



CENTRE GOUVERNEMENTAL  
DE CYBERDÉFENSE

# SI-10

Validation de la saisie d'information

Juill. 2026



# Intégrité des systèmes et des données

*System and Information Integrity*

## SI-10 – Validation de la saisie d'information (-F-)

### Énoncés :

Vérifier la validité des saisies d'information suivantes : [\[Affectation : saisies d'information dans le système définies par l'organisation\]](#).

**Responsable :** Aucun

### Discussion :

Des règles de vérification de la validité de la syntaxe et des valeurs sémantiques des saisies du système – jeu de caractères, longueur, plage numérique, valeurs acceptables – sont mises en place pour s'assurer qu'elles respectent les définitions précisées en matière de format et de contenu. Par exemple, si l'organisation indique que seules les valeurs numériques entre 1 et 100 sont acceptées dans le champ d'une application donnée, les valeurs « 387 », « abc » ou « %K% » seront des saisies non valides qui seront refusées par le système. Les entrées valides varieront probablement d'un champ à l'autre dans l'application logicielle. Les applications suivent habituellement des protocoles bien définis qui utilisent des messages structurés (c'est-à-dire des commandes ou des requêtes) pour établir des communications entre les modules logiciels ou les composants de système. Les messages structurés peuvent contenir des données brutes ou non structurées parsemées de métadonnées ou d'information de contrôle. Si des applications logicielles utilisent des données saisies par un attaquant pour construire des messages structurés sans encoder de tels messages de manière adéquate, l'attaquant peut alors insérer des commandes malveillantes ou des caractères spéciaux qui pourraient faire en sorte que les données soient interprétées comme de l'information de contrôle ou des métadonnées. Par conséquent, le module ou le composant qui reçoit les saisies corrompues effectuera des opérations erronées ou interprétera les données incorrectement. Les saisies transmises aux interpréteurs sont filtrées au préalable pour empêcher que leur contenu soit interprété accidentellement comme des commandes. La validation des saisies permet de s'assurer que les saisies sont exactes et correctes et de prévenir des attaques, comme les scripts intersites et toute une gamme d'attaques par injection.