목차

JBoss EAP 7 X-Frame-Options 설정

문제

- 'ClickJacking' 공격으로부터 보호하기 위해 X-Frame-Options 헤더가 HTTP 응답에 포함되지 않습니다.
- 최근 JBoss EAP 7 시스템에 대한 침투 테스트를 실시했으며 XSS 보호 문제가 제기되었습니다.
- QID-11827을 수정하려면 http 응답 헤더를 추가해야 합니다.

설정

다음은 JBoss EAP 7에서 X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Content-Security-Policy 및 Strict-Transport-Security 헤더를 구성하는 단계입니다. 필요에 따라 추가합니다. 조직에서는 특정 값이 필요한지 여부에 특히 주의를 기울입니다.

XML 직접 수정

standalone.xml 또는 domain.xml의 undertow subsystem의 섹션 <filters> 에 필수 응답 헤더를 추가합니다

```
<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 subsystem의 섹션 <host>에 해당 필터 참조를 추가합니다.

```
<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 EAP를 다시 시작하고 테스트를 다시 실행하세요.

JBoss CLI를 사용하는 방법

```
/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()
```

주의사항

- `content-security-policy` 적용시 모든 외부 참조 링크는 동작하지 않으므로 주의하여야 한다. 즉 사이트외부에서 링크로 끌어다 사용하는 자바스크립트나 스타일의 경우 모두 동작하지 않게된다. 외부참조링크를 꼭 써야 하는경우 `Content-Security-Policy-Report-Only: policy` 를 적용하도록 한다.

참조링크

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