Solusi Langkah demi Langkah dengan Tangkapan Layar By Aldi

Question Analysis

Description

Figure 1 CTF Question

Nama pengguna adalah godam, seperti yang dinyatakan dalam deskripsi. Informasi ini akan digunakan sebagai petunjuk tambahan untuk menyelesaikan tantangan ini nantinya.

First Hint

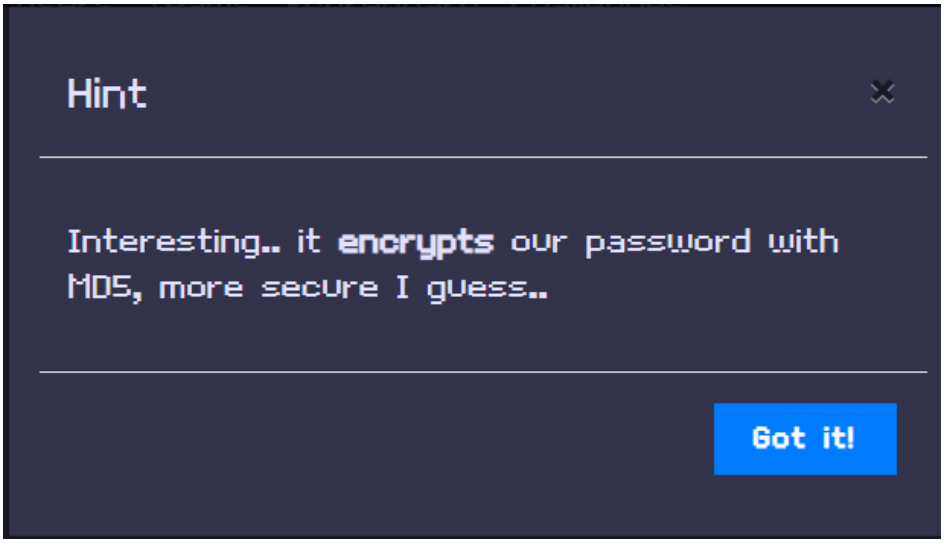


Figure 2 CTF Hint 1

Adapun petunjuk ini menyatakan bahwa kata sandi dienkripsi dengan hash MD5.

Second Hint

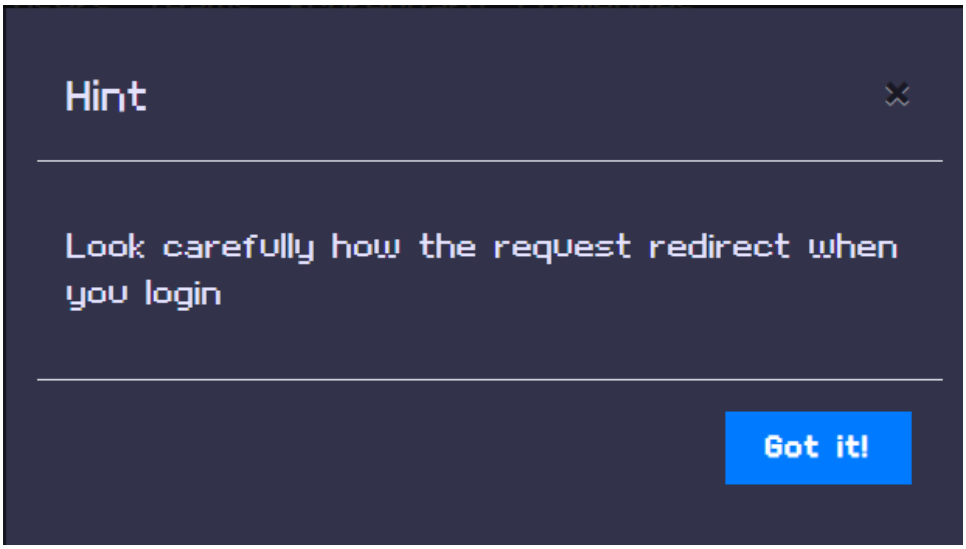


Figure 3 CTF Hint 2

Mengenai petunjuk ini, dinyatakan bahwa penulis perlu memeriksa permintaan pengalihan selama proses login.

Developer tools analysis

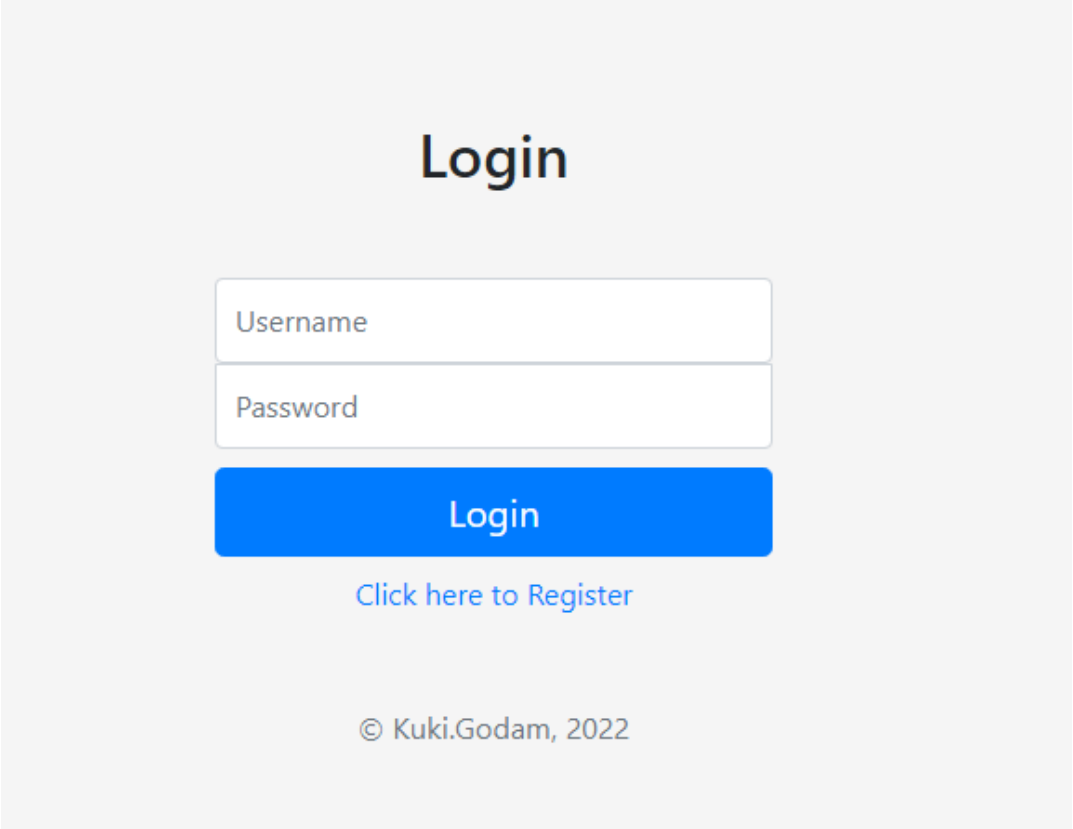


Figure 4 Login Page

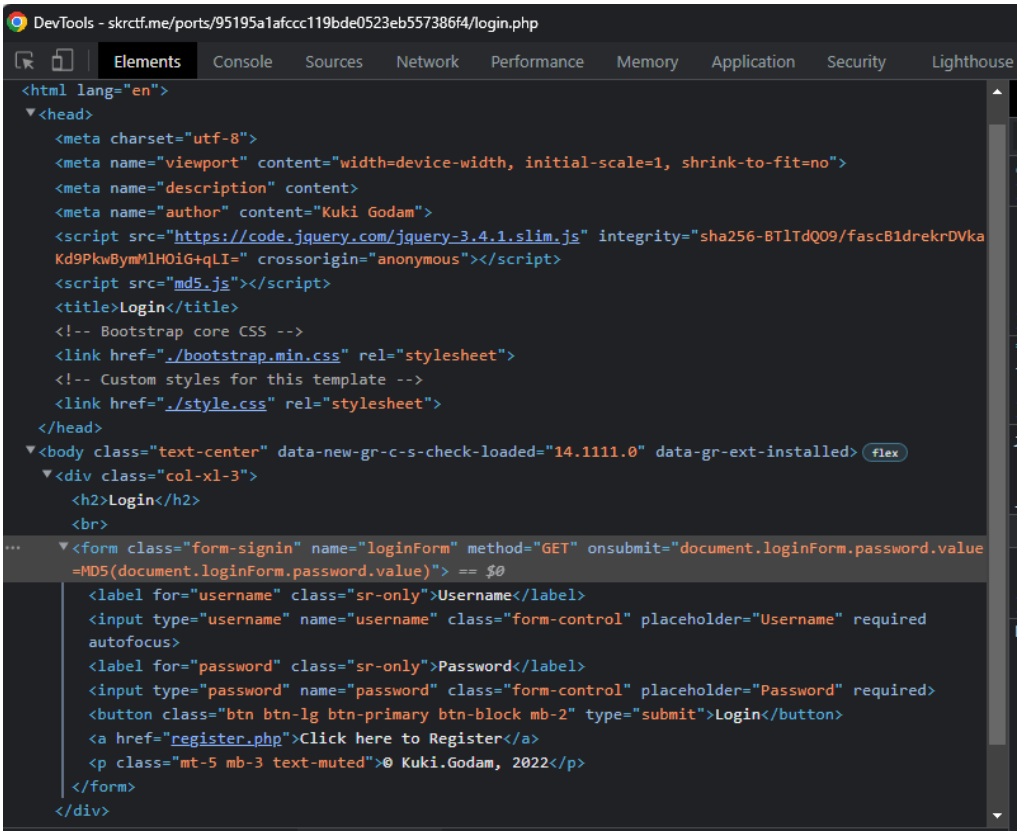


Figure 5 Source Code for login page

Di awal tantangan, halaman login ini akan menjadi antarmuka pertama yang akan berinteraksi dengan pengguna. Namun, tidak banyak informasi yang diberikan pada halaman ini meskipun sudah melihat melalui alat pengembang.

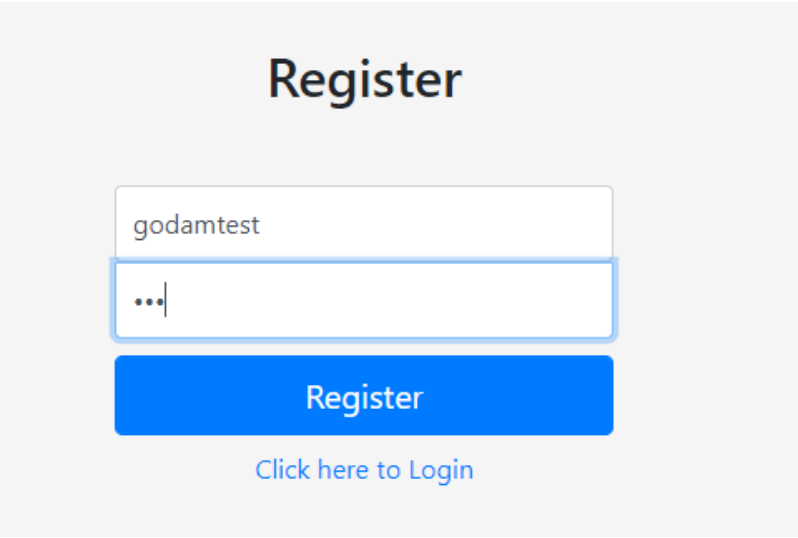


Figure 6 Registration Page

```
<!DOCTYPE html>
<html lang="en">
▼<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content>
    <meta name="author" content="Kuki Godam">
    <script src="https://code.jquery.com/jquery-3.4.1.slim.js" integrity="sha256-BTlTdQO9/fascB1drekrDVkaKd9PkwBymMlHOiG+qLI=" crossorigin="anonymous"></script>
    <script src="md5.js"></script>
    <title>Register</title>
    <!-- Bootstrap core CSS -->
    <link href="./bootstrap.min.css" rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="./style.css" rel="stylesheet">
  </head>
▼<body class="text-center"> flex
  ▼<div class="col-xl-3">
      <h2>Register</h2>
      <br>
...   ▼<form class="form-signin" name="registerForm" method="GET" onsubmit="document.registerForm.password.value=MD5(document.registerForm.password.value)"> == $0
        <h5 class="text-success">Registered successfully!</h5>
        <label for="username" class="sr-only">Username</label>
        <input type="username" name="username" class="form-control" placeholder="Username" required autofocus>
        <label for="password" class="sr-only">Password</label>
        <input type="password" name="password" class="form-control" placeholder="Password" required>
        <button class="btn btn-lg btn-primary btn-block mb-2" type="submit">Register</button>
        <a href="login.php">Click here to Login</a>
        <p class="mt-5 mb-3 text-muted">© Kuki.Godam, 2022</p>
      </form>
```

Figure 7 Source Code for registration page

Pada halaman registrasi, tab sumber mirip dengan halaman login di mana informasi yang diberikan menunjukkan kata sandi yang dimasukkan oleh penulis akan dienkripsi dengan hash MD5 pada form submit.

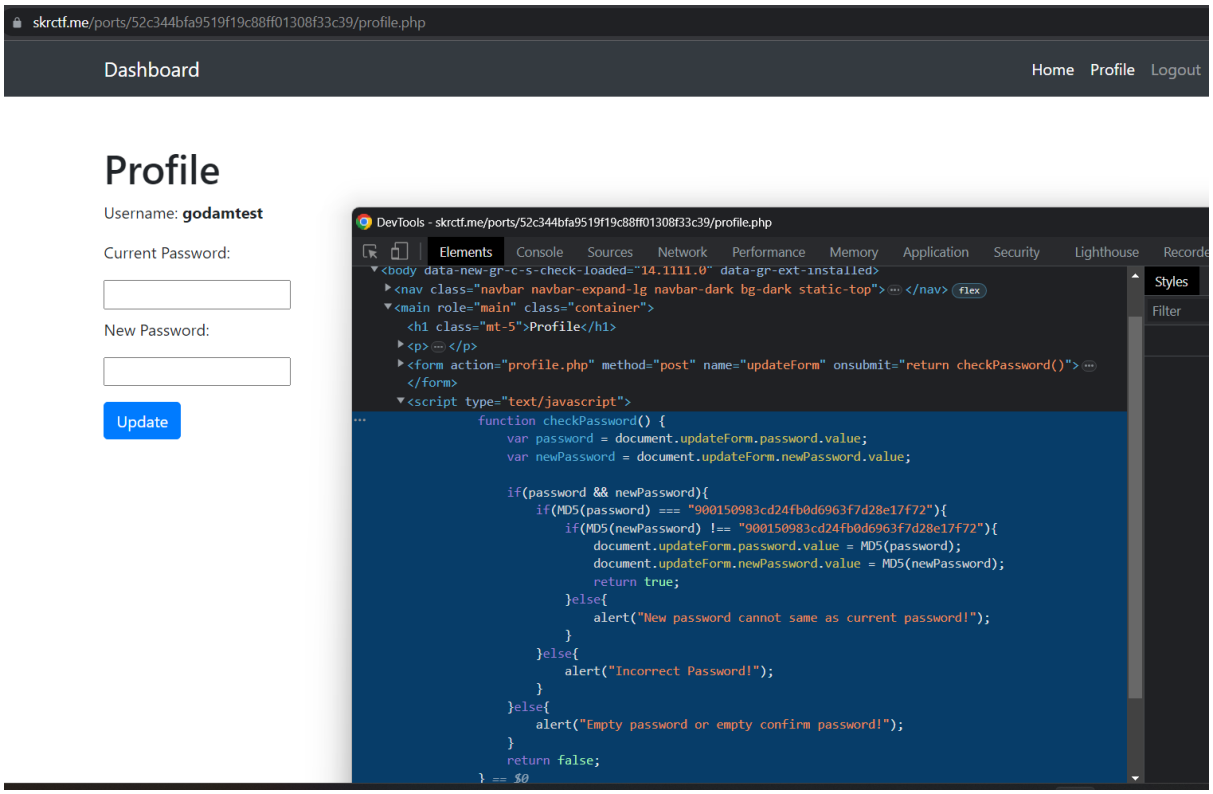


Figure 8 Profile Page with source code

Setelah masuk ke sistem dengan akun yang baru saja dibuat, penulis melihat bahwa sistem menyimpan kata sandi hash md5 di kode sumber halaman profil untuk tujuan otentikasi. Namun, menyimpan informasi sensitif di sisi klien menjadikannya sebuah kerentanan potensial.

BurpSuite analysis

Seperti yang dinyatakan pada petunjuk 2 bahwa perlu untuk melihat pengalihan permintaan saat login. Jadi, BurpSuite, alat eksploitasi web akan digunakan untuk analisis yang akan datang karena salah satu alat yang disediakan oleh BurpSuite, Burp Proxy, adalah mencegat permintaan HTTP dan memungkinkan pengguna untuk melihat atau memodifikasinya sebelum mengirimkannya ke server target (PortSwigger, 2023).

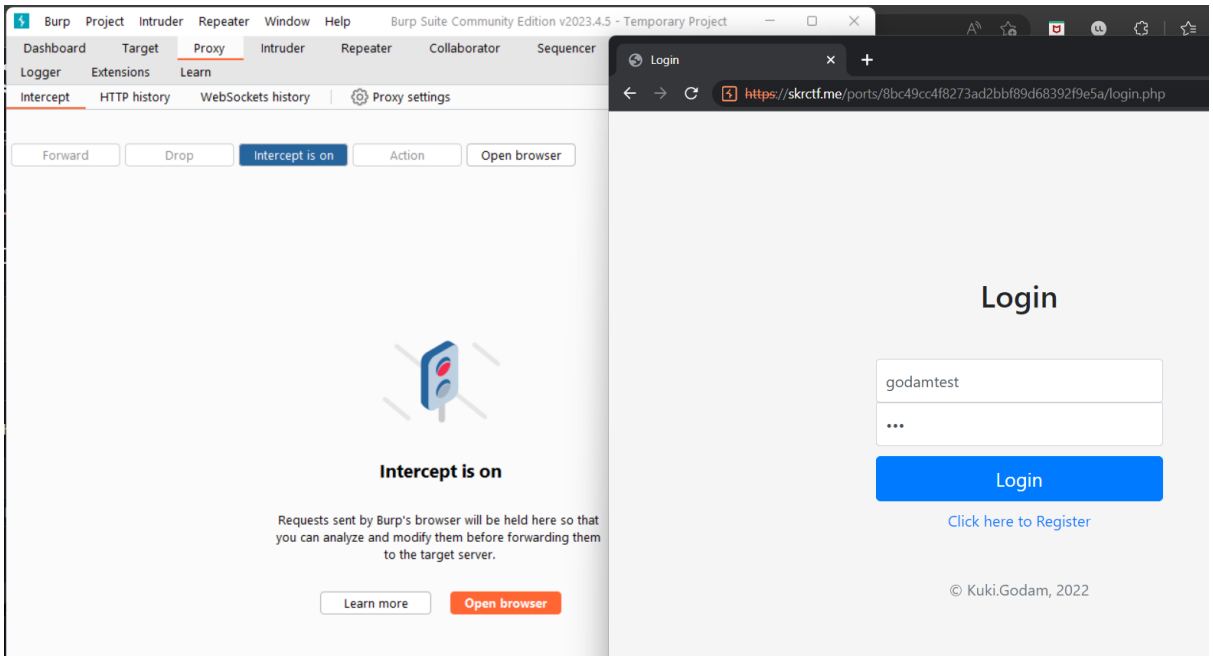


Figure 9 BurpSuite

Permintaan pertama yang akan penulis cegat adalah permintaan pengiriman formulir halaman login. Untuk memulai proses penyadapan, penulis akan mengaktifkan mode penyadapan pada BurpSuite dan menyadap permintaan setelah mengirimkan formulir login.

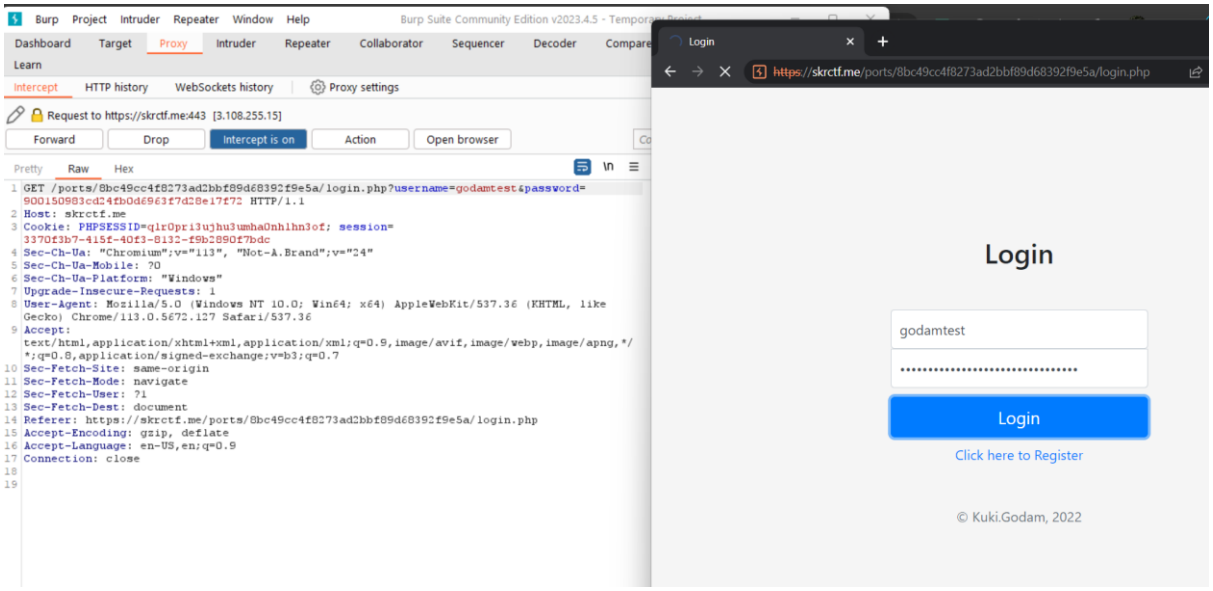


Figure 10 Intercepted Login Request

Ini adalah permintaan yang dicegat di mana penulis dapat melihat dan memodifikasi. Permintaan yang dicegat menunjukkan nama pengguna dan kata sandi yang telah digunakan untuk masuk.

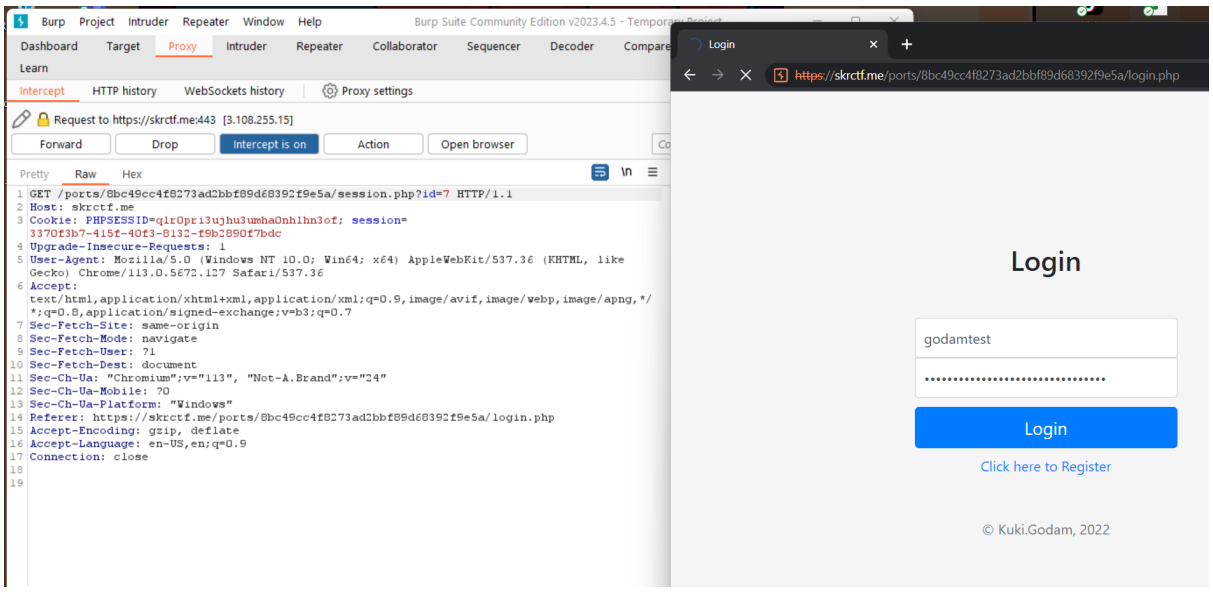


Figure 11 Redirected Request

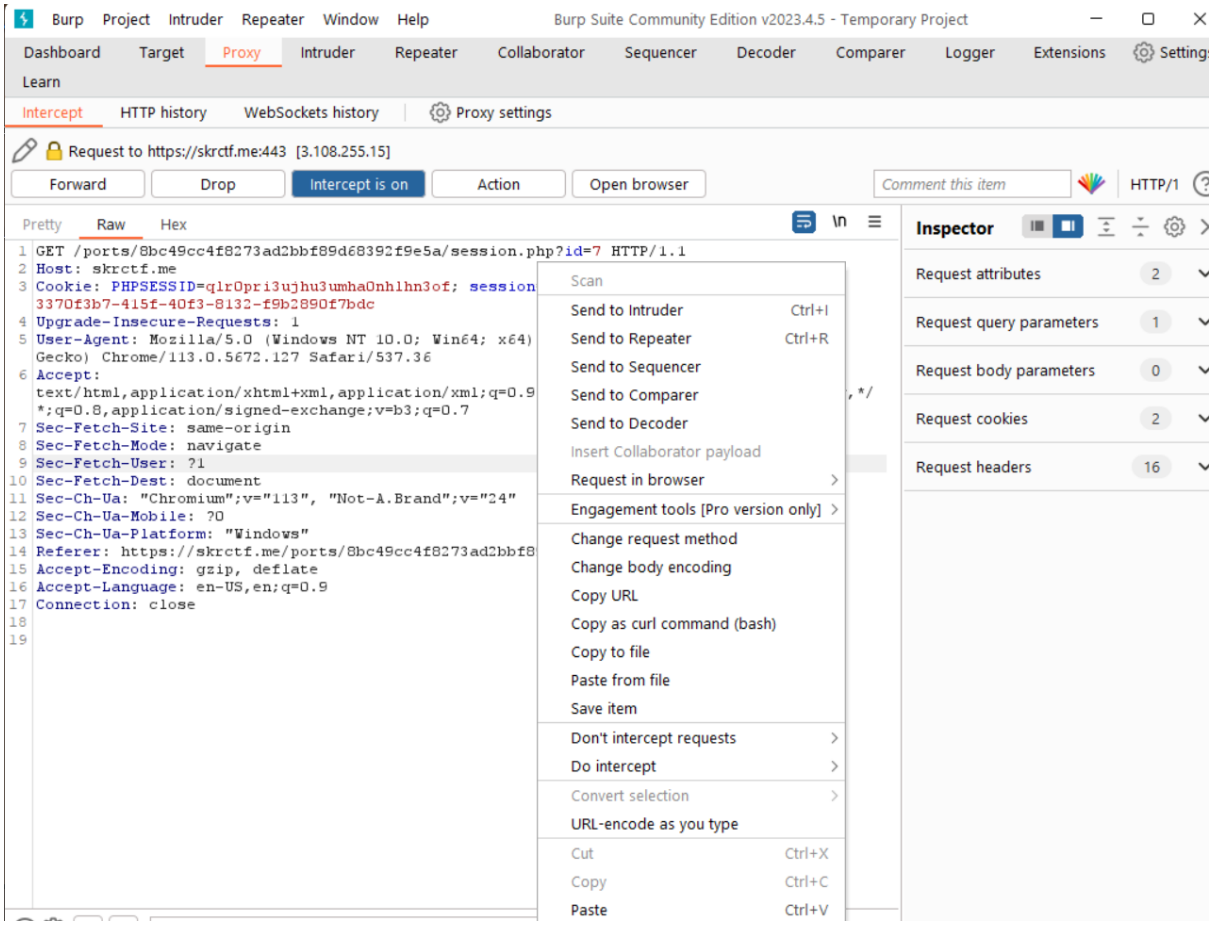


Figure 12 Send to Intruder

Kemudian, permintaan pengalihan berikutnya akan menyertakan id sesi untuk tujuan login. Ini akan menjadi kerentanan karena penulis dapat memodifikasi id sesi untuk menyamar sebagai orang lain. Meskipun id sesi untuk akun yang baru dibuat ini dibenarkan bahwa rentang id yang mungkin untuk akun yang ditargetkan adalah dari 1 hingga 6. Namun, untuk berhubungan dengan skenario kehidupan nyata, penulis mungkin perlu menguji ribuan id untuk membajak sesi. Jadi, penulis harus menggunakan alat BurpSuite lain, Intruder untuk membajak id sesi secara kasar. Untuk melakukannya, penulis harus mengirimkan permintaan kepada penyusup.

Attack with BurpSuite Intruder

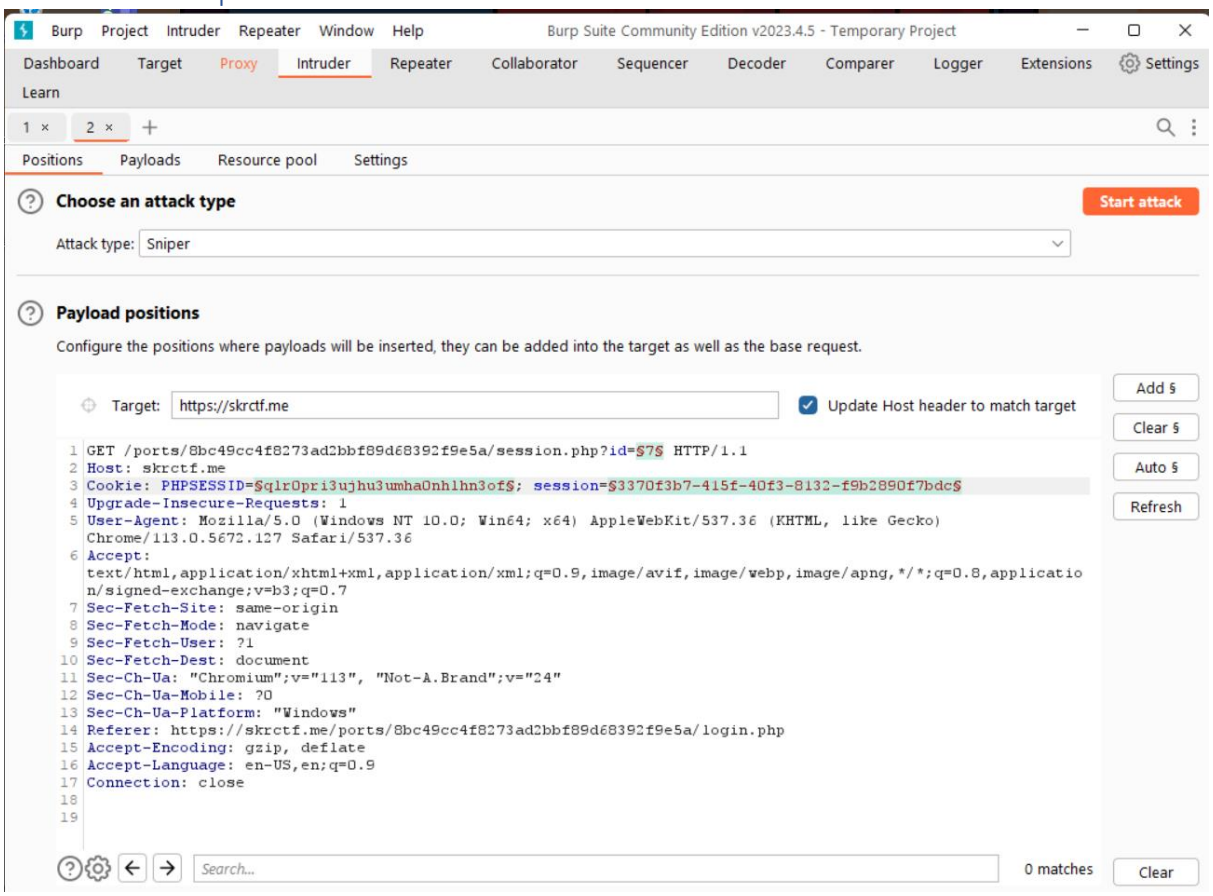


Figure 13 BurpSuite Intruder

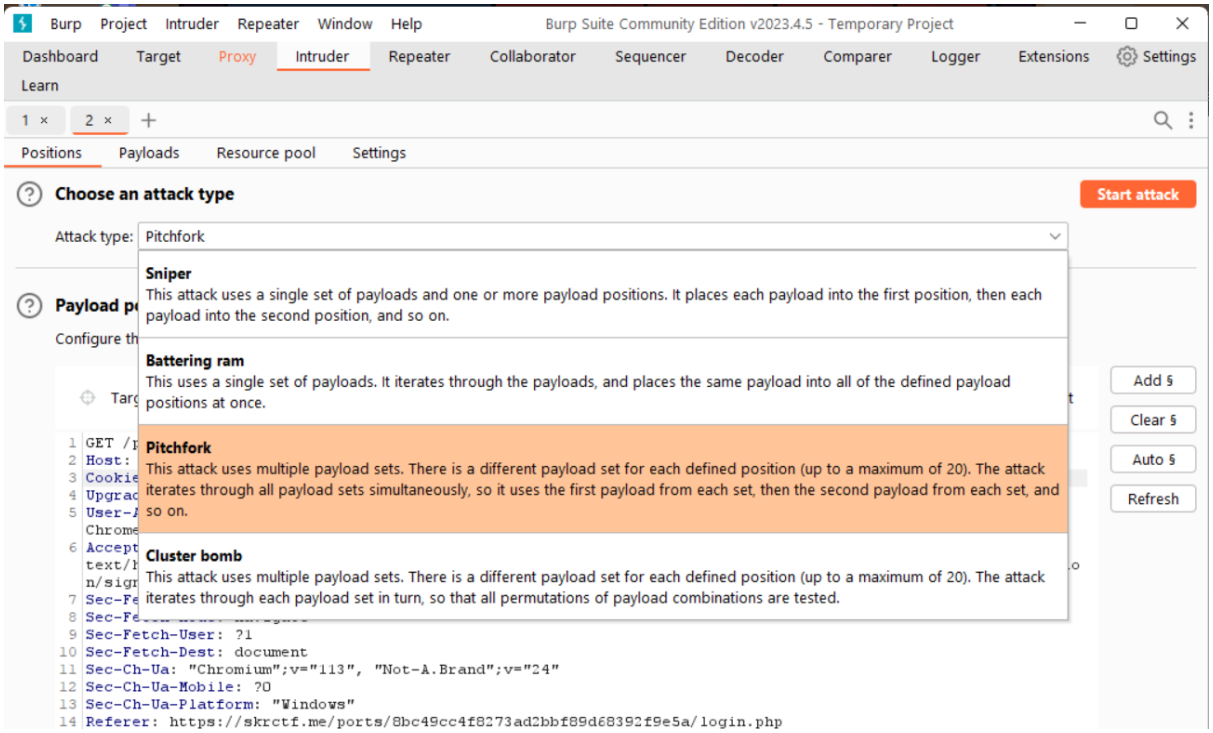


Figure 14 Pitchfork

Pilih PitchFork sebagai jenis serangan karena mode PitchFork memungkinkan beberapa muatan, ketiga id sesi dan id akun disorot dengan simbol § untuk menunjukkan bahwa itu adalah posisi muatan (Portswigger, 2023).

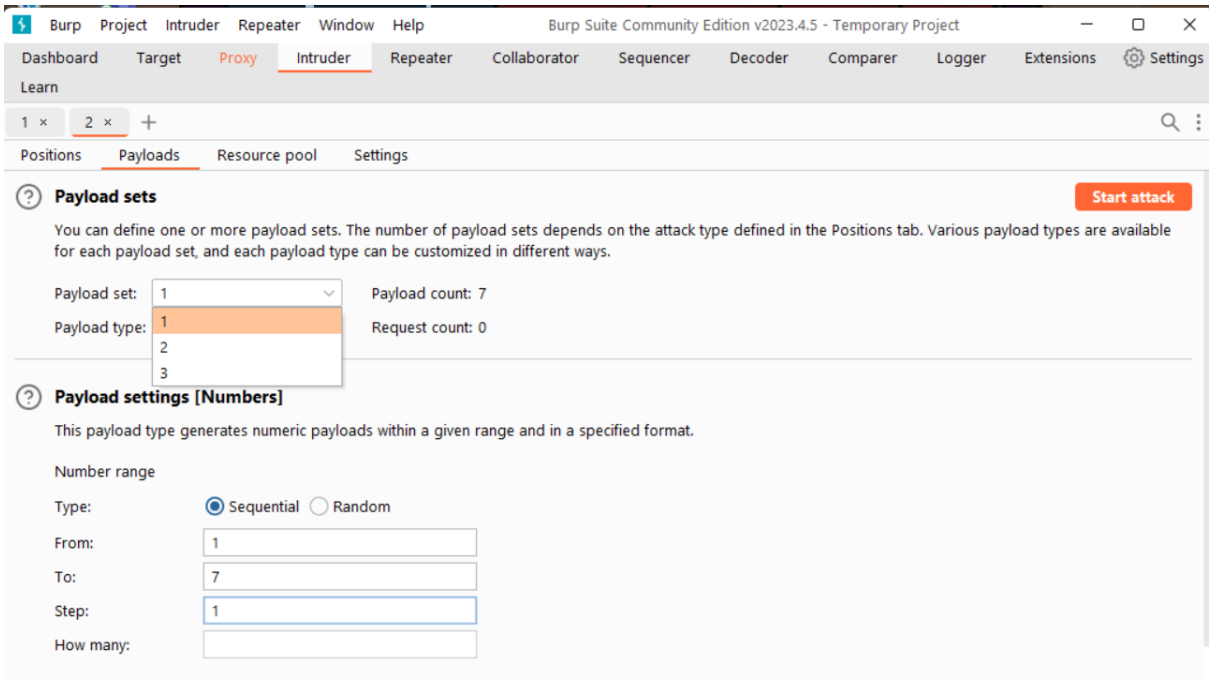


Figure 15 Set Payloads

Kemudian, atur jenis muatan ke nomor untuk semua muatan dengan nomor berurutan dari 1 hingga 7.

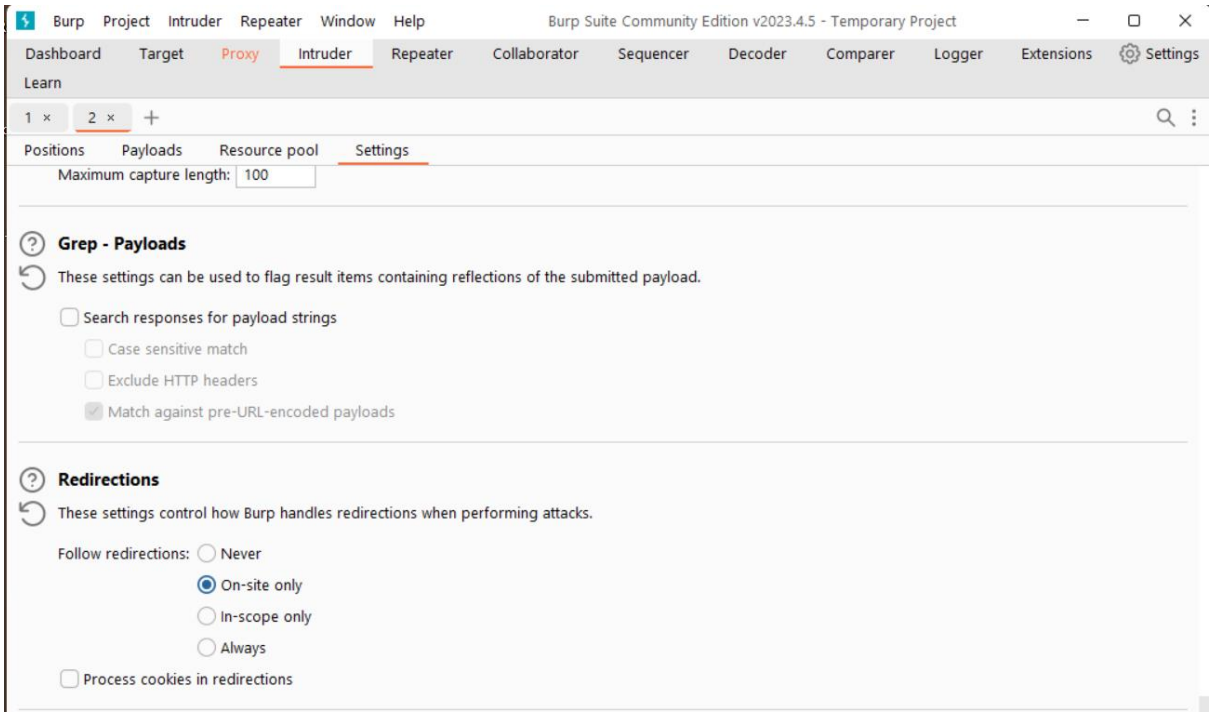


Figure 16 Set Redirections

Kemudian, centang opsi Hanya di tempat di bawah bagian Pengalihan sehingga BurpSuite akan mengembalikan semua permintaan dan respons yang dialihkan.

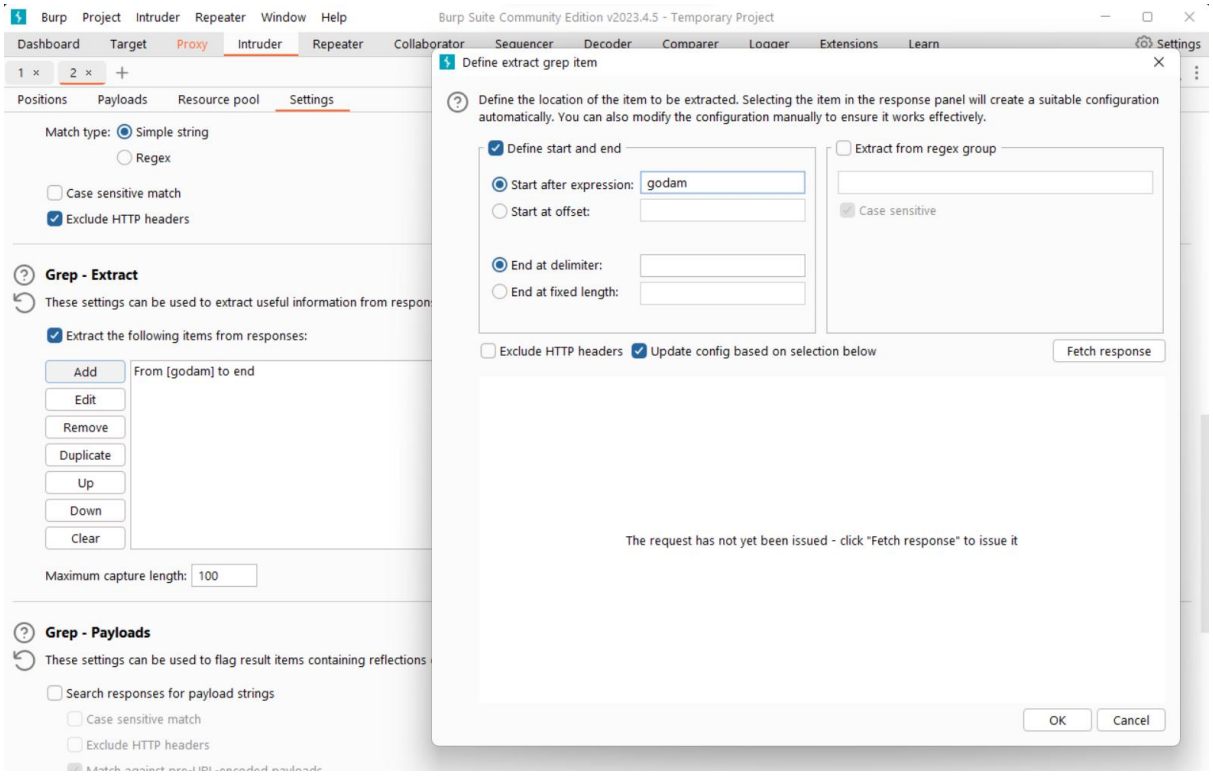


Figure 17 Set Grep

Karena halaman pertama setelah penulis login menampilkan username, maka penulis melakukan asumsi bahwa respon server mungkin akan menyertakan username “godam” pada kode HTML sehingga penulis menambahkan fungsi grep dimana BurpSuite akan menyorot hasil yang memiliki kata “godam”.

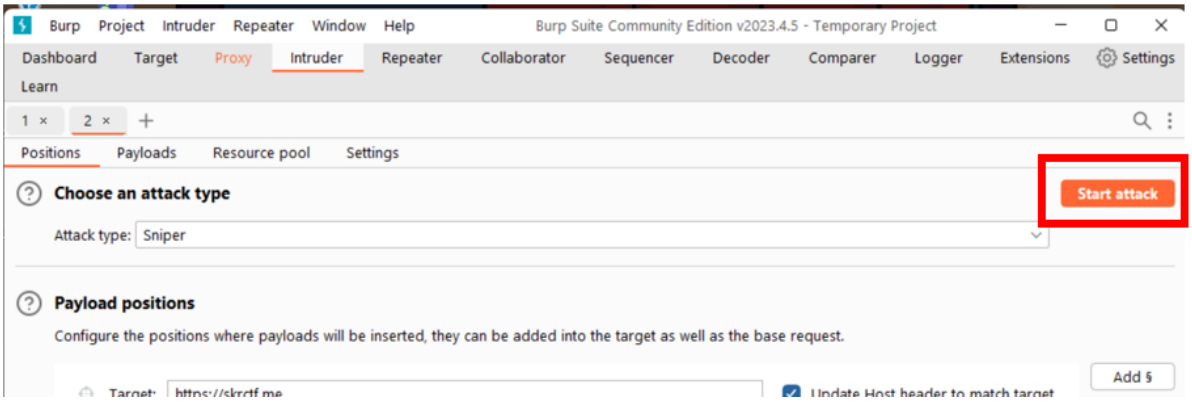


Figure 18 Start Attack

Mulai serangan.

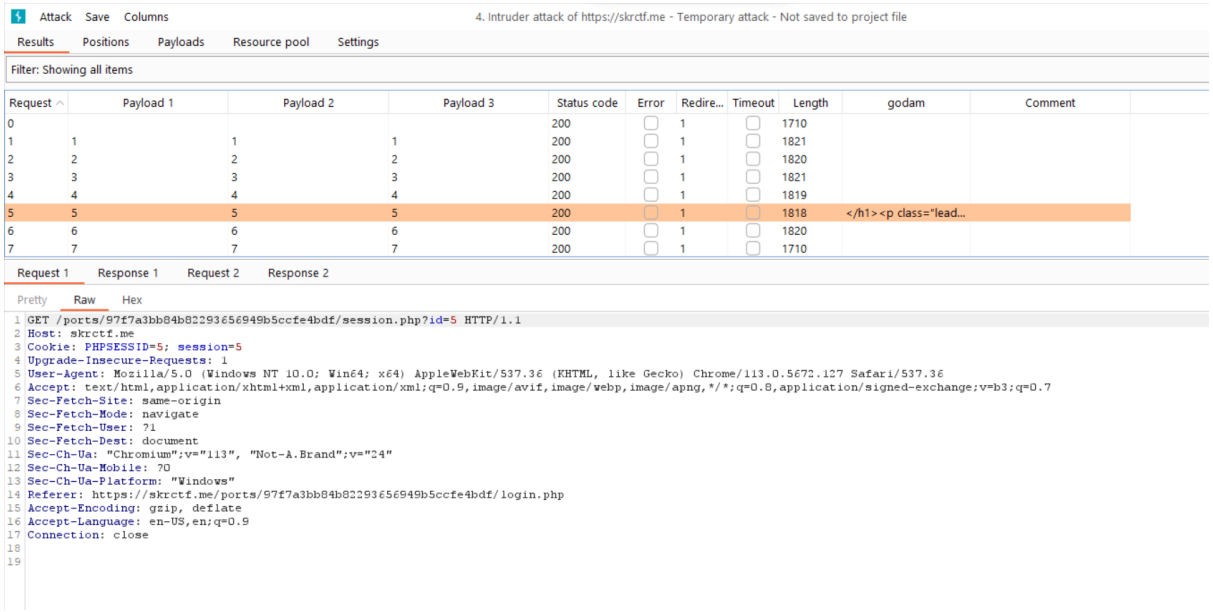


Figure 19 Attack Result

Ini adalah hasil serangan. Karena penulis telah menambahkan fungsi grep, BurpSuite akan mengembalikan sebuah blok kode di bawah kolom godam untuk setiap nilai yang cocok. Berdasarkan gambar di atas, penulis akan mengetahui bahwa request yang menggunakan session id 5 akan masuk ke akun godam.

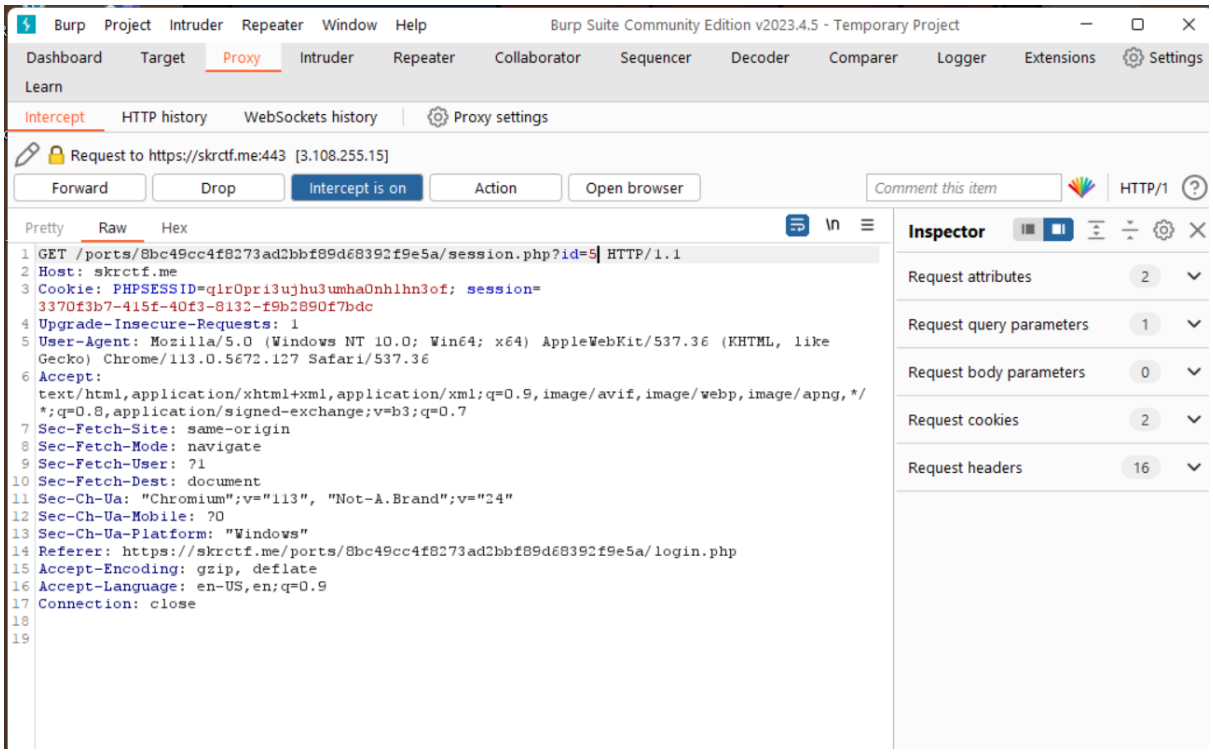


Figure 20 Modify request

Jadi, kembali ke BurpProxy di mana penulis dapat memodifikasi id sesi menjadi 5.

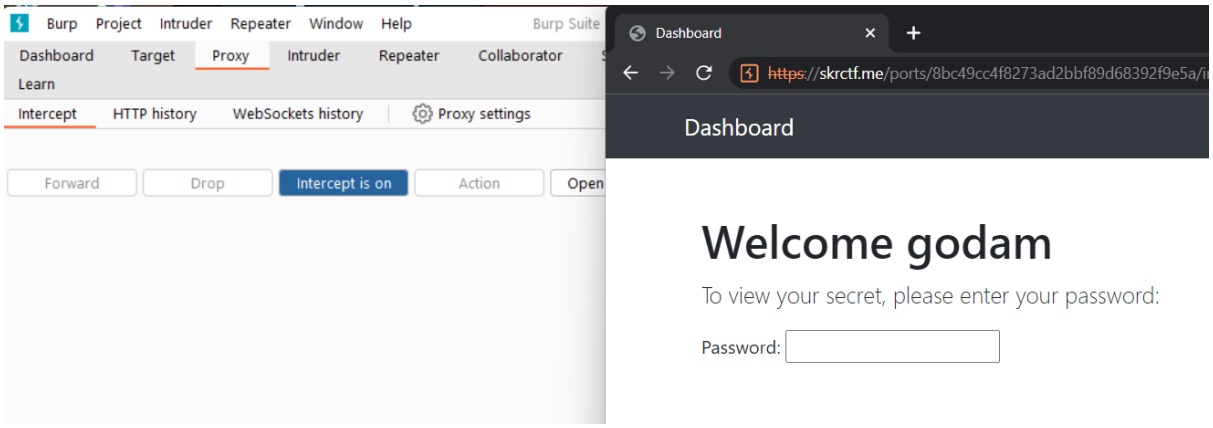


Figure 21 logged in as godam

Setelah meneruskan permintaan tersebut, penulis berhasil masuk ke akun godam.

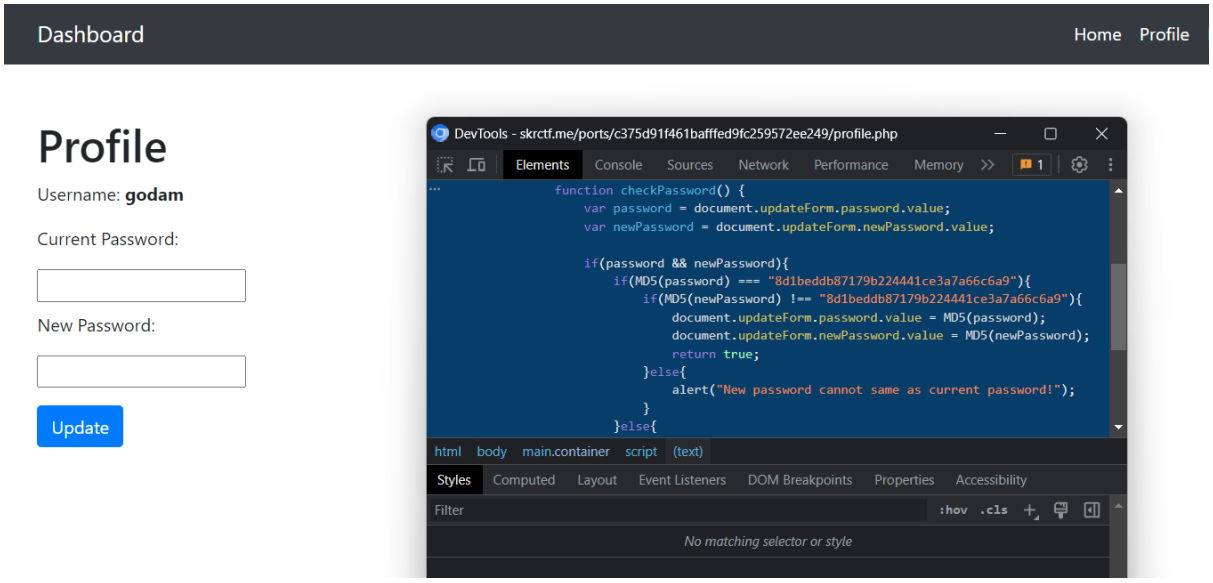
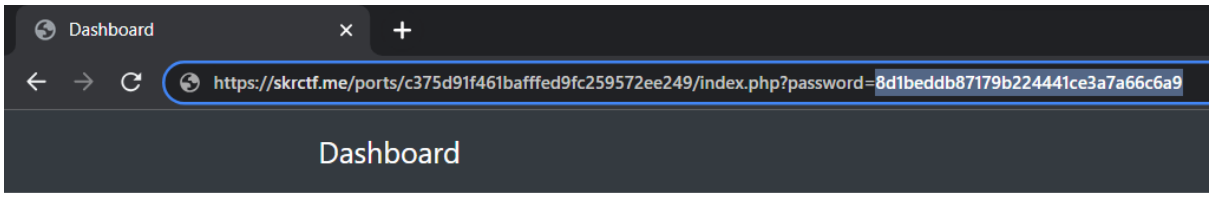


Figure 22 find md5 hashed password

Seperti yang telah disebutkan di atas, kerentanan pertama dari sistem ini adalah kata sandi ter-hash md5 disimpan di dalam kode sumber halaman profil, sehingga penulis bisa

mendapatkan kata sandi ter-hash milik Godam yaitu 8d1beddb87179b224441ce3a7a66c6a9.



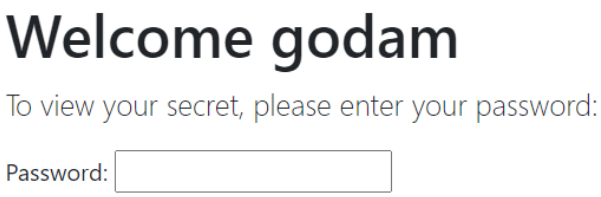
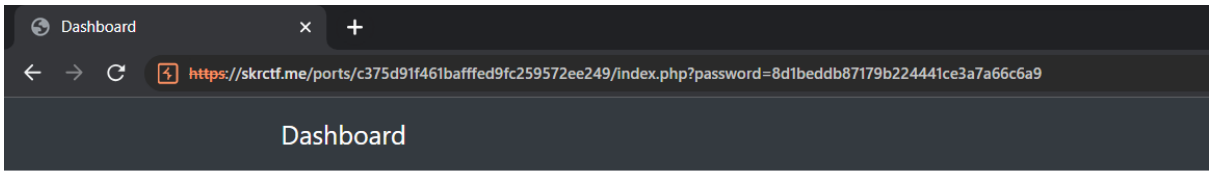


Figure 23 modify url



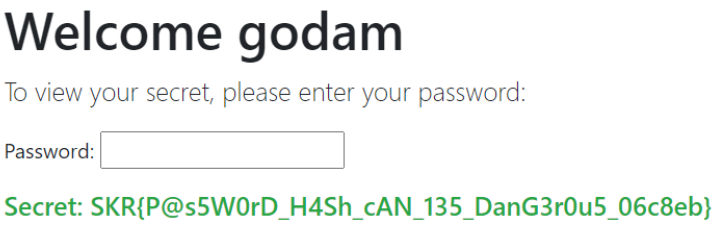


Figure 24 found flag

Selanjutnya, masuk ke index.php di mana flag disimpan. Masukkan kata sandi ter-hash sebagai argumen untuk parameter kata sandi di URL, penulis kemudian akan mendapatkan flag.

Justification

Seperti yang ditunjukkan pada solusi langkah demi langkah, penulis melakukan 2 analisis utama untuk menemukan kerentanan sistem untuk menemukan flag. Pertama-tama, analisis alat pengembang. Developer tool adalah alat yang tersedia di sebagian besar browser web seperti Chrome, Firefox, dan lainnya yang menyediakan fitur untuk memeriksa kode sumber, sesi lokal, dan masih banyak lagi (Nobledesktop, n.d.).

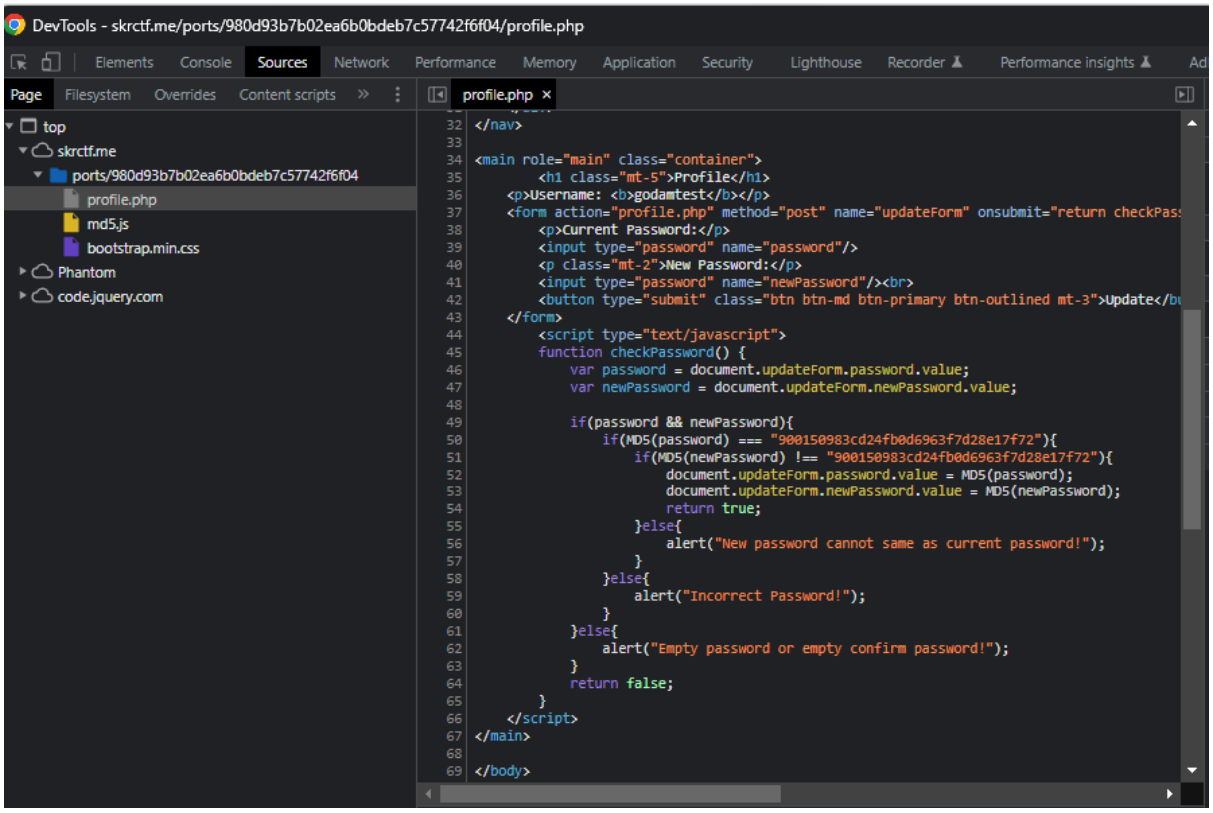


Figure 25 Source Tab

Namun, dalam proses penangkapan flag, satu-satunya kerentanan yang berguna yang telah disebutkan sebelumnya terletak pada kode sumber yang dapat penulis temukan melalui kode tersebut. Penulis dapat memeriksa HTML, CSS, dan JavaScript di bawah tab sumber, yang dapat memberikan penulis wawasan ke dalam sistem (Howard University CyberSecurity Center, n.d.).

Kedua, pemeriksaan permintaan HTTP menggunakan BurpSuite. Seperti yang telah disebutkan di atas, BurpSuite adalah seperangkat alat penetrasi web dimana penulis telah menggunakan dua alat yang disediakan yaitu BurpSuite Proxy dan BurpSuite Intruder untuk melakukan analisis dan penyerangan terhadap aplikasi web. Pertama, penulis menggunakan BurpSuite Proxy karena fiturnya yang dapat mencegat permintaan dan respon dari aplikasi web untuk melihat dan memodifikasi konten (GeeksForGeek, n.d.), dari sinilah penulis dapat menganalisa

kerentanan yang mungkin terjadi pada permintaan atau respon tersebut. Kedua, BurpSuite Intruder adalah alat untuk melakukan bruteforce atau serangan kamus pada kolom input, permintaan HTTP dan lainnya (Kucukkarakurt, 2022). Oleh karena itu, penulis menggunakan BurpSuite Intruder untuk membajak sesi godam.