Node Guardians

✉️ cizeon@cizeon.xyz
Twitter/X: @cizeon
NG: 670101944462

Qui suis-je?

- Ancien élève **Alyra**
  - Promotion Rinkeby - Sept 2022
- Pentesteur chez **Nettitude**
  - Audit de code
  - Recherche de vulnérabilité
  - Reverse-engineering
  - Un peu de web3
- Apprenti **Node Guardians** :-)
  - @Sam: si je dis des bêtises, ne pas hésiter à me corriger!

Après Alyra

Qu'est ce qu'on apprend chez Alyra!

- De solides bases!
  - Solidity
  - Unit-test
  - Du front
  - De la Defi, NFT, …
- Comparable à une **auto-école!**
- **Ce n'est que le début de l'aventure**

Continuer à se former!

- **Évidemment développer ses propres projets!**
- Mais aussi continuer à se former
- Pas mal de plateformes mais **axées débutants**:
  - CryptoZombie
  - Alchemy School
  - Youtube, …

Plafond de verre

- Peu de plateformes entre **le niveau intermédiaire et le niveau expert**.
  - Plafond de verre

- Exemples de plateformes:
  - Ethernaut
  - Damn Vulnerable DeFi
  - Capture The Ether
  - **Node Guardians :-)**

Node Guardians

Qu'est ce que Node Guardians

- **Plateforme d'apprentissage**
  - Repose sur un système de quêtes

- Un aspect **gamification** à la manière d'un RPG D&D
  - Histoires
  - Craft d'objet
  - Ça me rappelle les artworks de Baldur's Gate 1 & 2 :-)

Mais aussi

- **Du staking**
  - Deprecated?

abdel.stark ✨ 🐺 - 🏔️🔊 and Sam liked

Node Guardians ✔
@nodeguardians

The Cairo month dawns tomorrow. So what to expect?

⚔️ **Quests**

- Unsafe Math - 13th September at 3pm UTC
- Storage Collision - 20th September at 3pm UTC
- Calldata Spoofing - 27th September at 3pm UTC

🧮 **Scoring**

The first 10 solvers for each quest will earn between 1 to 10 points, with 10 points going to the fastest solver.

Top 5 guardians will be declared after the aggregation of scores on Sept 30.

🎁 **Loot**

- Legendary custom merchandise
- Be among the first to unlock new V1 achievements.
- Intro to leading @Starknet ecosystem projects
- An undisclosed treasure for the victorious

Types de quêtes

- **Des exercices de dev**
  - Implémenter des fonctions dans un smart contrat
  - Utiliser le moins de gaz possible
  - Passer des test unitaires!

- **Des CTFs**
  - Modifier ou hack d'un contrat on chain (Görli)

Types de quêtes

- **De la lecture :-)**
  - Avec un questionnaire pour valider la quête

- **Organisation des quêtes**:
  - En campagnes autour d'un thème
  - Ou en stand-alone

Les thèmes abordés

- **Cairo** (pas encore regardé)
- **Solidity**:
  - Gas optimization
- **Assembly**:
  - Yul
  - EVM Memory layout
- **Design patterns**:
  - Proxy contracts
  - Diamonds
  - Storage

Les thèmes abordés

- **Chiffrement**
  - Elliptic Curves avec implémentation
- **Rekt**
  - Exploitation de gros hack passés

Les thèmes abordés

- **Les quêtes en standalone**:
  - Tous les sujets abordés
  - Certaines sont vraiment passionnantes

  - Flash loan, attaques sur des Oracles, casser de la RNG, implémenter des arbres de Merkle, ECC, …

Avantages

- **On est pas pris par la main**
  - On nous donne des outils
  - Des conseils
  - Mais jamais la solution!

- Le système est vraiment malin!

Conseils

- Le niveau de difficulté peut devenir élevé.
  - **À voir après la formation!**
- Être **confortable** avec l'idée de **galérer** un peu :-D

À quoi ça ressemble ?

Les quêtes

Installation

- Créer un repository **privé** pour Node Guardians

- Cloner un repo de Node Guardians dessus.
  - Accepter l'application Github Node Guardians sur ce repo.

- Créer un jeton pour donner les droits à Node Guardians d'y accéder.

Installation de la partie dev

- Ensuite, tout se fait avec l'outil **quest**
- Lancer les tests
- Submit sa solution
- Il y a des tests publiques
- Et des tests privés qui tournent chez Node Guardians

Installer une quête

```
$ quest find stealing-souls
$ cd campaigns/bad-accounts/stealing-souls
$ quest test 1
$ quest submit
```

Pour les CTFs

- Liberté totale, perso:
  - Remix
  - Forge avec scripts
- Déployer le contract cible
- Fork de Görli
- Faire son dev/test dessus
- Penser à explorer le contrat déployé avec Etherscan

Exemple de quête

Exemple d'un challenge Rekt

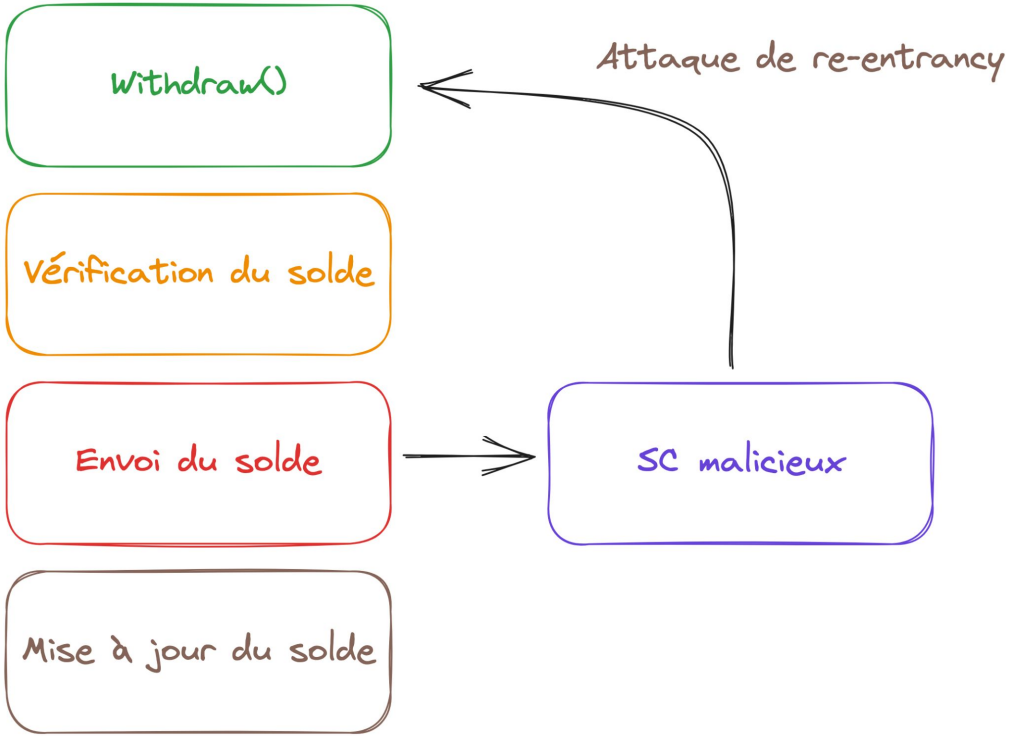
- Je ne vais pas donner la solution :-)
- Mais je vais faire le même travail que NG & Rekt
  - Partir d'un hack du monde réel et voir comment il a été implémenté sur NG

Cream Finance

- Le 10 février 2021, Cream Finance décide d'ajouter le token AMP en lending
- Cela a rendu une attaque de type **re-entrancy** possible
- **Rekt: $18.8M**

https://rekt.news/cream-rekt/

Re-entrancy attack



Pourquoi AMP?

- Lors d'un envoi d'ether **sur un smart contract**, on peut executer du code via:
  - *receive()* ou *fallback()*

- Avec un ERC-20, ce n'est pas possible, mais:
  - Certains ERC-677
  - ERC-777 → **AMP** :-)

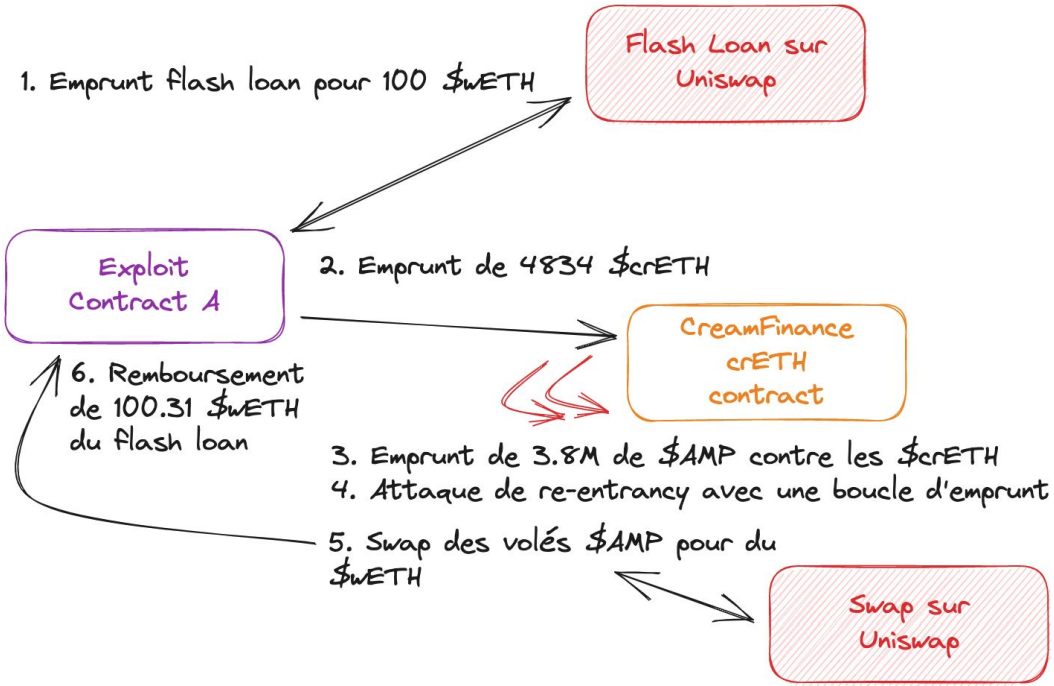
La vraie faille

```
function borrowFresh(address payable borrower, uint borrowAmount) internal returns (uint)
{
    [...]

    doTransferOut(borrower, borrowAmount);

    /* We write the previously calculated values into storage */
    accountBorrows[borrower].principal = vars.accountBorrowsNew;
    accountBorrows[borrower].interestIndex = borrowIndex;
    totalBorrows = vars.totalBorrowsNew;

    [...]
}
```

Oops!

- Le principale et l'intérêt ne sont mis à jour qu'après le transfert des fonds :-(
- On peut emprunter autant de fois que l'on veut avec le même collaréral.

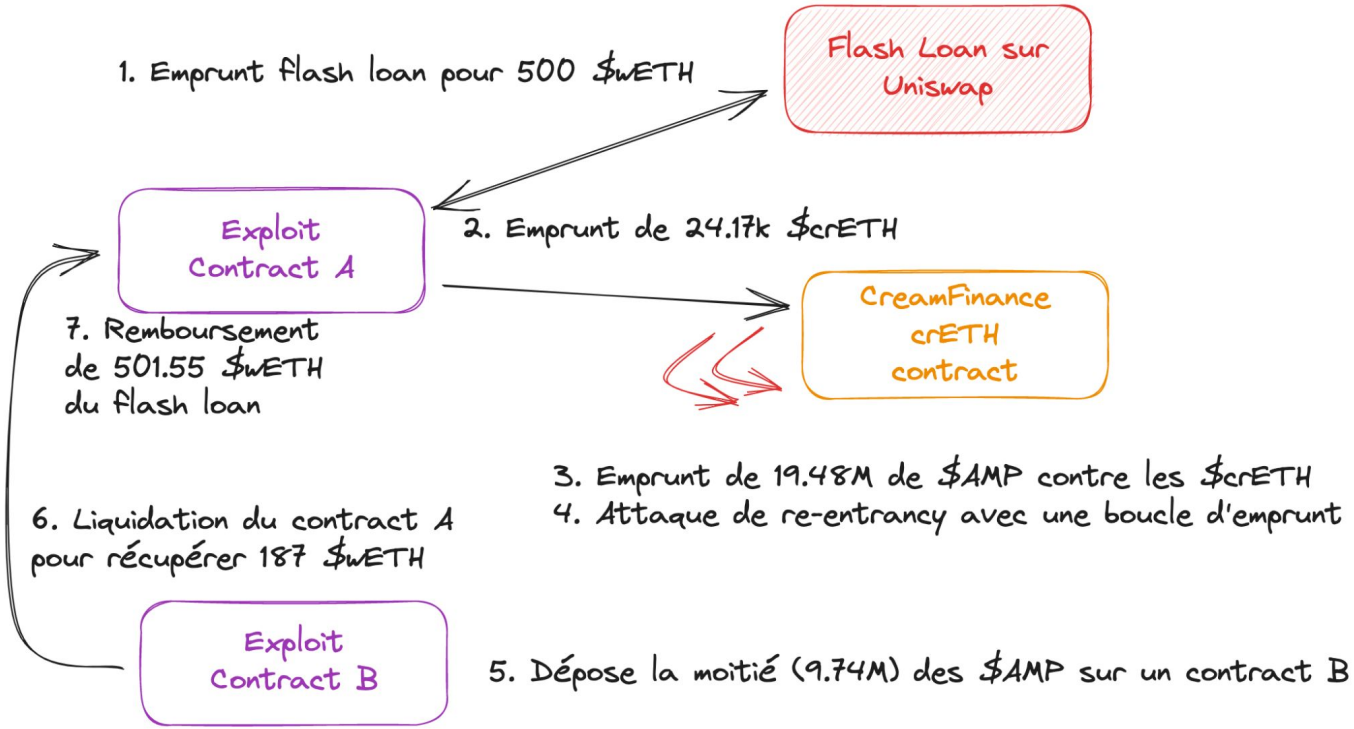
La première attaque



La première attaque

- From Uniswap V2: WISE 8 To 0xbd51Cb...4c83D1FA For 100 $182,029.00 Wrapped Ethe... (WETH...)
- From Cream.Finance: crETH Token To 0xbd51Cb...4c83D1FA For 4,834.46999826 Cream Ether... (crETH...)
- From Cream.Finance: crAMP Token To 0xbd51Cb...4c83D1FA For 3,896,000 $9,268.47 Amp... (AMP...)
- From 0xbd51Cb...4c83D1FA To Uniswap V2: AMP 2 For 1,649,668.813982746997229183 $3,924.51 Amp... (AMP...)
- From Uniswap V2: AMP 2 To 0xbd51Cb...4c83D1FA For 29.31 $53,352.70 Wrapped Ethe... (WETH...)
- From 0xbd51Cb...4c83D1FA To Uniswap V2: WISE 8 For 100.31 $182,593.29 Wrapped Ethe... (WETH...)
- From 0xbd51Cb...4c83D1FA To Cream Finance Flashloan Attacker For 2,246,331.186017253002770817 $5,343.95 Amp... (AMP...)

La deuxième attaque



La deuxième attaque

- From Uniswap V2: WISE 8 To 0x38c404...dF0bD22B For 500 $913,185.00 Wrapped Ethe... (WETH...)
- From Cream.Finance: crETH Token To 0x38c404...dF0bD22B For 24,172.23547176 Cream Ether... (crETH...)
- From Cream.Finance: crAMP Token To 0x38c404...dF0bD22B For 19,480,000 $46,192.34 Amp... (AMP...)
- From 0x38c404...dF0bD22B To 0x0ec306...9475A125 For 9,740,000 $23,096.17 Amp... (AMP...)
- From 0x0ec306...9475A125 To Cream.Finance: crAMP Token For 9,740,000 $23,096.17 Amp... (AMP...)
- From 0x38c404...dF0bD22B To 0x0ec306...9475A125 For 9,068.6218 Cream Ether... (crETH...)
- From 0x0ec306...9475A125 To Cream.Finance: crETH Token For 9,068.6218 Cream Ether... (crETH...)
- From 0x0ec306...9475A125 To 0x38c404...dF0bD22B For 187.583432458943489116 $342,596.75 Wrapped Ethe... (WETH...)
- From 0x38c404...dF0bD22B To Uniswap V2: WISE 8 For 501.55 $916,015.87 Wrapped Ethe... (WETH...)

La quête NG

Conclusion

- J'espère que je vous ai donné envie :-)
- Je n'ai pas encore fait toute les quêtes
  - Cairo incoming!
- Il y en a régulièrement des nouvelles!

Sam? Question?