SÃ©curiser lâ??accÃ¨s au portail

Description

Dimensional Insight a implÃ©mentÃ© les en-tÃªtes de sÃ©curitÃ© HTTP dans DivePort pour amÃ©liorer la sÃ©curitÃ© de votre site Web. Ces en-tÃªtes fournissent des instructions sur la communication avec le site Web pour attÃ©nuer les attaques malveillantes.

Les informations de cet article s'appliquent aux versions 7.0.51 et supÃ©rieures de DivePort.

ParamÃ¨tres de sÃ©curitÃ© implÃ©mentÃ©s par dÃ©faut

Dimensional Insight recommande fortement lâ??utilisation des paramÃ¨tres par dÃ©faut suivants :

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

Cet en-tÃªte force le navigateur web Ã utiliser une connexion HTTPS fiable (mÃªme lorsqu'un utilisateur demande une connexion HTTP) aprÃ¨s la premiÃ¨re connexion HTTPS rÃ©ussie.

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-tÃªte oblige le navigateur Ã envoyer des informations URL limitÃ©es Ã des sites externes liÃ©s depuis DivePort, et uniquement lorsque le site liÃ© utilise Ã©galement HTTPS. Cela rend plus difficile pour les attaquants potentiels de voir quelles pages DivePort sont consultÃ©es par les utilisateurs. Remarque: si le suivi de l'activitÃ© des utilisateurs Ã l'aide de *Referer* n'est pas requis, DI recommande de dÃ©finir cette stratÃ©gie sur "same-origin".

Pour plus dâ??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-tÃªte dÃ©sactive certaines fonctionnalitÃ©s du navigateur lors de l'affichage des pages DivePort. Cela permet de limiter les interactions des sites Web tiers lorsqu'ils sont intÃ©grÃ©s Ã DivePort.

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

Ces options peuvent Ãªtre personnalisÃ©es en modifiant le fichier *portaldb.json* et en ajoutant de nouveaux paramÃ¨tres "infos" dans la section "portal" :

```
"http.strict-transport-security"
```

Remplacer cet en-tÃªte n'est pas recommandÃ©. La valeur par dÃ©faut de cet en-tÃªte doit Ãªtre correcte dans la plupart des cas.

```
"http.referrer-policy"
```

Si le suivi de l'activitÃ© de l'utilisateur Ã l'aide de "Referer" n'est pas requis, il est recommandÃ© de le dÃ©finir sur "same-origin", mais la valeur par dÃ©faut de cet en-tÃªte devrait Ãªtre correcte dans la plupart des cas.

```
"http.feature-policy"
```

Remplacer cet en-tÃªte n'est pas recommandÃ©. La valeur par dÃ©faut de cet en-tÃªte devrait Ãªtre correcte dans la plupart des cas.

Recommandations

DivePort ne dÃ©finit pas de valeurs par dÃ©faut pour les en-tÃªtes de sÃ©curitÃ© suivants. Cependant, vous pouvez leur spÃ©cifier des valeurs dans la section portal-infos du fichier *portaldb.json* :

Content-Security-Policy. Cet en-tÃªte spÃ©cifie les directives qui vous permettent de restreindre les ressources que les utilisateurs peuvent charger sur le site.

ParamÃ©trage recommandÃ© :

```
"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-tÃªte empÃªche DivePort de s'afficher Ã l'intÃ©rieur d'un IFRAME dans un autre site Web. Cela permet de se prÃ©munir contre les attaques de dÃ©tournement de clics (clickjacking).

ParamÃ©trage recommandÃ© :

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

Remarque : ce paramÃ¨tre interfÃ¨re lorsque DivePort est destinÃ© Ã Ãªtre intÃ©grÃ© dans une autre application Web. Si cela est nÃ©cessaire, 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-tÃªte empÃªche le navigateur de surveiller le contenu (sniffing) pour dÃ©terminer les types de fichiers tÃ©lÃ©chargÃ©s depuis DivePort.

ParamÃ©trage recommandÃ© :

```
"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 sÃ©curitÃ© mais peut Ãªtre utilisÃ© pour tester des politiques pour l'en-tÃªte Content-Security-Policy.

ParamÃ©trage :

```
"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

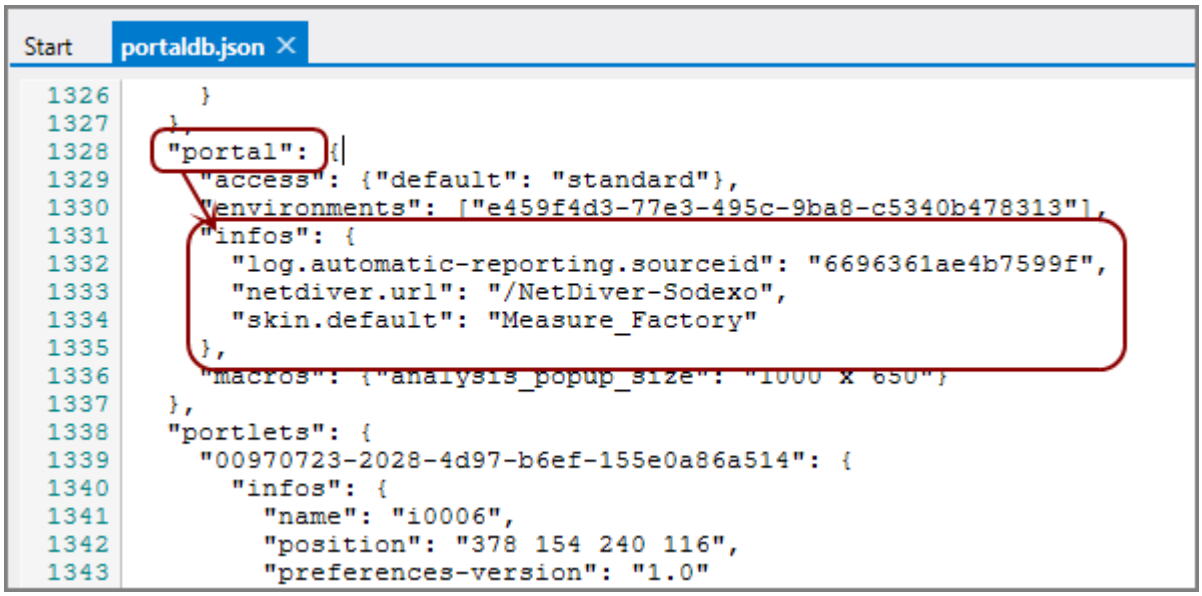
Ã?dition du fichier portaldb

Le fichier *portaldb.json* se trouve dans le rÃ©pertoire *DI\Solution\webdata\<diveport>\database* et contient tous les paramÃ¨tres de configuration du portail. Vous pouvez Ã©diter les attributs dans ce fichier pour modifier des fonctions DivePort.

Remarque : faire une copie de sauvegarde du fichier *portaldb.json* et arrÃªter Apache Tomcat avant d'Ã©diter le fichier.

Les attributs peuvent Ãªtre ajoutÃ©s dans la section portal-infos du fichier portaldb. Pour trouver la section portal-infos dans le fichier *portaldb.json*, rechercher "portal" (en incluant les guillemets) puis chercher "infos".

IMPORTANT : Assurez-vous d'ajouter une virgule Ã la fin de chaque attribut d'info portail, exceptÃ© pour la derniÃ¨re ligne.



Tags

1. DivePort
2. navigateur