

Cheat program for an old game

Кольцов Михаил

Кравцун Андрей

Тищенко Олеся

Что хотели сделать

- Понять, как происходил взлом игр раньше
- Потренироваться во взломе на старой игре
- Получить программу, которая даёт преимущество в игре

Что ломали

- Игра с открытым исходным кодом
- Написана на C\C++
- Не имеет античит-способностей
- Minesweeper, Doom

Как ломали

- CheatEngine: приятный просмотр памяти
- Читали исходный код
- Сканировали и меняли память (WinApi, ptrace)

```
class Cell final : public QLabel {  
private:  
    int _y;  
    int _x;  
    enum {none, flagged, asked};  
    int status;  
    bool m_pressed;  
    bool entered;  
  
public:  
    bool opened;  
    bool shown;  
    bool is_empty;  
    ...  
}
```

40001000000000000010

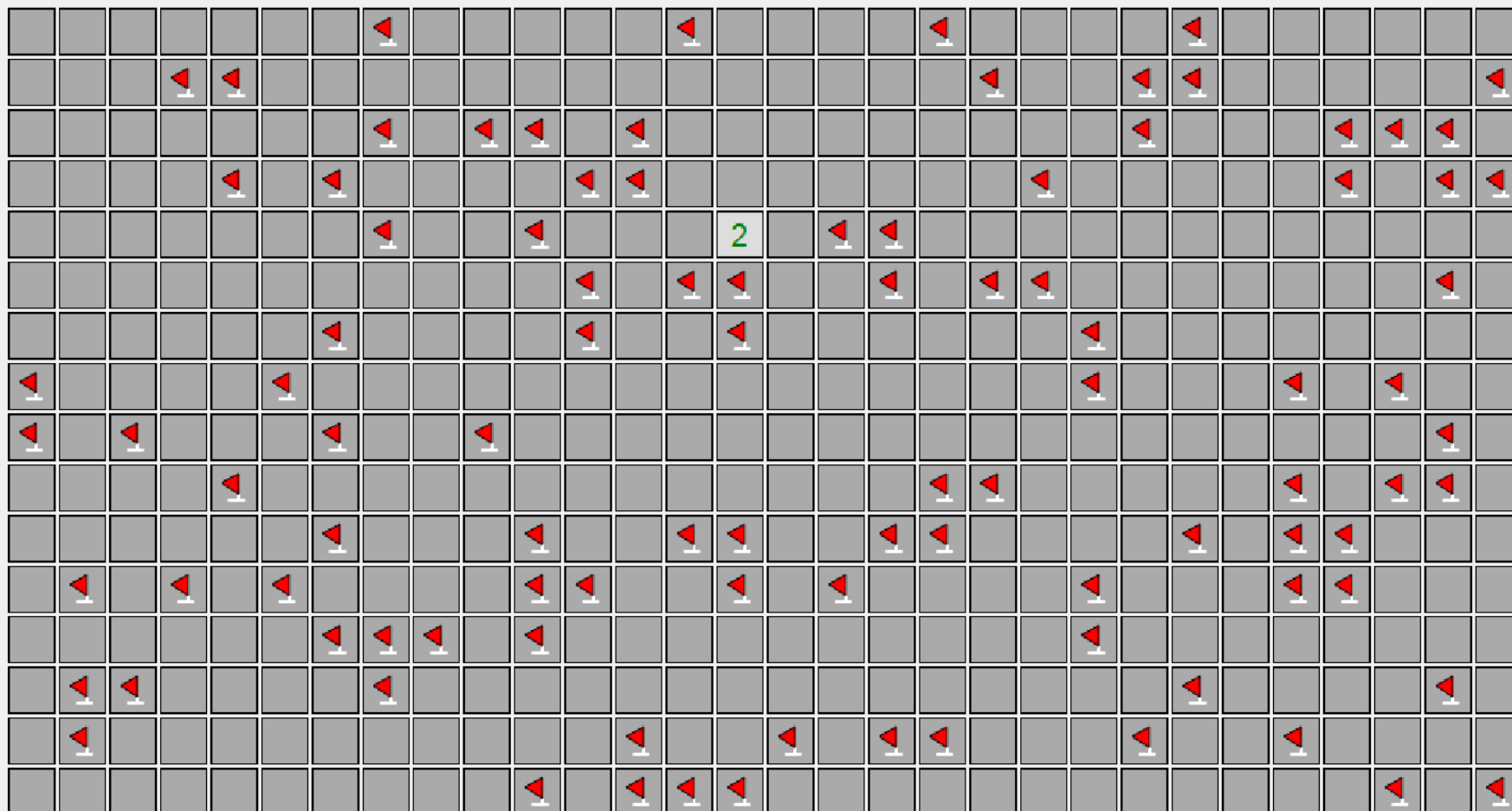
Что получилось

- Помечаем мины в Minesweeper
- Изменяем здоровье в Doom

Minesweeper



Game Help



Кто что делал

- Миша: принимал решения, придумал и написал детектор мин в Сапёре, изучал WinApi
- Леся: придумала и добавила визуальное отображение мин, копалась в памяти сапёра
- Андрей: работал над Doom, реализовал изменение здоровья

ССЫЛКИ

- [Репозиторий](#)
- [SEWiki](#)
- [видео по DOOM](#)
- [видео по Minesweeper](#)

Спасибо за внимание!