JBoss EAP 7 X-Frame-Options

JBoss EAP 7 X-Frame-Options

- ClickJacking   X-Frame-Options   HTTP
    .
-     JBoss EAP 7   XSS   .
- QID-11827   http   .

    JBoss EAP 7   X-Frame-Options, X-XSS-Protection, X-Content-Type-Options,
Content-Security-Policy   Strict-Transport-Security   .
                    .   .

XML

standalone.xml   domain.xml   undertow subsystem   <filters>

```
<response-header name="x-frame-options" header-name="X-Frame-Options"
header-value="SAMEORIGIN"/>
<response-header name="x-xss-protection" header-name="X-XSS-Protection"
header-value="1; mode=block"/>
<response-header name="x-content-type-options" header-name="X-Content-Type-
Options" header-value="nosniff"/>
<response-header name="content-security-policy" header-name="Content-
Security-Policy" header-value="default-src https:"/>
<response-header name="strict-transport-security" header-name="Strict-
Transport-Security" header-value="max-age=31536000; includeSubDomains;"/>
```

undertow subsystem   <host>   .

```
<filter-ref name="x-frame-options"/>
<filter-ref name="x-xss-protection"/>
<filter-ref name="x-content-type-options"/>
<filter-ref name="content-security-policy"/>
<filter-ref name="strict-transport-security"/>
```

JBoss EAP   .

JBoss CLI

```
/subsystem=undertow/configuration=filter/response-header=x-frame-
options:add(header-name="X-Frame-Options",header-value="SAMEORIGIN")
/subsystem=undertow/configuration=filter/response-header=x-xss-
protection:add(header-name="X-XSS-Protection",header-value="1; mode=block")
/subsystem=undertow/configuration=filter/response-header=x-content-type-
options:add(header-name="X-Content-Type-Options",header-value="nosniff")
/subsystem=undertow/configuration=filter/response-header=content-security-
policy:add(header-name="Content-Security-Policy",header-value="default-src
https:")
/subsystem=undertow/configuration=filter/response-header=strict-transport-
security:add(header-name="Strict-Transport-Security",header-value="max-
age=31536000; includeSubDomains;")
/subsystem=undertow/server=default-server/host=default-host/filter-ref=x-
frame-options:add()
/subsystem=undertow/server=default-server/host=default-host/filter-ref=x-
xss-protection:add()
/subsystem=undertow/server=default-server/host=default-host/filter-ref=x-
content-type-options:add()
/subsystem=undertow/server=default-server/host=default-host/filter-
ref=content-security-policy:add()
/subsystem=undertow/server=default-server/host=default-host/filter-
ref=strict-transport-security:add()
```

- content-security-policy
  .
    .   Content-Security-Policy-Report-Only:
  policy   .

- https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
- https://access.redhat.com/solutions/3026641