithm=MD5,
    response="cafe8f2f33c3858e019d42b66ed91419",
    qop=auth, nc=00000001, cnonce="deed038837005329"
```

FIN ACK