

### 1.1.1 CSP Kullanımı Eksikliği (Missing CSP) (CWE-346)

**Açıklık Önem Derecesi:** Düşük

**Açıklığın Etkisi:** XSS saldırılarına karşı savunmasız kalma

**Açıklığın Barındıran Dosyalar/Satırlar:**

Proje Dosyası/Dosya Adı	Satır Numarası

**Açıklığın Açıklaması:**

Content-Security-Policy yanıt başlığı güncel web tarayıcılarda XSS saldırılarını önleyen bir http güvenlik başlığıdır. Web tarayıcılarının görüntülediği web uygulamalarda xss zararlısı gelirse bu xss zararlısının web tarayıcıda çalışmasını önler ve son kullanıcının güven içinde web uygulamada gezinmesini sağlar.

Bu başlık ile yeni web tarayıcılarda XSS önlenmektedir. Not: Bu başlık ile ayrıca Clickjacking saldırıları da önlenmektedir.

Kurum uygulamasının csp kullanmadığı tespit edilmiştir:

:::: BULGU ::::

(Örnek Bulgu)

( Spring Framework configure metodu)

( CSP enable eden kod satırı bulunmamakta )

```
src/main/java/tr/.../security/WebSecurityConfiguration.java
55
56 @Override
57 protected void configure(HttpSecurity http) throws Exception {
58     http.cors().and().csrf().disable().authorizeRequests()
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83     http.headers().frameOptions().disable();
84     http.exceptionHandling().authenticationEntryPoint(restAuthenticationEntryPoint);
85 }
86
87 @Override
88 protected void configure(AuthenticationManagerBuilder builder) throws Exception {
89     builder.userDetailsService(userDetailsService).passwordEncoder(new PasswordEncoder() {
90         @Override
91         public String encode(CharSequence cs) {
92             return cs.toString();
93         }
94     });
95 }
```

Şekil XX. Content-Security-Policy Eksikliği

### Açıklığın Önemi:

Java uygulamalarda - Spring Framework'ünde - CSP aktiveleştirme ayarları şu alternatif yöntemlerden biri ile yapılabilir:

Java

```
// Adding CSP Header Using Spring Security Java Configuration
@Configuration
public class SpringSecurityConfig extends WebSecurityConfigurerAdapter {
    @Override
    protected void configure(HttpSecurity http) throws Exception {
        // Add CSP headers
        http.headers()
            .contentSecurityPolicy("script-src 'self' https://example.com;
object-src https://example.com; report-uri /csp-report-endpoint/");
    }
}
```

XML

```
// Adding CSP Header Using Spring Security XML Configuration
<http>
  <!-- ... -->

  <headers>
    <content-security-policy policy-directives="script-src 'self'
https://apis.example.com">
    </content-security-policy>
  </headers>
</http>
```

CSP web uygulama back-end (arka uç) kaynak kodlarında, web sunucu yapılandırma dosyalarında veya front-end (ön uç) 'daki html <head> bölümünde <meta> etiketleri ile tanımlanabilir.

PHP uygulamalarda CSP şu şekilde eklenebilir:

PHP:

```
<?php

// Restricting Content-Security-Policy to
// Only Obtain Embedded Content from Current
// Web-Application

header("Content-Security-Policy: default-src 'none'; script-src 'self';
connect-src 'self'; img-src 'self'; style-src 'self';");

?>
```

Javascript uygulamalarda CSP şu şekilde eklenebilir:

JS:

```
/* Setting The CSP Header Explicitly */

app.use(function(req, res, next) {
  res.setHeader("Content-Security-Policy", "script-src 'self'");
  return next();
});
```

## Referanslar:

1. Web Penetration Testing in Kali Linux, sayfa 122-127

2. <https://blog.appcanary.com/2017/http-security-headers.html#hsts>
3. <https://www.tbs-certificates.co.uk/FAQ/en/hsts-iis.html>
4. <https://hstspreload.org/>
5. <https://security.stackexchange.com/questions/64979/mitigating-sslstrip-by-only-serving-a-site-over-https>
6. <http://sectools.org/tool/sslstrip/>
7. <https://www.cyberciti.biz/faq/nginx-send-custom-http-headers/>
8. <https://geekflare.com/tomcat-http-security-header/>
9. <https://docs.spring.io/spring-security/site/docs/current/reference/html/headers.html>
10. <https://spring.io/guides/gs/securing-web/>
11. <https://spring.io/blog/2013/08/23/spring-security-3-2-0-rc1-highlights-security-headers>
12. <https://www.dailyrazor.com/blog/glassfish-vs-tomcat/>
13. <http://www.edu4java.com/en/servlet/servlet1.html>