VIRTUAL

OSSIR – 12/12/2017

Stéphane Jourdois / Romain Castel

digital security | econocom

Digital Security est structurée autour de **2 expertises**, portées par **6 prestations** différentes

EXPERTISES

Sécurité du SI

Sécurité des objets connectés (IoT)

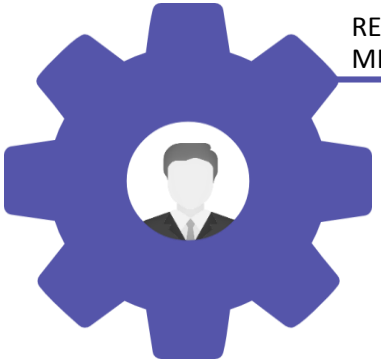
PRESTATIONS

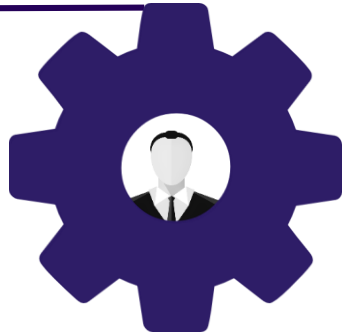
- Audit
- Conseil
- Formations
- Services CERT
- Sécurité Opérationnelle
- Intégration & Projet

Le test d'intrusion

Les objectifs

Le point de jonction





LIVRABLES

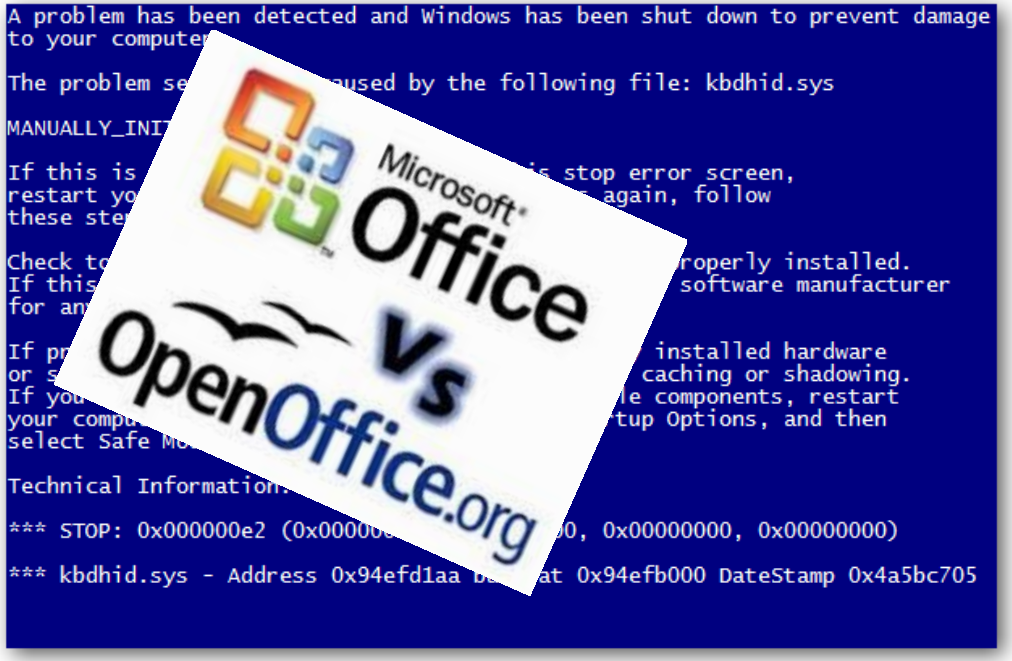
Le pentesteur

La production des livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment.

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: kbdhid.sys

MANUALLY_INITIATED_CRASH

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use safe mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical Information:

*** STOP: 0x000000e2 (0x00000000, 0x00000000, 0x00000000, 0x00000000)

*** kbdhid.sys - Address 0x94efd1aa base at 0x94efb000 DateStamp 0x4a5bc705
```

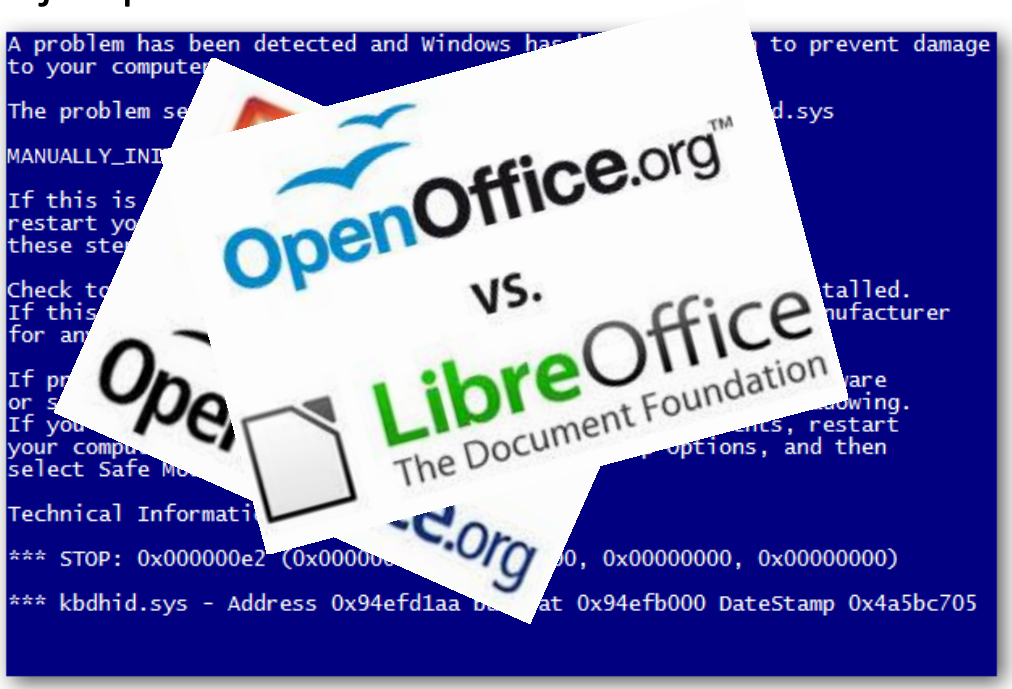
Le pentesteur

La production des livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment.



Le pentesteur

La production des livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment.



Le pentesteur

La production de livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment.

Le pentesteur

La production de livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment

Le pentesteur

La production de livrables est un corollaire obligatoire à toutes ses missions, mais il feint de l'ignorer jusqu'au dernier moment

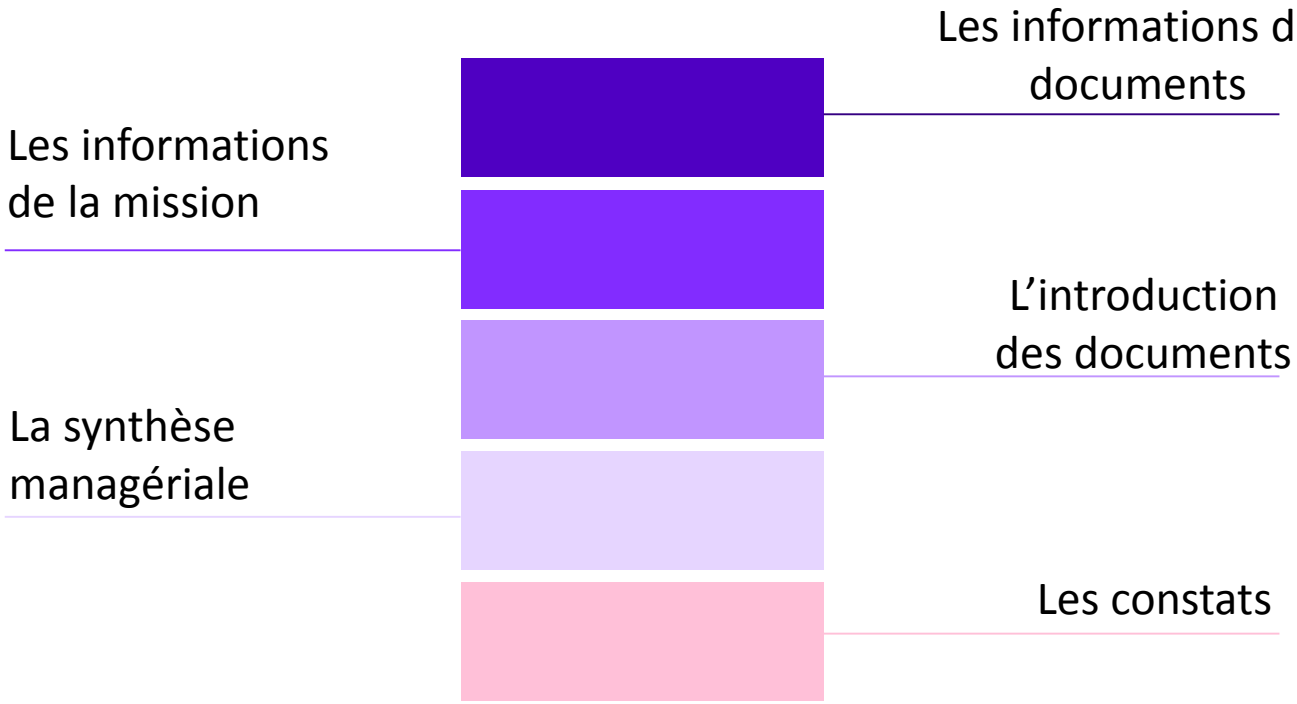
Les moments d’une mission

Le cadrage			
Les tests			
La formalisation	 PLUS RAPIDE	 PLUS HOMOGENE	 PLUS EFFICACE
La restitution			

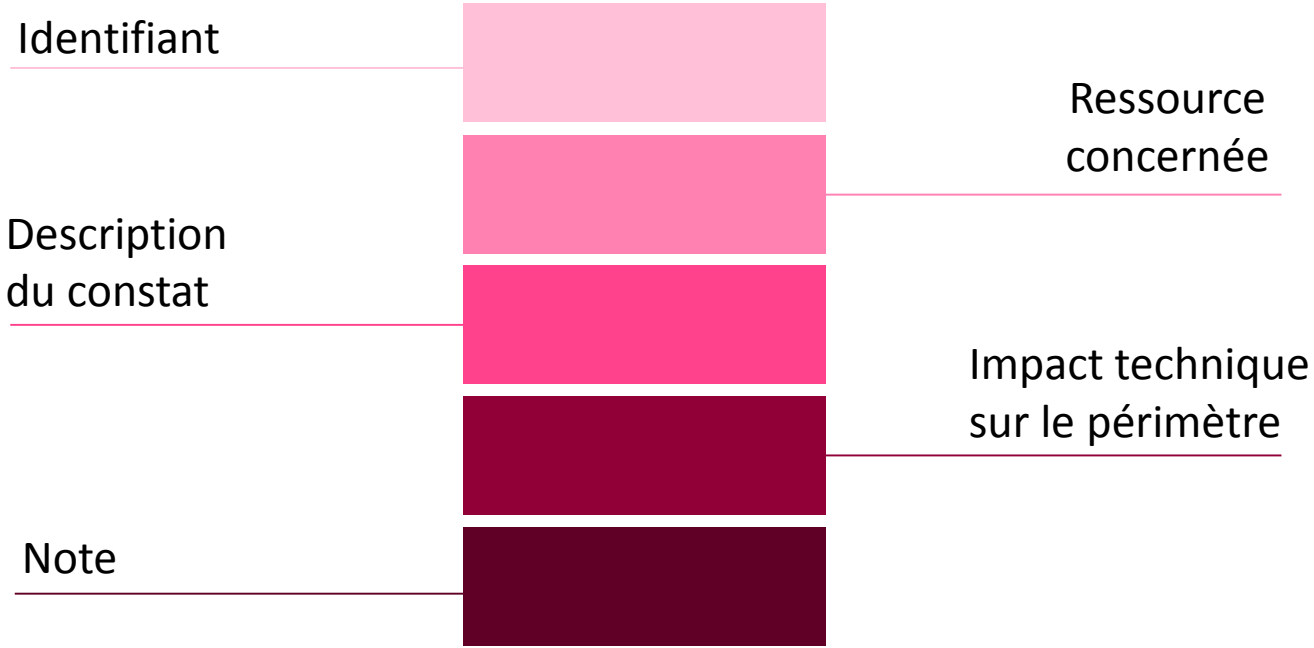
Démo

Cahier des charges

La définition des informations nécessaires



La définition d’un Constat



Le fichier d'entrée en trois parties

```
<Constats Statut="prerapport" Lang="fr" Virralversion="1.1" Lasocietequiaudite="Digital Security" Gradation="Gradation">
    <Reference>TODO</Reference>
    <NomClient>CLIENT</NomClient>
    <TitreProjet>Authentification Web</TitreProjet>
    <TitrePresentation>Restitution</TitrePresentation>
    <TitreDocument>Audit de sécurité</TitreDocument>
    <DescriptionDocument>Rapport d'audit</DescriptionDocument>
    <VersionRapport>1.0</VersionRapport>
    <AuteursDocument>…
    <DateAudit>01/06/2014</DateAudit>
    <DatePresentation>[A définir]</DatePresentation>
    <MajsDocument>
        <MajDocument>…
    </MajsDocument>
    <Auditeurs>
            <Contact>…
    </Auditeurs>
    <Commanditaires>
            <Contact>…
    </Commanditaires>
    <Audites>
        <Contact>…
    </Audites>
    <Diffusions>
        <Diffusion>…
    </Diffusions>
    <DocumentsReference>
        <DocumentReference>…
    </DocumentsReference>
```

```
<ObjetDuDocument>
</ObjetDuDocument>

<Demarche>
</Demarche>

<Perimetre>
</Perimetre>

<Evaluation>
</Evaluation>

<Niveau></Niveau>

<Bilan></Bilan>

<Positifs>
    <Positif></Positif>
</Positifs>

<Negatifs>
    <Negatif></Negatif>
</Negatifs>
```

```
<Section Titre="je suis une section avec vuln">
    <Constat Titre="Je permet d'ecrire du texte">
        <Text>

        </Text>
    </Constat>
    <Vuln Impact="1" Pop="1" Diff="1">
        <Titre> </Titre>
        <Ressource> </Ressource>
        <Introduction Titre="">
            <Text> </Text>
        </Introduction>
        <Description>   </Description>
        <ImpactTechnique>   </ImpactTechnique>
    </Vuln>

    <Reco Complexite="1">
        <Titre> </Titre>
        <Correcteur> </Correcteur>
        <Description>   </Description>
    </Reco>
</Section>
```

Version 0.1

Proof of concept

LaTeX

Avec

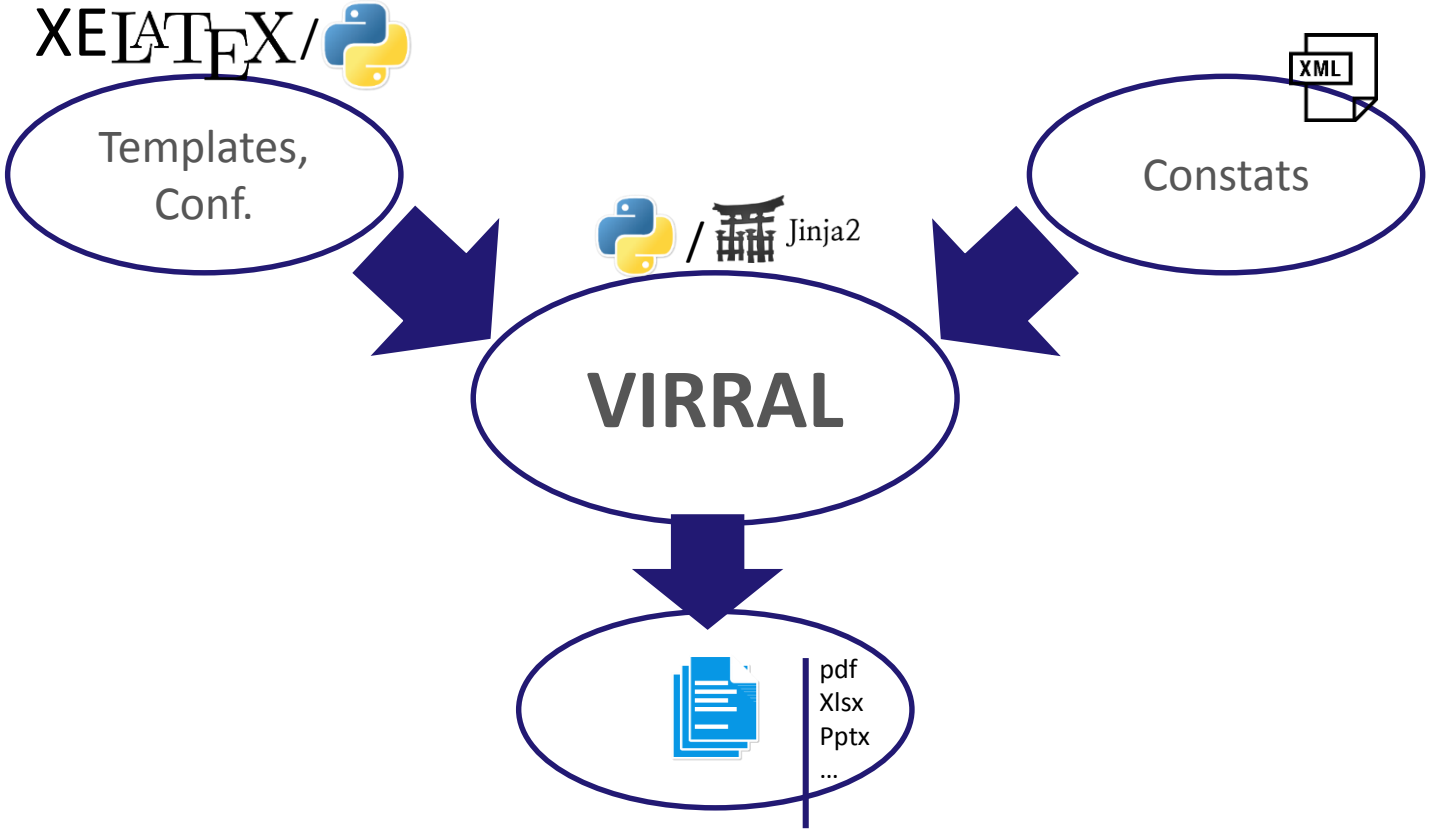
PDF LaTeX

et

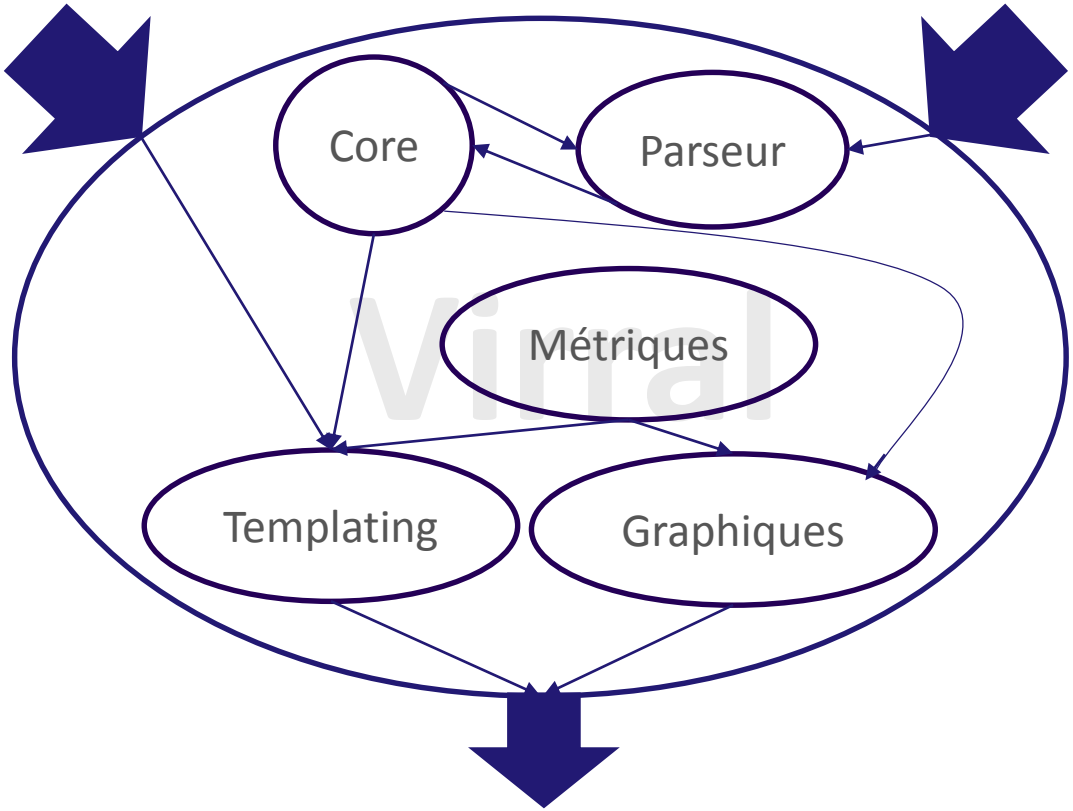
Des includes {
dans des includes {
dans des includes{

Très peu d'optimisation du temps !

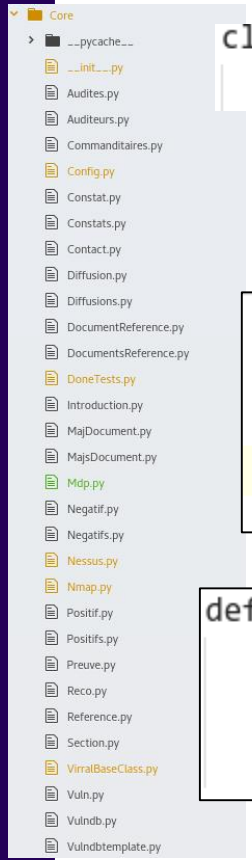
Version 1.0


XELaTeX/
Templates,
Conf.
XML
Constats
/ Jinja2
VIRRAL
pdf
Xlsx
Pptx
...

Version 1.0



Le moteur

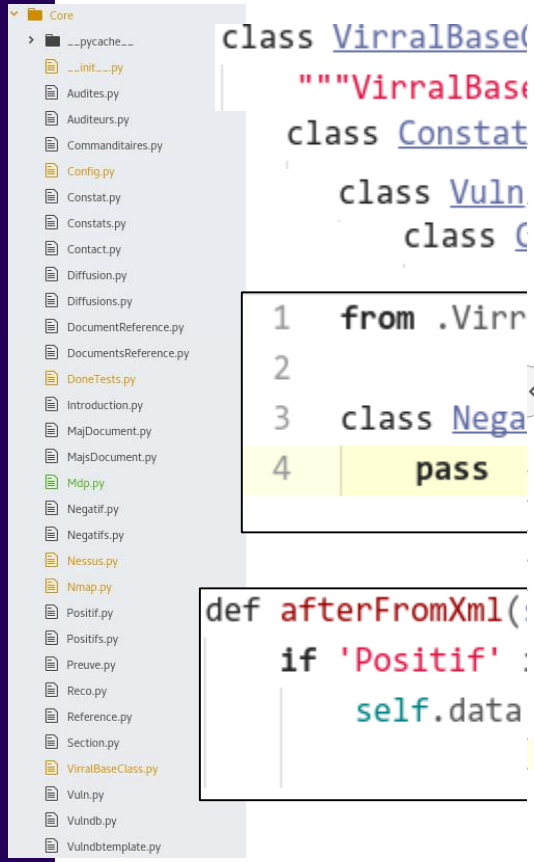



```
class VirralBaseClass():
    """VirralBaseClass class."""
    class Constats(VirralBaseClass):
        class Vuln(VirralBaseClass):
            class Commanditaires(VirralBaseClass):
```

```
1  from .VirralBaseClass import VirralBaseClass
2
3  class Negatif(VirralBaseClass):
4      pass
```

```
def afterFromXml(self):
    if 'Positif' in self.data and self.data['Positif'].__class__.__name__ == "Positif":
        self.data['Positif'] = [ self.data['Positif'] ]
```

Le moteur




```
class VirralBase(
    """VirralBase
    class Constat
        class Vuln
            class C
```

```
1  from .Virr
2
3  class Nega
4      pass
```

```
def afterFromXml(
    if 'Positif'
        self.data
```

```
230  # Use this CLASS METHOD to get a Virral Core Object from an xml Element node
231  @classmethod
232  def fromXml(cls, node, params = None):
233      if 'Virral.Core.' + node.tag in sys.modules:
234          Object = getattr(sys.modules['Virral.Core.' + node.tag], node.tag)(params)
235      elif 'Virral.NessusCore.' + node.tag[0] + node.tag[1:] in sys.modules:
236          Object = getattr(sys.modules['Virral.NessusCore.' + node.tag[0] + node.tag[1:]], node.tag[0] + node.tag
237      elif 'Virral.QualysCore.' + node.tag[0] + node.tag[1:] in sys.modules:
238          Object = getattr(sys.modules['Virral.QualysCore.' + node.tag], node.tag)()
239      else:
240          Object = VirralBaseClass(params)
241      Object.beforeFromXml()
242      Object.tag = node.tag
243      if node.text is None and len(node) == 0:
244          Object.text = "TODO"
245      else:
246          Object.text = node.text
247      for attr in node.attrib:
248          Object.attributes[attr] = node.attrib[attr]
249      for childnode in node:
250          child = cls.fromXml(childnode, Object.params)
251          Object.rawData.append(child)
252          if childnode.tag in Object.data and Object.data[childnode.tag] is not None:
253              if isinstance(Object.data[childnode.tag],list):
254                  Object.data[childnode.tag].append(child)
255              else:
256                  Object.data[childnode.tag] = [ Object.data[childnode.tag], child ]
257          else:
258              Object.data[childnode.tag] = child
259      Object.afterFromXml()
260
261      return Object
```

Notre système de gradation

Severite.py

≈ Impact x Menace

Priorité.py

≈ Complexité x Sévérité Max.

Menace.py

≈ Population x Difficulté d'exploitation

Notre système de gradation

Severite.py

Sévérité		Impact			
		Très fort	Fort	Moyen	Faible
Menace	Très forte	critique	critique	majeure	moyenne
	Forte	critique	majeure	moyenne	mineure
	Moyenne	majeure	moyenne	moyenne	mineure
	Faible	moyenne	mineure	mineure	mineure

Menace.py

Menace		Population			
		Internet	Internet autorisé	Intranet	Intranet autorisé
Difficulté dexploitation	Facile	Très forte	Forte	Forte	Forte
	Moyenne	Très forte	Forte	Moyenne	Moyenne
	Difficile	Forte	Moyenne	Moyenne	Faible
	Très Difficile	Moyenne	Moyenne	Faible	Faible

Priorite.py

Priorité (P) = complexité de mise en œuvre × sévérité de la vulnérabilité

Valeur calculée	Intitulé	Description
$P > 10$	Immédiatement	La recommandation devrait être appliquée en urgence.
$5 < P < 10$	Court terme	La recommandation ne peut être mise en œuvre sans un minimum de vérifications, mais devrait néanmoins être mise en place dans un délai court.
$P < 5$	Moyen Terme	La recommandation nécessite une étude complémentaire avant d'être mise en œuvre, ou peut être embarquée dans un train de modifications ultérieur, sans urgence significative.

Vues des systèmes de gradation

Impact	Population	Difficulté	Menace	Sévérité
2/4	2/4	2/4	2/4	2/4
Moyen	Intranet	Difficile	Moyenne	moyenne

```
<Vuln Impact="2" Pop="2" Diff="2">
```

Gravité	Pop	Diff	Probabilité	Risque
5/5	2/4	4/4	3/5	4/4
Catastrophique	Intranet	Facile	Assez probable	Risques inacceptables

```
<Vuln Diff="4" ImpactX="5" Pop="2">
```

Impact	Probabilité	Risque
3/10	4/10	1/4
Crit 3	Intranet habilité	mineure

```
<Vuln CVSSAccessComplexity="0.71" CVSSAccessVector="0.395" CVSSAuthentication="0.704"
CVSSAvaibilityImpact="0" CVSSConfidentialityImpact="0.275" CVSSIntegrityImpact="0">
```

Développement des systèmes de gradation

```
class Impact(BaseMetric):
    type = "Impact"

    params = {
        'seuils': [
            { 'seuil': 0, 'color': Color('000000'), 'colorOver': Color('ffffff'), 'fr': 'nom1', 'en': 'name1' },
            { 'seuil': 1, 'color': Color('606060'), 'colorOver': Color('ffffff'), 'fr': 'nom2', 'en': 'name2' },
            { 'seuil': 2, 'color': Color('a0a0a0'), 'colorOver': Color('000000'), 'fr': 'nom3', 'en': 'name3' },
            { 'seuil': 3, 'color': Color('ffffff'), 'colorOver': Color('000000'), 'fr': 'nom4', 'en': 'name4' },
        ],
        'name':{'fr':'Impact', 'en':'Impact'},

    }
```

Développement des systèmes de gradation

```
class Impact(BaseMetric):
    type = "Impact"

    params = {
        'seuils': [
            { 'seuil': 0, 'color': Color('000000'), 'colorOver': Color('ffffff'), 'fr': 'nom1', 'en': 'name1' },
            { 'seuil': 1, 'color': Color('606060'), 'colorOver': Color('ffffff'), 'fr': 'nom2', 'en': 'name2' },
            { 'seuil': 2, 'color': Color('a0a0a0'), 'colorOver': Color('000000'), 'fr': 'nom3', 'en': 'name3' },
            { 'seuil': 3, 'color': Color('ffffff'), 'colorOver': Color('000000'), 'fr': 'nom4', 'en': 'name4' },
```

```
class Severite(BaseMetric):
    type = "Severite"
    params = {
        'fr': '''Le tableau ci-dessous présente les différents niveaux de difficulté d'exploitation en termes de c
        'requires': [ 'Menace', 'Impact' ],
        'seuils': [
            { 'seuil': lambda m, i: 0  < m * i, 'color': Color('000000'), 'colorOver': Color('ffffff'), 'fr': 'min
            { 'seuil': lambda m, i: 3  < m * i, 'color': Color('606060'), 'colorOver': Color('ffffff'), 'fr': 'moy
            { 'seuil': lambda m, i: 7  < m * i, 'color': Color('a0a0a0'), 'colorOver': Color('000000'), 'fr': 'maj
            { 'seuil': lambda m, i: 10 < m * i, 'color': Color('ffffff'), 'colorOver': Color('000000'), 'fr': 'cri
        ],
        'name':{'fr':'Severite', 'en':'severity'}
    }
```

L’interconnexion avec une base de connaissances

Objectif faciliter la relecture

Faire en sorte que les vulnérabilités soient toujours de la même qualité d’un pentesteur à un autre

Laisser des libertés

L’interconnexion avec une base de connaissances

L’interconnexion avec une base de connaissances

```
Voici un exemple d'exploitation de cette attaque sur le formu
§§xsssurformulaire::  AJOUTER SCREENSHOT FORMULAIRE§§

Quand une charge malveillante est ajoutée à ce formulaire, ce

§§xssdanshtml::  AJOUTER SCREENSHOT SOURCE HTML§§

Effectivement, la charge est déclenchée et un pop-up apparait

§§xssexploitation::  AJOUTER SCREENSHOT EXECUTION CHARGE§§

\textbf{Dans la mesure du temps imparti, il n'a pas été possi
```

L’interconnexion avec une base de connaissances

```
Voici un exemple d'exploitation de cette attaque sur le formu
§§xsssurformu
Quand une cha
§§xssdanshtml
Effectivement
§§xssexploita
\textbf{Dans
```

```
<Vulndb Id="XSS">
<ressource>Liste des ressources consernées</ressource>
<parametresvulnérable>Liste des paramètres vulnérables
        \begin{itemize}
        \item Persistante:
            \begin{itemize}
            \item URL
                \begin{itemize}
                \item Méthode
                \item PARAMS
                \end{itemize}
            \end{itemize}
        \item Non persistante:
            \begin{itemize}
            \item URL
                \begin{itemize}
                \item Méthode
                \item PARAMS
                \end{itemize}
                \end{itemize}
        \end{itemize}</parametresvulnérable>
<xsssurformulaire>AJOUTER SCREENSHOT FORMULAIRE</xsssurformulaire>
<xssdanshtml>AJOUTER SCREENSHOT SOURCE HTML</xssdanshtml>
<xssexploitation>AJOUTER SCREENSHOT EXECUTION CHARGE</xssexploitation>
</Vulndb>
```

L’interconnexion avec une base de connaissances

```
Voici un exemple d'exploitation de cette attaque sur le formu
§§xsssurformu
Quand une cha
§§xssdanshtml
Effectivement
§§xssexploita
\textbf{Dans
```

```
<Vulndb Id="XSS">
<ressource>Liste des ressources consernées</ressource>
<parametresvulnérable>Liste des paramètres vulnérables
        \begin{itemize}
        \item Pers
            \begin
            \item
                \b
                \i
                \i
                \e
            \end{i
        \item Non
            \begin
            \item
                \b
                \i
                \i
                \e
                \e
        \end{itemi
<xsssurformulaire>A
<xssdanshtml>AJOUT
<xssexploitation>A
</Vulndb>
```

Une vulnérabilité de type Cross Site Scripting a été identifiée sur le site. Les paramètres suivants sont vulnérables à cette attaque :Startspec Liste des paramètres vulnérables

- Persistante :
  - URL
    - Méthode
    - PARAMS
- Non persistante :
  - URL
    - Méthode
    - PARAMS

Endspec Voici un exemple d’exploitation de cette attaque sur le formulaire suivant : Startspec AJOUTER SCREENSHOT FORMULAIRE Endspec

Quand une charge malveillante est ajoutée à ce formulaire, celle-ci se retrouve bien interprétée par le navigateur comme l’on peut le voir dans la source HTML :

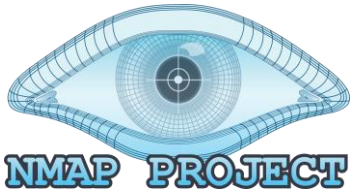
Startspec AJOUTER SCREENSHOT SOURCE HTML Endspec

Effectivement, la charge est déclenchée et un pop-up apparait affichant le contenu des cookies de l’utilisateur lors de la navigation sur le site :

Startspec AJOUTER SCREENSHOT EXECUTION CHARGE Endspec

Démo

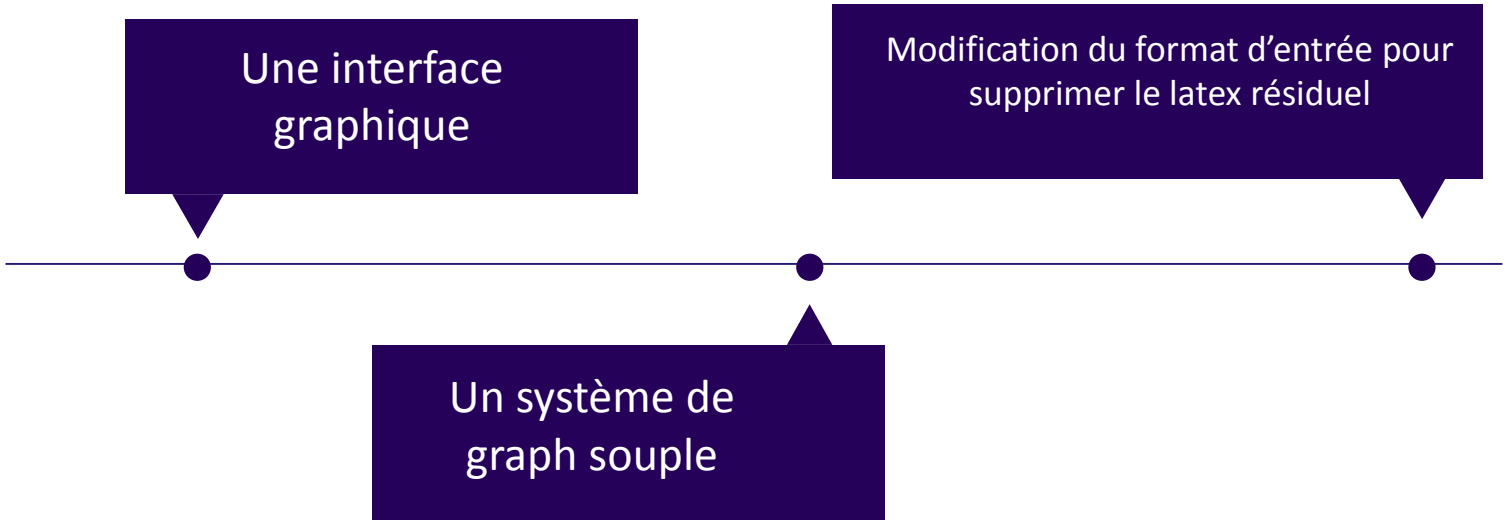
Les plug-ins



Testssl

Pipal

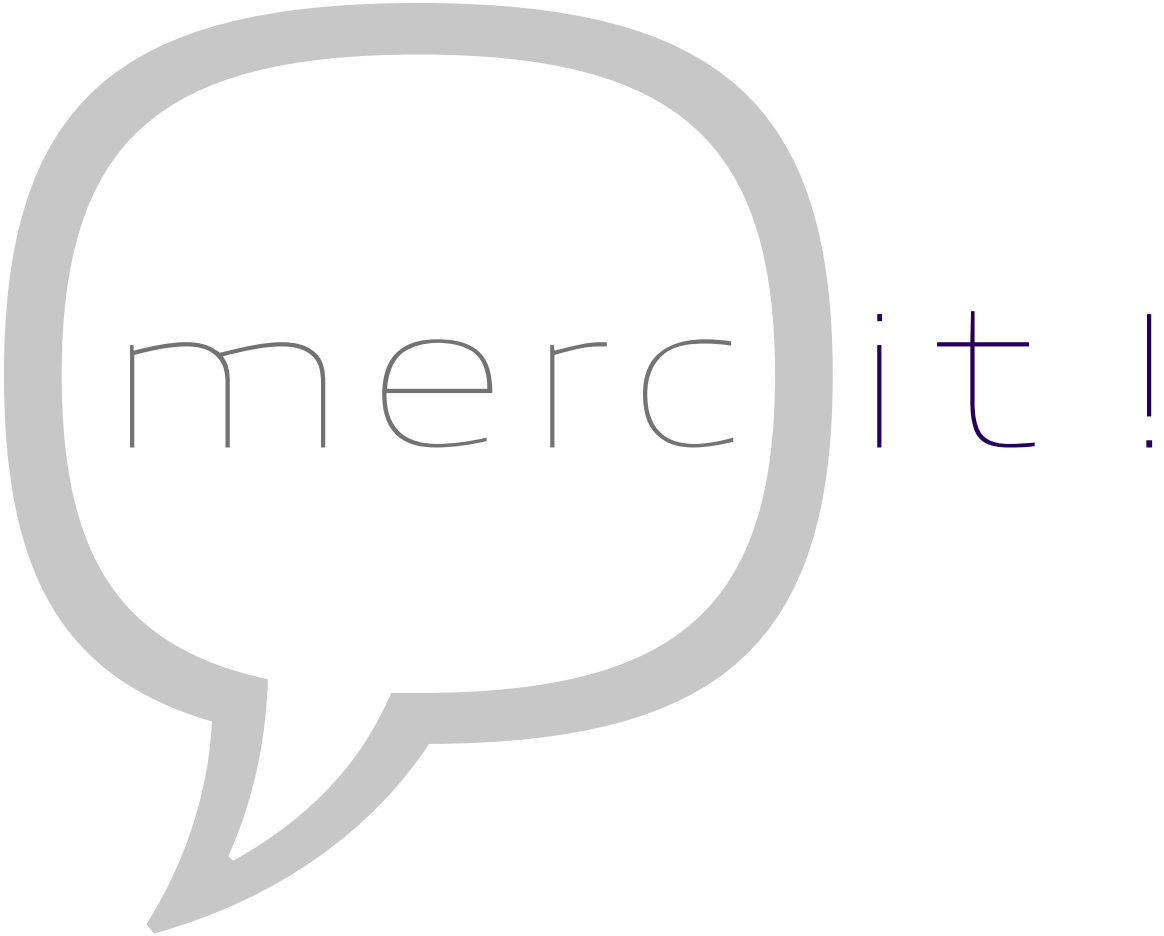
L’avenir


Une interface graphique
Modification du format d’entrée pour supprimer le latex résiduel
Un système de graph souple

Nos objectifs aujourd'hui

- Pas un projet libre… pour l'instant au moins
- Prise de contact avec des acteurs du domaine
- Recherche de « partenaires » intéressés :
  - Auditeurs
  - Commanditaires

Mutualisation de l'effort


merc it !

Contact

Stéphane JOURDOIS
Directeur Technique

Tél. : +33 [0] 1 70 83 85 52
e-mail : stephane.jourdois@digitalsecurity.fr

Contact

Romain CASTEL
Consultant sécurité sénior

Tél. : +33 [0] 1 70 83 85 57
e-mail : romain.castel@digitalsecurity.fr

digital security | econocom

Digital Security - Econocom

@iotcert

www.digitalsecurity.fr