

Sécuriser l'accès au portail

Description

Dimensional Insight a implémenté les en-têtes de sécurité HTTP dans DivePort pour améliorer la sécurité de votre site Web. Ces en-têtes fournissent des instructions sur la communication avec le site Web pour atténuer les attaques malveillantes.

Les informations de cet article s'appliquent aux versions 7.0.51 et supérieures de DivePort.

Paramètres de sécurité implémentés par défaut

Dimensional Insight recommande fortement l'utilisation des paramètres par défaut suivants :

`Strict-Transport-Policy: max-age=31536000`

Cet en-tête force le navigateur web à utiliser une connexion HTTPS fiable (même lorsqu'un utilisateur demande une connexion HTTP) après la première connexion HTTPS réussie.

Pour plus d'informations : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

`Referrer-Policy: strict-origin-when-cross-origin`

Cet en-tête oblige le navigateur à envoyer des informations URL limitées à des sites externes liés depuis DivePort, et uniquement lorsque le site lié utilise également HTTPS. Cela rend plus difficile pour les attaquants potentiels de voir quelles pages DivePort sont consultées par les utilisateurs. Remarque: si le suivi de l'activité des utilisateurs à l'aide de *Referer* n'est pas requis, DI recommande de définir cette stratégie sur "same-origin".

Pour plus d'informations : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

`Feature-Policy: fullscreen 'none'; microphone 'none'; camera 'none'; payment 'none'`

Cet en-tête désactive certaines fonctionnalités du navigateur lors de l'affichage des pages DivePort. Cela permet de limiter les interactions des sites Web tiers lorsqu'ils sont intégrés à DivePort.

Pour plus d'informations : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

Ces options peuvent être personnalisées en modifiant le fichier *portaldb.json* et en ajoutant de nouveaux paramètres "infos" dans la section "portal" :

`"http.strict-transport-security"`

Remplacer cet en-tête n'est pas recommandé. La valeur par défaut de cet en-tête doit être correcte dans la plupart des cas.

`"http.referrer-policy"`

Si le suivi de l'activité de l'utilisateur à l'aide de "Referer" n'est pas requis, il est recommandé de le définir sur "same-origin", mais la valeur par défaut de cet en-tête devrait être correcte dans la plupart des cas.

"http.feature-policy"

Remplacer cet en-tête n'est pas recommandé. La valeur par défaut de cet en-tête devrait être correcte dans la plupart des cas.

Recommandations

DivePort ne définit pas de valeurs par défaut pour les en-têtes de sécurité suivants. Cependant, vous pouvez leur spécifier des valeurs dans la section portal-infos du fichier *portaldb.json* :

Content-Security-Policy. Cet en-tête spécifie les directives qui vous permettent de restreindre les ressources que les utilisateurs peuvent charger sur le site.

Paramétrage recommandé :

```
"http.content-security-policy": "default-src 'self' 'unsafe-inline'"
```

Pour plus d'information : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy>

X-Frame-Options. Cet en-tête empêche DivePort de s'afficher à l'intérieur d'un IFRAME dans un autre site Web. Cela permet de se prémunir contre les attaques de détournement de clics (clickjacking).

Paramétrage recommandé :

```
"http.x-frame-options": "sameorigin"
```

Remarque : ce paramètre interfère lorsque DivePort est destiné à être intégré dans une autre application Web. Si cela est nécessaire, recherchez comment utiliser la directive *allow-from*.

Pour plus d'information : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

X-Content-Type-Options. Cet en-tête empêche le navigateur de surveiller le contenu (sniffing) pour déterminer les types de fichiers téléchargés depuis DivePort.

Paramétrage recommandé :

```
"http.x-content-type-options": "nosniff"
```

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

Content-Security-Policy-Report-Only. Cela n'a pas d'effet direct sur la sécurité mais peut être utilisé pour tester des politiques pour l'en-tête Content-Security-Policy.

Paramétrage :

```
"http.content-security-policy-report-only"
```

Pour plus d'informations : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy-Report-Only>

Édition du fichier portaldb

Le fichier *portaldb.json* se trouve dans le répertoire *DI\Solution\webdata\<diveport>\database* et contient tous les paramètres de configuration du portail. Vous pouvez éditer les attributs dans ce fichier pour modifier des

