

Аппаратно-программные средства WEB

Аутентификация HTTP

Сергей Геннадьевич Синица

КубГУ, 2020

sin@kubsu.ru

Аутентификация HTTP

Идентификация?

Аутентификация?

Авторизация?

Аутентификация HTTP

- 1) Сервер получает запрос и проверяет заголовок Authorization
- 2) Веб-приложение проводит аутентификацию и авторизацию
- 3) Если ОК, то ответ как обычно
- 4) Если нет, то 401 Unauthorized и WWW-Authenticate
- 5) Получив 401 браузер показывает диалог ввода логина и пароля для реалма, повторяет запрос передавая логин:пароль в заголовке Authorization

Аутентификация HTTP (RFC2617)

Два вида:

- basic: передается пароль и логин прямым текстом;
- digest: передается хэш пароля.

Пример Basic

```
<?php
if (empty($_SERVER['PHP_AUTH_USER']) ||
    empty($_SERVER['PHP_AUTH_PW']) ||
    $_SERVER['PHP_AUTH_USER'] != 'admin' ||
    $_SERVER['PHP_AUTH_PW'] != '123') {
    header('HTTP/1.1 401 Unauthorized');
    header('WWW-Authenticate: Basic realm="My site"');
    header('Content-Type: text/html; charset=UTF-8');
    print '<h1>401 Требуется авторизация</h1>';
    exit();
}
```


Пример Basic

Apache .htaccess:

AuthType Basic

AuthName "My Protected Area"

AuthUserFile /path/to/.htpasswd

Require valid-user

Apache .htpasswd:

username:eCcl50kn3MEX

Пример Basic

HTTP/1.1 401 Unauthorized

Date: Thu, 27 Sep 2012 12:41:19 GMT

Server: Apache/2.2.16 (Debian)

X-Powered-By: PHP/5.3.3-7+squeeze3

WWW-Authenticate: Basic realm="My site"

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 75

Keep-Alive: timeout=15, max=99

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

<h1>401 Требуется авторизация</h1>

Пример Basic

GET /auth.php HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0

(X11; Linux x86_64; rv:14.0)

Gecko/20100101 Firefox/14.0.1

Accept: text/html,
application/xhtml+xml,
application/xml;q=0.9,
/;q=0.8

Accept-Language: ru,en-us;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Connection: keep-alive

Cache-Control: max-age=0, max-age=0

Authorization: Basic YWRtaW46MTIz

Пример Basic

Authorization: Basic base64(login:password)

Пример Digest

HTTP/1.0 401 Unauthorized

Server: HTTPd/0.9

Date: Sun, 10 Apr 2005 20:26:47 GMT

WWW-Authenticate: Digest

realm="testrealm@host.com",

qop="auth,auth-int",

nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",

opaque="5ccc069c403ebaf9f0171e9517f40e41"

Content-Type: text/html

Content-Length: 311

...

Пример Digest

```
GET /dir/index.html HTTP/1.0
Host: localhost
Authorization: Digest username="Mufasa",
realm="testrealm@host.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="/dir/index.html",
qop=auth,
nc=00000001,
cnonce="0a4f113b",
response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

Пример Digest

```
HA1 = MD5("Mufasa:testrealm@host.com:Circle Of Life")  
    = 939e7578ed9e3c518a452acee763bce9
```

```
HA2 = MD5( "GET:/dir/index.html" )  
    = 39aff3a2bab6126f332b942af96d3366
```

```
Response = MD5(HA1 : nonce : nc : cnonce : qop : HA2)
```

```
Response = MD5("939e7578ed9e3c518a452acee763bce9:\  
                dcd98b7102dd2f0e8b11d0f600bfb0c093:\  
                000000001:0a4f113b:auth:\  
                39aff3a2bab6126f332b942af96d3366" )  
    = 6629fae49393a05397450978507c4ef1
```


Последний вариант Digest

Если algorithm = MD5 или не указан:

HA1 = MD5(username : realm : password)

Если algorithm = MD5-sess:

HA1 = MD5(MD5(username : realm : password) :
nonce : cnonce)

Если qop = auth-int:

HA2 = MD5(method : digestURI : MD5(entityBody))

Если qop = auth или auth-int:

Response = MD5(HA1 : nonce : nonceCount :
clientNonce : qop : HA2)

Если qop не задан:

Response = MD5(HA1 : nonce : HA2)

Сравнение Basic / Digest

Basic передает пароль открытым текстом

Basic прост в реализации

Оба не обеспечивают защиту от атаки Man in a Middle

Digest имеет необязательные параметры

Многие реализации Digest на сервере хранят пароль

Задание

Basic передает пароль открытым тестом

Basic прост в реализации

Оба не обеспечивают защиту от атаки Man in a Middle

Digest имеет необязательные параметры

Многие реализации Digest на сервере хранят пароль

Литература

1. Интернет-программирование: учебное пособие / С.Г. Сеница. Краснодар: КубГУ, 2013.
2. Рекомендация RFC2617 HTTP Authentication: Basic and Digest Access Authentication
<http://www.ietf.org/rfc/rfc2617.txt>