

Apache HTTPD	3
Method	3
Apache httpd logfile permission(umask)	3
rpm	3
envvars	3
apachectl	4
Host Header Poisoning / Injection	4
.....	5
Content-Security-Policy (CSP)	5
.....	6
.....	6
X-Content-Type-Options	6
.....	7
.....	7
X-Frame-Options	7
.....	7
.....	7
X-XSS-Protection	7
.....	8
.....	8
CSRF (Cross-Site Request Forgery)	8
.....	8
.....	8
.....	10

Apache HTTPD

— 2025/07/09 01:09

Method

/etc/httpd/conf.d/method.conf

```
<Location "/*">
  <LimitExcept GET POST>
    Order deny,allow
    Deny from all
  </LimitExcept>
</Location>
```

Apache httpd logfile permission(umask)

644 . umask가 0022

umask

rpm

rpm /etc/sysconfig/httpd 가 .

```
umask 0027
```

envvars

rpm . apache apachectl
envvars . ()

```
# pick up any necessary environment variables
if test -f /APP/httpd-2.4.39/bin/envvars; then
  . /APP/httpd-2.4.39/bin/envvars
fi
```

envvars	envvars	umask	가
.	.	.	.
umask 0027	#<-	4	.

apachectl

apachectl	envvars	(Redhat JBCS(Jboss core services)
) apachectl	umask	.
umask 0027	#<-	4
.	.	.
.	umask	.

Host Header Poisoning / Injection

HTTP Host Header
example.com

. www.example.com

- Apache HTTPD

RewriteEngine On RewriteCond %{HTTP_HOST} !^(www.example.com example.com)\$ [NC] RewriteRule .* - [F]
VirtualHost
<VirtualHost _default_:*> DocumentRoot /www/default </VirtualHost>

- JBoss EAP 7 Undertow expression-filter

/subsystem=undertow/configuration=filter/expression-filter=host-checker:add(expression="not(equals(%{i,Host}, www.example.com) or equals(%{i,Host}, example.com)) -> response-code(403))" /subsystem=undertow/server=default-server/host=default-host/filter-ref=host-checker:add
xml

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1">
  <buffer-cache name="default"/>
  <server name="default-server">
    ...
    <host name="default-host" >
      ...
      <filter-ref name="host-checker"/>
    </host>
  </server>
  <filters>
    ...
    <expression-filter name="host-checker"
expression="not(equals(%{i,HOST}, www.example.com) or equals(%{i,HOST},
example.com)) -> response-code(403)"/>
  </filters>
</subsystem>
```

• JBoss EAP 6 rewrite

```
<subsystem xmlns="urn:jboss:domain:web:2.1" default-virtual-server="default-
host" native="false">
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
  <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
  <virtual-server name="default-host" enable-welcome-root="true">
    <alias name="localhost"/>
    <alias name="example.com"/>
    <!-- added -->
    <rewrite pattern="^/(.*)$" substitution="-" flags="F">
      <condition test="%{HTTP:HOST}"
pattern="!(www.example.com|example.com)" flags="NC"/>
    </rewrite>
  </virtual-server>
</subsystem>
```

- <https://access.redhat.com/solutions/3166341>
- <https://access.redhat.com/solutions/3057511>

Content-Security-Policy (CSP)

Content-Security-Policy (CSP) HTTP CSP 가
 . CSP Same-Origin-Policy(SOP) . CSP
 , 가

가 Policy

가

Content-Security-

```
<IfModule mod_headers.c>

# Content-Security-Policy
Content-Security-Policy 가

Header set Content-Security-Policy "default-src 'self'"

#
Header set Content-Security-Policy "default-src 'self' *.mydomain.com"

#
가

Header set Content-Security-Policy-Report-Only "policy"

#
Header set Content-Security-Policy "default-src 'self'; img-src
*.cloudflare.com; script-src 'self' www.google-analytics.com
*.cloudflare.com"

</IfModule>
```

- <https://content-security-policy.com/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy>

X-Content-Type-Options

X	가	HTTP	nosniff	가	X-Content-
Type-Options	가	nosniff	MIME	MIME	MIME
	MIME		,	가 MIME	
		가		MIME	MIME
	MIME				
			HTTP		
nosniff	X-Content-Type-Options				

```
<IfModule mod_headers.c>
    Header set X-Content-Type-Options nosniff
</IfModule>
```

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

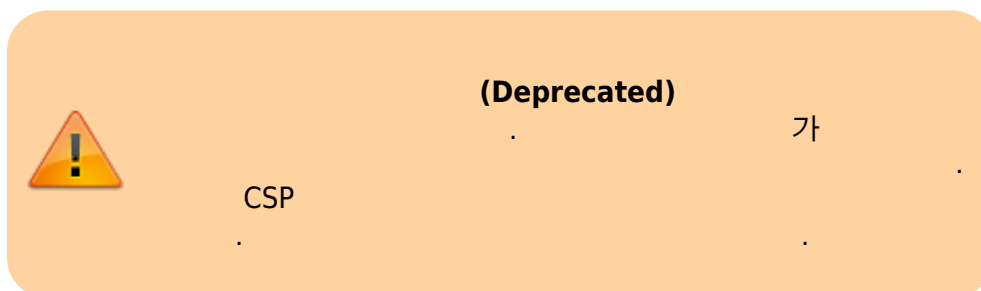
X-Frame-Options

X-Frame-Options HTTP header가 frame, iframe, object frame, iframe object 가 HTTP 가 X-Frame-Options

```
<IfModule mod_headers.c>
    Header set X-Frame-Options DENY
</IfModule>
```

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

X-XSS-Protection



XSS HTTP X-XSS-Protection 가 , X-

XSS-Protection

가

0

.

```
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
</IfModule>
```

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>

CSRF (Cross-Site Request Forgery)

				가		
		. SameSite		(CSRF)		.
	(CSRF)	SameSite	Lax	Strict		.
80		SameSite	None	Lax		.
None		Secure				.

```
<ifmodule mod_headers.c>
# none
Header always edit Set-Cookie (.*) "$1; Secure; SameSite=None;"

# strict
Header always edit Set-Cookie (.*) "$1; SameSite=strict"
</ifmodule>
```

Analytics

가

.

atl.kr

가

Google

```
<IfModule mod_headers.c>
# -----
----
# 1. CSRF (SameSite Cookie Attribute)
# -----
----
```

```
# SameSite=Lax 가 .
# 'Lax' CSRF , GET
# 'Strict' ,
Header edit Set-Cookie ^(.*)$ "$1; SameSite=Lax"

# -----
----
# 2. (CSP)
# -----
----
# atl.kr Google Analytics(GA4)
Header set Content-Security-Policy "default-src 'self'; \
script-src 'self' https://www.googletagmanager.com
https://www.google-analytics.com; \
style-src 'self' 'unsafe-inline'; \
img-src 'self' data: https://www.google-analytics.com
https://stats.g.doubleclick.net; \
connect-src 'self' https://*.google-analytics.com; \
font-src 'self'; \
object-src 'none'; \
frame-ancestors 'self'; \
form-action 'self'; \
base-uri 'self'; \
upgrade-insecure-requests;"

# -----
----
# 3.
# -----
----
# (Clickjacking) ( )
Header set X-Frame-Options SAMEORIGIN

# MIME (Sniffing)
Header set X-Content-Type-Options nosniff

# HSTS (Strict-Transport-Security): HTTPS
Header set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"

# Referrer-Policy:
Header set Referrer-Policy "strict-origin-when-cross-origin"

# Permissions-Policy:
Header set Permissions-Policy "geolocation=(), midi=(), camera=(),
microphone=()"
</IfModule>
```

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie#samesitesamesite-value>

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

Permanent link:
https://atl.kr/dokuwiki/doku.php/apache_httpd_%EB%B3%B4%EC%95%88%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80?rev=1752023393

Last update: 2025/07/09 01:09

