

# Dofus 2 & 3

Rétro-ingénierie et recherche de vulnérabilité



# # Whoami

- DevSecOps @Icodia
- @n0xyne sur Discord
- n0x.cc



TLP:CLEAR



# # Dofus

- MMORPG Français
- Made by Ankama
- 15M joueurs
- 20+ ans



# ## Timeline

- **Dofus 1** : 2004 - 2009
- **Dofus 2** : 2009 - 2024
- **Dofus 3** : Décembre 2024



# ## Communautés RE

## LÉGAL

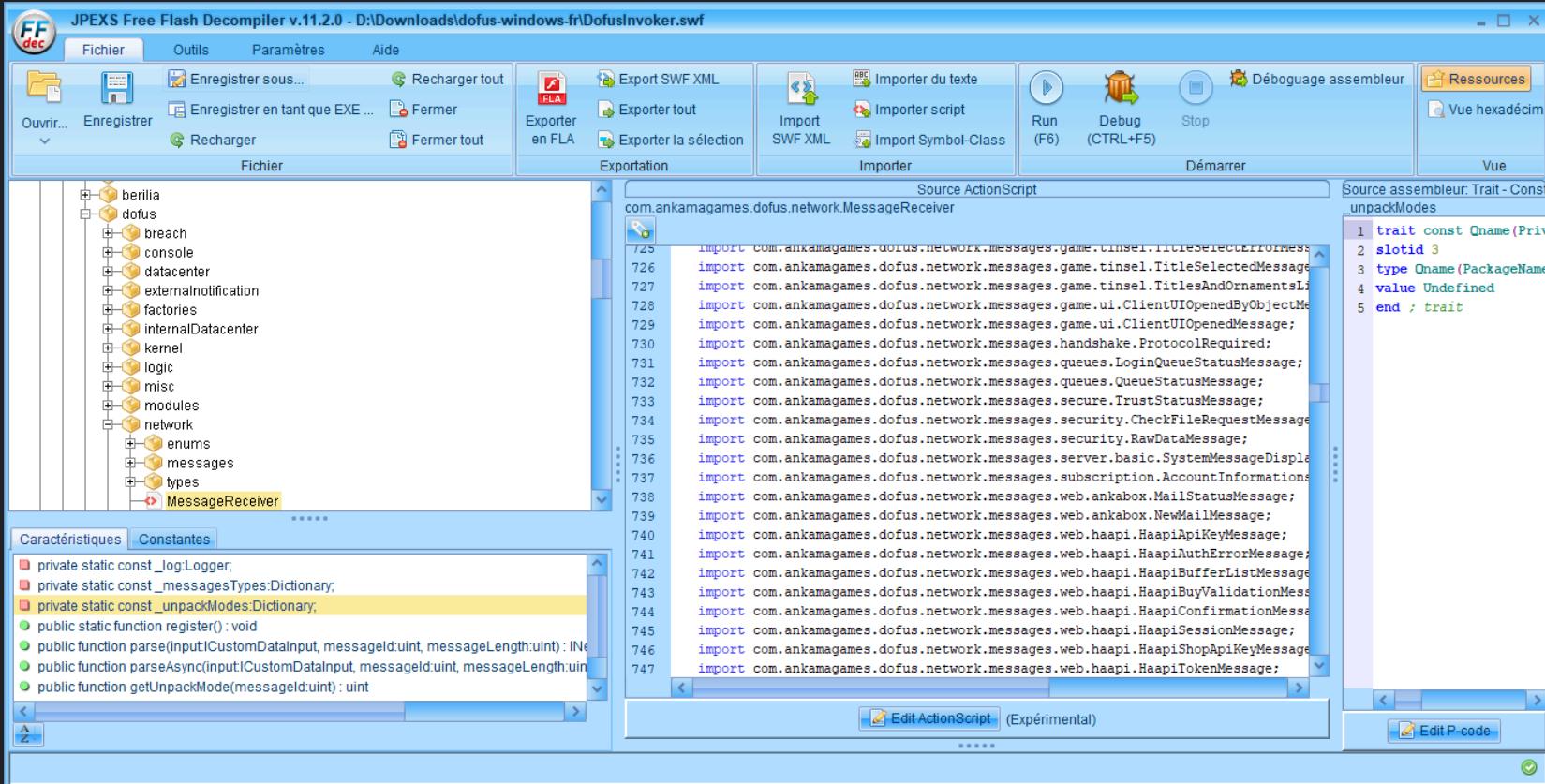
- Rétro-ingénieur
- Curieux
- Pentester
- Ankama

## ILLÉGAL

- Bots
- Serveurs privé
- Hacker



# ## RE: Flash

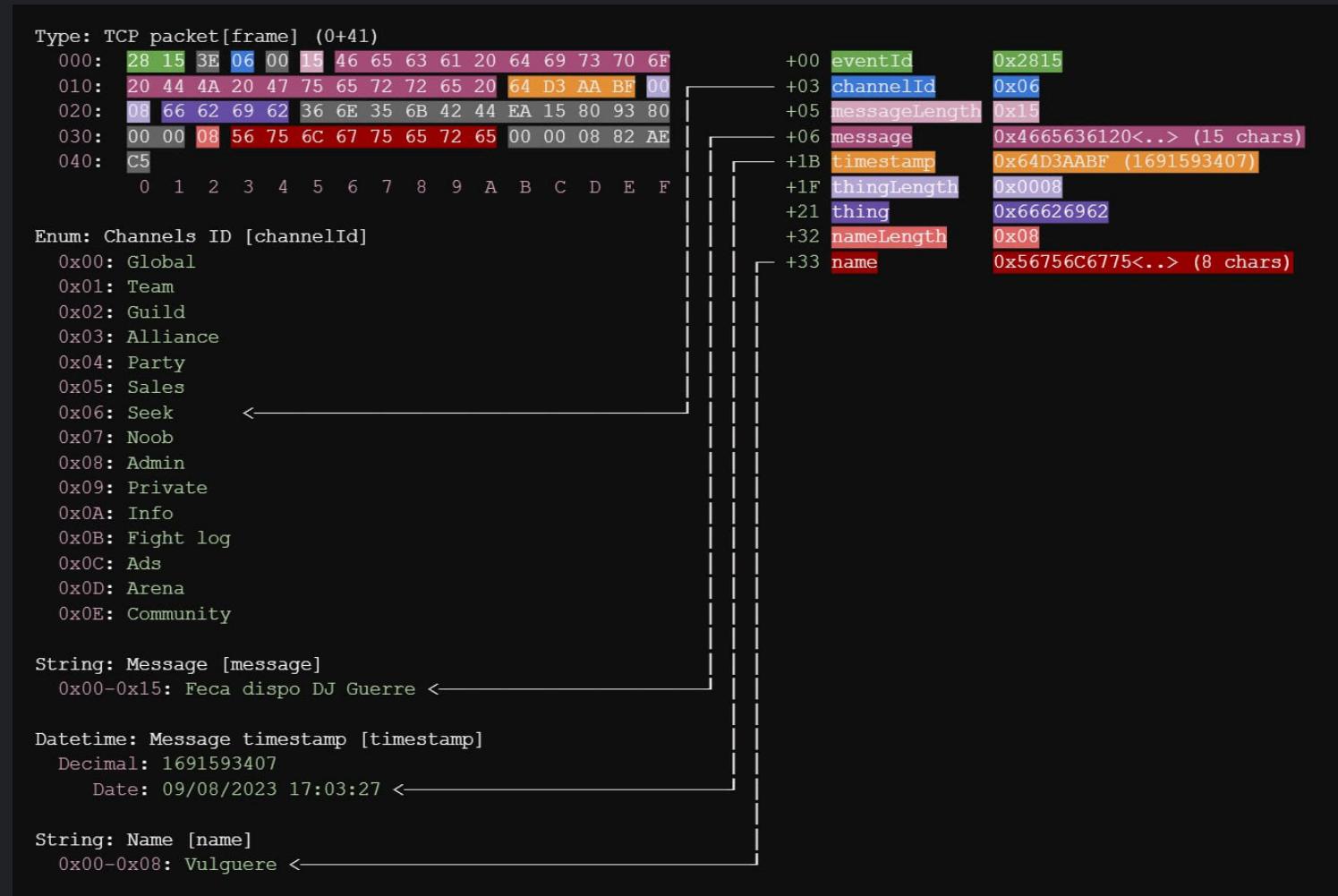


# ### RE: Flash

- 4000+ messages (événements, requêtes, réponses)
- Code "obfusqué" (noms, ids, ...)
- Librairies dépréciées depuis 10+ ans (crypto, lua, ...)
- Encore très utilisé malgré l'arrivée de Dofus 3



# ### RE: Flash - Network



# ### RE: Flash - Fun artifacts

-- TODO: Huge overhead, but simple. Rewrite.

6 -- TODO: Fix this as soon as Alchemy team clarifies situations

```
313     -- TODO: Really?  
314     error("namespace objects can not be resolved to actual value")
```

```
424     -- TODO: Why is this not a configurable function as with callobj?
425     --
426     -- Looks really slow, especially for
427     -- as3.class.a.b.c.new() kind of thing.
```

```
173     -- TODO: HACK! There should be a legal way to do this!
174     local mt = debug.getmetatable(assert(as3.new("String")))
```



# ## RE: Unity

```
ChannelMessageEvent X
1  using System;
2  using System.CodeDom.Compiler;
3  using System.Diagnostics;
4  using Com.Ankama.Dofus.Server.Game.Protocol.Common;
5  using Google.Protobuf;
6  using Google.Protobuf.Collections;
7  using Google.Protobuf.Reflection;
8  using Il2CppDummyDll;
9
10 namespace Com.Ankama.Dofus.Server.Game.Protocol.Chat
11 {
12     // Token: 0x02000A85 RID: 2693
13     [Token(Token = "0x2000A85")]
14     [DebuggerDisplay("{ToString(),nq}")]
15     public sealed class ChatChannelMessageEvent : IMessage<ChatChannelMessageEvent>, IMessage, IEquatable<ChatChanne
16     {
17         // Token: 0x170018C5 RID: 6341
18         // (get) Token: 0x06006F8B RID: 28555 RVA: 0x00002050 File Offset: 0x00000250
19         [Token(Token = "0x170018C5")]
20         [DebuggerNonUserCode]
21         [GeneratedCode("protoc", null)]
22         public static MessageParser<ChatChannelMessageEvent> Parser
23         {
24             [Token(Token = "0x6006F8B")]
25             [Address(RVA = "0xBDEFD0", Offset = "0xBDD5D0", VA = "0x180BDEFD0")]
26             get
27             {
28                 return null;
29             }
30         }
31
32         // Token: 0x170018C6 RID: 6342
33         // (get) Token: 0x06006F8C RID: 28556 RVA: 0x00002050 File Offset: 0x00000250
34         [Token(Token = "0x170018C6")]
35         [DebuggerNonUserCode]
36         [GeneratedCode("protoc", null)]
37         public static MessageDescriptor Descriptor
38         {
39             [Token(Token = "0x6006F8C")]
40             [Address(RVA = "0xBDEEB0", Offset = "0xBDD4B0", VA = "0x180BDEEB0")]
41             get
42             {
43                 return null;
44             }
45         }
46
47         // Token: 0x170018C7 RID: 6343
48         // (get) Token: 0x06006F8D RID: 28557 RVA: 0x00002050 File Offset: 0x00000250
49         [Token(Token = "0x170018C7")]
50         [GeneratedCode("protoc", null)]
51         [DebuggerNonUserCode]
52         private MessageDescriptor Descriptor
53         {
54             [Token(Token = "0x6006F8D")]
55             [Address(RVA = "0xBDF540", Offset = "0xBDBB40", VA = "0x180BDF540", Slot = "8")]
56             get
57             {
58                 return null;
59             }
59 }
```



# ### RE: Unity

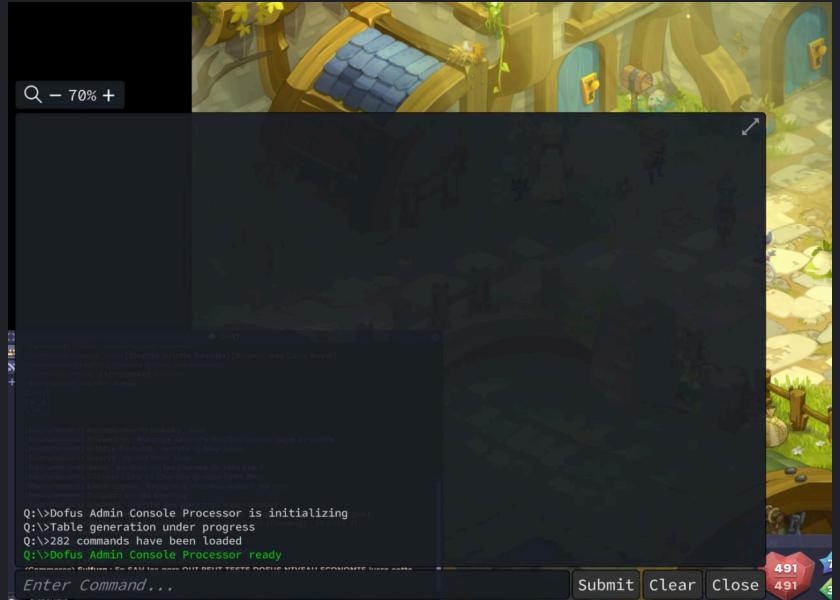
- IL2CPP
- Protobuf + gRPC
- Rendu & UI custom

rer l'Assembly  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Account  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Achievement  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Admin.Console  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alliance.Conquest  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alliance.Information  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alliance.Member  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alliance.Rank  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alliance.Recruitment  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Alteration  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Anomaly  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Area  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Arena  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Atlas  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Bak  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Basic  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Breach  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Challenge  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Character  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Character.Management  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Chat  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Choice  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Client.Verification  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Common  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Connection  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Contact  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Context  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Cosmetic  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Debt  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Debug  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Dialog  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Document  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Element  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Emote  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Exchange  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Fight  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Fight.Preparation  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Finish.Move  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Game.Action  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Gamemap  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Application  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Chest  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.House  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Information  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Member  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Rank  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Guild.Recruitment  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Haapi  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Haven.Bag  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.House  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Interactive.Element  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Inventory  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Job  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Living.Object  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Moderation  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Pet  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Quest  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Raid  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Reward  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Skill  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Tutorial  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Universe  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Vocation  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Wardrobe  
↳ {} Com.Ankama.Dofus.Server.Game.Protocol.Zone



# ### RE: Unity - Outils

- dnSpy (decompiling)
- BeplnEx (overlay)
- UABEA (assets export)
- Doduda (client cli)



# # Recherche de vulnérabilité

1. TextMeshPro
2. Injections & bypass
3. RCE One-Click



# # TextMeshPro

- Racheté en 2018 par Unity et rendue propriétaire
- Par défaut sur Unity
- Intégré dans uGUI
- Bugs, ambiguïtés, "features" non-documenté



# ## Balises

## Officiellement

<align>	<allcaps>	<alpha>
<b>	 	<color>
<cspace>	<font>	<font-weight>
<gradient>	<i>	<indent>
<line-height>	<line-indent>	<link>
<lowercase>	<margin>	<nobr>
<noparse>	<page>	<pos>
<rotate>	<s>	<size>
<smallcaps>	<space>	<sprite>
<strikethrough>	<style>	<sub>
<sup>	<u>	<uppercase>
<voffset>	<width>	

...

```
new MarkupTagDescriptor("ACTION", "action", "// <action>"),
new MarkupTagDescriptor("SLASH_ACTION", "/action", "// </action>"),
MarkupTagDescriptor.linefeed,

new MarkupTagDescriptor("CLASS", "class", "// <class>"),
new MarkupTagDescriptor("TABLE", "table", "// <table>"),
new MarkupTagDescriptor("SLASH_TABLE", "/table", "// </table>"),
new MarkupTagDescriptor("TH", "th", "// <th>"),
new MarkupTagDescriptor("SLASH_TH", "/th", "// </th>"),
new MarkupTagDescriptor("TR", "tr", "// <tr>"),
new MarkupTagDescriptor("SLASH_TR", "/tr", "// </tr>"),
new MarkupTagDescriptor("TD", "td", "// <td>"),
new MarkupTagDescriptor("SLASH_TD", "/td", "// </td>"),
MarkupTagDescriptor.linefeed,
```



# # POC Injection - 1/5 (16/08)

```
<mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

prend vous commandes 1-199 ou 1-200" MP pour plus d'infos  
Vous avez gagné 302 133 250 points d'expérience.



(Commerce) Marveen : [Dofus Ocre] av



# ## Fix - 1/5 (16/08)

## Noparse

The `<noparse>` tag creates a scope that TextMesh Pro does not parse.

This is useful for rendering text that TextMesh Pro normally interprets as a rich text tag, without disabling rich text tags.

**Example:**

```
Use <noparse><b></noparse> for <b>bold</b> text.
```

# Use **<b>** for bold text.

*Prevent parsing of some tags*

```
<noparse>CONTENT</noparse>
```



# # POC Injection - 2/5 (16/08)

```
</noparse><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```



# ## Fix - 2/5 (17/08)

</



Interdit

<noparse>

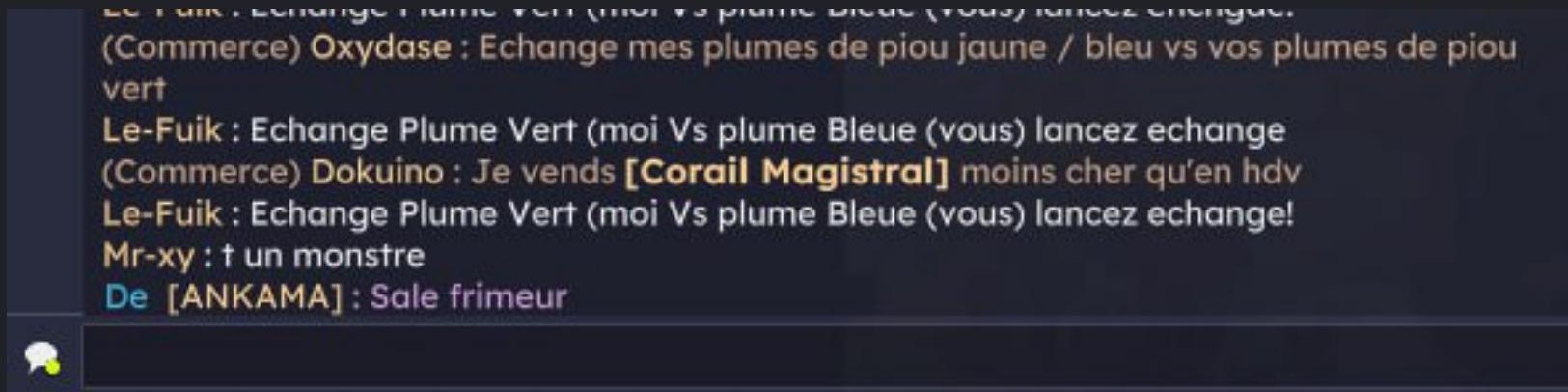


Supprimé



# # POC Injection - 3/5 (17/08)

```
<<noparse>/noparse><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```



# ## Fix - 3/5 (19/08)

</noparse>



Interdit

<noparse>



Interdit



# # POC Injection - 4/5 (19/08)

```
</noparse ><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

[23:58] SI UN JOUEUR VOUS DEMANDE DE  
RÉALISER UNE RECHERCHE SUR  
INTERNET, ASSUREZ VOUS QUE CE N'EST  
PAS UNE TENTATIVE DE PHISHING [ICI](#)



# # Fix - 4/5 (23/08)

<



Interdit



# # POC Injection - 5/5 (23/08)

```
\u003cmark color="#6897BB">x\u003c/mark>\u003cmark color="#F2F3F3">x\u003c/mark>\u003cmark color="#7C0002">x\u003c/mark>
```

\u003c -> <  


```
<mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

prend vous commandes 1-199 ou 1-200" MP pour plus d'infos  
Vous avez gagné 302 133 250 points d'expérience.



(Commerce) Marveen : [Dofus Ocre] av



# # Fix - 5/5 (02/12)

<

>



&lt;



&gt;



# ## POC Injection - 6/5 (05/01)

To be continued



# # POC RCE 1-Click



# # Questions

