Отчет по машине “Titanic” на hackthebox lvl:easy(Для новичка как,я не совсем изи я бы сказал))  
  
Первым делом я бы хотел сказать что не особо разбираюсь во всем этом но мне достаточно интересно была проходить эту машину, в общем я потратил 4 часа чтобы получить флаг пользователя и рут флаг тоже,первые 3 часа я пытался разобраться сам использовал свой мозг и знания и честно скажу использовал чатгпт но даже с ним у меня не получалось выполнить титаник,затем я поискал какие либо гайды и инструкций чтобы разобраться как все делается в итоге смог все таки найти гайд вот ссылка на него https://medium.com/@talha.cys/htb-titanic-fd1a0d596e3e.  
  
**Глава 1  
разведка через nmap**  
 За первые три часа я выяснил что сайт титаника находится на порту 80(http)просканировав с помощью инструмента nmap, nmap -sC -sV 10.10.11.55 и скан мне выдал эту информацию,далее я ввел домен и дал айпишку в редакторе нано с помощью команды sudo nano /etc/hosts и зашел на сайт Titanic.htb,как выяснилось этот сайт содержит в себе не кликабельные вкладки типо services,about и т.д  
  
**Фаззинг поддоменов**  
Затем я покликал еще и нашел полю для регистраций на титаник чтобы получить билет туда я понял что она мне скидывает файл в типе json каждый раз когда я регистрируюсь.  
После я провел фаззинг поддоменов и выяснил что существует такой поддомен dev.titanic.htb туда и зашел предварительно загрузив его в /etc/hosts.  
  
**Анализ исходного кода app.py**  
Покликав на вкладки в сайте dev.titanic.htb я нашел поле для регистраций зарегался и еще порыскав в сайте нашел исходный код app.py что в таких сайтах с gitea обычное дело.Исследовав код я понял что билеты загружаются без фильтрации пути и что это можно использовать как уязвимость и начать эксплуатацию пути.  
  
  
  
**Глава 2**  
**Эксплуатация путей** (LFI)  
Наша цель получить конфиденциальные файлы точнее доступ к ним  
Сначало я ввел команду curl <http://titanic.htb/Tickets/../../../../etc/passwd> это была проверка уязвимости на возможность читать произвольные файлы.В итоге я не получил ничего интересного поскольку был доступ к внутренним файлам я попробовал получить информацию с конфигурационных файлов и исследуя открытые источники обнаружил /data/gitea/conf/app.ini и решил дальше исследовать этот путь что привело меня к вот этой команде curl <http://titanic.htb/Tickets/../../../../data/gitea/conf/app.ini> с помощью которого я узнал о том какие базы данных имеются на сайте,затем я загрузил гитеа дб  
curl http://titanic.htb/Tickets/../../../../data/gitea/gitea.db -o gitea.db и извлек базу данных из sqlite3 и внутри него извлек таблицу пользователей всю информацию оттуда в текстовый файл с помощью которого я получил данные пользователей и их хэши  
  
  
  
**Глава 3**  
**Извлечение хэшей из базы данных и получения флага пользователя**  
Сначало надо было узнать какое хэширование делается тут по открытым источником выяснилось что тут используется хэширование SHA-256 PBKDF2 перед тем как использовать hashcat нужно преобразовать данные в base64 формат что я и сделал с командой  
 sqlite3 gitea.db "SELECT passwd, salt, name FROM user" | while IFS='|' read -r hash salt name; do

hash\_b64=$(echo "$hash" | xxd -r -p | base64)

salt\_b64=$(echo "$salt" | xxd -r -p | base64)

echo "${name}:sha256:50000:${salt\_b64}:${hash\_b64}"

done > gitea.hashes  
затем я наконец то запустил hashcat   
hashcat -m 10900 -a 0 gitea.hashes /usr/share/wordlists/rockyou.txt –username  
предварительно загрузив словарь rockyou.txt   
в итоге я получил два пароля преобразованных из хэша   
один из которых подошел к девелоперу,потом я зашел через SSH как пользователь ssh [developer@titanic.htb](mailto:developer@titanic.htb) и наконец получил свой первый флаг открыв cat user.txt  
   
  
  
 **Глава 4  
Эскалация привилегий и получения уже root флага**  
чтобы перейти на уровень root мне нужно была найти доступные для записи каталоги   
find / -writable -type d 2>/dev/null   
фишка в том что нужна найти каталоги с ограниченным доступом и лучше не обращать внимание на /tmp, /var/tmp, и /dev/shm так как в них наименьший шанс в повышений привилегий.  
После того, как я нашел доступные для записи корневые каталоги, я исследовал /opt/scriptsи обнаружил скрипт оболочки с именем identify\_images.sh. Проверив его содержимое с помощью cat, я обнаружил, что он использует ImageMagick для обработки изображений в /opt/app/static/assets/images. Поскольку нам нужно выполнить наш собственный скрипт как root, я проверил версию ImageMagick и обнаружил, что это 7.1.1-35, которая уязвима для выполнения произвольного кода — идеально для повышения привилегий.

Я нашел в сети доказательство концепции (PoC) для эксплуатации уязвимости ImageMagick для выполнения произвольного кода. Поэтому я перешел к /opt/app/static/assets/imagesкоманде эксплойта и запустил ее, изменив ее в соответствии с целевой средой.ну и с помощью скрипта использовавший бибилотеку я смог внедрить вредный эксплойт и вот наша директория выдала это gcc -x c -shared -fPIC -o ./libxcb.so.1 - << EOF #include <stdio.h> #include <stdlib.h> #include <unistd.h> \_\_attribute\_\_((constructor)) void init() { system("cp /root/root.txt root.txt; chmod 754 root.txt"); exit(0); } EOF developer@titanic:/opt/app/static/assets/images$ ls entertainment.jpg exquisite-dining.jpg favicon.ico home2.jpg home.jpg libxcb.so.1 luxury-cabins.jpg metadata.log read.txt root.txt  
  
Я вижу тут файл root.txt глаза горят и я открываю его и наконец получаю root флаг и заканчиваю титаник   
  
  
  
  
**Саморефлексия**Это было достаточно трудно для меня особенно когда я первые три часа делал без гайда скажу что без гайда у меня получилось сделать на процентов 50 наверное я остановился на эксплуатаций путей а с гайдом конечно все стало в миллард раз понятнее я думаю тут сложнее всего новичку понять какую методику взлома можно использовать потому что есть много всего и сложно именно сразу подобрать ключ к этому понятию для меня тут было непонятнее всего что использовать в качестве методику для взлома, за три часа я смог все таки выяснить что нужно использовать уязвимость путей LFI что мне помогло в дальнейшем взломать титаник.  
Вообщем мне понравилось как нибудь летом еще порешаю задачки на хакзебокс чтобы прокачать себя в этой сфере было интересно было непонятно и был азарт взломать на этом не остановлюсь.