

Dodatkowe zabezpieczenia wynikające z testów bezpieczeństwa

Last updated by | Janusz Bossak | 29 cze 2022 at 12:20 CEST

W pliku web.config.txt jest zakomentowanych kilka wpisów, które polepszają bezpieczeństwo aplikacji ale nie zawsze mogą być użyte.

1. Dodatkowe nagłówki:

```
<customHeaders>
<add name="content-security-policy" value="script-src 'unsafe-inline' 'unsafe-eval' 'self' ; object-src 'self'; img-src 'self' data:; frame-src 'self'; child-src 'self' ; base-uri 'self'; form-action 'self'; frame-ancestors 'self'; worker-src 'self' blob: ; connect-src 'self' https://amodit.pl ; upgrade-insecure-requests"/>
<add name="X-Content-Type-Options" value="nosniff" />
<add name="X-XSS-Protection" value="1; mode=block" />
<add name="X-Frame-Options" value="sameorigin" />
<add name="Strict-Transport-Security" value="max-age=31536000"/>
<add name="Referrer-Policy" value="strict-origin-when-cross-origin" />
</customHeaders>
```

Jeżeli mamy włączone pobieranie skryptów z Google Tag Manager to w content-security-policy trzeba w script-src dodać adresy wszystkich podłączonych serwisów zaczynając od

<https://www.googletagmanager.com> , w postaci:

script-src 'unsafe-inline' 'unsafe-eval' 'self' <https://www.googletagmanager.com> 

Strict-Transport-Security - można włączyć tylko jeżeli mamy SSL

Wpis z raportu Sisoft

- Strict-Transport-Security; let a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP. The header is configured however, max-age parameter (in seconds) is too short. (Strict-Transport-Security: max-age=15724800;) It should be valid for 1 year = 31536000.
- Content-Security-Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
- X-Frame-Options; can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid clickjacking attacks by ensuring that their content is not embedded into other sites.
- X-Content-Type-Options is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed. This allows to opt-out of MIME type sniffing, or, in other words, it is a way to say that the webmasters knew what they were doing.
- Referrer-Policy is a new header that allows a site to control how much information the browser includes navigations away from a document and should be set by all sites

2. Zabezpieczenie cookie - odkomentować tylko gdy mamy SSL

```
<httpCookies requireSSL="true" />
```

3. Ukrycie wyświetlania szczegółów błędów - zamienić Off na RemoteOnly

```
<customErrors mode="Off" defaultRedirect="error.aspx" />
```