

# Web-11 Далекие земли

## (1/2)

Ты нашёл портал, который перемещает на дальние острова Энда. В этих землях разбросано множество шалкеров - говорят, их около тысячи! А один из этих шалкеров содержит древнюю книгу с флагом.

**Рекомендуемые утилиты:** burp suite, python

**Цель работы:** Найти и скачать изображение с флагом

**Критерий оценки:** Предоставление правильного флага

## Решение

Перейдя на главную страницу, можно увидеть картинки. Если внимательно посмотреть источник можно заметить везде `/images`.

```
<div class="gallery-item" data-url="/images/grass_block.png">
  
  <div class="gallery-item-title">
    Блок травы
  </div>
</div>

<div class="gallery-item" data-url="/images/diamond_ore.png">
  
  <div class="gallery-item-title">
    Алмазная руда
  </div>
</div>

<div class="gallery-item" data-url="/images/redstone.png">
  
  <div class="gallery-item-title">
    Красный камень
  </div>
</div>
```

При переходе на `/images/`, видим листинг всех картинок в этой папке.

### Index of /images/

<a href="#">../</a>		
<a href="#">bow.png</a>	30-Oct-2025 22:18	8271
<a href="#">chest.png</a>	30-Oct-2025 22:18	45517
<a href="#">crafting_table.png</a>	30-Oct-2025 22:18	44185
<a href="#">diamond_ore.png</a>	30-Oct-2025 22:18	53913
<a href="#">flag.png</a>	17-Jan-2026 15:19	43296
<a href="#">furnace.png</a>	30-Oct-2025 22:18	49286
<a href="#">grass_block.png</a>	30-Oct-2025 22:18	56197
<a href="#">pickaxe.png</a>	30-Oct-2025 22:18	15341
<a href="#">potion.png</a>	30-Oct-2025 22:18	8007
<a href="#">redstone.png</a>	30-Oct-2025 22:18	7628
<a href="#">sword.png</a>	30-Oct-2025 22:18	8499

Находим картинку `flag.png` с публичным флагом, который не видно на главной странице.



vsosh{f1rst\_fl4g\_1n\_publ1c\_1m4g3s}

## Флаг

vsosh{f1rst\_fl4g\_1n\_publ1c\_1m4g3s}

## (2/2)

Оказывается, ты нашел не обычный портал в Энд. Он работает как прокси, но его защита настроена странно! При определенных условиях он позволяет заглянуть в далекие земли. А где-то там есть сундук с приватными изображениями флага, недоступный через обычный портал.

**Рекомендуемые утилиты:** burp suite

**Цель работы:** Использовать портал-прокси для телепортации в запретную зону и прочитать флаг с картинки

**Критерий оценки:** Предоставление правильного флага

## Решение

При взгляде на главную страницу можно заметить странную картинку, у которой путь начинается с `/private_images`.

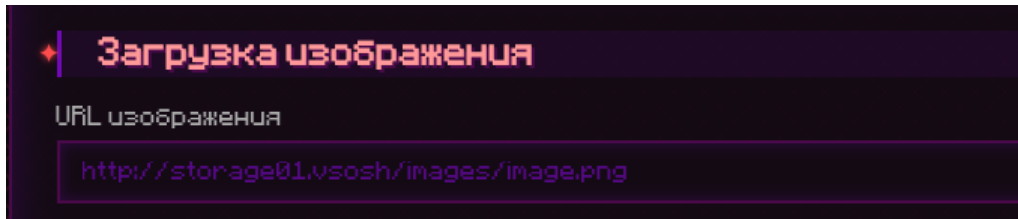
```
<div class="gallery-item" data-url="/private_images/Loading_Random.png">
  
  <div class="gallery-item-title">
    Загрузка
  </div>
</div>
</div>
```

Перейдя на `/private_images/` видим листинг всех приватных картинок. Там есть `flag.png`, однако доступ к нему ограничен.

# Index of /private\_images/

<a href="#">../</a>		
<a href="#">Loading_Random.png</a>	30-Oct-2025 22:18	993
<a href="#">flag.png</a>	17-Jan-2026 15:19	44

Попробуем достучаться через image proxy. В строке ввода и в html коде есть подсказка какие домены внутри нашей сети - `storage01.vsosh` и `storage03.vsosh`.



Попытаемся получить доступ до этого nginx с `/private_images` изнутри сети. Для этого будем перебирать ссылки вида `http://storage0x.vsosh/private_images/flag.png`, так как видим паттерн из целых цифр в названиях доменов, что сигнализирует о наличии IDOR уязвимости.

На `http://storage06.vsosh/private_images/flag.png` нам выдает флаг, так как мы нашли внутренний домен нашего nginx.

✦ Загрузка изображения

URL изображения

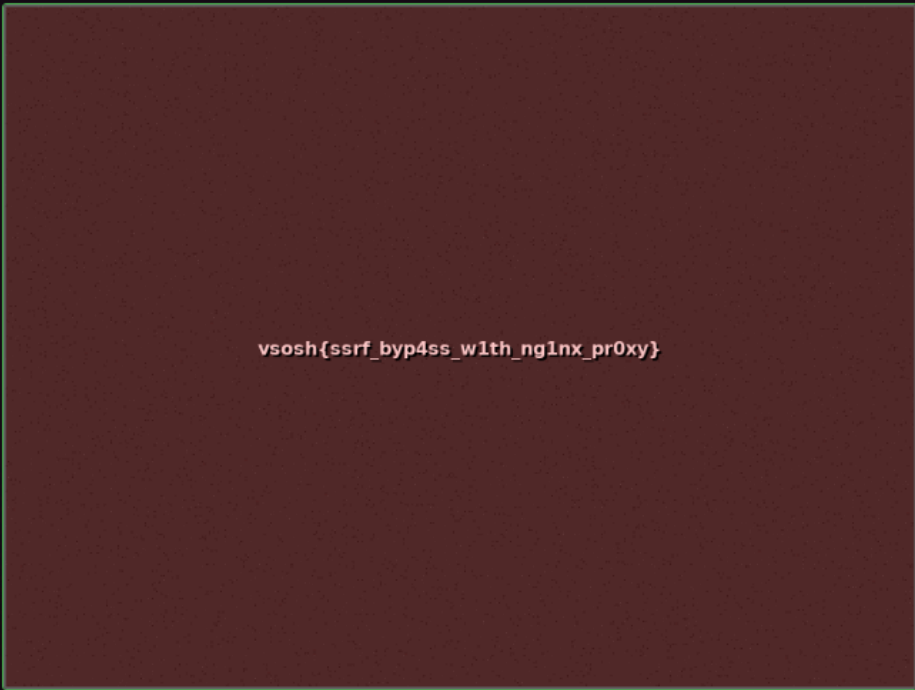
Ширина (px)

Высота (px)

Качество (1-100)

ЗАГРУЗИТЬ ИЗОБРАЖЕНИЕ

Изображение успешно загружено!



Флаг

vsosh{ssrf\_byp4ss\_w1th\_ng1nx\_pr0xy}