

# Multiple Cross-Site Scripting vulnerabilities in Sage XRT Business Exchange



Mickaël Benassouli Antoine Gicquel

www.synacktiv.com

5 boulevard Montmartre 75002 Paris

## **Vulnerabilities description**

#### Sage XRT Business Exchange

Sage XRT Business Exchange is a secure cloud-based platform to manage the entire banking operations of a company. It allows users to process payment chains, manage electronic signatures, and collaborate with their team anywhere, anytime.

#### The issues

Synacktiv has identified multiple vulnerabilities in Sage XRT Business Exchange that allows an attacker to execute JavaScript code in the context of other users' browsers. The attacker needs to be authenticated to reach the vulnerable features.

A vulnerability is present in the *Filters* and *Display model* features (*OnlineBanking* > *Web Monitoring* > *Settings* > *Filters* / *Display models*). The name of a filter or a display model is interpreted as HTML and can thus embed JavaScript code, which is executed when displayed. This is a stored XSS.

Another vulnerability is present in the *Notification* feature (*OnlineBanking* > *Configuration* > *Notifications* and alerts > *Alerts* \*). The name of an alert is interpreted as HTML when displayed, and can thus embed JavaScript code, which is executed when displayed. This is a stored XSS.

Finally, a vulnerability is present in the *File download* feature, accessible via */OnlineBanking/cgi/isapi.dll/DOWNLOADFRS*. When requesting to show the list of downloadable files, the contents of three form fields are embedded in the JavaScript code without prior sanitation. This is essentially a self-XSS.

### Affected versions

The following versions are affected others version have not been tested:

• 12.4.302

#### Timeline

| Date       | Action   |  |  |
|------------|--|--|--|
| 07/06/2022 | Advisory sent to Sage.                                   |  |  |
| 20/06/2022 | Attribution of the following CVE Number : CVE-2022-34323 |  |  |



## **Technical description and Proof-of-Concept**

#### **Vulnerabilities discovery**

The application uses user-supplied data pulled from the database to build web pages that are displayed to other users as part of their normal browsing behavior. However, it does not perform an appropriate encoding before reusing that data. Therefore, an authenticated attacker can create records that will be stored and, once inserted in the final pages, will tamper with their normal content and behavior.

Stored XSS were identified on the following endpoints:

• Filters and Display Models

Sage XRT Business Exchange has a *Filters* feature, accessible via *OnlineBanking* > *Web Monitoring* > *Settings* > *Filters*. When injecting malicious HTML in the name of a filter, it gets interpreted in the *Filters* feature home page:

| $\leftarrow \rightarrow \mathbf{G}$                                   | OA https://   | .em.cloud-by-sag   |
|---|---|--|
| Sage XRT B  | usiness Exchang   | e  |
| Accueil Paramétrage   | <ul> <li>Suivi des flux -</li> </ul>                                  |  |
| Pour créer un filtre, vous c<br>fois toutes les informations          | levez au préalable fournir les é<br>s fournies, cliquez sur le boutor | léments qui permettront d'identifier є<br>n ' Enregistrer '. |
| Identification  |   |  |
| Libellé : <input o<="" td=""/> <td>nfocus=alert(1)&gt;</td> <td></td> | nfocus=alert(1)>  |  |
| Type de filtre : Fichiers   | i émis 🗸 🗸  |  |
| Définition du filtre  |   |  |
| Cet écran permet de filtrer   | la liste de fichiers. Pour créer                                      | un filtre, vous devez définir les critèr                     |
| Application   |   |  |
| Entité  |   |  |
| Protocole   |   |  |
| Service   |   |  |
| Client  |   |  |
| Montant : Entre 1   | et 2  |  |
| Application   |   |  |
| 🗹 Filtre par défaut   |   |  |
| Utilisation du filtre :   |   |  |
|   | <ul> <li>Uniquement par celui</li> </ul>                              | i qui l'a créé   |
|   | <ul> <li>Toute personne habil</li> </ul>                              | itée   |
| Enregistrer   |   |  |

Illustration 1: Malicious HTML injected in the Libellé (french for Label) field



| Second Restance     Accend   Page 1/1 - 1 dement(s) trouvé(s)   Tot ésuitats par page     Tot ésuitats par page   Accend filtre   Pour ajouter un filtre, eliquez sur le bouton ' Ajouter un filtre '     Ajout d'un filtre   Pour ajouter un filtre, eliquez sur le bouton ' Ajouter un filtre '   Couter un filtre   (a)  | $\leftarrow$ $\rightarrow$ C O A https://  | e.  | m.cloud-by-sage.fr        | /OnlineBar        | iking/cgi    | /isapi.dll   | ☆           |
|---|--|---|---------------------------|-------------------|--------------|--------------|-------------|
| Accuell Paramétrage Suivi des flux •<br>Les écrans de sélection de Suivi des flux personnalisés. Il est également possible de définir un filtre par défaut en cliquant sur le boutor<br>tétai d'un filtre, le modifier ou le supprimer, cliquez sur sa description.<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Dage 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>Les | Sage XRT Business Exch   | ange  |                           |                   |              |              |             |
| Les écrans de sélection de Suivi des flux peuvent être personnalisés. Il est également possible de définir un filtre par défaut en cliquant sur le bout<br>tetai d'un filtre, le modifier ou le supprimer, cliquez sur sa description.<br>Liste des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>20 résultats par page<br>R R 1 N N 1 N 1 N 1 N 1 N 1 N 1 N 1 N 1   | Accueil Paramétrage - Suivi des flux -   |   |                           |                   |              |              |             |
| Liste des filtres - Page 1/1 - 1 élément(s) trouvé(s)<br>20 résultats par page K 1 3 3 3<br>1d Libélié Type de filtre Utilisation du filtre Statut<br>75 Fichiers émis Uniquement par celui qui l'a créé Filtre par défaut<br>Ajout d'un filtre<br>Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '<br>Ajouter un filtre<br>Pour ajouter un filtre duite du filtre '<br>Ajouter un filtre .<br>CK  | Les écrans de sélection de Suivi des flux peuvent<br>détail d'un filtre, le modifier ou le supprimer, clique | être personnalisés. Il<br>z sur sa description. | est également possible de | définir un filtre | par défaut e | n cliquant s | ur le bouto |
| 20 v résultats par page       K ( ) X       X       X         1       Litellé       Type de fittre       Utilisation du fittre       Statut         75       Fichiers émis       Uniquement par celui qui l'a créé       Fittre par défaut         Ajout d'un fittre       Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '       Ajouter un filtre         Pour ajouter un filtre       .em.cloud-by-sage.fr       1  | Liste des filtres - Page 1/1 - 1 élément(s) trouvé(  | s)  |                           |                   |              |              |             |
| Ideele     Pype de linte     Oblisation du linte     Statut       75     Fichiers émis     Uniquement par celui qui l'a créé     Filtre par défaut       Ajout d'un filtre     Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '     Ajouter un filtre  | 20 ✓ résultats par page  | Turo da filma                                   |                           | <u>N N N</u>      |              | Create       |             |
| Ajout d'un filtre<br>Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '<br>Ajouter un filtre<br>em.cloud-by-sage.fr<br>1   | 75   | Fichiers émis                                   | Uniquement par celu       | i qui l'a créé    | _            | Filtre       | par défauí  |
| Ajout d'un filtre<br>Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '<br>Ajouter un filtre   |  |   |                           |                   |              |              |             |
| Pour ajouter un filtre, cliquez sur le bouton ' Ajouter un filtre '<br>Ajouter un filtre<br>em.cloud-by-sage.fr<br>1  | Ajout d'un filtre  |   |                           |                   |              |              |             |
| Ajouter un filtre<br>.em.cloud-by-sage.fr<br>1  | Pour ajouter un filtre, cliquez sur le bouton ' Ajoute   | r un filtre '                                   |                           |                   |              |              |             |
| em.cloud-by-sage.fr<br>1  | Ajouter un filtre  |   |                           |                   |              |              |             |
| em.cloud-by-sage.fr   |  |   |                           |                   |              |              |             |
| em.cloud-by-sage.fr   |  |   |                           |                   |              |              |             |
| 1<br>OK   | •  | .en   | n.cloud-by-sage.fr        |                   |              |              |             |
| ок с  | 1  |   |                           |                   |              |              |             |
| ок <mark>ок</mark> ал   |  |   |                           |                   |              | _            |             |
|   |  |   |                           |                   |              | 0            |             |

Illustration 2: Interpretation of the HTML in the Filters home page

The same issue is present in the Display models feature (OnlineBanking > Web Monitoring > Settings > Display models):

| $\leftarrow \   \rightarrow$        | C  | ÓA             |                             | .em. <b>clo</b> | ud-by-sage.fr/OnlineBanking/cgi/i                            | sapi.dll/FrameMain          |
|-------------------------------------|--|----------------|-----------------------------|-----------------|--|-----------------------------|
| sage                                | XRT Business I   | Exchan         | ige                         |                 |  |                             |
| Accueil                             | Paramétrage - Suivi des  | flux ▼         |                             |                 |  |                             |
| Pour créer                          | un modèle, vous devez définir  | les informatio | ons que vous souhaitez voir | figurer sur l   | es états du Suivi des flux. Pour cela, sélectionne           | z les données que vous souh |
| Identifica                          | tion   |                |                             |                 |  |                             |
| Libellé :                           | <input onfocus="ale&lt;/td"/> <td>rt(1)&gt;</td> <td></td> <td></td> <td></td> <td></td> | rt(1)>         |                             |                 |  |                             |
| Type de                             | modèle : Fichiers émis 🗸   | ·              |                             |                 |  |                             |
| Caractéri                           | istiques   |                |                             |                 |  |                             |
| List<br>Ap<br>Cli<br>Da<br>Da<br>En | te des champs disponibles :<br>plication<br>ent<br>te<br>te Exec/Echéance                |                |                             | <               | fficher les champs dans cet ordre :<br>Déplacer vers le haut | Déplacer vers le bas        |
| Applicatio                          | on defend  |                |                             |                 |  |                             |
| L Mode                              | ele par detaut   |                |                             |                 |  |                             |
| Enr                                 | egistrer   |                |                             |                 |  |                             |

Illustration 3: Malicious HTML injected in the Libellé (french for Label) field



| $\leftarrow \ \rightarrow \ \mathbf{G}$ | ○ A https://                | .em. <b>cloud-by-sage.fr</b> /OnlineBanking/cgi/isapi.dll/ 😭 | 3 |
|---|-----------------------------|--|---|
| Sage XRT E                              | Business Exchange           |  |   |
| Accueil Paramétrage                     | s → Suivi des flux →        |  |   |
| Identification                          |                             |  |   |
| Libellé :                               |                             |  |   |
| Type de modèle : <sup>Fic</sup>         | hiers émis                  |  |   |
| Caractéristiques                        |                             |  |   |
| Liste des champs d                      | sponibles : Afficher les ch | namps dans cet ordre :                                       |   |
| Client<br>Date                          | Application                 |  |   |
| Entité<br>Fichier d'origine             | e                           |  |   |
|   | Déplacer vers               | le haut Déplacer vers le bas                                 |   |
| Application                             | •                           | .em.cloud-by-sage.fr   |   |
| Modèle par défaut                       | 1                           |  |   |
| _                                       |                             | ок   |   |
| Modifier                                | Supprii.                    |  |   |

Illustration 4: Interpretation of the HTML in the Display models edit page



#### • Notifications and alerts:

This feature is available via the following path in the UI: *OnlineBanking > Configuration > Notifications and* alerts. Its purpose is to notify an administrator, for instance when a transaction is made. Once again, the name of an alert is interpreted as plain HTML when displayed back:

| $\leftarrow \rightarrow G$   | 🛇 🖰 https://  | .em.cloud-by-sage.fr/OnlineBanking/cgi/isa 🏠   |  |  |  |  |  |
|--|---|--|--|--|--|--|--|
| Sage XRT BI  | usiness Exchange  |  |  |  |  |  |  |
| Accueil Paramètres ut  | tilisateur - Notifications et al  | iertes -   |  |  |  |  |  |
| Un certain nombre de tâch<br>événements devant déclen<br>cliquant sur 'Plus d'options'<br>Alerte | es étant automatisées, vous pouve<br>icher une alerte, définissez pour ch<br>'. Cliquez ensuite sur le bouton 'En | z définir les personnes à informer via l'envoi d'alertes en fonction de l'événeme<br>aque alerte, les groupes de destinataires. Vous pouvez affiner la définition de l<br>registrer'. La fréquence d'envoi des alertes dépend d'une tâche planifiée. |  |  |  |  |  |
| Libellé :  |   | <input onfocus="alert(1)"/>  |  |  |  |  |  |
| Application :  |   | Virement compte v  |  |  |  |  |  |
| Catégorie de trans   | action :  | Virements de trésorerie 🗸  |  |  |  |  |  |
| Alertes sur statut de trans  | saction   |  |  |  |  |  |  |
|  | 1er et 2nd gr   | oupes de destinataires   |  |  |  |  |  |
| Statut 'A complét  | ier'  | · ·  |  |  |  |  |  |
| Statut 'En attente   | ə'  | • •  |  |  |  |  |  |
| Statut 'Validé'  |   | • •  |  |  |  |  |  |
| Statut 'Autorisé'<br>Illustration 5: Malicio   | ous HTML injected in th   | → ↓<br>ne <i>Libellé</i> (french for <i>Label</i> ) field  |  |  |  |  |  |



| $\leftarrow \rightarrow$              | С  | 08         | https://                                     | .en                                  | n. <b>cloud-by</b>                | -sage.                  | <b>fr</b> /Online              | Bankir                | ng/cgi/is                  | sap 🛣                    |                   |
|---------------------------------------|--|------------|--|--------------------------------------|-----------------------------------|-------------------------|--------------------------------|-----------------------|----------------------------|--------------------------|-------------------|
| sag                                   | e XRT BI                                   | usine      | ss Exchan                                    | ge                                   |                                   |                         |                                |                       |                            |                          |                   |
| Accueil                               | Paramètres ut                              | ilisateur  | <ul> <li>Notifications</li> </ul>            | et alertes 👻                         |                                   |                         |                                |                       |                            |                          |                   |
| La créatio<br>le cycle d<br>l'alerte. | on d'alertes vous j<br>e traitement), et s | ermet de   | notifier une ou plus<br>ins critères. Pour c | ieurs personnes<br>réer une nouvelle | en fonction de<br>alerte, cliquez | la pertin<br>z sur le b | ence des info<br>outon 'Ajoute | rmations<br>r une ale | s que vous<br>rte'. Pour r | souhaitez<br>modifier ou | recevoi<br>suppri |
| Liste de                              | es alertes - Page :                        | 1/1        |  |                                      |                                   |                         |                                |                       |                            |                          |                   |
| 20                                    | <ul> <li>résultats par p</li> </ul>        | age        |  |                                      | K                                 | < 1                     | > >> >>                        | 4                     |                            |                          |                   |
| Libellé                               |  |            |  |                                      |                                   |                         | Application                    |                       |                            |                          |                   |
|                                       |  |            |  |                                      |                                   |                         | Virement cor                   | npte à c              | ompte                      |                          |                   |
| test                                  |  |            |  |                                      |                                   |                         | Virement cor                   | npte à c              | ompte                      |                          |                   |
| Ajout d                               | une alerte                                 |            |  |                                      |                                   |                         |                                |                       |                            |                          |                   |
| Pour ajou                             | iter une alerte, cli                       | quez sur l | e bouton 'Ajouter u                          | ne alerte'.                          |                                   |                         |                                |                       |                            |                          |                   |
| Ajout                                 | er une alerte                              |            |  |                                      |                                   |                         |                                |                       |                            |                          |                   |
|                                       |  |            | •  | .em                                  | .cloud-by-s                       | sage.fr                 |                                |                       |                            |                          |                   |
|                                       |  |            | 1  |                                      |                                   |                         |                                |                       |                            |                          |                   |
|                                       |  |            |  |                                      |                                   |                         |                                |                       |                            | ок                       |                   |

Illustration 6: Interpretation of the HTML in the Alerts home page



• File download:

This feature is available at the following URI: /OnlineBanking/cgi/isapi.dll/DOWNLOADFRS. When clicking the "Display the list" button, a POST request is sent to the server. The values of the OVPNAME, JDAY and FREQUENCY parameters of the request are then embedded directly in the JavaScript of the page returned by the server, as demonstrated here:

- The request:

```
POST /OnlineBanking/cgi/isapi.dll/DOWNLOADFRS HTTP/2
Host: **********.em.cloud-by-sage.fr
Cookie: SESSIONID=UR****[...]****==; _ga=GA1.2****[...]****98; _gid=GA1.2****[...]****62;
i18next=fr-FR
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
[...]
STATUS=&FUNCNAME=&TITLE=&PRINT_ID=&PRINT_NAME=&INF0=YES&LIST=YES&SERVICE=UPLOAD&OVPNAME=.
%27%3Balert%281%29%3B%27&DATE=.&JDAY=.%27%3Balert%282%29%3B%27&FREQUENCY=.%27%3Balert
%283%29%3B%27
```

- Extract from the server's response:

```
<!--
[...]
// ----
function InitForm() {
document.FormDOWNLOAD.OVPNAME.value=
'.';alert(1);'';document.FormDOWNLOAD.JDAY.value=
'.';alert(2);'';document.FormDOWNLOAD.FREQUENCY.value =
'.';alert(3);'';ChangeDate();
}
[...]
// -->
```



Illustration 7: First alert (parameter OVPNAME)



|  | ○ 읍 ब https://   | .em. <b>cloud-by-sage.fr</b> /OnlineBanking/cgi/isapi 😭                     |
|--|--|---|
| Pour obtenir la liste de                 | s fichiers à disposition, sélectionnez le                                    | type de service à récupérer puis cliquez sur le bouton "Afficher la liste". |
| Critères de sélection                    |  |   |
| Type du fichier à rece<br>Origine du fic | voir : E - Fichiers à envoyer à la ban<br>hier : Toutes v<br>Date : Toutes v | we v Afficher is liste  |
| Liste des fichiers dis                   | ponibles   |   |
| Id. du fichier                           |  | Nom du fichier  |
| Extraire Tous                            | Accun  |   |
|  | •  | .em.cloud-by-sage.fr  |
|  | 2  |   |
|  | Ne pas a<br>à nouve  | utoriserem.cloud-by-sage.fr à vous solliciter<br>au<br>OK                   |

Illustration 8: Second alert (parameter JDAY)



Illustration 9: Third alert (parameter FREQUENCY)



#### Impact

Depending on the cookies attributes, an authenticated attacker could either steal an administrator cookie or perform actions on the website on behalf of an administrator, such as adding a new user and granting them administrator privileges. With their newly obtained administrator privileges, an attacker would be able to gain remote command execution as detailed in the advisory on multiple authenticated blind SQL Injections in XRT.