

## Mémoire de fin d'études

### Master MIAGE La triche sur un Serious Game



**M. Minh-Huy LE**  
M2 Miage Classique  
2016/2017

*Maître de stage :* **M. Henri DARMET**  
*Enseignants tuteurs :* **M. Fabrice LEGOND-AUBRY**



# Remerciements

Je désire dans un premier temps remercier Monsieur Henri DARMET pour m'avoir laissé l'opportunité de travailler sur le projet I-Learning, me permettant ainsi de développer mes compétences. C'est en effet au sein de l'entreprise VISEO que j'ai pu effectuer les recherches que je vous présenterais dans ce mémoire. Le projet I-learning m'a permis d'acquérir une expérience dans un domaine captivant et en pleine expansion à l'ère du digital. Je remercie également toutes les équipes avec lesquelles j'ai eu l'occasion de collaborer au sein de VISEO, pour leur gentillesse et leur partage de savoir-faire. Cette expérience fut pour moi aussi enrichissante professionnellement qu'humainement parlant.

Par ailleurs, je souhaite remercier le corps enseignant, les intervenants professionnels ainsi que toutes les équipes pédagogiques ayant participé à l'enrichissement de ma formation [Master 2 \(M2\) Méthodes Informatiques Appliquées à la Gestion des Entreprises \(MIAGE\)](#).

Je souhaite plus particulièrement remercier Monsieur Julien BORDENEUVE pour son aide, ses conseils et les pistes d'amélioration apportées sur la résolution de ma problématique mais également Monsieur Fabrice LEGOND-AUBRY pour m'avoir aidé à déterminer le sujet de mon mémoire ainsi que pour son suivi durant toute la durée du stage.

C'est grâce à toutes ces personnes que je ressors aujourd'hui en toute confiance de cette formation, prêt à intégrer le milieu du travail dans un domaine qui me passionne : le développement informatique.

# Table des matières

<b>Remerciements</b> . . . . .	<b>3</b>
<b>Table des figures</b> . . . . .	<b>6</b>
<b>Introduction</b> . . . . .	<b>9</b>
<b>I Contexte et problématique</b> . . . . .	<b>10</b>
I.A Contexte . . . . .	10
I.B Problématique . . . . .	11
<b>II Serious Game</b> . . . . .	<b>12</b>
II.A Qu'est ce qu'un Serious Game ? . . . . .	12
II.B Le marché des Serious Game . . . . .	13
II.C Les différents types de Serious Game ? . . . . .	14
II.D Quelles sont ses avantages et ses limites? . . . . .	19
II.D.1 Avantages et limites génériques . . . . .	20
II.D.2 Avantages et limites spécifique à un domaine . . . . .	21
II.E Pourquoi tricher dans un Serious Game ? . . . . .	24
<b>III Les attaques</b> . . . . .	<b>25</b>
III.A Qu'est ce qu'une attaque ? . . . . .	25
III.B Quels sont les différents d'attaques pour tricher ? . . . . .	26
III.C Exploitation des vulnérabilités . . . . .	27
III.C.1 Session hijacking . . . . .	27
III.C.2 Code inspection . . . . .	28
III.C.3 Code modification . . . . .	29
III.C.4 Objet modification . . . . .	32
III.C.5 Cross Site Scripting (XSS) . . . . .	33
III.C.6 Injection . . . . .	34
<b>IV Protection</b> . . . . .	<b>35</b>
IV.A Protection globale . . . . .	35
IV.A.1 La mise à jour . . . . .	35
IV.A.2 Identifier les vulnérabilité des composants . . . . .	35
IV.A.3 Mauvaise configuration . . . . .	35
IV.A.4 Les guides - Bonnes pratiques . . . . .	35
IV.B Protection coté client . . . . .	36
IV.B.1 Offuscation . . . . .	36
IV.B.2 Protection contre les modifications . . . . .	36
IV.C Protection coté serveur web . . . . .	37
IV.C.1 Controle coté serveur . . . . .	37

IV.D Protection Serious Game . . . . .	37
IV.D.1 Disposition . . . . .	37
IV.D.2 Les corrections . . . . .	38
IV.D.3 Question sur mesure . . . . .	39
IV.D.4 Réponses variables . . . . .	40
IV.D.5 Double authentification . . . . .	40
IV.D.6 Le règlement . . . . .	41
IV.D.7 La multi-participation . . . . .	42
IV.D.8 Comportement anormale . . . . .	42
<b>Bilan . . . . .</b>	<b>43</b>
A Conclusion . . . . .	43
B Perspective . . . . .	44
<b>Bibliographie . . . . .</b>	<b>45</b>
<b>Glossaires . . . . .</b>	<b>51</b>
<b>Annexes . . . . .</b>	<b>54</b>
A Debugguer avec chrome . . . . .	54
B Snapshot memory avec chrome . . . . .	56
C Event Listener Breakpoints . . . . .	58
C.1 Modification étape 1 . . . . .	58
C.2 Modification étape 2 . . . . .	61

# Table des figures

I.1	SVG [2]	11
I.2	Evenements ou actions réalisable sur l'application [3]	11
II.1	Les jeux sérieux[8]	12
II.2	Chiffre d'affaire des jeux sérieux 2011-2016 [25]	13
II.3	L'entraînement du Dr Kawashima [30]	14
II.4	CodinGame - Pratice [35]	15
II.5	Les clients de CodinGame [41]	17
II.6	Minecraft Education Edition [46]	18
II.7	Le Sensorama est sorti dans les années 1950 [52]	19
II.8	Behind the scenes of the Army's helicopter training program [21]	23
III.1	Possibilités attaques [60]	25
III.2	OWASP Top 10 Application Security Risks - 2017 (image modifier) [61]	26
III.3	Utilisation cookie [72]	27
III.4	Question sur java basic	28
III.5	Debug sur le côté client	29
III.6	Snapshot memory	29
III.7	SD Client - Connexion à chargement Dashboard	30
III.8	Event Listener Breakpoints	30
III.9	Dashboard Admin	31
III.10	Quiz Vue Admin	32
III.11	Modification depuis le console	32
III.12	Attaque XSS [63]	33
III.13	Forme de données correctes en JSON [79]	34
III.14	Forme de données exploitées en JSON [79]	34
IV.1	Fonction anonyme [71]	37
IV.2	Les corrections sur le projet I-Learning	38
IV.3	Transformation pseudo en chiffre	40
IV.4	Mot mystère [80]	41
1	Developer Tools	54
2	Observation du fichier index.html	54
3	Block gestion fichier	55
4	Classes en javascript	55
5	BreakPoint	56
6	BreakPoint avec condition	56
7	Developer Tools Memory	56
8	Snapshot memory	57
9	Snapshot memory filtrer	57
10	Aperçu de l'objet depuis Snapshot	57

11	Event mouse . . . . .	58
12	Event Timer . . . . .	58
13	Break point avec l'événement timer . . . . .	59
14	Event Keyboard . . . . .	59
15	Break point avec l'événement keyboard . . . . .	60
16	Code modifié pour l'étape 1 . . . . .	60
17	Modification fichier . . . . .	60
18	Historique des modifications du fichier . . . . .	61
19	Erreur du serveur : No token . . . . .	61
20	Code modifier pour l'étape 2 . . . . .	61
21	Vue dashboard admin . . . . .	62
22	Vue formation admin . . . . .	62
23	Vue création quiz admin . . . . .	62
24	Vue dashboard collaborateur . . . . .	63
25	Vue formation collaborateur . . . . .	63
26	Vue quiz collaborateur . . . . .	63



# Introduction

Dans le cadre de la formation **M2 MIAGE** en rythme classique, chaque étudiant de l'université Paris Ouest Nanterre doit effectuer un stage de 5 mois au sein d'une entreprise ainsi que réaliser un mémoire afin de répondre à une problématique importante dans le monde du développement. J'ai effectué mon stage de fin d'étude au sein de l'entreprise VISEO, celle-ci m'a confié le développement d'un "jeu sérieux".

Plus connu sous le nom de "serious game", "le jeu sérieux" a pour objectif d'enseigner de manière synthétique et ludique à travers différents jeux. L'enseignement avec le serious game devient alors un enseignement plus amusant, moins formel et en conséquent plus attractif vis-à-vis des générations "digitales natives". Ce concept est en pleine expansion : bien que déjà présent dans de nombreux secteurs tels que l'industrie aérospatiale et de la défense mais également dans l'industrie automobile, de l'éducation et de l'énergie ; nombreux sont les marchés à s'y intéresser un peu plus chaque jour [4, 6, 7].

C'est avec l'aide de mon tuteur d'enseignement que mes recherches ont porté sur une problématique précise dans le domaine des serious game : la triche. J'ai eu la chance de résoudre cette problématique au sein de VISEO où j'ai pu développer de nouvelles idées et mettre en application des pratiques sur le projet I-Learning ( Serious game).

Après avoir rappelé le contexte dans lequel se trouve le serious game, nous pourrons alors en déterminer les différentes problématiques d'un serious game, sa définition ainsi que les triches réalisables pour pouvoir enfin en conclure des solutions et moyens pour protéger un jeu sérieux des tentatives de triche et en tirer une conclusion ainsi qu'un axe d'amélioration pour l'évolution du serious game.

# I Contexte et problématique

## I.A. Contexte

De plus en plus nombreux sont les "jeux sérieux" à être proposés au sein des entreprises afin de former efficacement les collaborateurs. Ils sont d'une telle efficacité, qu'il existe maintenant plusieurs sortes de catégories à des différents secteurs d'entreprises. Nous pouvons par exemple remarquer l'avancée des serious game à l'aide de la réalité augmentée. Le but final étant d'allier plaisir et apprentissage dans des conditions proche du réel.

Au sein de l'entreprise VISEO, le projet I-learning dans lequel j'ai été intégré cette année avait tout d'abord été pensé par Monsieur Henri DARMET et son développement en [JavaScript \(JS\)](#) confié à des stagiaires durant la période 2015/2016. L'I-Learning ou autrement appelé "Interactive-Learning" a pour but de former les collaborateurs et stagiaires de manière ludique et attractive afin de remplacer et/ou être complémentaires aux formations plus formelles qui pourraient être proposées par la [Directions ressources humaines \(DRH\)](#). À l'aide de mon équipe, j'ai repris ce projet afin d'implémenter de nouveaux jeux et apporter des améliorations aux fonctionnalités déjà existantes et que j'ai pu finaliser mes recherches sur le thème de mon mémoire.

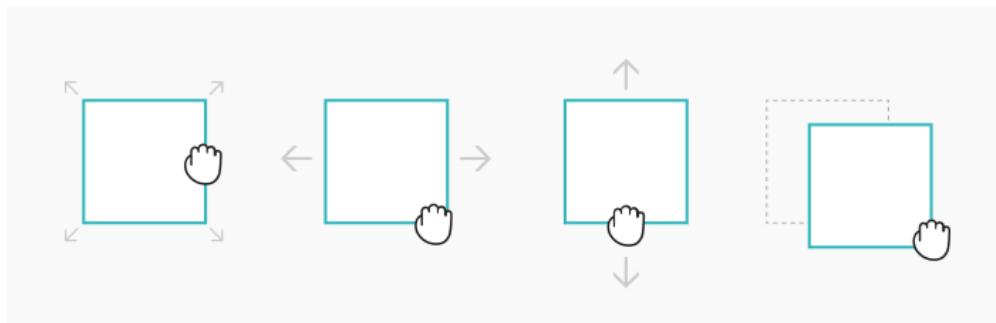
Le projet I-Learning est codé en Full [JS](#), sur le côté back-end, nous utilisons NodeJS qui permet de faire du [JS](#) coté serveur. Le serveur est intégré avec un module Express qui permet de gérer plus facilement les [Uniform Resource Locator \(URL\)](#) pour naviguer de page en page [Hypertext Markup Language \(HTML\)](#). Cette technologie était un choix de l'ancienne équipe afin de pouvoir exposer les modèles assez rapidement. La performance n'était pas un critère important car au départ, ce projet était un [Proof Of Concept \(POC\)](#), c'est à dire une réalisation expérimentale à partir d'une idée afin d'en déterminer sa faisabilité ou non. Les données sont stockées dans MongoDB, une [Base de données \(BDD\) Not Only SQL \(NoSQL\)](#) qui permet de gérer les données non rationnelles, ce qui permet d'avoir une souplesse de structure de données. La [BDD](#) stock ses documents en format [JavaScript Object Notation \(JSON\)](#), il y est donc plus facile de convertir les données en objet [JS](#) pour le coté front-end. De la même manière, si l'on souhaite insérer les données, il n'y a pas besoin de convertir en un format spécialisé pour sauvegarder dans MongoDB. Puisque le format de [JS](#) est semblable au format de [JSON](#), ils fonctionnent tous avec des pairs de clés et valeurs.

Sur le côté front-end, nous utilisons le [Scalable Vector Graphics \(SVG\)](#) qui constitue le squelette de l'application Web. La décision du choix des technologies a été prise par d'anciens stagiaires en fonction de la demande et des besoins du projet : ceux-ci ont étudié les technologies tendances dans le domaines afin d'en choisir une entre Adode Flash, Canvas et [SVG](#). C'est finalement [SVG](#) qui a été retenu, il permet de manipuler les [Document Object Model \(DOM\)](#) avec sa structure en arbre. Contrairement à Adode Flash et le Canvas, qui ne manipulent pas des [DOM](#). Par ailleurs, Adode Flash doit utiliser un plugin pour fonctionner alors que [SVG](#) et le canvas sont des éléments graphiques natif de [HTML 5](#) [1].



**Figure I.1:** SVG [2]

Le choix d'implémenter **SVG** est aussi un choix stratégique pour VISEO : le but est de montrer au client qu'on peut effectivement faire une application web totalement différent des applications web classique qui permet ainsi d'agrandir les offres de VISEO et les parts de marché pour l'entreprise. Sur le front-end on utilise le **JS** pour manipuler des éléments **SVG** comme l'affichage, les événements, les actions, les touches claviers, du drap and drop et autres. C'est grâce au projet I-Learning, que j'ai pu auditer le code et appliquer certaines pratiques et déterminer des points faibles liés au serious game.



**Figure I.2:** Evenements ou actions réalisable sur l'application [3]

## I.B. Problématique

La triche est un acte effectué de manière volontaire la plupart du temps, par des personnes pour une ou plusieurs de ces raisons :

- obtenir les meilleurs résultats possibles sur un serious game évalué
- être meilleur que ses collaborateurs
- contourner la sécurité du système

Certaines entreprises utilisant les serious game afin d'évaluer un potentiel candidat ou déterminer une possible augmentation de salaire, la tricherie devient donc un enjeu important pour celles-ci qui se verrait donc bernées par l'utilisateur du serious game.

Malheureusement, le projet I-Learning au sein de l'entreprise VISEO présente des failles de sécurité laissant ainsi la possibilité aux utilisateurs de tricher. En effet, celui-ci étant toujours en phase de développement, l'aspect sécurité du jeu n'a pas encore été abordé.

Qu'est qu'un serious game, pourquoi y a t-il des tricherie ? Comment tricher et par quels moyens ? Comment éviter la triche sur un serious game ? Nous allons tout d'abord rappeler le contexte d'un serious game, les impacts et les raisons de tricheries sur celui-ci, puis nous analyserons quels sont les moyens de tricherie pour en déterminer plusieurs solutions anti-tricheries à mettre en place.

## II Serious Game

### II.A. Qu'est ce qu'un Serious Game ?

Le terme "Serious Game" vient de l'anglais, qui signifie "jeu sérieux", ce sont des jeux qui ont pour but d'enseigner, renforcer les compétences ou améliorer sa santé d'une personne. Il peut s'agir également d'un choix économique pour les entreprises de former via des jeux sérieux. Elle comporte parfois un scénario qui permet à l'utilisateur de faire une immersion totale dans un univers hors scolaire [8]. Le concept du serious game est un mélange de jeu, d'apprentissage et de simulation intéressante afin de rendre la formation plus agréable et moins formelle. Elle permet ainsi de se former en conséquent et évoluer tout en jouant, elle se fait très souvent de son plein gré.

Pour rendre un serious game attractif, il faut travailler sur la profondeur de son contenu, sa théorie et son design. Un jeu non travaillé sur ces trois derniers aspects risquera de devenir vite ennuyeux et en conséquent d'en perdre son utilisateur, à contrario un jeu travaillé d'avantages sur son design que son contenu risque de perdre son intérêt. Il est donc important de bien balancer ces différents aspects. En résumé, un serious game est un concentré d'e-learning assemblé (la technologie, les outils informatiques, etc...) dans un jeu afin d'en tirer une formation plus amusante pour l'utilisateur [9].



Figure II.1: Les jeux sérieux[8]

Bien qu'en grande évolution ces dernières années, le jeu sérieux n'est pourtant pas né d'hier... C'est en effet en 1980 que le premier jeu sérieux voit le jour sous le nom "Army Battlezone" : un jeu stimulant à partir de char d'assaut en **Three-dimensional space (3D)**, il

faut alors tuer un maximum d'adversaire possible. Ce jeu développé par Atari a été réalisé suite à la demande de l'armée Américaine afin d'entrainer les équipages d'un véhicule de combat d'infanterie. Le choix de former des soldats via un jeu sérieux est avant tout un choix économique. En effet, il est plus rentable de placer un budget sur un jeu réutilisable à l'infini que sur un entraînement grandeur nature où il aurait fallu allouer des moyens humains, matériel (terrains, chars, munitions, essence...) et financier. De plus un entraînement réel aurait pu entraîner des blessés. Le jeu sérieux représentait donc une alternative intéressante pour l'armée [10, 11].

## II.B. Le marché des Serious Game

Il existe de multides d'études sur le marché des serious game, comme celui du cabinet Metaari et le cabinet Market&Market. Malheureusement ces études ne sont pas similaires et se contredisent parfois sur les chiffres transmis. néanmoins ces études montrent toutes deux l'évolution importante de la gammification liées à ces jeux sérieux [4].

Contrairement à l'époque où les jeux vidéo ont de mauvaise réputation, du fait que beaucoup de jeunes sont addictes et jouent durant des heures délaissant leur scolarité. Le jeu sérieux est aujourd'hui présent dans tous les secteurs : allant de la défense à l'éducation et en passant par la santé, l'agriculture et autres..., il est également diffusé à l'échelle mondiale (l'Amérique, l'Europe, l'Asie et l'Afrique). Selon le rapport de Ambient Insight de 2012, un cabinet d'analyse des technologies d'apprentissages devenu maintenant Metaari, le **Chiffre affaire (CA)** des jeux sérieux serait de 1.2 milliard de dollars en 2011. Avec une estimation d'évolution global de 15.4%, et ce chiffre serait amener à doubler en 2015 soit 2.5 milliards de dollars [4, 25].

Region	2011 Revenues in \$US Millions	2016 Revenues in \$US Millions	Five Year CAGR 2011-2016
North America	\$286.73	\$514.83	12.4%
Latin America	\$21.51	\$77.22	29.1%
Western Europe	\$83.15	\$136.43	10.4%
Eastern Europe	\$11.47	\$36.04	25.7%
Asia	\$813.18	\$1,723.20	16.2%
The Middle East	\$2.87	\$6.18	16.6%
Africa	\$10.04	\$25.74	20.7%
<b>Total</b>	<b>\$1,228.95</b>	<b>\$2,519.64</b>	<b>15.4%</b>

**Figure II.2:** Chiffre d'affaire des jeux sérieux 2011-2016 [25]

Les établissements des différents secteurs, et domaines (automobile, médical, les grandes entreprise et autres) commencent à adopter la gamification (utilisation des mécanismes du jeu dans d'autres domaines). Les entreprises utilisent le serious game à des fins d'enseignement, d'amélioration de santé, d'autres avec un choix stratégique d'économie. La gamification peut alors varier en fonction des secteurs et entreprises en fonction du type de serious game. Chaque catégorie de serious game peut être en lien avec ou un plusieurs secteurs, nous détaillerons ces liens dans la partie II.C. Ils n'ont pas les mêmes objectifs, ils visent chacun un secteur particulier, mais dans l'ensemble de tous, ils essayent de s'ouvrir à un public de tout âges.

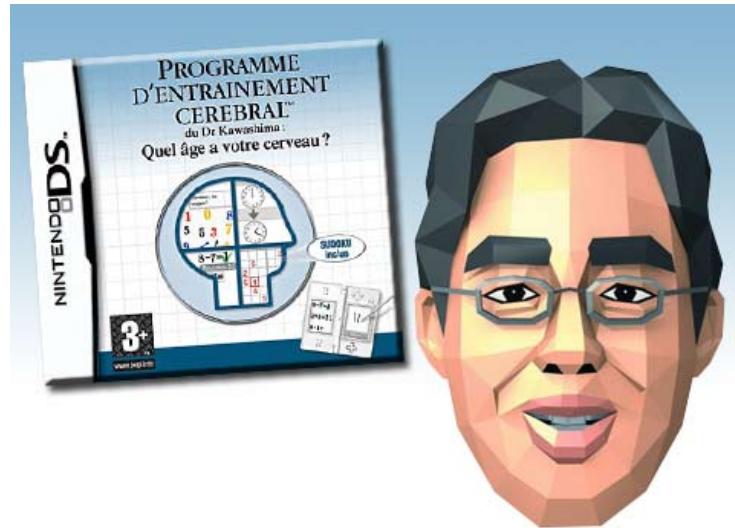
On ne vise plus les adolescents qui sont les joueurs habituels, mais également les joueurs occasionnels, les senior, les particuliers, et les retraités [24].

Quoi qu'il en soit, le serious game a de belle perspective d'avenir, avec une estimation d'une grosse progression d'une croissance de 22% et le CA au niveau mondial en 2021 de 6.9 milliards d'euros. Pour vous donner une ordre de grandeur, le CA du célèbre fast food McDonald dans le monde est de 24.62 milliards de dollars en 2016 [4, 5].

## II.C. Les différents types de Serious Game ?

Les évolutions technologiques permettent aux sérious game d'évoluer constamment et dans tous les secteurs pour tous les âges au point qu'on puisse les retrouver au quotidien. Selon Ambient Insight, il en existe une multitude, l'on peut en déterminer précisément dix catégories avec quelques exemples de jeux [27, 28] :

- **les brain trainers :** ce sont des jeux d'entraînement cérébral visant à améliorer la réactivité, la mémoire, la réflexion... Le but est de stimuler le cerveau afin de garder son état optimal. Il existe énormément de mini-jeux de type cérébraux, il y a les exercices de calculs, les test d'attention, logique... Chaque mini-jeux permettait de stimuler une zone particulière du cerveau afin que la totalité du jeu puisse stimuler la totalité du cerveau. Il y a Mario qui en fait partie par sa complexité à se souvenir des pièges, des raccourcis, des astuces... ce jeu fait appel à la mémoire visuo-spatiale. Parmi les jeux cérébraux réalisés, n'oublions pas de citer un des plus connus : le célèbre "Programme d'entraînement cérébral" sorti en 2005 sur Nintendo DS. Si son nom ne vous dites rien il se pourrait que cette image II.3 vous évoque quelques souvenirs [29].

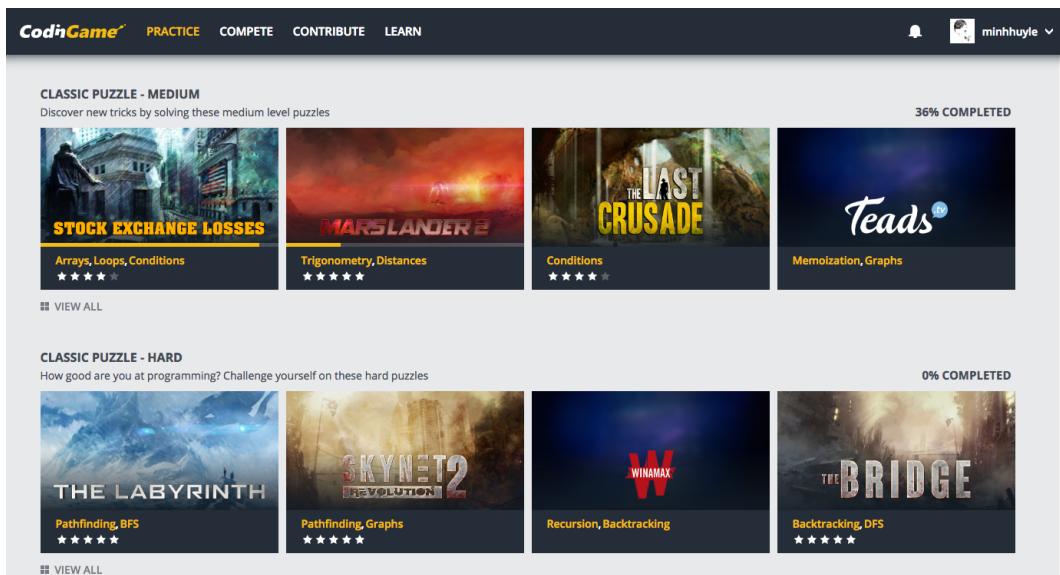


**Figure II.3:** L'entraînement du Dr Kawashima [30]

Le jeu "L'entraînement du Dr Kawashima" de Ryuta Kawashima compose un package de mini jeux, par exemple les jeux de calculs, mémorisation, test de rapidité, sudoku... Lorsque l'utilisateur a fini une série de jeux, le personnage fictif (Dr Kawashima) estime la santé de votre cerveau par rapport au bonnes et mauvaises réponses mais également par rapport au temps que vous avez effectué. Au fur à mesure que l'utilisateur réalise des séries de mini jeux, l'utilisateur mémorise les gestes ce qui peut rendre la temps de réaction plus courte. Pour la deuxième génération du jeu "Dr Kawashima's Athletic

"Training" de Ryuta Kawashima, on peut voir qu'il n'y a plus de simple exercices. Mais un mélange avec les jeux de plateformes comme Mario [29].

- **les jeux basés sur les connaissances** consiste tout simplement à s'appuyer sur les souvenirs. Ce genre de jeu n'est pas nouveau, il est présent dans nos vies au quotidien comme des blind tests avec lesquels on a une information incomplète et il faut trouver l'information qui manque, trouver l'auteur d'une poésie, trouver le titre ou encore le chanteur de la chanson, ou encore le célèbre jeu en forme de quiz présenté dans 50 pays différents, le but de ce jeu est de répondre à une suite de douze questions sans se tromper. Il existe trois paliers, lorsqu'on atteint un palier la somme du gain est sauvegardé et on peut avoir trois jokers afin de nous aider à atteindre le sommet qui correspond à une somme d'un millions d'euros (la monnaie peut être changée selon le pays). Les spectateurs peuvent non seulement suivre, mais de réaliser les quiz depuis chez soi. Même s'ils n'ont rien à gagner, ils permettent de tester leur connaissances. Ce jeu télévisé était tellement un succès, qu'on a adapté à un jeu sérieux qui porte le même nom que le show "Who Wants to Be a Millionaire", il est sorti sur trois consoles, la Nintendo DS, PlayStation 3 et la WII [31, 32, 33, 34].
- **les jeux basés sur les compétences** sont ceux qui proposent des exercices en forme de jeux pour les joueurs. Ils requièrent souvent une compétence, une connaissance spécifique pour résoudre le problème. En réalisant ces différents exercices, on aide l'utilisateur à acquérir et améliorer ses compétences. Ce qui réduit le temps de reconnaissance d'un problème, permet de faire gagner en créativité et en stratégie pour résoudre un problème. Comme le site CodinGame qui propose des différents défis à relever, les développeurs doivent observer, réfléchir et montrer une habileté pour résoudre un exercice. Même s'il compose différentes difficultés allant du plus facile au plus difficile comme on peut le voir sur la figure II.4, l'utilisateur doit être un minimum à l'aise dans un langage de programmation. Il doit être rigoureux pour bien comprendre l'énoncé, il peut tester son code autant de fois qu'il le souhaite pour voir le résultat de son code par rapport aux tests afin d'avoir un score maximal [35].



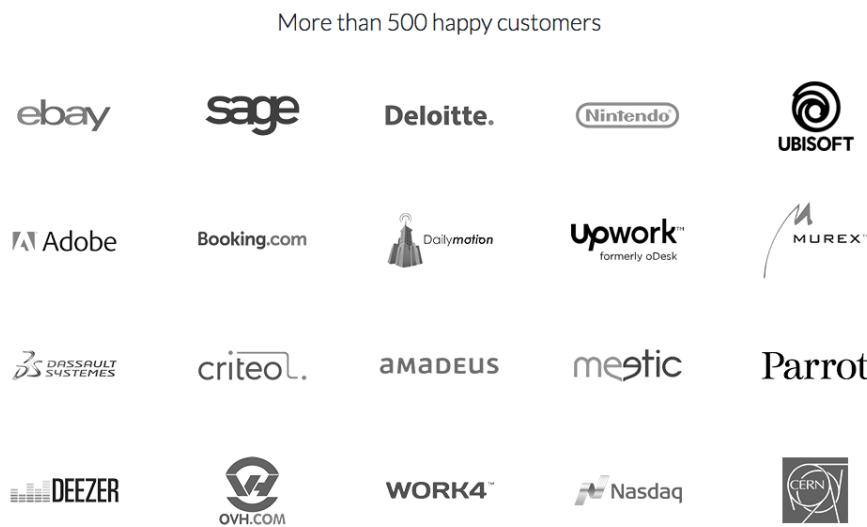
**Figure II.4:** CodinGame - Practice [35]

CodinGame ne propose pas seulement des défis avec seul le but de réussir le test. Mais il propose des "Clash of code" où les développeurs s'affrontent sur un même problème choisi aléatoirement, parfois il faut gérer son temps pour être celui le plus rapide. Ou

il faut simplement écrire le moins de code possible, de temps en temps il n'y a pas de consigne mais simplement les tests il faut deviner le code source comme le principe du **Test-driven development (TDD)**. Si on reste toujours dans le domaine du développement logiciel, il y a d'autres jeux Leek Wars ou on doit écrire un programme d'un **Intelligence artificielle (IA)** qui sera lu par notre poireau et que celui-ci suivra à la lettre pour objective d'abattre notre ennemis. Il y a également CodeCombat qui propose des petites challenges qui ressemble un peu à CodinGame mais qui reste moins riche.

- **les jeux d'apprentissage des langues**, qui ont pour simple but d'apprendre ou d'améliorer une ou plusieurs langues étrangères. Les jeux d'apprentissages sont très souvent en forme de jeu de rôle, où vous pouvez incarner un personnage fictif dans un scénario particulier (enquête policière, recherche d'un savoir perdu...). On peut voir ceci à travers des jeux comme "Les Éonautes" et "Mingoville" qui proposent des versions pour l'éducation nationale. Il y a des jeux un peu plus adaptés pour les enfants "Dino-lingo", "KidiLangues", "Dora l'Exploratrice" le célèbre dessin animé adapté en jeu qui apprend aux enfants les mots de base en anglais, voir même compter. Ces jeux peuvent être très intéressants, car les jeunes sont de plus en plus nombreux à avoir des difficultés à écrire correctement. Cette lacune est dû aux évolutions technologie, les langages **Short Message Service (SMS)**, les autos correcteurs ou les commandes vocales dans laquelle on prend habitude de ne plus écrire sois-même. Ces problèmes ne viennent pas seulement de la technologie. Il y a également une part de responsabilité de l'éducation nationale, les suppressions d'heures de cours de français, et la mixation des cultures, intégrant ainsi des enfants ressortissants de pays étrangers ne parlant pas la langue française. Les professeurs doivent prendre en charge plus d'élèves, ceux qui rend difficile les suivis des élèves en difficultés. Les médias sont aussi fautifs, les fautes qui ne sont pas détectées par les correcteurs ont un impact sur un grand nombre de lecteurs ou spectateurs. Ces jeux sont idéalement utilisés pour cibler les adultes qui ne s'accrochent pas aux formations classiques. La plupart de ces adultes qui décident de réviser ou apprend une autre langue est du aux besoins de leur travail (compétence nécessaire, évolutions de carrières). Il y a ceux qui rédigent beaucoup avec la langue nationale, ceux qui doivent communiquer à l'internationale, ils doivent avoir une maîtrise correcte de la langue [38, 39].
- **les jeux éducatifs pour les très jeunes enfants** permettent de faire découvrir de nouveaux formes, vocabulaires, développer sa créativité, améliorer sa mémoire et le sens de l'observation via les jeux très simples. Il y a différent niveau d'apprentissage, la composition des séries de jeux et l'objectifs varie selon la tranche d'âge du jeu. Un jeu pour les enfants de 2 ans, n'a pas la même efficacité pour les enfants de 3 ans [40].
- **les jeux d'évaluation** sont utilisés pour définir un profil, mesurer ou évaluer une connaissance. Les entreprises ont déjà adopté pour leur recrutement, il passe très souvent en général par les sites que plutôt de créer eux-mêmes les jeux sérieux, comme sur le site de CodinGame qui propose des défis. Les défis CodinGame sont des épreuves de programmation en ligne, les développeurs peuvent ensuite postuler de manière anonyme auprès des sociétés. Ils doivent résoudre des problèmes de programmation, à la fin de cette épreuve les entreprises peuvent visualiser les scores, le classement, le code source et prendre de leur choix de contacter les candidats. Ils ne sont pas tous des entreprises, certains peuvent être des amateurs de code qui s'intéressent simplement à partager un ou plusieurs exercices. La plateforme supporte à l'heure actuelle 15 langages de programmation C, C++, C#, PHP, Java, Javascript, Python, Ruby, Scala, Dart, Go, Pascal, Haskell, Objective-C et Perl. Bien sûr le service est gratuit, si on souhaite faire les jeux en privé et envoyer à plus de personnes, avoir plus de questions il faudra cette fois payer le

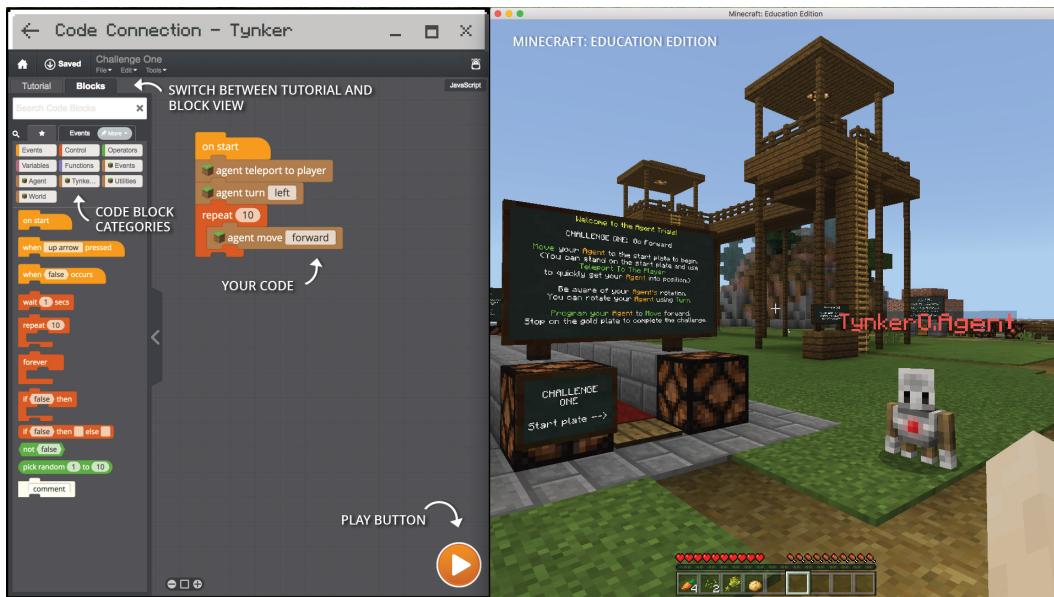
service. On peut voir déjà, qu'il y a plus de 500 entreprises qui ont utilisés CodinGame pour leur recrutement [41].



**Figure II.5:** Les clients de CodinGame [41]

Dans les jeux sérieux de type d'évaluation, il y a également "Neurodecision" qui permettent aux conseillers financiers d'évaluer le profil d'investisseur de leur clients en conformité avec les nouvelles exigences européennes [42].

- **jeux de rôles éducatifs** dans lequel on incarne un personnage virtuel dans un environnement fictif du jeu (jungle, espace, laboratoire...). Le personnage possède des actions, selon le contexte du jeu le personnage devra réaliser des missions, des quêtes ou entraînements afin d'avancer dans le jeu. L'action est différente selon le contexte de l'apprentissage, cuisiner des plats, opérer un patient, séparer les composants chimiques, etc... Au fur à mesure de l'évolution, le personnage possède de nouvelles compétences, qui lui permet d'aller dans les terrains plus lointaines. Les quêtes deviennent de plus en plus complexes, qu'il faut parfois ajuster correctement ses actions et sa capacité pour accomplir la quête. Lorsque la quête est remplie, le joueur recevra une récompense à la hauteur de la difficulté. Très souvent dans les **Role-playing game (RPG)**, il y a des niveaux normaux dans lesquels le joueur peut mettre en pratique la théorie. Puis il y a quelques niveaux qui mettent le joueur à rude épreuve, où le joueur doit mettre tout sa dextérité pour accomplir la mission comme tuer un boss. Le jeu "Minecraft Education Edition" est très riche dans ce domaine, il permet d'apprendre aux enfants à réaliser des constructions d'un bâtiment, une maison, ils peuvent construire bloc par bloc ou avec des lignes de commandes. Dans le jeu, on permet aux joueurs de construire des circuits électriques, on peut même créer des portes logiques OR, AND, NOR et autres. Le jeu est tellement complet, que vous pouvez même créer des diodes, alimenter un ou plusieurs circuits. Vous pouvez aller plus loin en imaginant un système d'automatisation, un ascenseur, des pièges pour vous défendre, il y a des joueurs qui sont allés plus loin en réalisant un ordinateur sur Minecraft. Pour construire tous ces mécanismes, le joueur doit retenir la recette pour créer des objets. Il existe même un mode qui permet au joueur de programmer un agent, il exécute le programme qui a été écrit par le joueur. Le joueur peut donc accomplir de grandes choses via ces agents, ce qui est un très bon début pour apprendre à coder [43, 44, 45].



**Figure II.6:** Minecraft Education Edition [46]

Il existe également d'autres jeux, moins riches, qui se concentrent sur un domaine. Comme ChemCaper, un jeu pour les enfants à partir de 10 ans, qui les apprend les notions de chimie. Le joueur doit réaliser des combinaisons, des liaisons chimiques, une familiarisation aux outils et méthodes utilisées dans les laboratoires pour créer des créatures "Petticles" et affronter des ennemis. Chaque Petticle a une caractéristique unique inspirée des particules de la réalité [47].

- **les jeux éducatifs basé sur la localisation** ont quelques variantes de diversités d'applications. Dans l'éducation on a des applications qui associent les activités (agriculture, industrie, entreprise) varié selon les lieux, l'apprentissage des noms des pays en donnant à chaque fois un nom de pays qu'il faudra placer au bon endroit pour avoir des points. Dans le style touristique on a ceux qui nous racontent une histoire selon l'endroit, selon le monument parfois avec une musique qui nous berce et nous laisse immerger totalement dans l'environnement. Qui pose parfois un souci avec le **Global Positioning System (GPS)**, comme la perte de précision dans un tunnel [48, 49].
- **les jeux éducatifs en réalité augmentée** arrivés sur les smartphones ont complètement déboussoler les consoles portables (gameboy, les Nintendo DS, les PSP, ...). Les enfants ne préférant avoir un smartphone ou une tablette comme console de jeu. Ces consoles portables voient ces clients les plus fidèles opter pour une solution moins chères, plus dynamique et plus adapté. Dû au fait qu'il y a beaucoup de jeux qui sont développés pour les smartphones, ces jeux coûtent beaucoup moins cher allant de quelques euros à une dizaine d'euros comparé à les jeux sur les consoles qui pourraient coûter une soixantaine d'euros. Les jeux sur smartphones sont très souvent gratuits pour la plupart, il gagne de l'argent soit par un abonnement de petit prix, avec la publicité ou encore grâce au achat complémentaire (plus de niveaux, plus de décors, une option personnalisée, ...). Les jeux réalité augmentée combinent le monde réel et les outils numériques, offrant à l'utilisateur une expérience d'interaction en temps réel. Il y a Masterpiece le jeu qui permet d'apprendre à dessiner à partir d'un modèle, avec l'appareil photo qui convertit la photo en un dessin dans laquelle on peut essayer de suivre les traits. Le jeu Words qui utilise les photos afin de faire deviner les mots, dans lequel on est limité à un nombre d'erreurs maximum par photo, un peu comme un pendu. Il permet de jouer en multijoueur, et qui aide à enrichir son vocabulaire avec des amis [50, 51].

- les jeux éducatifs en réalité virtuelle permet d'apprécier autrement que par la seul sens la vue, elle permet en effet de simuler d'autres sens supplémentaires afin d'offrir à l'utilisateur une expérience inoubliable et une sensation proche du réel grâce à une forme d'interaction personne-environnement. Il faut savoir que la Réalité Virtuelle (RV) ne date pas d'aujourd'hui, même s'il en ce moment les casques réalité font une fureur. Le premier expérience en réalité virtuelle est dans les années 1950, par un prototype surnommé le Sensorama figure II.7 mis au point par Morton Leonard Heilig qui s'est inspiré de son expérience de photographie. Le Sensorama permet à l'utilisateur de vivre une expérience inédite à l'époque qui simule plusieurs sens la vue, l'ouïe, l'odorat et le toucher. En 1966, le professeur Thomas A. Furness III a introduit la technologie RV au sein de l'Armée de l'Air, pour simuler des vols [52].



**Figure II.7:** Le Sensorama est sorti dans les années 1950 [52]

C'est en 1970 à l'Université de l'Utah, que le premier casque de RV a été créé par le professeur Daniel Vickers. Dans les années 80, les recherches ont continué et on a essayé de commercialiser pour le grand public, malgré son prix 100 \$ l'unité ce fut un échec par son manque de popularité auprès des consommateurs et difficile à utiliser. Malgré son échec pour les particuliers, le secteur médical, l'industrie automobiles et militaires sont très friantes pour cette technologie. C'est à partir de 2014, que sa population auprès des consommateurs a fait un bond, après la conférence Steam Dev Days, une annonce a été faite pour promouvoir les jeux vidéo en réalité virtuelle sur leur plateforme Steam. Dans la même année Facebook rachète la société Oculus VR puis rebaptisé Oculus Rift et Sony annoncent leur projet de casque de réalité virtuelle Playstation VR pour sa console de salon. C'est que à partir cette année que le grand public s'intéresse à les jeux en réalité virtuelle et c'est ceux qui a favorisé les développements des jeux sérieux en RV pour le grand public. Comme les jeux, Le Monde de Comenius qui permet aux étudiants d'étudier l'anatomie et les différents mécanismes du corps humain et au Japon, suite au tsunami, les chercheurs de l'université de technologie Aichi sont en train de travailler à une simulation qui formera la population à affronter un désastre similaire [52, 53].

## **II.D. Quelles sont ses avantages et ses limites?**

Nous avons pu voir les différents types de serious game, et observer chaque catégories répond à un besoin spécifique et touche à des types de clients particuliers. Il sera difficile de décrire tout ses avantages et ses limites, c'est pourquoi nous allons voir en plusieurs parties. Ceux

qui sont génériques à un ensemble de jeux sérieux, et ceux qui sont spécifique à une utilisation ou domain particulier.

### ***II.D.1. Avantages et limites génériques***

Il est difficile de dire que tous les serious games ont les mêmes avantages, ceci dépendra seulement de son contexte d'utilisation. Mais entre tous ces serious games, il existe des avantages et des limites clés :

#### **Les avantages**

- **La motivation des apprenants**, c'est la clé de la passion qui donne une mystérieuse énergie psychique aux utilisateurs. Le fait que c'est en forme de jeu, l'utilisateurs aura l'impression de s'amuser et ceci a un impact sur la motivation surtout quand c'est sur le long terme. Les joueurs sont plus motivés car ils peuvent pratiquer, et pas juste écouter de simple théorie. Ils réalisent les exercices plus par obligation mais par plaisir [54].
- **L'apprentissage par essais et erreurs** permettent à chacun d'essayer, d'échouer autant de fois qu'il le souhaite. Ils ont des retours sur leurs erreur ce qui leur permet d'améliorer leur compréhension et d'ajuster leur hypothèse [54].
- **La prise en compte des différentes rythmes d'apprentissage** permet à chacun d'avoir son propre rythme, les personnes qui ont réussi l'exercice, peuvent passer à un autre niveau sans attendre ceux qui ont des lacunes sur le niveau précédent, il n'y a donc pas de rythme imposé par un professeur/formateur [54].
- **La stimulation** est bien meilleur, les joueurs semblent échanger et réagir plus efficacement afin d'avancer dans le jeu. Certains vont réaliser des guides, des conseils, ou même construire eux même les autres niveaux par le désir d'avoir des cadeaux, des points ou un status particulier (VIP, Pro...). On peut imaginer grâce à cette méthode d'échange contre des récompenses, on peut ainsi compléter le jeu sérieux de manière très efficace, sans à dépenser beaucoup d'argent [54].
- **L'accessibilité** est très important, dans une époque où tout personne possède un appareil numérique. La gamification attire de plus en plus de monde, car elle est accessible à tout moment, sur toutes plateformes (smartphone, tablette, ordinateur). On n'a plus d'horaire fixe comme les écoles ou les formations, dans le bus sur le trajet du travail ou de l'école à 7h du matin, on peut se former via smartphone.
- **Barrières de l'âge et culturelle** sont supprimés à travers le jeu. On n'a plus peur d'apprendre car on a 40 ou 60 ans, car la barrière de l'âge est brisé. Qu'on soit d'origine africaine, asiatique ou européenne, de n'importe quel religion. Sa disposition qui permet à chacun être traiter de manière égale, car à travers le jeu nous sommes un personnage totalement anonyme et nous portons un nom d'emprunt , un pseudo que nous avons choisi. Il y a donc pas de peur de moquerie devant les autres car on n'a pas compris l'exercice, car on est plus âgé que les autres ou encore à cause de l'accent pour les prises de paroles pour les exercices orales.

#### **Les limites**

Il est vrai que les jeux sérieux sont très efficaces pour trasmettre des connaissances ou appliquer des théories. Car l'homme se souvient de 30% de ce qu'il voit et de 90% de ses actions. Mais ces jeux sérieux ne sont pas des outils magiques qui peuvent tout réaliser. Ils peuvent même avoir un effet inverse lorsqu'ils sont mal réalisé, ceci est liées à plusieurs facteurs [55].

- **La mauvaise qualité** rend le jeu non pertinent, il fait perdre tout son intérêt de gamification. Il faut donc bien étudier la profondeur du jeu, et faire le bon choix de jeu selon les compétences et les connaissances à acquérir. Ajuster le juste milieu, qu'il ne soit que divertissement et qu'il ne soit pas aussi formel que les formations classiques. Il faut faire en sorte que l'utilisateur comprenne le message ou l'exercice. Il faut faire assez simple, pour que les apprenants comprennent les intentions des concepteurs sinon ils peuvent délaisser le jeu s'il est trop compliqué et ce n'est pas le but. Cela peut varier selon les candidats, car on ne réagit et ne réfléchit pas de la même façon. Il faut faire en sorte de proposer ou laisser des indices dans le jeu [54].
- **L'absence d'intégration** du jeu par le médiateur peut être la cause de la réussite du jeu. Il ne suffit pas simplement de mettre en place le jeu sérieux, il est indispensable de faire des retours afin d'améliorer l'apprentissage comme expliquer comment fonctionne le système afin que le joueur puisse démarrer sans trop se perdre [54].
- **Les contraintes matérielles et logistiques** peuvent être problématique, pour certains établissement comme les écoles. Ils ne disposent pas forcément de tout le matériel nécessaire, ceci peut avoir des conséquences sur les dépenses de l'établissement. L'enseignant doit prendre la responsabilité de contrôler et assurer l'entretien du matériel, ceci peut être problématique si la personne n'a pas les compétences nécessaires [54].
- **Le coût du jeu sérieux** est un problème pour certaines entreprises, le prix peut aller de 50 000 euros, en moyenne, et jusqu'à 150 000. Pour les entreprises qui ont déjà adopté telle que Air France, Axa, EDF, L'Oréal, Michelin, Renault... Le prix n'étant pas réellement un problème pour eux vu la taille de l'entreprise. Car pour avoir un retour sur investissement avec le serious game, il faudrait environ un effectif de 300 salariés. Mais ceci devient de moins en moins vrais, des **Petites et moyennes entreprises (PME)** comment à s'y intéresser et font chuter les prix. De plus, les entreprises ne sont plus obligé de tout développer à partir du néant, il existe maintenant des librairies, des moteurs graphiques, des outils de production qui permettent un développement plus structurés et rapides. De créer soi-même, on peut utiliser ceux qui sont déjà existants qui sont très souvent gratuit ou avec une somme très modeste, mais qui inclus au fait qu'on ne choisit pas les questions. On peut également demander à des entreprises qui sont spécialisées, comme CodinGame de le faire pour nous avec un prix qui sont dans les 300 euros par mois [41, 56, 57, 58].

### II.D.2. Avantages et limites spécifique à un domaine

Le serious game est présent dans de nombreux domaines, décrire les avantages et limites de tous les domaines serait une utopie. Nous allons sélectionner et décrire une partie de ces domaines, de sorte qu'ils soient totalement variés afin de montrer la pertinence et les limites de la gamification.

- **Le domaine de santé :** Aide à mieux former efficacement les aides soignants, les chirurgiens qui répondent à des enjeux de sécurité lors d'interventions initiales auprès d'un patient grâce à des systèmes qui rendent le virtuel de plus en plus proche de la réalité (la **3D**, la réalité augmentée, la réalité virtuelle). Ces joueurs sont mis dans certaines conditions avec des patients qui ont des problèmes concrets. Ils peuvent donc adopter ceux qu'ils ont vus dans le jeu et réagir plus rapidement dans de vrais cas. Ceci les permettent pas seulement de pratiquer, mais d'observer des cas qui ne sont pas très courant grâce à la simulation [14].

Il permet également de sensibiliser et ralentir les maladies telle que l'Alzheimer. La maladie d'Alzheimer est une pathologie complexe qui entraîne une perte progressive de la

mémoire. Le Dr Harrison, psychologue à l'Imperial College de Londres a estimé qu'avant 2050, le coût de traitement de la maladie d'Alzheimer aux Etats-Unis pourrait atteindre un trillion de dollars. Il y a peu d'articles qui parlent des effets bénéfiques des jeux, mais il est reconnu que cela conduit à l'amélioration des fonctions cognitives. D'après Harrison, il serait préférable d'utiliser les jeux pour retarder la maladie d'Alzheimer. Ce qui pourraient augmenter la qualité de vie des patients et surtout éviter une détrastre économique [12, 13].

Mais malheureusement, les jeux ne soignent pas la maladie, elle permet comme préciser précédemment de ralentir la maladie. Et cela ne reflète pas forcément la réalité où les cas des patients peuvent être plus complexe que le jeu. Il y a même des cas où les jeux sérieux ne semblent pas faire effet, comme celui des enfants asthmatiques. Les enfants comprennent mieux leur maladie, ils reçoivent des exercices de respirations, les études des fonctions pulmonaires n'ont pas montré de bénéfice. Ils sembleraient qu'on ne parvient pas à modifier les comportements des jeunes patients concluent les chercheurs [15].

- **Le domaine de l'éducation nationale :** De plus en plus utilisés dans le domaine éducatif, car les études montrent qu'il y a une meilleure d'apprentissage. Catherine Cerezo, de l'Université Paris 10, a expérimenté sur des enfants de [Cours moyen 2e \(CM2\)](#), dans le cadre de l'enseignement de l'histoire sur les jeux sérieux. Les recherches ont montré que les élèves ont une meilleure estime de soi. Elle a remarqué que les joueurs ont également développé des compétences d'ordre méthodologique telles que la persévérance, la rigueur mais aussi le calme, éléments indispensables à la pratique du jeu vidéo comme aux situations d'apprentissages. Les élèves sont également plus intéressé et vouloir plus découvrir des monuments, des personnages historiques. Acteur privé de l'enseignement à distance, Tarin Hess de la 21st Century Learning Solutions et Gunter Glenda, de l'Université de Floride, ont fait une étude sur les étudiants de l'université sélectionner au hasard. On leur proposer à un groupe étudiants des cours via à des jeux sérieux en ligne et à un autre groupe les mêmes cours mais avec le style académique. Les résultats ont montré que les étudiants qui sont formés via les jeux en lignes ont une meilleure moyenne et une surmotivation. Ces jeux permet d'avoir plus de temps pour la pédagogie, et les permet gagner en autonomie [16, 17].

Malgré le fait qu'on a trouvé qu'il permet aux élèves de niveau primaire au secondaire d'avoir une meilleure estime de soi, ceci n'est pas un outil magique, il doit être suivi d'un accompagnement par les enseignants et le croisement avec d'autres méthodes pédagogiques. Il faudra notamment s'assurer de la compatibilité des postes de travail avec les nouvelles technologies du jeu sérieux. Sans oublier de la disponibilité d'internet, s'il est suffisant pour un certain nombre d'étudiants et les détails de l'utilisation du dispositif [16, 18].

- **Le domaine militaire :** Les simulateurs existent dans le domaine militaire depuis très longtemps car au départ il n'existe pas encore, et le domaine militaire était les seuls à pouvoir investir dans le niveau du budget, la technologie, la recherche, du temps... Ces simulateurs permettent aux soldats de réaliser une pratique intensive d'une compétence en vue d'un perfectionnement et de l'acquisition d'automatismes et de réflexes. De plus il permet de former les soldats avec un budget qui coûte beaucoup moins cher que de confier un vrai appareil à un pilote débutant. Sans à mobiliser des grands effectifs pour un exercice de déploiement, plus besoin de munitions en grande quantité pour les exercices de tirs de routine ce qui assure la formation dans de meilleures conditions de sécurité [19].



**Figure II.8:** Behind the scenes of the Army's helicopter training program [21]

Il existe différents types de simulations, et chacun apportent une compétence spécifique [20] :

- **La simulation numérique** : ce type de simulation ne mettant en oeuvre que du logiciel représente l'ensemble des modèles stratégiques qui permet d'évaluer et améliorer chaque aspect stratégique et tactique du comportement, il fait appel à des opérateurs manipulant des pions tactiques élaborés de manière prédéfinies, il peut également y avoir une interaction humaine : celà représente l'ensemble de la catégorie "jeux de guerre" présente sur ordinateur.
- **La simulation interactive** : cette simulation permet à l'homme d'intéragir à l'aide d'une IHM (interface homme-machine) informatique, malheureusement cette simulation n'est représentatives des gestes et actions réelles néanmoins elle permet par le jeu du scénario d'en tirer des décisions.
- **La simulation pilotée** : qui permet de se familiariser avec les commandes du système représenté via une simulation dans laquelle un homme joue son propre rôle dans un environnement simulé.
- **La simulation instrumentée** : cette simulation permet de mettre en oeuvre des moyens humains et matériels réels afin d'en simuler les effets et ainsi en tirer des analyses.
- **La simulation temps réel** : permet de simuler une action en temps réel. Elle aide ainsi à pouvoir chronométrier et définir un temps donné.

L'utilisation des simulations ont néanmoins des limites [20]:

- Pour l'entraînement, il est compliqué de simuler et/ou reproduire toutes les contraintes ergonomiques, psychologiques, physiologiques ou environnementales (stress, fatigue) qu'il y aurait pu réellement avoir sur un champ de bataille grandeur nature.
- Il est difficile de suivre les évolutions d'armement de tous les pays, ce qui demande une veille constante afin d'adapter le simulateur en conséquent.
- Le soutien peut être compliqué dans le traitement des cycles de vies des technologies employées.
- Le simulateur peut comme le soutien, être une variable d'ajustement budgétaire si il y a une limite de moyens financiers.
- Il peut être compliqué d'avoir des formations en adéquation avec les programmes de coopération, il faut donc réaliser des partenariats avec l'état afin de privilégier des moyens nationaux.

- L'outil de simulation mis en place doit pouvoir s'adapter à tous les systèmes d'armements, en soit il doit être maléable et compatible avec tous, ce qui peut s'avérer être une difficulté importante dans la veille et l'évolution technologique..
  - Malgré le fait qu'on utilise les simulateurs, certains règlementation nécessite la pratique réel afin de valider des réels aptitudes de mise en œuvre (nombre de vol pour les pilotes) ou de certification des équipements utilisés.
- **Le domaine recrutement :** Dans un contexte économique, le recrutement des talents est un enjeu stratégique vital pour les entreprises qui doit sans cesse tout les jours confronter à la concurrence. Ils ne suffisent plus simplement de recruter, mais de trouver la perle rare, et attirer des talents. Il faut dénicher également le "perfect match" qui s'épanouira au sein de l'entreprise avec une total efficacité et performance du candidat. Grâce au serious game, on peut donc de trouver ces types de candidat, par sa dimension pragmatique et ludique. Il aide à faire un premier filtre de candidats, c'est un outil qui met en avant certains savoirs-faire des candidats plus facilement que dans un [Curriculum vitae \(CV\)](#) [22, 23]

Même si à travers les jeux sérieux, on peut trouver des bon éléments, mais rien nous garantit c'est cette candidat n'a pas tricher ou encore demander à un ami qui est bien meilleur de passer l'exercice d'évaluation pour lui lorsque l'évaluation se fait à distance. De plus cette outil permet de tester la compétence mais fait perdre totalement le coté humaine, comme la communication. On doit donc comme même vérifier ces quelques aspects sur un entretien pour assurer son coté relationnel.

## II.E. Pourquoi tricher dans un Serious Game ?

La triche est un phénomène bien connu, on a tous triché dans un examen d'école, un jeu de société avec des amis au moins une fois dans sa vie. Cette acte est parfois improvisé, mais il est souvent volontaire et le serious game n'échappe pas à cette pratique. Comme les jeux sérieux n'apportent pas les mêmes avantages et n'ont pas les mêmes buts.

Les intérêts des tricheries sont variés, certains domaines des jeux sérieux ne composent aucun intérêt de tricher. Dans les secteurs comme l'éducation nationale ou les [Entreprises de Services Numérique \(ESN\)](#), il y a de beaucoup de tentations de tricheries. Dans les ESN, lorsque les enjeux sont des récompenses matériels comme une augmentation de salaire, une promotion, ou simplement un travail, il est très probable qu'il y a des triches. Il y a pas seulement des récompenses matériels qui attirent tricheurs, il y a aussi de la jalouse, lorsqu'on a envie d'être le meilleur que d'autre ce qui peut conduire à du sabotage des travaux d'atelier ou simplement obtenir son diplôme.

Il n'y a pas de tricherie dans les domaines telles que la santé ou militaire. Les personnes qui souhaitent améliorer leur état de santé comme l'Alzheimer ne vont pas aller tricher car ça n'aide pas à améliorer leur état. Les malentendant pour les jeux d'apprentissage de langage des signes, n'ont absolument pas intérêt, voir même envie de tricher. De même pour les praticiens, les infirmières ou les chirurgiens, il n'y a aucun intérêt pour eux à tricher. Car ils ne vont pas assimiler les bons gestes et nuire donc à leur pratique dans de réelles conditions qui peuvent tuer des patients ce qui est très grave. Et dans le domaine du militaire, les soldats n'ont pas intérêt à tricher, car le but est de les préparer pour dans de réelles conditions ils ont plus de chance de réussite et de survie. Les soldats vont risquer leur vie en trichant dans un serious game qui les entraîne pour les terrains sensibles, il est donc pas logique de tricher dans ce cas. Il y a beaucoup d'autres cas qu'il y a pas d'intérêt de tricher, car la formation est beaucoup plus précieux à leur yeux que la gloire ou une récompense qu'on peut les donner.

## III Les attaques

Dans ce chapitre, nous allons montrer ce que c'est une attaque, les différents types attaques, nous verrons en détails quelques une. Nous allons appliquer certaines des attaques sur le projet I-Learning. Afin de ne pas perdre le lecteur dans les tests instruisons, nous exposons ici seulement les résultats de ces attaques cependant le détaille de ce teste instruisons sont disponible dans l'annexe.

### III.A. Qu'est ce qu'une attaque ?

Une attaque est l'origine de l'exploitation d'une faille d'un système informatique en attaquant l'intégralité, la confidentialité ou encore la disponibilité. Attaquer l'intégralité consiste à modifier le message/donnée originale, pour ce qui est de la confidentialité c'est obtenir les informations sans autorisations. Et pour ce qui est la disponibilité, cela consiste à nuire l'application/serveur afin qu'il ne peut plus réaliser ces services comme il devrait. Pour contrer ces attaques, il faut connaître l'origine et le type d'attaque afin de mettre des mesures préventives. Il faut comprend, que le pirate peut intervenir à n'importe quel maillon de la chaîne (de l'utilisateur au composant jusqu'à l'alimentations électrique) [60].

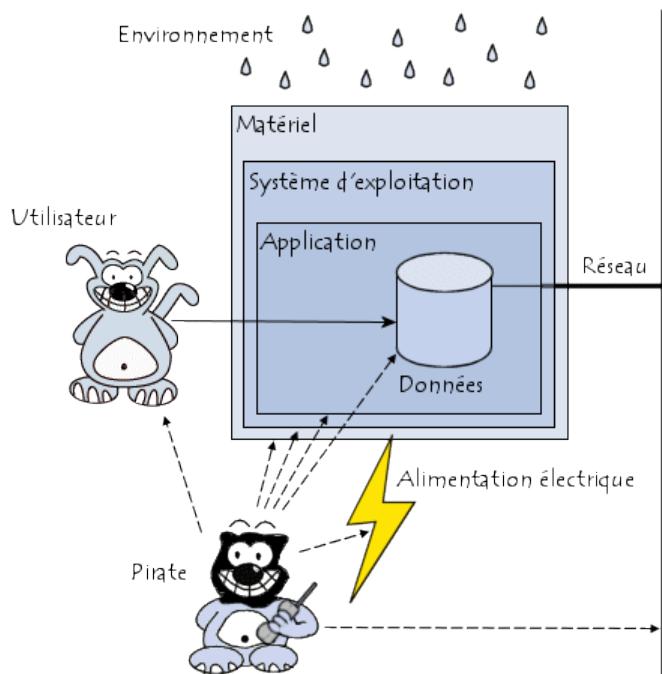


Figure III.1: Possibilités attaques [60]

Certaines des noms des attaques qui seront décrire à la suite seront laisser en anglais car elles sont plus parlants et parfois ne donne pas vraiment de sens de les traduire.

### III.B. Quels sont les différents d'attaques pour tricher ?

Tricher dans un serious game est totalement différent des triches des examens classique sur feuilles présent dans les collèges, les universitaires, les concours de sélections d'entrée école, et autres... Dans les examens classique, pour tricher certains vont essayer de faire des antisèches, qui les caches souvent dans la trousse ou dans la poche. Certains sont beaucoup plus créatives, vont écrire plus petit et de cacher dans le stylo ou sous les angles. Avec les matières scientifiques qui ont besoin une calculatrice pour réaliser l'examen, et beaucoup des étudiants exploitent ce besoin pour tricher. Avec les calculatrice scientifique, les candidats peuvent rentrer des formules, voir un texte dans l'appareil. Certains calculette de dernière génération peuvent même prendre des photos, et afficher un [Portable Document Format \(PDF\)](#) en couleur. C'est pourquoi certains universités ou les grandes écoles interdisent les calculatrices scientifiques lorsqu'il n'est pas nécessaire à l'utilisation. A partir de 2018, l'éducation nationale compte supprimer l'usage des calculatrices programmables pour éviter la fraude au baccalauréat, les étudiants vont devoir réviser correctement ou tricher avec l'ancien méthode avec des antisèches [59].

Pour tricher dans les jeux sérieux, les apprenants doivent savoir attaquer le système. Nous pouvons voir l'ensembles des attaques répertoriés par OWASP sur ce lien [62]. Il faut savoir que certaines de ces attaques ne sont pas applicable pour tricher comme [Distributed Denial of Service \(DDoS\) attack](#). Il y a aucun sens d'attaquer la disponibilité du serveur pour un tricheur car on rendra simplement le jeu hors service. On peut voir sur le figure III.2, le classement des vulnérabilités de sécurité applicatives web les plus critiques [61].



**Figure III.2:** OWASP Top 10 Application Security Risks - 2017 (image modifier) [61]

Nous allons mettre en pratique certaines de ces 10 vulnérabilités sur le projet I-Learning à travers ce chapitre, qui montre en attaquant l'intégralité et confidentialité, on peut tricher de plusieurs façon :

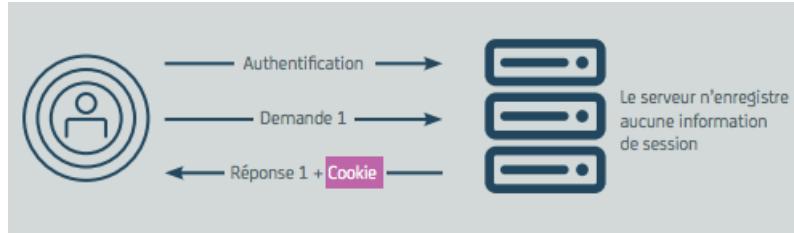
- Obtenir les bonnes réponses grâce aux failles d'injections par altération de données ou révélation d'informations. Il y a également des données non sécurisé, comme des données non chiffrées ou avec chiffrement faible.
- Faire du sabotage sur le compte des autres utilisateurs en volant l'authentification par la communications non sécurisées, par la prédiction ou encore par le brute force.
- On peut également exploiter les failles déjà cité pour augmenter son score avec les failles d'injections ou introduire sur un compte un admin pour changer son score.

## III.C. Exploitation des vunérabilités

Dans cette partie, on va voir les attaques côté client qui sont les attaques qui visent l'utilisateur pendant l'utilisation de l'application. L'application peut être une application de type bureau, web ou mobile.

### III.C.1. Session hijacking

La session hijacking est une attaque destinée à voler une session utilisateur. Comme le [Hyper-text Transfer Protocol \(HTTP\)](#) est sans état, les applications Web se servent des cookies afin de maintenir les états des actions des utilisateurs par exemple la connexion d'un utilisateur.



**Figure III.3:** Utilisation cookie [72]

On peut voir un exemple d'utilisation de cookie avec la figure ci-dessus. Lorsque l'utilisateur se connecte, et pour éviter qu'on remette à chaque fois le login et le mot de passe, on se sert du cookie pour garder l'état de la connexion. On peut également se servir du cookie pour lorsque l'utilisateur ferme la page et reviens sur la page, il n'a pas à s'authentifier de nouveau et que la connexion se fait via le cookie.

Malheureusement ces cookies peuvent être exploités par les sessions hijacking, et il a plusieurs types de sessions hijacking :

- Interception (Man in the middle) : consiste à intercepter un cookie par écoute du réseau entre le serveur et le client. Il existe deux sorts d'écoutes réseau, le passif et l'actif. Le passif consiste simplement à écouter le réseau sans modifier les packages de données qui circulent. L'actif consiste à modifier les données afin de perturber, ou berner le serveur et le client. Avec l'interception, le pirate peut récupérer bien plus que le cookie comme les clés de chiffrages, les mots de passe, etc ... Lors de l'interception du cookie, l'attaquant pourra à la suite utiliser pour accéder à l'application web, et bénéficier les droits de l'utilisateur.

- Prédiction : deviner une session valide en analysant l'algorithme de génération qui se serve de certaines informations connues (le login, la date, le type de navigateur, ...). Plus l'application possède d'utilisateurs, plus cette attaque sera facile à appliquer.
- Force brute : est une attaque qui consiste à générer des tentatives massives et en exploitant sa prédictibilité afin de trouver une session valide.
- Fixation : le but de cette attaque est de pousser l'utilisateur à se connecter (souvent par phishing) sur une session créée par le pirate. L'utilisateur se connecte, la session se créer avec la valeur qui a été mit en place par l'attaquant. Il accède ensuite sur le site avec la valeur de la session piéger. Le pirate peut utiliser un outil requérant l'application régulièrement afin d'éviter l'expiration de la session due à une période d'inactivité.
- Infection du navigateur (Man in the browser) : on fait en sorte d'implémenter un code qui permet d'envoyer la session de la victime.

Lorsque le pirate arrive à contourner une session, il peut se servir du compte de l'utilisateur afin de tricher. Si l'utilisateur est un administrateur, il peut voir ainsi toutes les bonnes, si l'utilisateur est un collaborateur le pirate peut consulter les jeux qui sont déjà effectués par la victime et ainsi éviter les mauvaises réponses. Mais il peut également saboter son compte afin que la victime a un score moins important [72, 73].

### ***III.C.2. Code inspection***

Actuellement, il y a aucun contrôle concernant les appels au serveur. À chaque action, le côté client fait appelle direct au serveur, et c'est au coté client qui va vérifier quelles sont les données à afficher.

Java

1 hashCode() renvoie

int      boolean

Cliquer sur une réponse pour passer à la question suivante

**Figure III.4:** Question sur java basic

Voici un exemple de vue qu'on peut voir sur le côté collaborateur/stagiaire, on peut voir le nom de la formation "Java" et la partie "Basic". On voit également la question ainsi que les réponses proposées. Le problème, c'est que même si les données qui ne sont pas affichées, ils sont sur le côté client, et ces données on peut les consulter sur le côté client. Il y a plusieurs façons d'observer ces données :

- Lire le code source depuis le côté client (navigateur), mettre des breakpoints pour les observers.

```

▼ rightAnswers: Array(1)
  ▼ 0: AnswerVueCollab
    ► border: Polygon
    ▼ content: Text
      anchorText: "middle"
      component: text
      fontName: "Arial"
      fontSize: 20
      id: "answerElementContent1"
      lineSpacing: 40
    ▶ lines: Array(0)
    messageText: "int"
    originalText: "int"

  ▶ this: QuestionVueCollab
    ► answersManipulator: Manipulator
    ► border: Polygon
    ► content: Text
      fontSize: 20
      height: 222.7999999999998
      imageLoaded: true
      imageSrc: ""
      invalidLabelInput: false
    ▶ invalidQuestionPictogramManip
    label: "hashCode() renvoie "
  
```

**Figure III.5:** Debug sur le coté client

On peut voir sur la figure à côté, la variable label est la question, et si on fouille un peu plus on voit la variable rightAnswers qui nous permet de voir la bonne réponse "int". Pour éviter de suivre tout le code, il faut mettre les breakpoints à des endroits qui semblent intéressants pour trouver l'information au plus vite. Tous les détails concernant le debug coté client sont décrits en annexe [A Debugguer avec chrome](#).

- Prend une photo de la mémoire de la page (JS Objet et tous les noeuds des DOM).

```

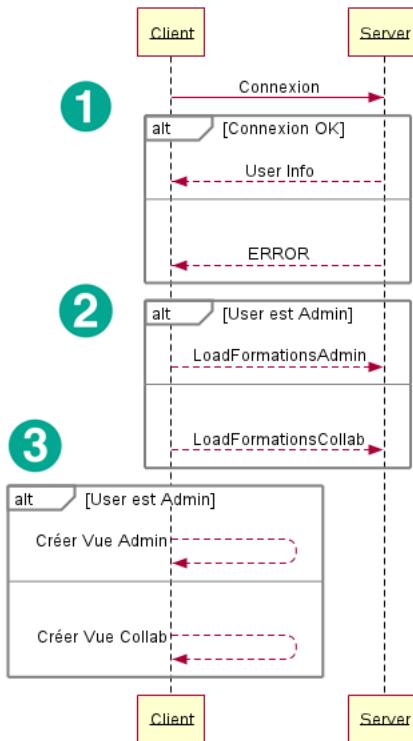
▼ correct :: system / Oddball @53
  ► map :: system / Map @319
  ► 2 :: "true" @655
  ► 4 :: "int" @379
  ► filled :: system / Oddball @53
  ► imageLoaded :: system / Oddball @53
  ► invalidLabelInput :: system / Oddball @55
  ► selected :: system / Oddball @55
  ► explanation :: @200475
  ► properties :: (object properties)[] @200477
  ► bgColor :: Array @169857
  ► colorBordure :: Array @169855
  ► label :: "int" @188579
  
```

**Figure III.6:** Snapshot memory

Avec le snapshot de la mémoire, on peut observer un ensemble d'objets avec le nom de la classe. Il comporte de légèrement différence avec la vue debug, mais on se repère assez rapidement. Et contrairement au debugguer, on n'a pas besoin de breakpoints. Ceci prend tous les objets en mémoire qui ont un lien avec le JS ou des objets DOM. Il faut ensuite chercher la donnée qui nous intéresse. On peut également enregistrer la mémoire avec toutes les actions de la page. Les détails sont disponibles en annexe [B Snapshot memory avec chrome](#).

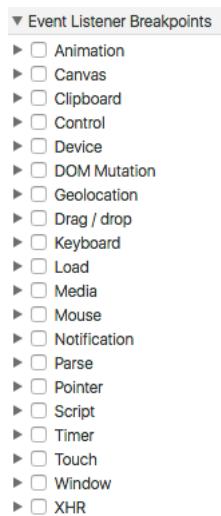
### III.C.3. Code modification

L'autre moyen de voir les bonnes réponses, c'est de modifier le code et de faire passer pour administrateur. Lors de la connexion, le côté front vérifie si on est administrateur ou collaborateur, il va ensuite charger les formations et instancier la vue correspondante à l'utilisateur.



**Figure III.7:** SD Client - Connexion à chargement Dashboard

On peut voir sur la figure ci-dessus, le diagramme de séquence lorsqu'on clique sur connexion. Ce qu'on va essayer de faire dans le premier temps, c'est de voir si on peut se faire passer pour admin sans se connecter avec le login et le mot de passe. On va donc modifier le comportement de l'étape 1. Faire en sorte que si on clique sur connexion ça n'envoie pas de requête sur le serveur, mais il va passer directement en mode admin. Pour trouver où est le code de l'exécution du bouton connexion, on peut faire comme ce qu'on a vu précédemment avec le debug de manière plus ou moins aléatoire. Où on peut se servir de "Event listener breakpoints", pour s'arrêter à une action/événement particulier.



**Figure III.8:** Event Listener Breakpoints

Comme le bouton connexion enclenche l'évènement click, on va raisonner de manière logique, en tentant "Mouse: click". Lorsqu'on tente de faire un click, on s'arrête bien dans

le code grâce au debug Event Listener Breakpoints. Mais le code où on est placé n'est pas celui qu'on souhaite avoir, on tombe sur les codes d'assez bas niveau. De plus il ne se passe absolument rien, on n'observe pas d'erreur comme "Veuillez remplir tous les champs" ou "Veuillez saisir une adresse email correcte" car on a laissé le champ vide. La raison est due au timeout, le fait qu'il se bloque sur le breakpoint n'a pas déclenché son évènement attendu.

Avec la première tentative, on a rien obtenu, ce qu'on va faire à la suite c'est étudier le comportement de connexion pour voir si on peut s'arrêter avec d'autres Event Listener Breakpoints. Et lorsqu'on étudie attentivement l'action du bouton connexion, on observe plusieurs comportements/événements :

- Lorsqu'on clique, un message apparaît si l'adresse email ou le mot de passe n'est pas bon, puis qui disparaît après un certain temps (Event responsable : Timer).
- On peut faire en sorte de faire connexion avec le bouton "Entrée" à la place d'un click (Event responsable : Keyboard).

Maintenant qu'on observe de nouveaux comportements du bouton connexion, on va tenter de s'arrêter avec ces events. Avec la tentative de l'événement "Timer", on s'arrête au niveau où on définit un timeout pour enlever le message d'erreur qui se trouve exactement dans la fonction qu'on souhaite atterrir "connexionButtonHandler". Ensuite on va tenter de voir avec le second événement "Keyboard" avec le bouton entrée. Lors de cette tentative, on atterrit sur un code un peu plus haut qui gère les touches claviers comme "Tab" ou "Entrée". On voit dans le management de la saisie de la touche "Entrée", que la fonction "connexionButtonHandler" est appelée.

Avec les deux événements précédents, on arrive bien à s'arrêter sur le code que nous voulons. À la suite de ceci, on modifie le code pour essayer de rentrer sans se connecter. Le résultat c'est qu'on a réussi à rentrer dans le "Dashboard Admin" avec les formations chargées. Les formations publiées et ceux qui ne sont pas encore publiés comme vous pouvez le voir sur la figure ci-dessous. Malgré le fait qu'on a réussi à charger la vue Dashboard Admin, les clicks sur les formations ne font absolument rien, aucune erreur n'est affichée côté client. De même si on tente de recharger la page, le serveur ne répond plus. Si on regarde le côté serveur, on voit qu'il a crashé, car il a essayé de charger un token à partir d'un user. Et comme on ne s'est jamais identifié, on n'a donc pas de token. Les détails d'étape par étape sont décrits en annexe [C.1 Modification étape 1](#).



**Figure III.9:** Dashboard Admin

Avec la tentative de faire passer pour administrateur en modifiant le comportement numéro 1 (Figure SD Client), ne nous a pas rapporté de bonnes réponses, car on a fait crashé le serveur avec le code modification. Ce que nous allons faire maintenant c'est essayer de se modifier le comportement numéro 2. C'est à dire que nous allons connecter avec un vrai

utilisateur non admin, et nous allons faire en sorte de modifier le code pour se connecter en tant qu'administrateur.

**Figure III.10:** Quiz Vue Admin

Résultat après la modification du code, on arrive bien à se connecter sur la vue Dashboard Admin avec les formations chargées. Contrairement à l'étape précédent cette fois-ci, on peut cliquer pour accéder à une formation et bien évidemment voir les bonnes réponses. On n'a également pas de problème avec le token car on s'est bien authentifié, les étapes détaillées sont expliquées en annexe [C.2 Modification étape 2](#). On peut également modifier le code pour faire en sort d'afficher que les bonnes réponses.

### III.C.4. Objet modification

Il y a également d'une autre manière de tricher avec le navigateur, c'est de modifier les données via la console du navigateur. Il suffit de chercher dans la variable Windows ou si on est passiants on pourrait chercher les noms des variables en lisant le code.

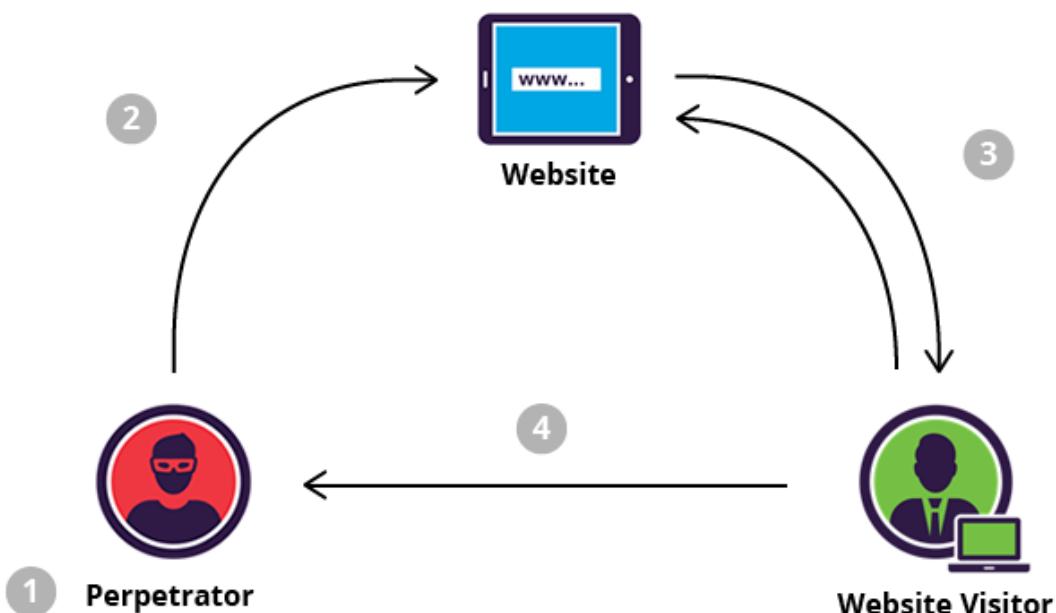
```
> window.test
<- undefined
> window.test = {name: "Modification", lastName: "depuis le console"}
<- > Object {name: "Modification", lastName: "depuis le console"}
> window.test
<- > Object {name: "Modification", lastName: "depuis le console"}
```

**Figure III.11:** Modification depuis le console

Si le pirate connaît bien la forme de donnée du jeu, il pourra modifier et envoyer comme données réelles sur le serveur.

### III.C.5. Cross Site Scripting (XSS)

Le **Cross-Site Scripting (XSS)** est une attaque qui a pour but d'injecter du code malveillant pour que l'utilisateur exécute depuis son navigateur. Il existe deux sortes de types attaques en **XSS**, le réfléchi et le stocké. On appelle l'attaque réfléchi car il n'est pas stocké sur le serveur ou dans un fichier. La victime reçoit cette attaque via un mail qui utilise les liens contenant le script injecté (en paramètre de **URL**). Lorsque la victime clique sur ce lien, le code malveillant qui est non filtré par le serveur va être exécuté par le navigateur. L'attaque stockée consiste à injecter le code malicieux sur le serveur, par exemple dans un commentaire qui sera visible pour tout monde. Lorsque l'utilisateur charge sa page, ceci va exécuter le code qui peut effectuer des manœuvres qui peuvent envoyer les cookies de l'utilisateur actuels. Ou encore, implémenter un "Keylogging" pour enregistrer ce que tape l'utilisateur.



**Figure III.12:** Attaque XSS [63]

1. Le pirate va chercher une faille dans le site, s'il peut injecter des données via **URL** paramètre ou encore des éléments **HTML**. Il peut combiner avec l'attaque précédent "Code modification" pour rentrer avec les droits admin.
2. L'attaquant crée une formation tout en injectant son script afin de pouvoir voler les cookies ou les mots de passe des utilisateurs.
3. L'utilisateur se connecte, et charge la formation avec le code injecté.
4. Sans se rendre compte que l'utilisateur envoie des données confidentielles à son attaquant. Le pirate peut se connecter par le biais de la session ou avec les informations saisies au clavier.

Les attaques peuvent être écrites en n'importe quel langage, tant qu'il est exposé à **XSS** et compatible avec le navigateur [64, 65].

### III.C.6. Injection

La base de données utilisée dans le projet est le MongoDB, elle nous permet de stocker un document, récupérer via une seule clé et c'est un serveur [NoSQL](#). Le terme [NoSQL](#), désigne les bases de données qui ne sont pas fondées sur l'architecture classique des bases de données relationnelles. Grâce à ceci, on n'est pas obligé d'avoir une structure similaire et qui nous évite de faire des jointures partout les tables. Par exemple on peut mettre dans la [BDD](#) un quiz avec trois questions qui et un autre avec dix questions. Il permet de répondre également à la cohérence, la haute disponibilité et la tolérance au partitionnement. Mais d'après le théorème de [Consistency Availability Partition tolerance \(CAP\)](#), les serveurs [NoSQL](#) ne peuvent avoirs seulement deux sur trois des caractéristiques [75].

Le No SQL, n'est pas signe de non injection, les serveurs tels que mongoDB utilisé derrière NodeJs n'assure pas la protection contre les attaques. Le mongoDB est dans le top 5 des serveurs les plus populaires, qui stocke ces données en [JSON](#). Le [JSON](#) est très utilisé entre les échanges de données avec les serveurs [76].

Imaginons pour se connecter, on a besoin d'un email et un mot de passe sous cette forme. Avec ces données correctes ci dessous lorsqu'on soumet on arrive bien à se connecter.

```
{
  "email" : "pentesterkunal@live.com",
  "password" : "scotch.io"
}
```

**Figure III.13:** Forme de données correctes en JSON [79]

Maintenant si on va essayer de contourner le serveur afin de se logguer sans à mettre une identification valide.

```
{
  "email" : {"$gt":""},
  "password" : {"$gt":""}
}
```

**Figure III.14:** Forme de données exploitées en JSON [79]

En mettant ces données, on arrive à se connecter sans à avoir à mettre un vrai email. L'opération \$gt permet de dire a MongoDB de donner ce qui plus grand que des caractères vides. Ce qui retourne "true" et qui laisse l'attaquant à se logguer sur le système [77, 78]. Le terme \$gt n'est pas la seule façon d'injecter, si on recherche plus en profondeur sur le langage, on peut voir d'autres par exemple \$ne qui signifie différent. Pour pallier à ce problème on peut convertir tous les valeurs entrants en une chaîne de caractères, pour que mongo ne l'exécute pas comme du code. Malgré le fait qu'on a mis les valeurs en string, le risque d'injection est encore là, avec l'opérator \$where qui est très dangereux car elle permet les chaines de caractères à être exécuté. De plus, elle n'est pas performance car elle ne garde pas les indexes, le scope n'est pas accessible (en Javascript). Et de plus avec la version 2.1 de Node.js Mongo, l'opération bug si on lui donne en argument une fonction, ceci retourne tout [79].

# IV Protection

## IV.A. Protection globale

### IV.A.1. La mise à jour

Rester bien à jour pour bénéficier les derniers patches afin de protéger des attaques sur votre serveur/applications. On en découvre tout les jours des vulnérabilités, qui sont exploitées à des fins malicieuses.

### IV.A.2. Identifier les vulnérabilité des composants

Identifier tous les composants utilisés librairies, framework et composants. Éviter de les exposer, ne déployer pas les composants/librairies que vous n'utilisez pas. Il faut obfrusquer les liens ou les chemins avec des mots clés qui permettraient d'identifier la librairie, on ne doit pas divulger les informations sur [Operating System \(OS\)](#), le serveur, la [BDD](#), tous les maillons qui pourraient nuire à l'application. Il faut faire en sorte de rendre plus difficile les attaques, en cachant/supprimant tout informations qui pourrait identifier la librairie ou la technologie, c'est ce qu'on appelle la sécurité par l'obscurité. Il faut maintenir à jour les composants utilisés, englober les composants qui sont identifiés à risque [66].

### IV.A.3. Mauvaise configuration

La mauvaise configuration peut causer parfois de sérieux problèmes. Des paramètres par défaut qui ne sont pas changés par exemple les logins et les mots de passe de l'administrateur. Ou encore des applications qui sont installées avec le serveur et dans lequel on a oublié d'enlever les configurations par défauts [67].

### IV.A.4. Les guides - Bonnes pratiques

Il existe des guides de bonnes pratiques qui permettent d'éviter des erreurs débutants comme [OWASP.org](#) qui décrit quelles sont les recommandations à appliquer. D'autres sites qui permettent de rester à jour des failles découvertes [thehackernews.com](#). Il faut faire également à en sorte l'application n'accepte que les mots de passe soient compliqués et assez long, l'OWASP conseille de fixer à 8 caractères minimum afin de minimiser les attaques. Il faudrait les composer de lettres majuscules, minuscules avec des chiffres et caractères spéciaux, c'est de cette façon qu'on ralentira le brute force. De même, il faut éviter de renvoyer toutes les erreurs en claire à l'utilisateur. Car si l'utilisateur connaît l'erreur, il gagnera du temps pour effectuer son attaque, alors que le but des protections et des préventions mises en place c'est pour le ralentir. Il faut également mettre en place des systèmes qui permet de bannir l'utilisateur temporairement ou définitivement lors des tentatives d'accès à l'authentification ou encore les

autres web services. Il faut limiter les méthodes GET avec des paramètres, et il faut traiter les données sortant pour se prémunir des attaques [XSS](#).

## ***IV.B. Protection coté client***

### ***IV.B.1. Offuscation***

Offuscation est une méthode qui utilise la minification, qui permet de réduire tout caractère inutile comme les commentaires, les espaces et les indentations. La minification permet de rendre le code moins lisible et de plus elle augmente la performance, car on réduit le temps de chargement vu que la taille du fichier est réduit mais rend également plus dure à debugguer. L'ofuscation utilise aussi le renommage des fonctions et des variables, ceux qui rendent le code incompréhensible. Il faut savoir que sur le côté client, s'il y a des failles on ne fait que ralentir l'attaquant. Il prendra du temps à comprendre, mais il pourra toujours attaquer [68].

Le problème est que si on met en place l'offuscation, c'est lorsqu'on souhaite debugguer qu'on se retrouve avec un code totalement incompréhensible. Il faut mettre en place une intégration seulement en production (lors du push sur les dépôts), comme ça lorsque qu'on est en développement on se retrouve pas à déboguer un code offusquer. On peut trouver plusieurs services d'après les recherches qui permettent d'offusquer les codes JavaScript et qui permet de geler le debug côté front, comme JSScrambler ou encore javascript-obfuscator qui sont compatible avec NodeJS. Bien évidemment, l'obfuscation a une répercussion auprès de la performance, comme la taille du code peut être augmenté et certaines options qui peut ralentir un peu plus.

### ***IV.B.2. Protection contre les modifications***

Comme on le sait, on ne peut faire confiance au client, car les utilisateurs malhonnêtes peuvent modifier le code source du côté client. Pour résoudre plus ou moins ce problème, on peut mettre en place le Mutation Observer. Elle nous permettra d'émettre des évènements lorsque les [DOM](#) sont modifiés et donc réagi à l'action. On peut faire observer une modification des [DOM](#), qui déclenche un évènement comme la déconnexion de l'utilisateur, encore supprimer la session utilisateur. Ou encore on peut tout effacer les objets [SVG](#), détacher tous les fichiers pour que le pirate puisse faire quoi ce soit. Il faut faire également attention à le désactiver lorsque ce sont nos actions qui sont la cause des modifications [69, 70].

Pour ce qui est des objets JavaScript, il y a plusieurs façons de rendre les objets immutables depuis la console du navigateur :

- `Object.freeze` : cette méthode permet de prémunir d'ajout de nouvelles propriétés. Ou encore d'effacement, et modification des propriétés. Problématique de cette méthode, est qu'elle applique seulement au parent, si on veut rendre l'objet enfant immuable il faut répéter l'action et de la même façon pour l'objet enfant de l'enfant.
- `Object.seal` : cette méthode est presque identique que celui de `Object.freeze`, sauf qu'on peut réaliser des modifications des propriétés déjà existants.
- `Object.preventExtensions` : comme son nom indique, cette méthode empêche seulement d'ajout des nouvelles propriétés.

Il faut bien évidemment choisir la bonne méthode selon le contexte et les besoins. Même si on a ces méthodes, on ne peut sceller tous les objets. Les objets qui ne sont pas scellés,

sont accessibles depuis la console et donc sont modifiables. Pour éviter qu'il soit accessible depuis la console, il faut éviter les variables globales et réaliser des fonctions anonymes.

```
(function(){
  /**
   * All the code that needs to be unexposed in the console here.
   */
  DO; // Send parameters inside the function if you need to
})
```

**Figure IV.1:** Fonction anonyme [71]

Malgré toutes ces protections, le code JavaScript est du côté du client, donc toujours accessible, et ça n'arrêtera pas le pirate. Cette méthode marchera peut être la première fois, mais les fois suivant ne fonctionnera plus avec. Ces objets restent modifiables, il suffit de le faire avant que les objets ne soient scellés ou par la modification d'une ou plusieurs parties du code [71].

## IV.C. Protection coté serveur web

### IV.C.1. Contrôle coté serveur

On a pu voir dans la partie les attaques, certaines sont réalisable car les validations sont réalisées par le client. De ce fait les données qu'on reçoit n'importe quoi, ce qui peuvent provoquer des graves dommages. Dans les règles de sécurités de bases, il ne faut jamais faire confiance au client comme on a pu voir la partie "code modification". Le client peut toujours modifier, ou désactiver les protections coté web, il faut donc s'assurer de filtrer ce qui vient du client afin d'assurer le bon fonctionnement de l'application.

Il faut voir la différence entre la validation des données coté client et coté serveur. Le contrôle coté client n'est pas fait pour sécuriser l'application, mais de filtrer un grand nombre de requêtes qui ne sont pas avec le bon format ou encore avec des données correctes. C'est une question d'optimiser les performances du serveurs, mais également une question d'estétique. Il vaut mieux un message qui apparaît pour nous prévenir que les données sont fausses, qu'une requête envoyé au serveur qui va la rejeter. C'est donc le serveur qui a la responsabilité de vérifier les formes de données, si elles sont correctes et de parser les données. Parser et contrôler les données permet de se protéger contre les injections qui peut nuire au serveur et à la BDD qui sont volontaires ou involontaires [74].

## IV.D. Protection Serious Game

Dans cette partie les protections proposées seront moins techniques, ça seraient plutôt des ruses ou stratagème qu'on pourra appliquer afin de rendre les tricheries plus difficiles.

### IV.D.1. Disposition

Très souvent les tricheurs coopèrent avec un ou plusieurs complices, ces complices peuvent les aider en fournit le questionnaire du jeu qu'ils ont passé. Certains de ces tricheurs vont essayer de faire le minimum en essayant d'apprendre seulement les dispositions des réponses dans l'ordre. En jouant avec la disposition du jeu, on peut perturber ce type de tricheur.

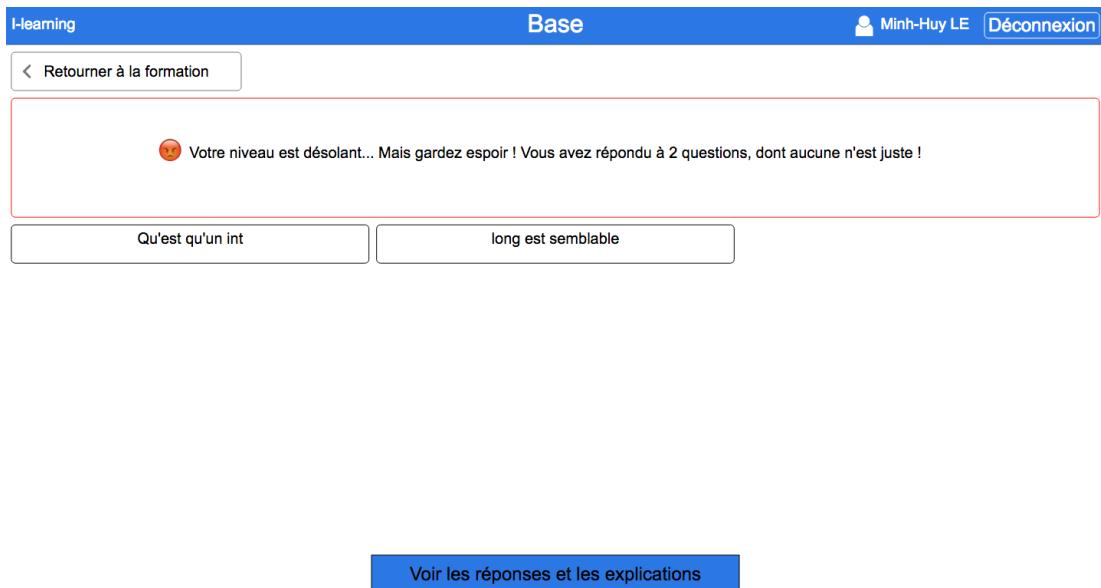
La disposition du jeu est celui le plus facile et rapide à mettre en place. Il suffit simplement de mélanger les ordres des questions, changer les emplacements des réponses d'une façon

aléatoirement. Ce stratagème piègera les premiers tricheurs, mais à la suite de cette échec, ces tricheurs vont avertir ces complices. Ils ne pourront pas se fier à l'ordre des questions et l'emplacement des réponses. Ce qui les oblige à apprendre tout par coeur, la question et les réponses pour les prochaines formations ou tests.

Pour contrer ceux qui apprendre par coeur la question et la réponse. On prépare une grande séries de questions, beaucoup plus qu'il en faut. Puis présenter aléatoirement seulement une partie de la série. Avec ce stratagème, connaitre les questions et les réponses par coeur ne lui servira à pas grand chose, car il ne lui sera pas en d'être certains de tomber sur les mêmes questions.

#### ***IV.D.2. Les corrections***

Dans les jeux sérieux, le concept met souvent à disposition du joueur une correction ou un retour lorsqu'il réalise des erreurs sur les parties du jeu. Ces corrections peuvent être instantané, c'est à dire lorsque qu'on soumet une erreur ou une série de réponses, l'explication vient et n'est disponible que pendant la session. Elle peut être très scolaire (en forme de révision), c'est à dire lorsqu'on finit une série de jeu, une correction est proposé et accessible à tout moment comme on peut observer sur la figure IV.2.



**Figure IV.2:** Les corrections sur le projet I-Learning

La correction ou les retours permet au joueur de mieux appréhender l'exercice et comprend ses erreurs. Nous allons voir ensuite comment se protéger avec les trois types de corrections : scolaire, instantané et vague.

#### **Correction scolaire**

Avec la correction scolaire, l'utilisateur peut donc voir toutes les séries de corrections quand il le souhaite des formations déjà réalisées. Chaque série compose toutes les questions de la série précisant pour chaque question les bonnes réponses et les réponses fausses. Le problème est qu'on peut accéder quand on le souhaite, il devient critique lorsque cet utilisateur se fait voler son login et mot de passe. L'attaquant peut donc tricher grâce aux séries de corrections de la victime si la victime a effectivement réalisé des formations via l'application. Sinon il doit voler les autres authentification afin d'obtenir tous les détails supplémentaires. Ou simplement de

prend le compte de la première victime, et réaliser la formation afin d'obtenir la correction, mais en réalisant ce geste l'attaquant prend un risque de se dévoiler. La victime pourra prendre connaissance qu'on lui a voler l'information, et avertir l'administrateur.

Pour éviter ce genre de tricherie, on peut envoyer par mail la correction sur la demande du joueur. Avec ce stratagème, on rend plus difficile l'attaque, car le pirate doit voler en plus le mot de passe de l'adresse mail de sa victime pour apercevoir la correction. Il doit prendre soin d'effacer sa trace s'il arrive à se faufler dans la boîte mail de la victime, effacement du mail provenant de I-Learning pour la demande correction.

On peut limiter le nombre des demandes de corrections par jour, ce qui fait que si l'attaquant arrive à voler l'adresse mail, le mot de passe du jeu et le mot de passe du mail. Mais il pourra seulement demander à la limite autorisé, où il devra chercher d'autres victimes ce qui augmente le risque d'être découvert. On peut mieux faire encore, en affichant un compteur des demandes réalisés par le joueur sur chaque formation. Si le tricheur arrive à introduire sur le compte de l'utilisateur, et en fait la demande de correction de la série. Le numéro de la demande va être incrémenter, grâce à système lorsque la victime revient sur l'application. Il pourra détecter qu'il y a un changement sur son compte avec les compteurs, prend des mesures pour éviter de nouveaux infiltrations comme informer l'administrateur afin de bannir le tricheur ou encore changer le mot de passe.

### **Correction instantané**

La correction instantané n'est pas si différent que la correction scolaire. Sauf qu'elle n'est accessible que temporairement, à un moment ou un état précis. Comme après la réalisation de la formation, on peut autoriser l'utilisateur à voir la correction pendant une limite de temps ou jusqu'à la fermeture de la session. Mais ça ne suffit pas, car le tricheur pourra relancer la formation afin d'obtenir la correction instanné.

Il faut donc limiter la réalisation du jeu, en autorisant seulement par la demande du joueur. Il doit confirmer via un lien qu'il recevra par mail lorsqu'il en fait la demande. Après confirmation, l'accès à la formation est limité par le nombre de fois avec une date d'expiration. Au delà de cette date, il ne pourra plus accéder, et doit faire à nouveau la demande et justifier pourquoi il souhaite refaire l'exercice.

### **Correction vague**

On peut faire en sorte de donner une correction vague, c'est à dire en donnant tout simplement le nombre de faute pour la séries de la correction sans préciser aux candidats la quelle entre elle est incorrecte. Pour l'apprentissage c'est une excellente méthode, si on souhaite que les apprenantes connaissent absolument tous les bonnes réponses. Vu qu'ils ne savent pas où est qu'ils ont faux, ils doivent tous relire l'exercice, relire les leçons et recommencer l'exercice afin d'avoir la totalité des réponses exactes. Pour évaluer un candidat, on peut soit lui donner le nombre de réponses qui sont incorrectes où tout simplement ne rien lui dire, et faire en sorte qu'il attend un retour du l'examinateur.

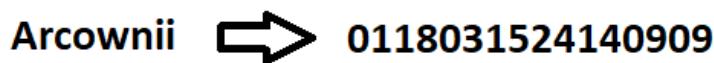
### ***IV.D.3. Question sur mesure***

Des questions sur mesure selon le candidat peut être une solution pour certains tricheurs. On créer un grand nombre de question par technologie, langage de programmation, et on regarde selon l'expérience, les compétences du candidat pour sélectionner des questions qui correspond à son niveau. On peut donc garantir que les chacuns des candidats aura un bundle de questions sur mesure, à conditions si on a un grand nombre de questions. Les candidats

ne peuvent donc pas prévoir les questions avec un complice ou encore voler un compte d'un autre candidat.

#### IV.D.4. Réponses variables

On peut faire en sorte d'avoir des questions avec des réponses variables, comme sur des questions "Parmis ces réponses, sélectionner les int". Ces entiers on peut générer aléatoirement, ou encore par rapport à le pseudo de l'utilisateur. Etant donnée que le speudo est unique, on est sûr que sur ce genre de questions, chaque utilisateur a différent réponses. C'est comme si on utilisé le pseudo comme une clé de cryptage, mais il faut fixer le pseudo à une grande taille au moins 8 caractères. Pour générer on prend le pseudo, changer les caractères en chiffre afin de pourvoir générer les réponses avec ces chiffres.



**Figure IV.3:** Transformation pseudo en chiffre

#### IV.D.5. Double authentification

Comme on a pu le voir le problème des authentifications, c'est qu'ils sont vulnérables aux attaque. On peut les attaquer avec le brute force qui permet de tester tout les combinaisons possibles. Un gestion d'authentification insuffisant, les droits sont mal gérer, ou sont mal protéger aux injections. Il peut être facilement voler, comme par le phishing qui est une technique d'obtenir les informations personnels ou confidentiel, en fesant croire à la victime qu'elle s'adresse à un tiers de confiance. Ou par un Keylogger, qui va mémoriser tout les touches claviers taper par la victime. On peut donc penser à protéger en inspirant les sites connus comme Facebook ou encore sur Gmail avec le double authentification.

Un double authentification est une authentification à deux facteurs. Il s'agit d'un processus qui permet d'ajouter une authentification supplémentaire comme son adresse email ou le numéro portable. Ce processus de sécurité simple permet de rajouter un niveau de sécurité en plus. Quand on dit sécurité, ce n'est pas forcément des processus compliquer. Sur Gmail, lorsqu'on vient de s'inscrire, le service nous permet d'insérer un numéro téléphone afin de faire une double authentification. Lorsque vous avez saisi le login et le mot de passe, Google vous envoit une clé sur votre téléphone portable afin de vérifier que c'est bien vous.

On pourra inspirer et en faire de même mais avec un style de jeu, on peut demander à l'utilisateur de définir un jeu de puzzle et une solution. Comme par exemple un jeu de mot caché, d'où on définit la grille et quelles sont les mots que l'utilisateur doit sélectionner pour pourvoir accéder sur le compte. On peut même penser à un ordre précise de sélection de mots un peu comme un coffre fort. Lorsqu'on se connecte sur le compte il doit résoudre le puzzle fait, si il échoue ou ne réalise pas exactement comme la solution définit, on peut soit bloquer directement l'utilisateur par son adresse [Internet Protocol \(IP\)](#) au bout du premier ou plusieurs tentatives.

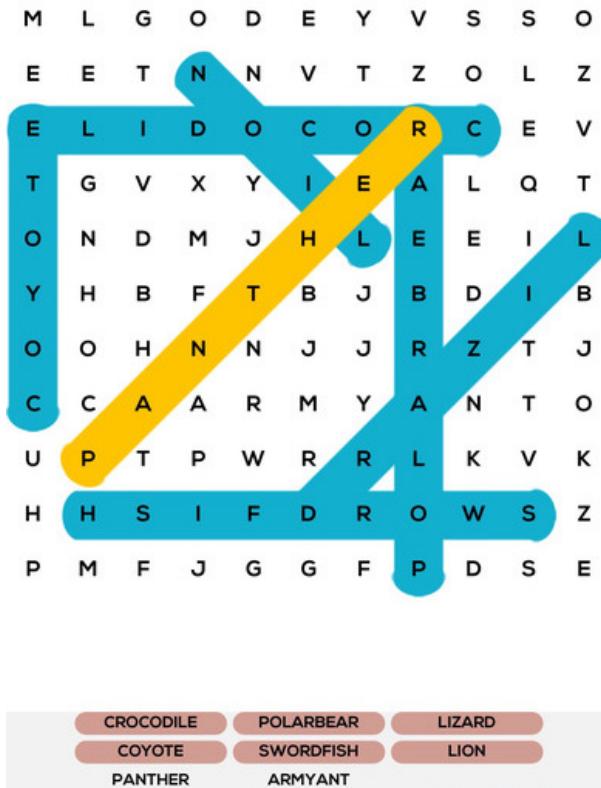


Figure IV.4: Mot mystère [80]

Ou on pourra penser à une autre manière du double authentification en demandant à l'utilisateur à travers d'une série de questions comme quels sont les jeux/formations qu'il a terminer. Avec les questions qui ne composent pas forcément des réponses, de cette manière, seul l'utilisateur pourra connaitre la réponse afin d'accéder son compte.

#### IV.D.6. Le règlement

Un jeu avec ses règles écrites, est parfois la meilleure protection contre les tricheurs. Dans certains applications et pays, c'est même obligatoires de rédiger dans les conditions générales d'utilisations. Si les règles sont pas claires, ne sont pas préciser ou encore transmit à l'oral, ceux qui peut amener à des tricheurs involontaires. Certains vont être consider comme tricheur par les autres alors qu'il joue tout simplement sans connaître des règles officiels. Le pire cas, c'est chaque joueur a sa propre perception des règles ceux qui peut nuire au jeu voir faire fuire des utilisateurs. Il faut donc énoncer clairements des règles, et préciser une possibilité de punissement aux joueur suspect de tricherie. Les punissements peuvent être divers selon le cas d'utilisation de la gamification. Imaginons si l'application est utilisé pour les consultants d'une ESN, on peut penser à les privés d'une augmentation lors de la réévaluation. Dans le cas d'un jeu sérieux en grande publique, ou dans les concours avec un prix pour les top 3, on pourrait pensé à un bannissement du joueur ou l'annulation de sa participation. En énonçant qu'il y a une possibilité de bannir un joueur suspect et une annulation de récompense, on va ainsi décourager les tricheurs à tenter quoi ce soit. Il faut faire en sorte que les joueurs puissent prendre connaissances des règles. Comme afficher les règles à coté de du jeu, ou lors de sa première visite le faire suivre un tutoriel avec les règles écrit en plein écran. Il faut mettre également dans les options, pour que l'utilisateur puisse revoir les règles quand il se souhaite de cette façon il ne pourra pas nier de ne pas avoir vu ou accéder aux conditions d'utilisations.

#### *IV.D.7. La multi-participation*

Lorsque les jeux incitent les joueurs à inviter des amis ou parrainer les autres utilisateurs afin de gagner des récompenses supplémentaires, celà peuvent provoquer très rapidement des tricheries. Cette triche est la plus répandue dans les jeux qui propose ce genre de parrainage. Car elle est très facile à réaliser, l'opération pour créer une nouvelle adresse mail dure environ 2 minutes (Yahoo, Hotmail, Gmail, etc.). Le tricheur va donc participer plusieurs fois, en créant des fausses comptes et se parrainer afin d'obtenir l'option de viralité. L'erreur la plus courante est de se baser sur l'adresse mail pour différencier chaque personne. La solution consiste à vérifier pas seulement l'adresse mail, mais également l'adresse IP de chaque participation. Si une personne participe plusieurs fois, elle sera détecter par son adresse IP et donc exclure l'ensemble des participants pour tricherie [81].

Mais ce genre de protection ne résoudre pas totalement le problème, car il existe des logiciels très simple qui sont capable de faire croire à l'application qu'il a une autre adresse IP. Ces logiciels sont énormes sur la toile, vous trouverez très rapidement en cherchant simplement sur internet, qui sont la pluparts gratuites. Il y a aussi des administrateurs réseaux qui travaillent dans le data center. Le datacenters est un centre de données, d'où sont stockés un nombre important de serveurs. Lorsque vous effectuez une recherche sur un moteur de recherche, c'est souvent le datacenter le plus proche qui se charge de fournir les résultats appropriés à votre demande. Avoir une adresse IP n'est pas difficile pour les administrateurs réseaux, ils ont souvent un droit administrateur ou un accès sur tous les machines. Il faut donc trouver une autre méthode, comme forcer les parrains à jouer au moins une heure tout les jours pendant un mois ou encore les forcer à jouer pour atteint un niveau, réussir à des jeux spécifiques afin que le parraineur puisse toucher à sa récompense promise. En mettant ceci en place on peut vite décourager les joueurs, car il faut effectuer un effort qui sont parfois pas rentable par rapport aux cadeaux.

#### *IV.D.8. Comportement anormale*

Détecter un comportement anormal, peuvent être une mesure de préventive des tricheurs. Comment déterminer le comportement anormal ? Il existe plusieurs type de comportement anormal, les personnes qui sont en dépression, les personnes handicapées, mais ces comportements ce sont pas ceux qu'on recherche. Le comportement anormal qu'on recherche est celui de violation des normes, innatendu ou peu fréquent. Comme une personne qui a l'habitude de travailler le matin pendant des mois, et tout à coup on observe une connection de sa part à 2 heure du matin. La personne qui réalise plusieurs formations en 5 minutes alors qu'il devrait durer 50 minutes, c'est ce qu'on appelle speed hacking, on pourra suspecter que cette personne de tricherie. De sorte qu'elle s'est fait voler son compte par un autre candidat, qui utilise le sien pour déterminer voir la correction, un sabotage du compte ou cette personne a une combine pour terminer tous les formations avec que des bonnes réponse [82].

On peut insérer également la localisation du compte pour détecter s'il a pas des changements inhabituel de localisation, ceux qui permet de détecter les voleurs de comptes. Les changements de style comme les technologies, langages des formations, que le collaborateur travaille sur un projet mobile iOS mais sur l'application on voit qu'il ne réalise que des formations de langage C. Il faut savoir également qu'il est parfois difficile de déterminer un comportement anormal. Car on ne peut prévoir tous les comportements, il se pourrait qu'il souhaite progresser, ou va être muter sur une autre mission et il faut donc prendre ce cas en compte. Et ne pas bloquer l'utilisateur directement, mais faire en sorte de prouver que c'est l'utilisateur en lui demandant de confirmer via des informations seul lui peuvent savoir.

# Bilan

## A. Conclusion

A travers de ce mémoire, nous avons pu voir ce que c'est un serious game. Qu'ils sont présentes dans notre vie quotidienne, que ce soit dans le domaine de automobile, militaire, les grandes entreprises ou chez les particuliers. Les différents types de jeux sérieux, ses avantages et ses limites. Malgré ses limites, ils représentent une part sur le marché, et ses avantages attirent les entreprises que ce soit en tant qu'utilisateurs ou fournisseurs. Nous avons vu également pourquoi il y a seulement des triches sur certains types de jeux et d'autres non. Nous avons étudié plusieurs types d'attaques pouvant être menées sur le projet d'I-Learning que mène VISEO afin de former ses collaborateurs et stagiaires. Cependant le panel de cyberattaques démontré n'est pas exhaustif, il existe une multitude d'autres attaques que nous n'avons pas pu aborder par manque évident de temps.

Malgré ces failles qui sont découvertes, la pluparts des applications ne sont pas du tout sécurisées car les développeurs n'y prêtent pas attention. Comme le contrôle des données qui sont effectués seulement coté client alors que selon les règles de sécurité il faudrait faire au minimum sur le coté serveur ou les deux. Il y a des développeurs qui ne savent même pas que les **BDD** sont vulnérable aux injections. Nous avons pu voir également les protections contre les attaques, qui est concentrée sur la problématique "Comment éviter la triche sur un serious game ?". On a pu apercevoir que pour empêcher les attaques il faut tout d'abord étudier l'application. Identifier tous les maillons de la chaîne afin d'analyser les risques à tout niveau, dans quel langage est développée l'application, quel **BDD** intégrer, sous quel **OS** est l'application, etc. Il faut donc sensibiliser les développeurs afin qu'ils se posent des questions et mettent des mesures préventives pour minimiser les risques. Pour assurer une bonne sécurité, il vaut mieux combiner un ensemble de protections qu'appliquer une seule et surtout de rester à veille aux nouveaux failles découvertes.

L'état actuel du projet d'I-Learning, n'a très peu de sécurité voir pas du tout, ce qui élargit les possibilités d'attaques sur l'application. Mais celui-ci n'est pas encore en production, on n'a pas pu évaluer l'impact de la sécurité ni disposer de données réelles afin d'analyser quelconque triche. Il ne faut pas s'attendre à ce que votre projet soit attaqué pour mettre en place des outils de sécurité et surtout ne pas attendre la fin du développement pour les mettre en place. Cela peut représenter beaucoup de travaux qui prendra du temps, mais également un coût supplémentaire qui peut être conséquence.

Bien qu'il existe des protections, il faut savoir qu'il n'existe aucune mesure de sécurité infaillible. Les protections ne sont là que pour ralentir les tricheurs, il sera toujours possible pour lui d'attaquer le projet. La question n'est pas "Comment mettre en place une sécurité infaillible ?" mais de se poser "Combien de temps il mettra avec la protection mise en place ?".

## **B. Perspective**

On pourrait aller plus loin en mettant tous les protections nécessaires sur le projet, et tenter à nouveau de tricher. Voir si la triche est possible : comparer le temps nécessaire pour attaquer le projet avant et après. Trouver des moyens de détecter les tricheries afin de bannir ou bloquer l'utilisateur jusqu'à ce que l'administrateur vérifie les faits pour prendre une décision finale. Mais malheureusement, par manque de temps, les protections n'ont pas tous été implémentées sur le projet d'I-Learning. De plus le projet n'a pas cessé d'évoluer, développement de nouvelles fonctionnalités pour arriver finalement à une refonte totale de l'application, principalement pour des problèmes d'architecture.

# Bibliographie

- [1] Wikipedia, **Document Object Model**. Publié/Modifié le 7 juillet 2017, dernier accès le 21 Juillet 2017  
[https://fr.wikipedia.org/wiki/Document\\_Object\\_Model](https://fr.wikipedia.org/wiki/Document_Object_Model)
- [2] flaticon, **Svg file format symbol Free Icon**. Publié/Modifié en 2015, dernier accès le 30 Juillet 2017  
[http://www.freepik.com/free-icon/svg-file-format-symbol\\_742222.htm#term=svg&page=1&position=14](http://www.freepik.com/free-icon/svg-file-format-symbol_742222.htm#term=svg&page=1&position=14)
- [3] JustInMind, **How to simulate a Drag and drop in your interactive wireframes**. Publié/Modifié date inconnue, dernier accès le 21 Juillet 2017  
<https://www.justinmind.com/support/how-to-simulate-a-drag-and-drop-in-your-interactive-wireframes/>
- [4] Equipe Serious Game blog, **Le marché des Serious Games continue sa bonne croissance en 2017**. Publié/Modifié le 30 Mars 2017, dernier accès le 7 Juillet 2017  
<http://www.serious-game.fr/marche-serious-games-continue-bonne-croissance-2017/>
- [5] statista, **Chiffres d'affaires de McDonald's 2006-2016**. Publié/Modifié en 2017, dernier accès le 22 Juillet 2017  
<https://fr.statista.com/statistiques/559250/chiffres-d-affaires-de-mcdonald-s/>
- [6] infoDSI, **Le point sur l'évolution des Serious Games, du e-learning/Mobile Learning, Gamification, Moocs, des solutions et logiciels RH à l'horizon 2016-2020**. Publié/Modifié le 12 décembre 2016, dernier accès le 7 Juillet 2017  
<http://www.infodsi.com/articles/166234/point-evolution-serious-games-learning-mobile-learning-gamification-moocs-solutions-logiciels-rh-horizon-2016-2020.html>
- [7] Michel LAVIGNE, **Pertinence et efficacité des serious games. Enquête de réception sur neuf serious games**. Publié/Modifié en 2013, dernier accès le 7 Juillet 2017  
[http://www.academia.edu/5981159/Pertinence\\_et\\_efficacit%C3%A9\\_des\\_serious\\_games.\\_Enqu%C3%A8te\\_de\\_r%C3%A9ception\\_sur\\_neuf\\_serious\\_games](http://www.academia.edu/5981159/Pertinence_et_efficacit%C3%A9_des_serious_games._Enqu%C3%A8te_de_r%C3%A9ception_sur_neuf_serious_games)
- [8] Jean-Luc RAYMOND, **Serious games : Définition, enjeux, choix**. Publié/Modifié le 12 septembre 2013, dernier accès le 7 Juillet 2017  
<https://jeanlucraymond.fr/2013/09/12/serious-games-definition-enjeux-choix/>
- [9] Qu'est-ce que l'e-learning ?, **Serious games : Définition, enjeux, choix**. Publié/Modifié date inconnue, dernier accès le 22 Juillet 2017  
<http://e-learning.prestataires.com/conseils/quest-ce-que-le-learning>

- [10] Steph, **L'apparition des serious games**. Publié/Modifié le 7 novembre 2006, dernier accès le 7 Juillet 2017  
<http://seriousgames.canalblog.com/archives/2006/11/07/3137235.html>
- [11] Wikipedia, **Battlezone**. Publié/Modifié le 19 avril 2017, dernier accès le 7 Juillet 2017  
<https://fr.wikipedia.org/wiki/Battlezone>
- [12] GENIOUS ADMIN, **Quels serious games concevoir pour la personne atteinte de la maladie d'Alzheimer ?**. Publié/Modifié le 5 novembre 2012, dernier accès le 16 Juillet 2017  
<http://www.sante-digitale.fr/quel-serious-game-concevoir-pour-la-personne-atteinte-de-la-maladie-dalzheimer-2/>
- [13] LUCIE BERTHOLIER, **Des Serious Games pour tester et évaluer la maladie d'Alzheimer**. Publié/Modifié le 13 décembre 2012, dernier accès le 16 Juillet 2017  
<http://www.serious-game.fr/des-serious-games-pour-tester-et-evaluer-la-maladie-dalzheimer/>
- [14] seriousfactory, **Le Serious Game Santé : un must pour former et sensibiliser !**. Publié/Modifié le 10 juin 2015, dernier accès le 31 Juillet 2017  
<https://www.seriousfactory.com/blog/seriousgame-sante-must-former-sensibiliser/>
- [15] seriousfactory, **Bénéfice limité des "serious games" chez les enfants asthmatiques**. Publié/Modifié le 13 janvier 2017, dernier accès le 8 août 2017  
[http://www.ticsante.com/Benefice-limite-des-serious-games-chez-les-enfants-asthmatiques-NS\\_3342.html](http://www.ticsante.com/Benefice-limite-des-serious-games-chez-les-enfants-asthmatiques-NS_3342.html)
- [16] Julien Bugmann, **JEUX SÉRIEUX ET ÉDUCATION : OÙ EN SOMMES-NOUS ?**. Publié/Modifié le 15 janvier 2015, dernier accès le 23 août 2017  
<https://www.reseau-canope.fr/agence-des-usages/jeux-serieux-et-education-ou-en-sommes-nous.html>
- [17] vousnousils, **Les serious games à la maternelle : un jeu d'enfant !**. Publié/Modifié le 7 janvier 2015, dernier accès le 23 août 2017  
<http://www.vousnousils.fr/2015/01/07/les-serious-game-a-la-maternelle-un-jeu-denfant-559573>
- [18] Brice Ancelin, **Adopter les serious games dans sa politique formation**. Publié/Modifié le date inconnue, dernier accès le 23 août 2017  
<http://www.formaguide.com/s-informer/quel-usage-des-serious-games-dans-la-formation->
- [19] lesseriousgames.wordpress.com, **Le Serious Game dans le militaire**. Publié/Modifié date inconnue, dernier accès le 26 août 2017  
<https://lesseriousgames.wordpress.com/le-serious-game-dans-le-militaire/>
- [20] CHEAr, **Avenir de la simulation pour l'entraînement des forces : quels bénéfices pour le fonctionnement et quelles limites ?**. Publié/Modifié en 2009, dernier accès le 27 août 2017  
[https://www.ihedn.fr/sites/default/files/atoms/files/sn45\\_t1\\_2.pdf](https://www.ihedn.fr/sites/default/files/atoms/files/sn45_t1_2.pdf)
- [21] NTSAToday, **ARMY Helicopter Flight Simulator Demo, I/ITSEC 2011**. Publié/Modifié le 30 Novembre 2011, dernier accès le 25 août 2017  
<https://www.youtube.com/watch?v=b3J09CVcBaY>

- [22] Marco Mosca, **Serious game : le diabolique outil d'Accenture pour recruter les meilleurs.** Publié/Modifié le 11 juillet 2013, dernier accès le 24 août 2017  
[https://www.challenges.fr/entreprise/serious-game-le-recrutement-high-tech-d-accenture\\_40358](https://www.challenges.fr/entreprise/serious-game-le-recrutement-high-tech-d-accenture_40358)
- [23] TALENTPEOPLE, **Tendance : le serious game pour minimiser les biais de recrutement.** Publié/Modifié le 20 février 2016, dernier accès le 24 août 2017  
<http://www.talentpeople.net/recrutement-serious-games/>
- [24] REDACTION, **Les jeux vidéos pour seniors et personnes âgées, un nouveau marché.** Publié/Modifié le 16 octobre 2009, dernier accès le 16 Juillet 2017  
<http://www.silvereco.fr/les-jeux-videos-pour-seniors-un-nouveau-marche/311022>
- [25] Sam S. Adkins, **The 2011-2016 Worldwide Game-based Learning Market: All Roads Lead to Mobile.** Publié/Modifié le 6 septembre 2012, dernier accès le 22 Juillet 2017  
<https://www.slideshare.net/SeriousGamesAssoc/sam-s-adkins-ambient-insightworldwidegamebasedlearningmarket>
- [26] leparisien, **Nintendo souffre de la concurrence des smartphones.** Publié/Modifié le 26 octobre 2016, dernier accès le 23 Juillet 2017  
<http://www.leparisien.fr/high-tech/nintendo-souffre-de-la-concurrence-des-smartphones-26-10-2016-6254778.php>
- [27] SSRH, **SSRH 2017: solutions RH, serious games, e-learning, gamification et Moocs.** Publié/Modifié le 23 mars 2017, dernier accès le 7 Juillet 2017  
<http://www.jobsferic.fr/SSRH-2017-solutions-et-logiciels-RH-Serious-Games-e-learning-Mobile-Learning-Gamification-et-Moocs.html>
- [28] Juliette Paoli, **LE SERIOUS GAME : UN MARCHÉ À 5 448,82 MILLIONS DE DOLLARS D'ICI 2020.** Publié/Modifié le 19 avril 2017, dernier accès le 7 Juillet 2017  
<http://www.solutions-numeriques.com/drh/le-serious-game-un-marche-a-5-44882-millions-de-dollars-dici-2020/>
- [29] Sylvie Dellus, **Que valent les jeux d'entraînement cérébral ?.** Publié/Modifié le 24 février 2011, dernier accès le 8 Juillet 2017  
<http://www.santemagazine.fr/que-valent-les-jeux-d-entrainement-cerebral-29747.html>
- [30] Guillaume Vallet, **STIMULATION ET REMÉDIATION DE LA MÉMOIRE.** Publié/Modifié le 19 avril 2017, dernier accès le 8 Juillet 2017  
[http://slides.com/larlekin/m2sca\\_stimremmem/fullscreen](http://slides.com/larlekin/m2sca_stimremmem/fullscreen)
- [31] Studyvox, **Jeu avec les bases de données littéraires, musicales... de studyvox.** Publié/Modifié 6 Juillet 2017, dernier accès le 9 Juillet 2017  
<http://studyvox.biwi.ca/jeuxbdd/jeuxindi/jouer.php>
- [32] Serious Game Classification, **Who Wants to Be a Millionaire.** Publié/Modifié en 2010, dernier accès le 14 Juillet 2017  
<http://serious.gameclassification.com/EN/games/42239-Who-Wants-to-Be-a-Millionaire/index.html>

- [33] MobyGames, **Who Wants to Be a Millionaire**. Publié/Modifié en 2010, dernier accès le 9 Juillet 2017  
[http://www.mobygames.com/game/who-wants-to-be-a-millionaire\\_\\_/](http://www.mobygames.com/game/who-wants-to-be-a-millionaire__/)
- [34] Wikipedia, **Who Wants to Be a Millionaire?**. Publié/Modifié le 14 mai 2017, dernier accès le 9 Juillet 2017  
[https://fr.wikipedia.org/wiki/Who\\_Wants\\_to\\_Be\\_a\\_Millionaire%3F](https://fr.wikipedia.org/wiki/Who_Wants_to_Be_a_Millionaire%3F)
- [35] codingame, **Pratice**. Publié/Modifié en 2017, dernier accès le 14 août 2017  
<https://www.codingame.com/training>
- [36] codecombat, **Home**. Publié/Modifié en 2017, dernier accès le 14 août 2017  
<https://codecombat.com/home>
- [37] leekwars, **Accueil**. Publié/Modifié en 2012, dernier accès le 14 août 2017  
<https://leekwars.com/>
- [38] Agnès LECLAIR, Alexandre CLAUDE, **Quand le langage SMS envahit les copies du bac**. Publié/Modifié le 19 mai 2008, dernier accès le 9 Juillet 2017  
<http://www.lefigaro.fr/actualite-france/2008/05/17/01016-20080517ARTFIG00653-quand-le-langage-sms-envahit-les-copies-du-bac.php>
- [39] Christophe CARMARANS, **Les Français de plus en plus fâchés avec l'orthographe**. Publié/Modifié le 5 février 2016, dernier accès le 9 Juillet 2017  
<http://www.rfi.fr/france/20150312-francophonie-orthographe-francais-sondage-declin-enseignement-dictee-sms-internet>
- [40] Dr. Randy Kulman, **Should Your Kids Play Serious Games?**. Publié/Modifié le 5 octobre 2011, dernier accès le 23 Juillet 2017  
<http://learningworksforkids.com/2011/10/example-science-of-play-related-post/>
- [41] codingame, **Turbocharge your tech screening with the ultimate code tests**. Publié/Modifié en 2016, dernier accès le 13 août 2017  
<https://www.codingame.com/work/solutions/coding-skill-assessment>
- [42] Hello Finance Team (B.A.), **Neurodecision: un outil « serious game » pour évaluer les profils d'investisseur**. Publié/Modifié le 14 juillet 2016, dernier accès le 13 août 2017  
<https://hello-finance.com/neurodecision/>
- [43] wikipedia, **Jeu vidéo de rôle**. Publié/Modifié le 4 juillet 2017, dernier accès le 26 Juillet 2017  
[https://fr.wikipedia.org/wiki/Jeu\\_vid%C3%A9o\\_de\\_r%C3%B4le](https://fr.wikipedia.org/wiki/Jeu_vid%C3%A9o_de_r%C3%B4le)
- [44] econocom, **MINECRAFT : UN OUTIL D'APPRENTISSAGE EFFICACE**. Publié/Modifié le 18 novembre 2016, dernier accès le 27 Juillet 2017  
<https://blog.econocom.com/blog/minecraft-un-outil-dapprentissage-efficace/>
- [45] minecraft, **Code Builder, Command Blocks, and More Come to Education Edition**. Publié/Modifié le 2 mai 2017, dernier accès le 27 Juillet 2017  
<https://education.minecraft.net/code-builder-command-blocks-and-more-come-to-education-edition/>
- [46] tynker, **How to Use Tynker with Minecraft: Education Edition**. Publié/Modifié date inconnue, dernier accès le 27 Juillet 2017  
<https://www.tynker.com/support/minecraft/ee/>

- [47] chemcaper, **About The Game**. Publié/Modifié en 2016, dernier accès le 30 Juillet 2017  
<https://chemcaper.com/about-the-game/>
- [48] ANTONIO FERNANDO COELHOON, **Location-based Games**. Publié/Modifié le 5 octobre 2015, dernier accès le 23 Juillet 2017  
<https://blog.eai.eu/location-based-games/>
- [49] EQUIPE SERIOUS GAME BLOG, **La cartographie sans crayon de couleur, c'est possible**. Publié/Modifié le 28 février 2007, dernier accès le 24 Juillet 2017  
<http://www.serious-game.fr/la-cartographie-sans-crayon-de-couleur-cest-possible/>
- [50] CHRISTOPHE COQUIS, **Osmo pour iPad : des jeux éducatifs géniaux en réalité augmentée**. Publié/Modifié le 22 juillet 2015, dernier accès le 23 Juillet 2017  
<https://www.geekjunior.fr/osmo-ipad-jeux-educatifs-geniaux-realite-augmentee-1671/>
- [51] Gabriel Mamou-Mani, **Les jeux éducatifs sur smartphones plus pédagogues que l'école ?**. Publié/Modifié date inconnue, dernier accès le 23 Juillet 2017  
<http://www.advergame.fr/les-jeux-educatifs-sur-smartphones-plus-pedagogues-que-l%E2%80%99ecole>
- [52] wikipedia, **Réalité virtuelle**. Publié/Modifié le 10 juillet 2017, dernier accès le 14 août 2017  
[https://fr.wikipedia.org/wiki/R%C3%A9alit%C3%A9\\_virtuelle](https://fr.wikipedia.org/wiki/R%C3%A9alit%C3%A9_virtuelle)
- [53] theconversation, **Dix applications « cool » de réalité virtuelle, des jeux, mais aussi du sérieux !**. Publié/Modifié le 3 mai 2016, dernier accès le 17 août 2017  
<http://theconversation.com/dix-applications-cool-de-realite-virtuelle-des-jeux-mais-aussi-du-serieux-57782>
- [54] Damien Djaouti, **Jeux sérieux : avantages et limites**. Publié/Modifié le 30 juin 2017, dernier accès le 13 Juillet 2017  
<http://www.sup-numerique.gouv.fr/cid101595/jeux-serieux-avantages-et-limites.html>
- [55] Sitzmann, Ely, **Jeux sérieux : avantages et limites**. Publié/Modifié en 2010, dernier accès le 13 Juillet 2017  
<http://www.actisia.com/quest-ce-que-le-serious-gaming/>
- [56] abilways-digital, **SERIOUS GAMES EN ENTREPRISE : COÛTEUX MAIS EFFICACES**. Publié/Modifié en 26 octobre 2015, dernier accès le 17 août 2017  
<http://www.abilways-digital.com/magazine/serious-games-en-entreprise-couteux-mais-efficaces/>
- [57] Charles Brisson, **Un jeu sérieux, combien ça coûte ?**. Publié/Modifié le 5 février 2012, dernier accès le 17 août 2017  
<http://cursus.edu/article/17973/jeu-serieux-combien-coute/#.WZVnFHcjG2x>
- [58] dynamique-mag, **Serious Games : à vous de jouer !**. Publié/Modifié le 2 mai 2012, dernier accès le 17 août 2017  
<http://www.dynamique-mag.com/actualite/serious-games-a-vous-de-jouer.573>
- [59] Elise Lambert, **Bac: les calculatrices programmables bientôt interdites pour éviter la triche**. Publié/Modifié le 10 avril 2015, dernier accès le 4 août 2017  
[http://www.lexpress.fr/education/bac-les-calculatrices-programmables-bientot-interdites-pour-eviter-la-triche\\_1670026.html](http://www.lexpress.fr/education/bac-les-calculatrices-programmables-bientot-interdites-pour-eviter-la-triche_1670026.html)

- [60] commentcamarche, **Piratage et attaques informatiques**. Publié/Modifié Juillet 2017, dernier accès le 10 Juillet 2017  
<http://www.commentcamarche.net/contents/47-piratage-et-attaques-informatiques>
- [61] owasp, **Top 10 2017-Top 10**. Publié/Modifié le 23 avril 2017, dernier accès le 8 août 2017  
[https://www.owasp.org/index.php/Top\\_10\\_2017-Top\\_10](https://www.owasp.org/index.php/Top_10_2017-Top_10)
- [62] owasp, **Category:Attack**. Publié/Modifié le 6 juin 2016, dernier accès le 8 août 2017  
<https://www.owasp.org/index.php/Category:Attack>
- [63] incapsula, **CROSS SITE SCRIPTING (XSS) ATTACKS**. Publié/Modifié date inconnue, dernier accès le 8 août 2017  
<https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html>
- [64] Jakob Kallin, Irene Lobo Valbuena, **XSS overview**. Publié/Modifié le 9 juillet 2016, dernier accès le 10 Juillet 2017  
<https://excess-xss.com/#xss-overview>
- [65] openclassrooms, **Protégez-vous efficacement contre les failles web**. Publié/Modifié le 8 mars 2017, dernier accès le 19 Juillet 2017  
<https://openclassrooms.com/courses/protegez-vous-efficacement-contre-les-failles-web/la-faille-xss-1>
- [66] Maurice McMullin, **OWASP Top Ten Series: Using Components With Known Vulnerabilities**. Publié/Modifié le 9 mai 2016, dernier accès le 19 Juillet 2017  
<https://kemptechnologies.com/blog/owasp-top-ten-series-using-components-with-known-vulnerabilities/>
- [67] OWASP, **Top 10 2013-A5-Security Misconfiguration**. Publié/Modifié le 23 juin 2013, dernier accès le 19 Juillet 2017  
[https://www.owasp.org/index.php/Top\\_10\\_2013-A5-Security\\_Misconfiguration](https://www.owasp.org/index.php/Top_10_2013-A5-Security_Misconfiguration)
- [68] petitchevalroux, **Obfuscuer, minifier et compresser du javascript**. Publié/Modifié le 6 février 2010, dernier accès le 19 Juillet 2017  
<http://dev.petitchevalroux.net/javascript/obfuscuer-minifier-compresser-javascript-javascript-308.html>
- [69] mozilla, **DOM MutationObserver – reacting to DOM changes without killing browser performance**. Publié/Modifié le 10 Mai 2012, dernier accès le 22 Juillet 2017  
<https://hacks.mozilla.org/2012/05/dom-mutationobserver-reacting-to-dom-changes-without-killing-browser-performance/>
- [70] anonyme, **Mutation Observer**. Publié/Modifié date inconnue, dernier accès le 3 Août 2017  
<http://jsbin.com/codopayivi/edit?html,css,output>
- [71] ourcodeworld, **How to prevent modification of an object in Javascript and prevent them from being accessible in the console**. Publié/Modifié le 9 juin 2016, dernier accès le 3 Août 2017  
<http://ourcodeworld.com/articles/read/167/how-to-prevent-modification-of-an-object-in-javascript-and-prevent-them-from-being-accessible-in-the-console>

- [72] ca, **Vol de session : une nouvelle méthode de prévention est née.** Publié/Modifié en 2014, dernier accès le 3 Août 2017  
<https://www.ca.com/content/dam/ca/fr/files/ebook/session-hijacking-a-new-method-of-prevention.pdf>
- [73] Hugo Etiévant, **Applications web : sécuriser la session utilisateur.** Publié/Modifié 25 août 2006, dernier accès le 3 Août 2017  
<http://cyberzoide.developpez.com/securite/session/#LD>
- [74] net-informations, **Client side validation and server side validation.** Publié/Modifié date inconnue, dernier accès le 8 Août 2017  
<http://net-informations.com/faq/asp/validation.htm>
- [75] neoxia, **NoSQL : 5 minutes pour comprendre.** Publié/Modifié mai 2017, dernier accès le 8 Août 2017  
<http://blog.neoxia.com/nosql-5-minutes-pour-comprendre/>
- [76] Sébastien Gioria, **NOSQL, NO Security ?.** Publié/Modifié date inconnue, dernier accès le 8 Août 2017  
<https://www.advens.fr/ressources/blog/nosql-no-security>
- [77] kunal relan, **MongoDB Injection in Node.js.** Publié/Modifié le 28 août 2016, dernier accès le 8 Août 2017  
<https://scotch.io/@kunalrelan/mongodb-injection-in-nodejs>
- [78] Petko D. Petkov, **HACKING NODEJS AND MONGODB.** Publié/Modifié le 11 août 2014, dernier accès le 8 Août 2017  
<http://blog.websecurify.com/2014/08/hacking-nodejs-and-mongodb.html>
- [79] zanon, **NoSQL Injection in MongoDB.** Publié/Modifié le 17 juillet 2016, dernier accès le 8 Août 2017  
<https://zanon.io/posts/nosql-injection-in-mongodb>
- [80] Quantis, Inc., **Mot Mystère - trouver le mot caché!.** Publié/Modifié le 4 avril 2016, dernier accès le 10 Août 2017  
<https://itunes.apple.com/fr/app/mot-myst%C3%A8re-trouver-le-mot-cach%C3%A9/id1014230781?mt=8>
- [81] reglementdejeu, **Le dépôt d'un règlement auprès d'un huissier de justice vous protège de la triche.** Publié/Modifié en 2017, dernier accès le 12 Août 2017  
<https://www.reglementdejeu.com/jeux-concours/depot-reglement.html>
- [82] experts-tourisme, **Psychopathologie - Définitions de comportement anormal.** Publié/Modifié date inconnue, dernier accès le 22 Août 2017  
<http://www.experts-tourisme.fr/psychopathologie-comportement-b870509.htm>

# Glossaires

**3D** Three-dimensional space. [12](#), [21](#)

**BDD** Base de données. [10](#), [34](#), [35](#), [37](#), [43](#)

**CA** Chiffre affaire. [13](#), [14](#)

**CAP** Consistency Availability Partition tolerance. [34](#)

**CM2** Cours moyen 2e. [22](#)

**CV** Curriculum vitae. [24](#)

**DDoS** Distributed Denial of Service. [26](#)

**DOM** Document Object Model. [10](#), [29](#), [36](#)

**DRH** Directions ressources humaines. [10](#)

**ESN** Entreprises de Services Numérique. [24](#), [41](#)

**GPS** Global Positioning System. [18](#)

**HTML** Hypertext Markup Language. [10](#), [33](#)

**HTTP** Hypertext Transfer Protocol. [27](#)

**IA** Intelligence artificielle. [16](#)

**IP** Internet Protocol. [40](#), [42](#)

**JS** JavaScript. [10](#), [11](#)

**JSON** JavaScript Object Notation. [10](#), [34](#)

**M2** Master 2. [3](#), [9](#)

**MIAGE** Méthodes Informatiques Appliquées à la Gestion des Entreprises. [3](#), [9](#)

**NoSQL** Not Only SQL. [10](#), [34](#)

**OS** Operating System. [35](#), [43](#)

**PDF** Portable Document Format. [26](#)

**PME** Petites et moyennes entreprises. [21](#)

**POC** Proof Of Concept. [10](#)

**RPG** Role-playing game. [17](#)

**RV** Réalité Virtuelle. [19](#)

**SMS** Short Message Service. [16](#)

**SVG** Scalable Vector Graphics. [10, 11, 36](#)

**TDD** Test-driven development. [16](#)

**URL** Uniform Resource Locator. [10, 33](#)

**XSS** Cross-Site Scripting. [33, 36](#)

# Annexes

## A. Debugguer avec chrome

La fenêtre ci-dessus est affichée lorsque vous faites inspecter sur chrome, on peut voir sur le top-bar la navigation sur la vue "Source". Avec lequel il y a trois blocs, celui de gauche un menu de fichiers, le central le fichier sélectionner, à droite le menu avec le debugger et le scope qui permet d'observer les variables.

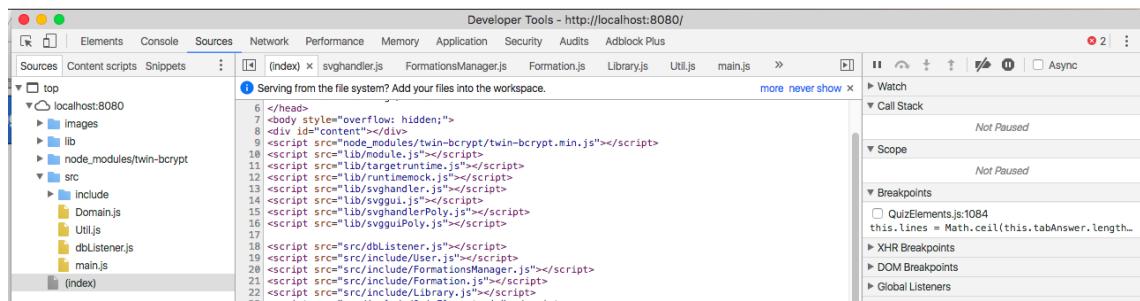


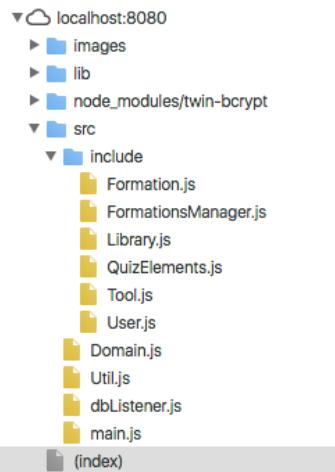
Figure 1: Developer Tools

On peut voir un le code du fichier sélectionner, avec quelque fichier js qui sont inclus dans la page.

```
<script src="src/Util.js"></script>
<script src="src/Domain.js"></script>
<script src="src/main.js"></script>
<script src="lib/enhancer.js"></script>
<script>
  const
    enhance = exports.Enhance(),
    targetRuntime = exports.targetRuntime(),
    SVG = exports.SVG,
    dbListener = new DbListener(true, false);
  var url = document.URL;
  var query = url.split('?')[1];
  var ID;
  var param;
  if (query) {
    param = query.split('=')[0];
  }
  var redirect = false;
  if (param == 'ID') {
    redirect = true;
    ID = query.split('=')[1];
  }
  main(SVG(targetRuntime), targetRuntime, dbListener, false, {redirect: redirect, ID: ID});
</script>
</body>
</html>
```

Figure 2: Observation du fichier index.html

Si on utilise le bloc de gestion de fichiers de gauche, on peut voir les fichiers qui sont chargés. On peut évidemment lire tous les codes de tous les fichiers, mais cela pourrait nous prendre énormément de temps.



**Figure 3:** Block gestion fichier

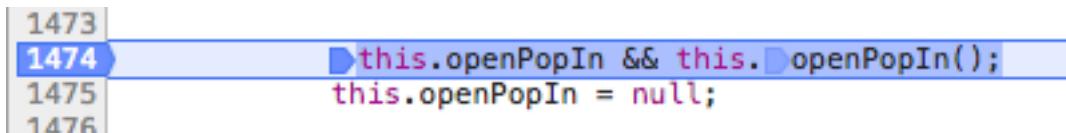
On pourrait également chercher plus intelligemment dans le fichier les mots clés, comme ici dans ces fichiers nous avons des classes. On va essayer de repérer les noms des classes pour voir si on peut trouver quelque chose qui va nous être utile très rapidement, et on voit il y a deux noms de classes qui pourraient nous intéresser "Answer" et QuizManaverVue.

```
/////////MODEL///////////
/** 
 * Réponse à un quiz. Cette réponse peut être correcte ou non. Une explication
 * @class
 */
class Answer {
    /**
 * @class
 */
class QuizManagerVue extends Vue {
    /**
     * construit un quiz associé à une formation
     * @constructs
     * @param quiz - objet qui va contenir toutes les informations du quiz créé
     * @param formation - formation qui va contenir le quiz
    */

    /**
     * @class
    */
class QuestionVue extends Vue {
```

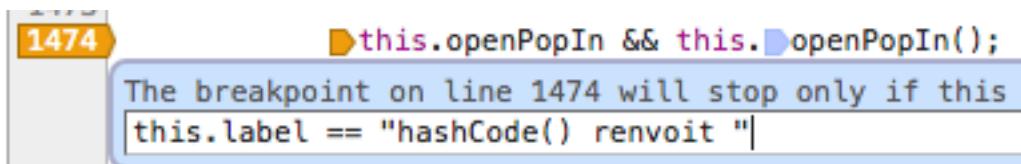
**Figure 4:** Classes en javascript

Pour utiliser le débuggeur côté client, il faut se placer dans le bloc central sur la ligne que vous souhaitez arrêter et cliquer sur le bar de gauche du bloc. Lors de l'exécution du code si elle passe par votre ligne, l'exécution va se mettre en pause là où il y a le break point. Et vous pouvez ensuite exécuter ligne par ligne, et suivre toutes les modifications de l'état des objets.



**Figure 5:** BreakPoint

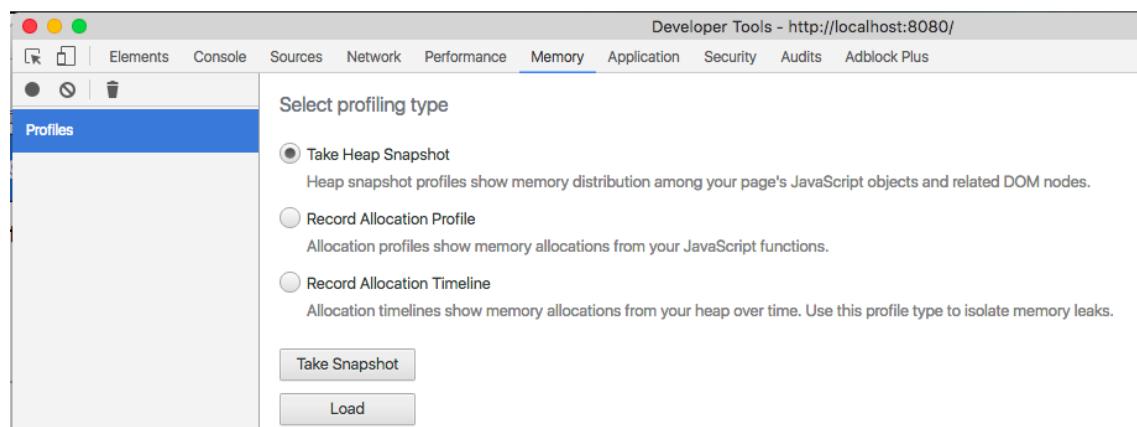
On peut mettre des conditions d'arrêt sur le break point, lorsqu'on cherche à s'arrêter sur une valeur ou à un état particulier de l'objet. Pour mettre la condition, il suffit de faire un clic droit sur le breakpoint et l'éditer comme le figure ci-dessous.



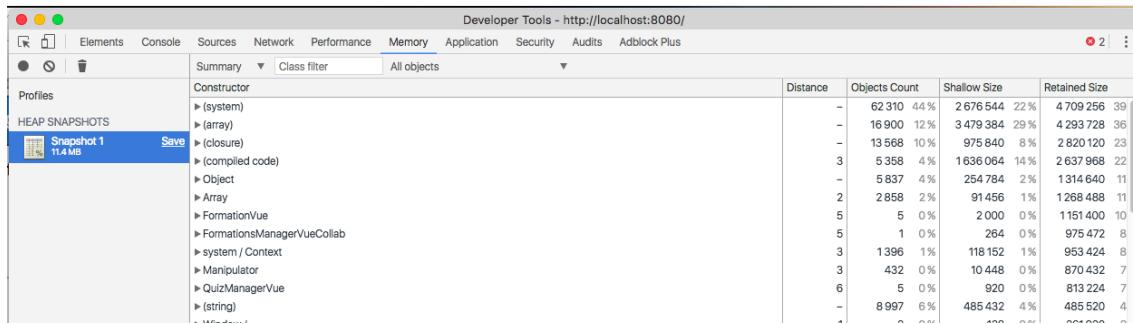
**Figure 6:** BreakPoint avec condition

## B. Snapshot memory avec chrome

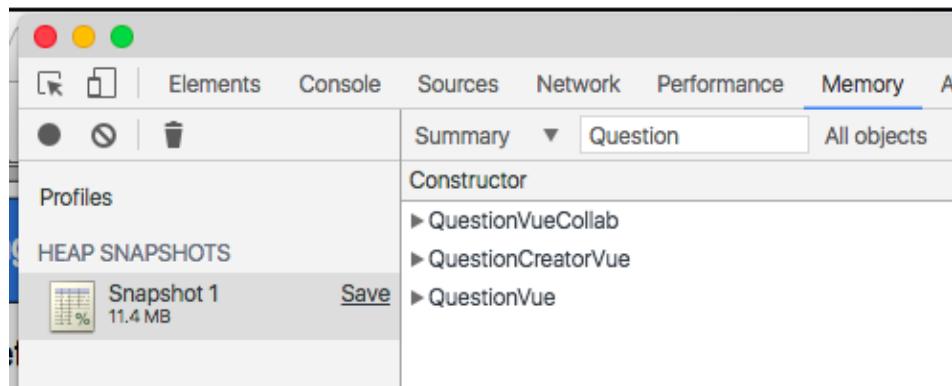
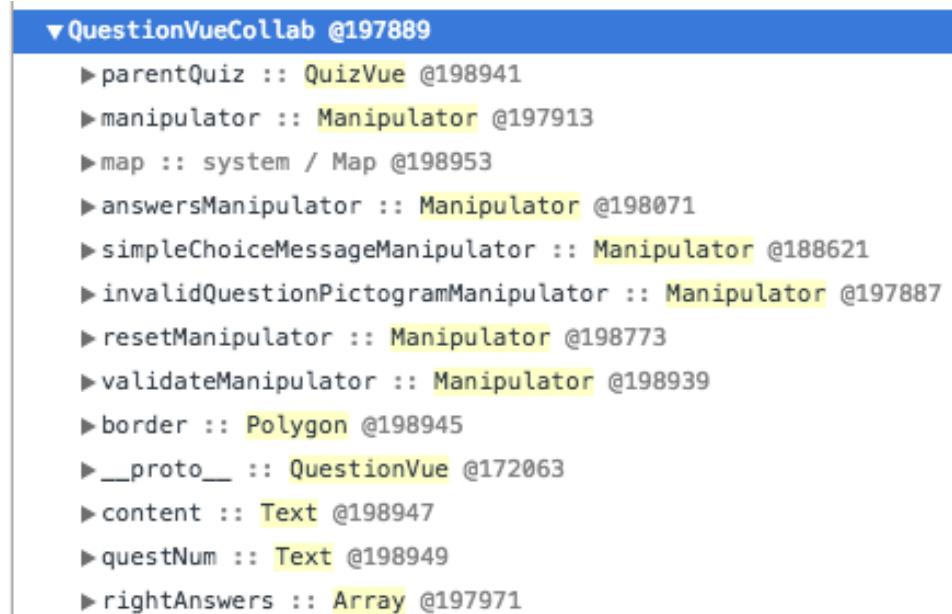
Il y a plusieurs types de photo mémoire, il y a celui qui prend une photo instantanée de la mémoire. Il y a celui qui enregistre tout, et le dernier qui enregistre par rapport à une chronologie.



**Figure 7:** Developer Tools Memory

**Figure 8:** Snapshot memory

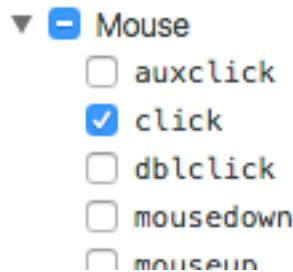
On peut voir un aperçu de la mémoire sur la figure ci-dessus, avec des précisions comme sa taille, le nombre de fois instancié, le nom de l'objet. On peut également essayer de fouiller dans tout les objets photographiés pour trouver ce qu'on cherche. Sinon on peut utiliser le filtre comme la figure ci-dessus.

**Figure 9:** Snapshot memory filtrer**Figure 10:** Aperçu de l'objet depuis Snapshot

## C. Event Listener Breakpoints

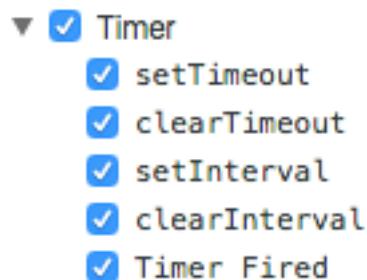
### C.1. Modification étape 1

Lors de la modification de l'étape 1, nous avons essayé de repérer avec event "mouse" qui ne nous a malheureusement pas amenés sur le code source que nous souhaitons.



**Figure 11:** Event mouse

À la suite de ceci, nous avons étudié le comportement de l'étape 1 pour essayer de trouver d'autres événements qui pourraient nous aider à trouver le code que nous souhaitons avoir.



**Figure 12:** Event Timer

Lorsqu'on essaye d'utiliser l'événement timer, on s'arrête exactement dans la fonction que nous souhaitons modifier "la connexion". Et si on observe plus attentivement, il nous pointe sur la ligne où ç'a été défini l'événement "timeout".

```

connexionButtonHandler() {
    this.mailAddressField.input.hideControl() && this.passwordField.input.hideControl();
    let emptyAreas = this.tabForm.filter(field => field.input.textMessage === '');
    emptyAreas.forEach(emptyArea => {
        emptyArea.input.color(ERROR_INPUT);
    });
}

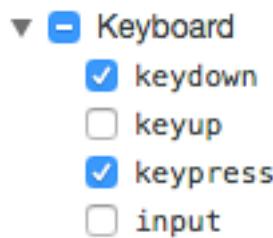
if (emptyAreas.length > 0) {
    let message = new svg.Text(EMPTY_FIELD_ERROR)
        .dimension(INPUT_WIDTH, INPUT_HEIGHT)
        .position(0, -MARGIN - BUTTON_HEIGHT)
        .color(myColors.red)
        .font(FONT, FONT_SIZE_INPUT)
        .mark("msgFieldError");
    this.connexionButtonManipulator.set(1, message);

    svg.timeout(() => {
        this.connexionButtonManipulator.unset(1);
        emptyAreas.forEach(emptyArea => {
            emptyArea.input.color(COLORS);
        });
    }, 5000);
} else {
    Server.connect(this.mailAddressField.input.textMessage, this.passwordField.input.textMessage,
        this.model.correct).then(data => {
        data = data && JSON.parse(data);
        if (data.ack === 'OK') {
            drawing.username = `${data.user.firstName} ${data.user.lastName}`;
            data.user.admin ? globalVariables.domain.adminGUI() : globalVariables.domain.learningGUI();
            let user = data.user;
        }
    });
}

```

**Figure 13:** Break point avec l'événement timer

Lors de l'étude du comportement de l'étape 1, on a découvert également l'événement "Keyboard" qui pourrait nous amener à le code chercher.

**Figure 14:** Event Keyboard

Avec l'événement keyboard, on s'arrête à un niveau au-dessus, on voit la gestion des touches claviers. Mais on voit également dans la gestion de la touche entrée, la fonction "connexionButtonHandler" qui est la même que celui nous a amené l'évenement timer.

```

    /**
     * handler global pour gérer les appuis sur les touches du clavier
     * @param event
     */
    keyDownHandler(event) {
        if (event.keyCode === 9) { // TAB
            event.preventDefault();
            let index = this.tabForm.indexOf(this.focusedField);
            if (index !== -1) {
                event.shiftKey ? index-- : index++;
                if (index === this.tabForm.length) index = 0;
                if (index === -1) index = this.tabForm.length - 1;
                svg.event(this.tabForm[index].input.glass, "click");
                this.focusedField = this.tabForm[index];
            }
        } else if (event.keyCode === 13) { // Entrée
            event.preventDefault();
            this.focusedField && this.focusedField.input.hideControl();
            this.connexionButtonHandler();
        }
    }
}

```

**Figure 15:** Break point avec l'évenement keyboard

On modifie le code à en sort que lorsqu'on clique, aucun appel au serveur est envoyé, et on créer un utilisateur "Kevin MITNICK" en admin.

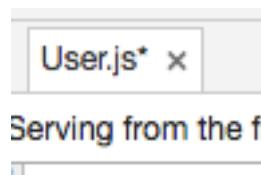
```

connexionButtonHandler() {
    this.mailAddressField.input.hideControl() && this.passwordField.input.hideControl();

    let data = {user:{firstName: "Kevin", lastName:"MITNICK", admin: "true"}}
    drawing.username = `${data.user.firstName} ${data.user.lastName}`;
    data.user.admin ? globalVariables.domain.adminGUI() : globalVariables.domain.adminGUI();
    let user = data.user;
    Server.getAllFormations().then(data => {
        let myFormations = JSON.parse(data).myCollection;
        globalVariables.formationsManager = classContainer.createClass("FormationsManagerVue", myFormations);
        if (user && user.lastAction && user.lastAction.formation) {
            util.goDirectlyToLastAction(user.lastAction);
        } else {
            globalVariables.formationsManager.display();
        }
    });
}

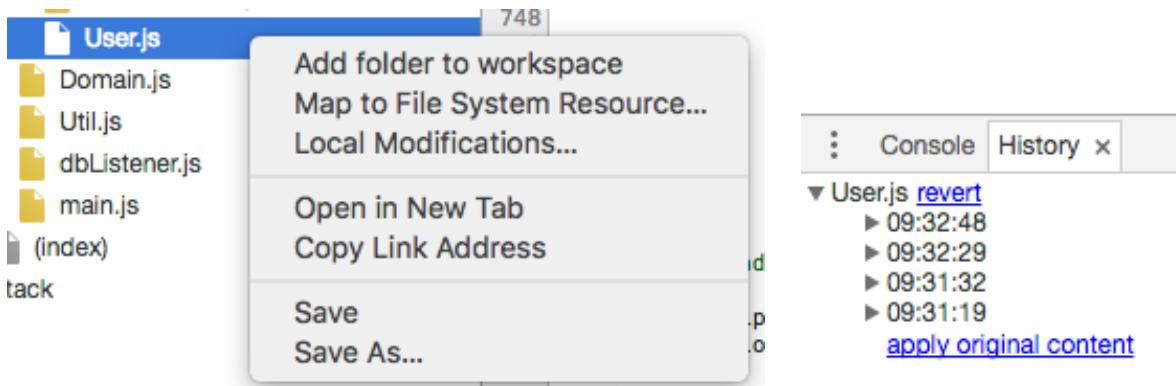
```

**Figure 16:** Code modifié pour l'étape 1



**Figure 17:** Modification fichier

Lorsqu'on modifie un fichier, on doit sauvegarder pour appliquer la modification et ne pas recharger la page. Sinon on risque de perd la modification, on peut voir également l'historique des modifications en faisant click droit puis "Local Modifications".



**Figure 18:** Historique des modifications du fichier

```
Error: No token
    at Promise (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/server/cookies.js:26:20)
    at Object.verify (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/server/cookies.js:24:12)
    at /Users/minhhuyle/Documents/Dev/VISE0/i-learning/server/controllers/routes.js:289:28
    at Layer.handle [as handle_request] (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/layer.js:95:5)
    at next (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/layer.js:95:5)
    at /Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/index.js:281:22
    at param (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/index.js:354:14)
    at param (/Users/minhhuyle/Documents/Dev/VISE0/i-learning/node_modules/express/lib/router/index.js:365:14)
```

**Figure 19:** Erreur du serveur : No token

Après la modification du code de l'étape 1, on a fait planter le serveur. Car on a fait une requête sur le serveur, comme on ne s'est jamais authentifié, on n'a pas de token ce qui cause les dégâts cotés back-end.

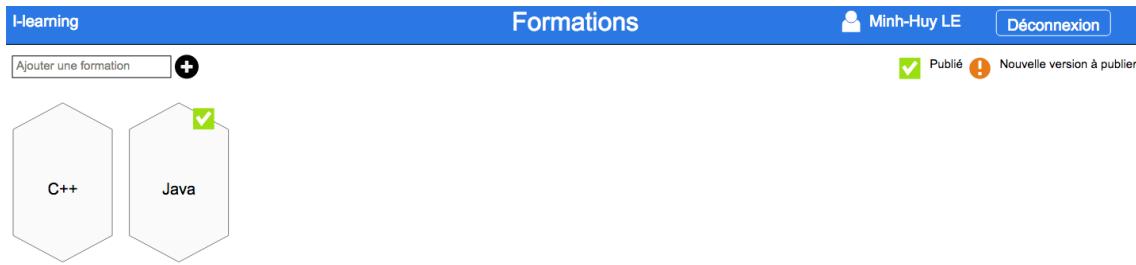
## C.2. Modification étape 2

Modification de l'étape 2, faire passer un utilisateur normal en utilisateur admin.

```
Server.connect(this.mailAddressField.input.textMessage, this.passwordField.input.textMessage,
    this.model.correct).then(data => {
    data = data && JSON.parse(data);
    if (data.ack === 'OK') {
        drawing.username = `${data.user.firstName} ${data.user.lastName}`;
        data.user.admin = true;
        data.user.admin ? globalVariables.domain.adminGUI() : globalVariables.domain.adminGUI();
        let user = data.user;
        Server.getAllFormations().then(data => {
```

**Figure 20:** Code modifier pour l'étape 2

Après la modification du code, on arrive à se connecter et parcourir tout en tant qu'admin.

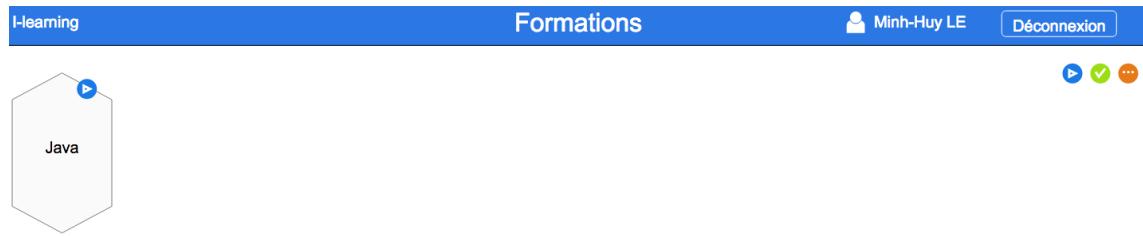


**Figure 21:** Vue dashboard admin

**Figure 22:** Vue formation admin

**Figure 23:** Vue création quiz admin

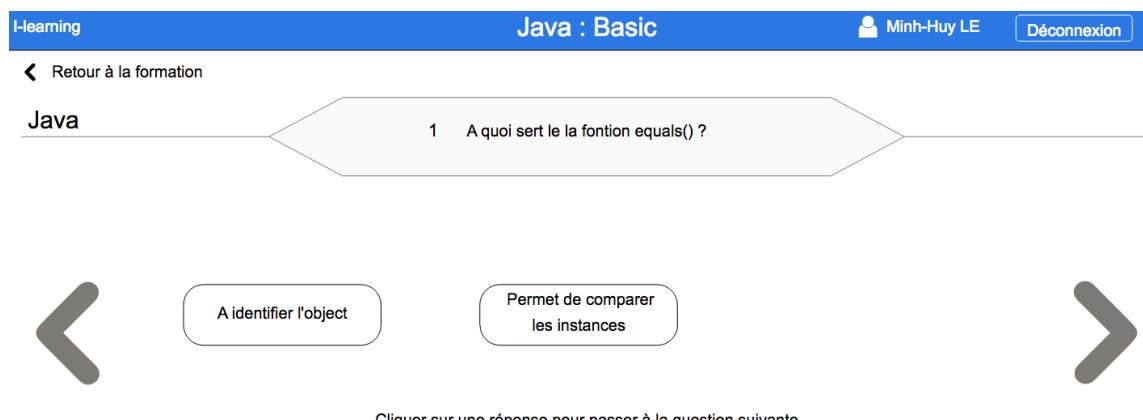
Lorsqu'on recharge la page, on perd la modification et on bascule donc en vue collaborateur (non admin).



**Figure 24:** Vue dashboard collaborateur



**Figure 25:** Vue formation collaborateur



Cliquer sur une réponse pour passer à la question suivante

**Figure 26:** Vue quiz collaborateur