

HTTP cookie 3

HTTP 3

 3

 4

 5

 6

 7

 RFC 6265, RFC 2109 8

 6.0~8.5 9

 6.0 9

 7.0 10

 8.0 ~ 8.5 11

 12

 16

HTTP cookie

: <https://meetup.toast.com/posts/172>

HTTP

- HTTP 가 .
-

()

- UID() 가 .12 (DB .)
- UID가 .\
- UID가

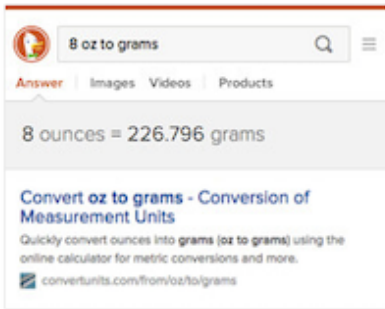
Name	Value	Domain	Path	Expires / Max-Age
JSESSIONID	564BEEA6D70D6851...	local-id.hangame.com	/	1969-12-31T23:59:59.000Z
LUT	W	.hangame.com	/	1969-12-31T23:59:59.000Z

Name	Value	Domain	Path	Expires / Max-Age
BID	B7OMN72YM6GFO38...	.hangame.com	/	2050-01-01T09:00:00.784Z
CAT	Y+1	.hangame.com	/	2018-11-21T00:37:34.514Z
HG_CP_LOGIN	"iNto0EJ2sxsKxoaitVu...	.hangame.com	/	1969-12-31T23:59:59.000Z
HG_JS	Y%5E27%5EM%5E%...	.hangame.com	/	1969-12-31T23:59:59.000Z
HG_LOGIN	c5U4eWNQ9GjS-_ouY...	.hangame.com	/	1969-12-31T23:59:59.000Z
HG_SP_LOGIN	"gYjFhmcAjqskoVTxfv...	.hangame.com	/	1969-12-31T23:59:59.000Z
LUT	W	.hangame.com	/	1969-12-31T23:59:59.000Z
NNB	LAS2L56ODPGVW	.hangame.com	/	2050-01-01T09:00:00.784Z
hgDomain	hangame	.hangame.com	/	1969-12-31T23:59:59.000Z
login	A08B6B53561B5A%2...	.hangame.com	/	1969-12-31T23:59:59.000Z

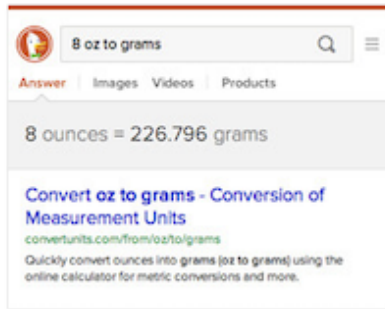
(,)

- 가, duckduckgo
-

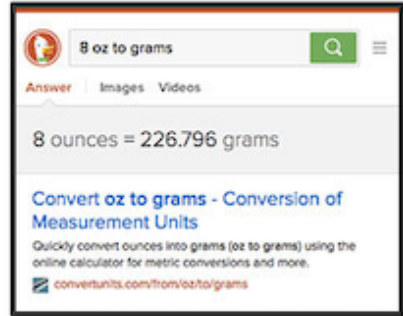
테마



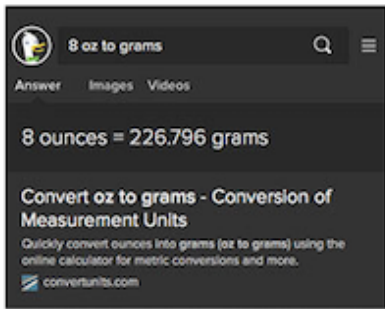
기본값



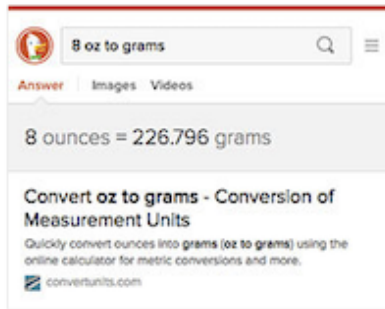
기본



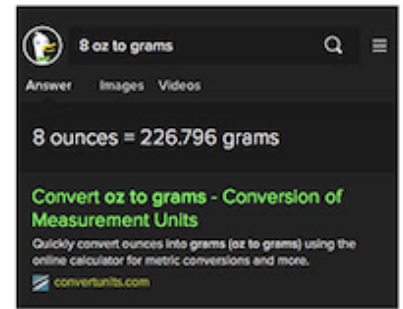
✓ 색상 대비



어둠



회색



터미널

Application					
Name	Value	Domain	Path	Expires / Max-Age	
ae	c	duckduckgo.com	/	2025-01-11T15:00:00.000Z	kers

()

가 가 가

가 ,

가

```
GET /test HTTP/1.1
Host: localhost:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
```

```

*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: ko,en-US;q=0.9,en;q=0.8

```

Set-Cookie

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: CookieName1=Example1; Expires=Tue, 27-Nov-2018 02:53:13 GMT
Set-Cookie: CookieName2=Example2; Expires=Tue, 27-Nov-2018 02:53:13 GMT
Set-Cookie: JSESSIONID=8EB8434C5776358C84017077E11A3300; Path=/
Content-Type: text/html;charset=ISO-8859-1
Content-Language: ko
Content-Length: 316

```

- Set-Cookie 가
- name : value 가

가 Set-Cookie 가

Name	Value	Domain	Path	Expires / Max-Age
CookieName1	Example1	localhost	/	2018-11-27T02:57:08.663Z
CookieName2	Example2	localhost	/	2018-11-27T02:57:08.663Z
JSESSIONID	8EB8434C5776358C84017077E11A3300	localhost	/	1969-12-31T23:59:59.000Z

가 가

```

GET /test HTTP/1.1
Host: localhost:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
DNT: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: ko,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=8EB8434C5776358C84017077E11A3300; CookieName1=Example1;
CookieName2=Example2

```

Domain

- Domain 가 .
- 가 .
- EX) hangame.com payco.com 가 .
- 가 .
- Domain 가 .
- hangame.com Domain .
- hangame.com 가 .
- hangame.com Domain hangame.com .
- accounts.hangame.com .

Path

- Domain 가 가 .
- Path가 Path가 .
- Path Set-Cookie .

Expires / Max-Age

- Expire Max-Age .
- Expire 가 .
- Max-Age 가 .

Secure

- Secure .
- 가 .

HttpOnly

- HttpOnly HTTP .
- HttpOnly가 API .

- 가 .
- Expires Max-Age 가 가 .
- Expires Max-Age 가 .
- 가 .

- (HTTPS)
- secure 가 HTTPS

Http-only

- API XSS
- cross-site tracing (XST) cross-site request forgery (XSRF)
- HttpOnly 가

Same-site

- 51
-

third-party

- 가
- 가

- , HTML5 , 가 가

0, 1

- 0 Netscape 1 RFC 2109
- RFC 2109 Netscape .3
- - Netscape Name, Value, Expires, Domain, Path, Secure, 가
 - RFC 2109 Name, Value, Comment, Domain, Max-Age, Path, Secure, Version
- - Netscape 가 Expires
 - RFC 2109 delta-seconds
 - Netscape
 - Netscape ; , ' ' RFC 2109 가

- Netscape - " , RFC 2109
- Netscape = = , RFC 2109

RFC 6265, RFC 2109

- RFC 2109 , RFC 6265
- RFC 6265가 RFC 2109 RFC 2965 .4
- Set-Cookie
- RFC 2109 Name, Value, Comment, Domain, Max-Age, Path, Secure, Version
- RFC 6265 Name, Value, Expires, Domain, Max-Age, Path, Secure, HttpOnly
- Comment 가 , Version 가
- Expires Date 가 가 , HttpOnly HTTP
 (가 API)
- - RFC 2109 가 300 , 4096 ,
 20
 * at least 300 cookies
 - * at least 4096 bytes per cookie (as measured by the size of the characters that comprise the cookie non-terminal in the syntax description of the Set-Cookie header)
 - * at least 20 cookies per unique host or domain name
 - RFC 6265 가 3000 , 4096 ,
 50 가
 - At least 4096 bytes per cookie (as measured by the sum of the length of the cookie's name, value, and attributes).
 - At least 50 cookies per domain.
 - At least 3000 cookies total.
 - RFC 6265 가
 - RFC 6265 가 Set-Cookie
- javax.servlet.http.Cookie
 - 6265



* This class supports both the RFC 2109 and the RFC 6265 specifications. * By default, cookies are created using RFC 6265.

- setVersion netscape, 2109 가


```
/**
 * Sets the version of the cookie protocol this cookie complies with.
 * Version 0 complies with the original Netscape cookie specification.
 * Version 1 complies with RFC 2109.
 * <p>
 * Since RFC 2109 is still somewhat new, consider version 1 as experimental;
 * do not use it yet on production sites.
 *
 * @param v
 *         0 if the cookie should comply with the original Netscape
 *         specification; 1 if the cookie should comply with RFC 2109
 * @see #getVersion
 */
public void setVersion(int v) {
    version = v;
}
```

- default 가 0 (netscape)가 가 .
- RFC 6265 Expires가 maxAge .

```
private final String name;
private String value;

private int version = 0; // ;Version=1 ... means RFC 2109 style

//
// Attributes encoded in the header's cookie fields.
//
private String comment; // ;Comment=VALUE ... describes cookie's use
private String domain; // ;Domain=VALUE ... domain that sees cookie
private int maxAge = -1; // ;Max-Age=VALUE ... cookies auto-expire
private String path; // ;Path=VALUE ... URLs that see the cookie
private boolean secure; // ;Secure ... e.g. use SSL
private boolean httpOnly; // Not in cookie specs, but supported by browsers
```

- maxAge Expires가 .

▼ Permanent Cookies	
▼ rfc6265	6265
Expires	Mon, 22-Oct-2018 00:21:45 GMT
Max Age	100
Domain	hangame.com

6.0~8.5 .

6.0

6.0

DIGEST 6.0.x Manager App WWW-Authenticate

- https://bz.apache.org/bugzilla/show_bug.cgi?id=52983

- - 401

```
HTTP/1.1 401 Unauthorized
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 10:00:00 EST
WWW-Authenticate: Basic realm="Tomcat Manager Application"
Set-Cookie: JSESSIONID=****removed****; Path=/manager
WWW-AuthenticateREDUNDANT: Basic realm="Tomcat Manager Application"
Content-Type: text/html
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 26 Mar 2012 03:39:09 GMT
Server: Coyote
```

- - 6.0.36
 - 401.jsp ()
 - 가 가
- ""

- https://bz.apache.org/bugzilla/show_bug.cgi?id=57896

- - ```
Name: foo
Value: bar "baz"
```
  - ```
Actual value:
[Cookie received: foo="bar "baz\""]
Expected value:
[Cookie received: foo="bar \"baz\""]
```
- - 6.0.45

7.0

7.0

JSESSIONID가

- https://bz.apache.org/bugzilla/show_bug.cgi?id=60854

- - 가 .
 - JSESSIONID 가 .
 - 가 2 JSESSIONID 가 .
- - alwaysUseSession="true" . (가 가)

ClusterSingleSignOn valve SingleSignOnEntry 가

- https://bz.apache.org/bugzilla/show_bug.cgi?id=57338

- - 7.0.62 .

8.0 ~ 8.5

8.0 ~ 8.5

Domain 가

- - domain .
 - [java.lang.IllegalArgumentException](#): An invalid domain [.hangame.com] was specified for this cookie
at org.apache.tomcat.util.http.Rfc6265CookieProcessor.validateDomain([Rfc6265CookieProcessor.java:203](#))
at org.apache.tomcat.util.http.Rfc6265CookieProcessor.generateHeader([Rfc6265CookieProcessor.java:145](#))
- - Domain .
 - LegacyCookieProcessor context.xml .

Request.parseCookies() NullPointerException

- https://bz.apache.org/bugzilla/show_bug.cgi?id=58578

- - 8.0.29 .

Rfc6265CookieProcessor 가

- https://bz.apache.org/bugzilla/show_bug.cgi?id=58445

- - 8.0.27 .

가 Rfc6265CookieProcessor가

- https://bz.apache.org/bugzilla/show_bug.cgi?id=60627
- - 8.5.12
 - version 0 RFC6265

Set-Cookie 가 RFC

- https://bz.apache.org/bugzilla/show_bug.cgi?id=60876
- - 8.5.13

가

HTTP Status 500 - Request processing failed; nested exception is java.lang.IllegalArgumentException: cookie value or attribute.

type Exception report

message Request processing failed; nested exception is java.lang.IllegalArgumentException: Control character in cookie value or attribute.

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
org.springframework.util.NestedServletException: Request processing failed; nested exception is java.lang.IllegalArgumentException: Control character in cookie value or attribute.  
org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:894)  
org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:778)  
javax.servlet.http.HttpServlet.service(HttpServlet.java:618)  
javax.servlet.http.HttpServlet.service(HttpServlet.java:725)  
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

root cause

```
java.lang.IllegalArgumentException: Control character in cookie value or attribute.  
org.apache.tomcat.util.http.LegacyCookieProcessor.needsQuotes(LegacyCookieProcessor.java:431)  
org.apache.tomcat.util.http.LegacyCookieProcessor.generateHeader(LegacyCookieProcessor.java:303)
```

- URLEncoder.encode

```
CookieController - =====  
CookieController - Name : CookieName1 Value : %C7%D1%B1%DB%C5%D7%BD%BA%C6%AE1  
CookieController - Name : CookieName2 Value : %22%C7%D1%B1%DB%C5%D7%BD%BA%C6%AE2%22  
CookieController - Name : %C7%D1%B1%DB%C5%D7%BD%BA%C6%AE3 Value : Value3  
CookieController - Name : CookieName4 Value : !@#$  
CookieController - Name : JSESSIONID Value : EC15422CDCB16E4A7B15776C44ED6841  
CookieController - =====
```

```
HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Set-Cookie: CookieName1=%C7%D1%B1%DB%C5%D7%BD%BA%C6%AE1  
Set-Cookie: CookieName2=%22%C7%D1%B1%DB%C5%D7%BD%BA%C6%AE2%22  
Set-Cookie: %C7%D1%B1%DB%C5%D7%BD%BA%C6%AE3=Value3  
Content-Type: text/html
```

- Tomcat 8.5

```
CookieController - =====  
CookieController - Name : CookieName1 Value : 한글테스트1  
CookieController - Name : CookieName2 Value : 한글테스트2  
CookieController - Name : %ED%95%9C%EA%B8%80%ED%85%8C%EC%8A%A4%ED%8A%B83 Value : Value3  
CookieController - Name : JSESSIONID Value : EA7DD1577F4C3FACD984DF3402C9E21  
CookieController - =====
```

```
HTTP/1.1 200  
Set-Cookie: CookieName1=한글테스트1  
Set-Cookie: CookieName2="한글테스트2"  
Set-Cookie: %ED%95%9C%EA%B8%80%ED%85%8C%EC%8A%A4%ED%8A%B83=Value3  
Content-Type: text/html; charset=ISO-8859-1
```

=가 = 가

```
CookieController - =====  
CookieController - Name : CookieName1 Value : Before  
CookieController - Name : CookieName2 Value : Before  
CookieController - Name : JSESSIONID Value : 395EBD87DEB6B5A44E67DB1943D88E15  
CookieController - =====
```

```
Accept-Encoding: gzip, deflate, br  
Accept-Language: ko,en-US;q=0.9,en;q=0.8  
Cookie: CookieName1=Before=After; CookieName2=Before==After; CookieName3======  
==; JSESSIONID=395EBD87DEB6B5A44E67DB1943D88E15
```


○ Url-safe base64 encode . (Encoding + /가 - _ .)

```
/**
 * This array is a lookup table that translates 6-bit positive
integer
 * index values into their "Base64 Alphabet" equivalents as
specified
 * in "Table 1: The Base64 Alphabet" of RFC 2045 (and RFC 4648).
 */
private static final char[] toBase64 = {
    'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M',
    'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z',
    'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
    'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
    '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', '+', '/'
};

/**
 * It's the lookup table for "URL and Filename safe Base64" as
specified
 * in Table 2 of the RFC 4648, with the '+' and '/' changed to '-'
and
 * '_'. This table is used when BASE64_URL is specified.
 */
private static final char[] toBase64URL = {
    'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M',
    'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z',
    'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
    'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
    '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', '-', '_'
};
```

- Java 8 java.util.Base64 getUrlEncoder().encode .
- 8 org.apache.commons.codec.binary.Base64 encodeBase64URLSafeString

가 가 가

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Request processing failed; nested exception is java.lang.IllegalArgumentException: Cookie name [(CookieName1)] is a reserved token

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```
org.springframework.web.util.NestedServletException: Request processing failed; nested exception is java.lang.IllegalArgumentException: Cookie name [(CookieName1)] is a reserved token
    org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:894)
    org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:778)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:635)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:742)
    org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

- Tomcat 6

- 가 value가
- value

```
makeCookie(response, "(CookieName1)", "Bracket");
makeCookie(response, "{CookieName2}", "Bracket");
makeCookie(response, "[CookieName3]", "Bracket");
makeCookie(response, "CookieName4", "(Bracket)");
makeCookie(response, "CookieName5", "{Bracket}");
makeCookie(response, "CookieName6", "[Bracket]");
```

.CookieController - Name : CookieName1 Value :	Accept-Encoding: gzip, deflate, br
.CookieController - Name : CookieName2 Value :	Accept-Language: ko,en-US;q=0.9,en;q=0.8
.CookieController - Name : CookieName3 Value :	Cookie: (CookieName1)=Bracket; {CookieName2}=Bracket; [CookieName3]=Bracket; CookieName4=(Bracket); CookieName5={Bracket}; CookieName6=[Bracket]; JSESSIONID=5E4B160512920A4D213E5E2D8EFEEBCB
.CookieController - Name : JSESSIONID Value : 5E4B160512920A4D213E5E2D8EFEEBCB	20A4D213E5E2D8EFEEBCB

- Tomcat 7

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Request processing failed; nested exception is java.lang.IllegalArgumentException: Cookie name [(CookieName1)] is a reserved token

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```
org.springframework.web.util.NestedServletException: Request processing failed; nested exception is java.lang.IllegalArgumentException: Cookie name [(CookieName1)] is a reserved token
    org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:894)
    org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:778)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:635)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:742)
    org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

- URLEncoder.encode

(Decoding)

CookieController - Name : (CookieName1) Value : Bracket	DNT: 1
CookieController - Name : {CookieName2} Value : Bracket	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
CookieController - Name : [CookieName3] Value : Bracket	Accept-Encoding: gzip, deflate, br
CookieController - Name : CookieName4 Value : (Bracket)	Accept-Language: ko,en-US;q=0.9,en;q=0.8
CookieController - Name : CookieName5 Value : {Bracket}	Cookie: %28CookieName1%29=Bracket; %7BCookieName2%7D=Bracket; %5BCookieName3%5D=Bracket; CookieName4=%28Bracket%29; CookieName5=%7BBracket%7D; CookieName6=%5BBracket%5D; JSESSIONID=5B0A4909254ED2D5897D9EBA5E937374
CookieController - Name : JSESSIONID Value : 5B0A4909254ED2D5897D9EBA5E937374	

- [1]https://en.wikipedia.org/wiki/HTTP_cookie#History
- [2]http://web.archive.org/web/20020803110822/http://wp.netscape.com/newsref/std/cookie_spec.html
- [3]<https://tools.ietf.org/html/rfc2109>
- [4]<https://tools.ietf.org/html/rfc6265>

From:
<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:
https://atl.kr/dokuwiki/doku.php/http_cookie%EC%99%80_%ED%86%B0%EC%BA%A3_%EB%B2%84%EC%A0%84%EB%B3%84_%EC%9D%B4%EC%8A%88?rev=1560319469

Last update: 2019/06/12 06:04

