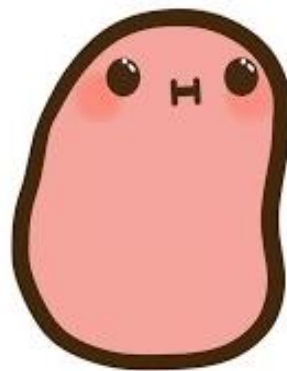


Intended Solution TP (Troll Pendahuluan)

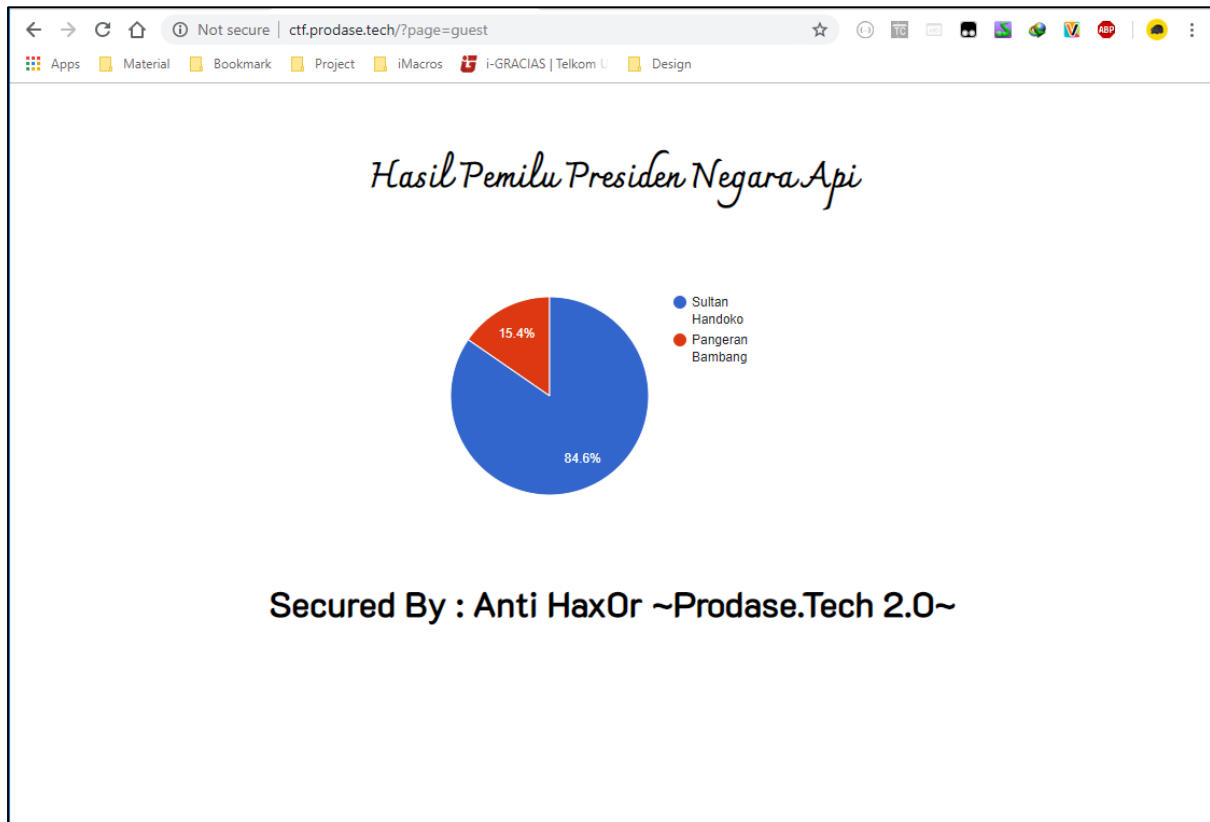
Modul 4



Problem Setter : NUB

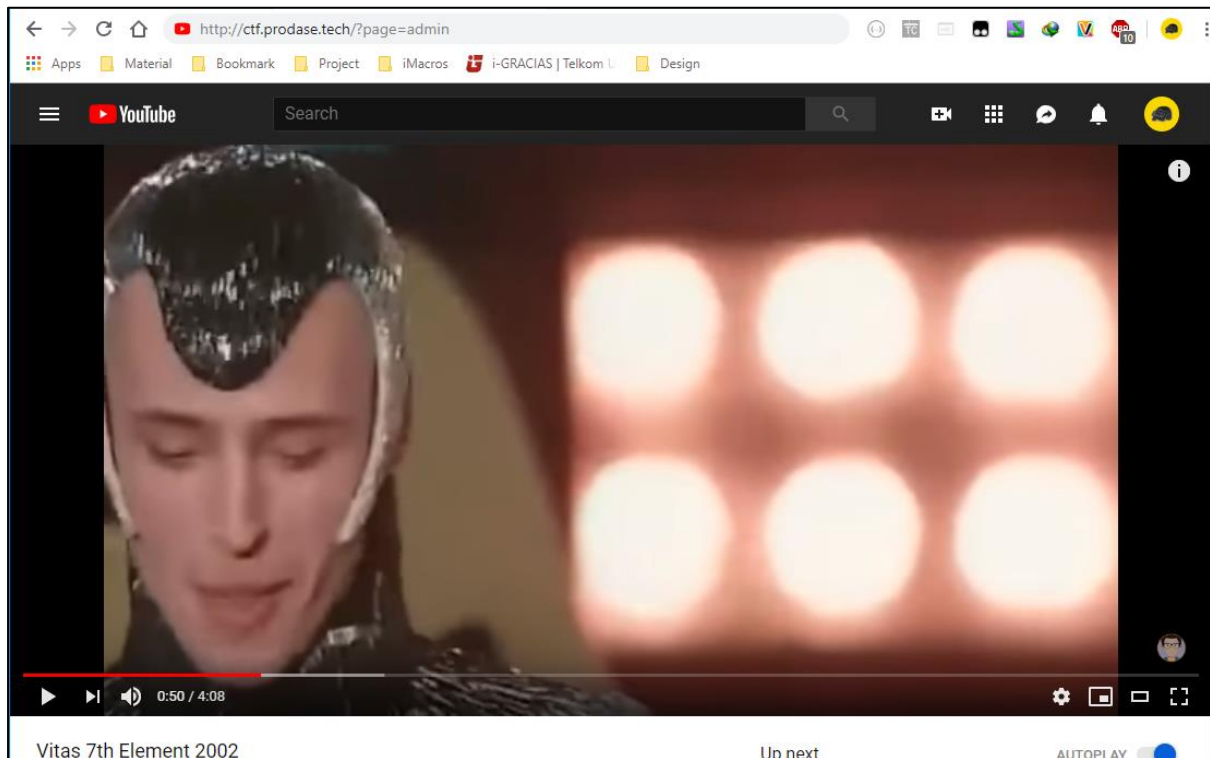
Problem

Praktikan diminta untuk dapat mengubah Hasil Pemilu Negara API (Bukan Tampilannya yang dirubah tapi Hasilnya)

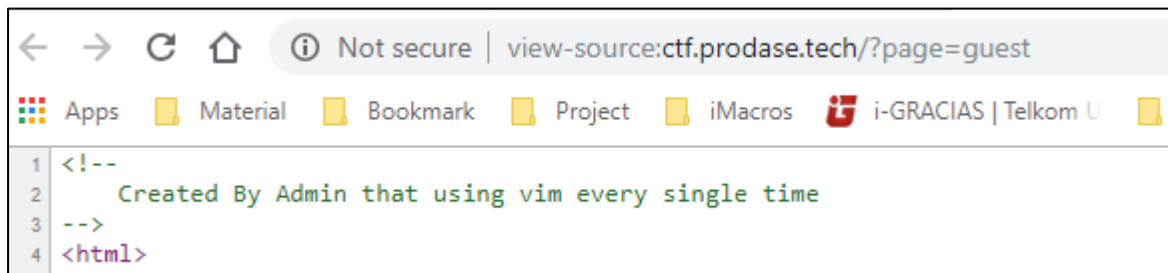


Pada URL <http://ctf.prodase.tech/?page=guest> terlihat bahwa pengunjung biasa hanya sebatas Guest sedangkan yang berhak melakukan perubahan adalah Admin, sehingga kita perlu masuk ke halaman admin.

Ketika kita ubah page menjadi admin <http://ctf.prodase.tech/?page=admin> atau nama lainya maka akan langsung di redirect menuju YouTube Vitas

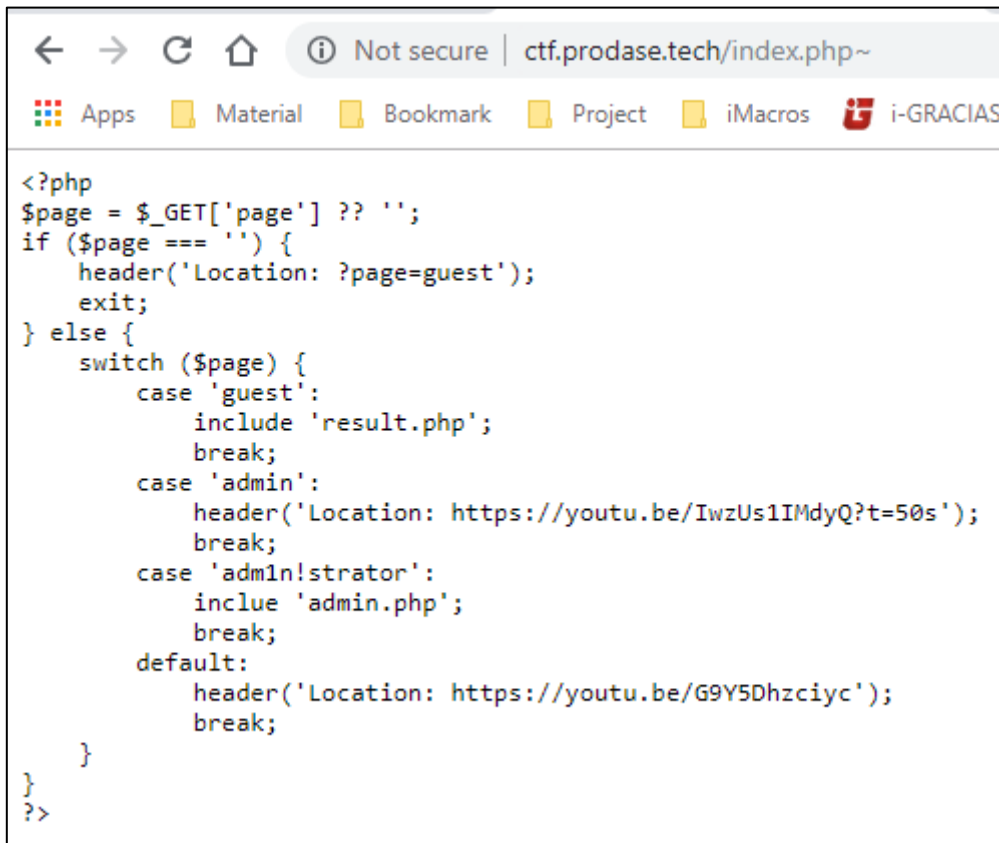


Lalu pada bagian Sourcecode terdapat komentar bahwa Admin selalu menggunakan Vim editor yang mana kita ketahui disini



<https://stackoverflow.com/questions/607435/why-does-vim-save-files-with-a-extension> Vim akan membuat salinan file dengan menambahkan Tilde (~) dibelakang extensi file (misal index.php menjadi index.php~)

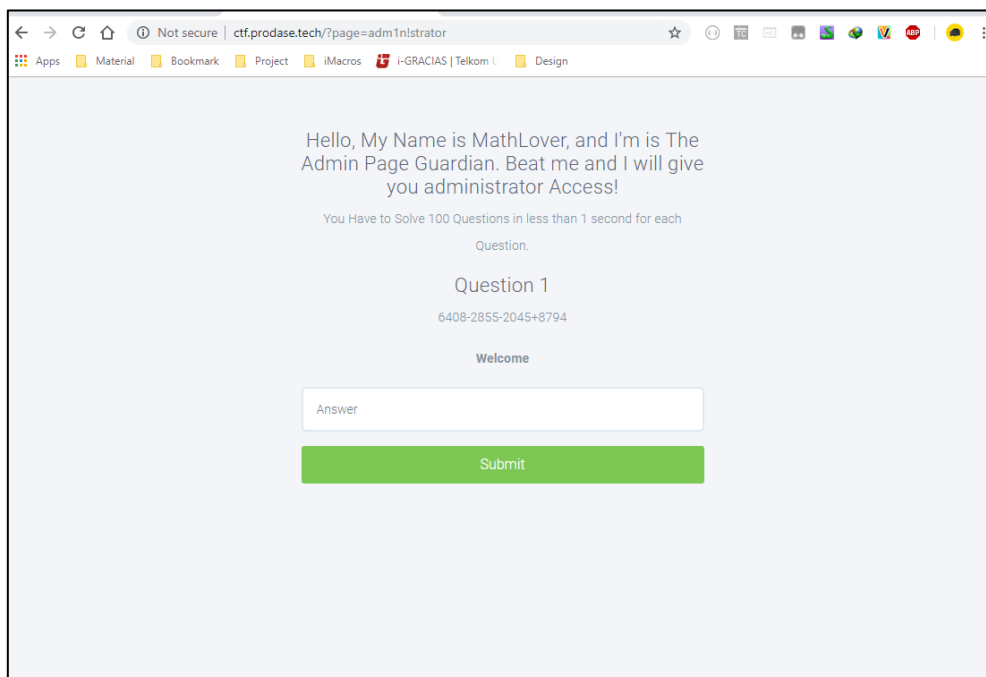
maka dari situ kita dapat melihat Backup file index.php



```
<?php
$page = $_GET['page'] ?? '';
if ($page === '') {
    header('Location: ?page=guest');
    exit;
} else {
    switch ($page) {
        case 'guest':
            include 'result.php';
            break;
        case 'admin':
            header('Location: https://youtu.be/IwzUs1IMdyQ?t=50s');
            break;
        case 'admin!strator':
            include 'admin.php';
            break;
        default:
            header('Location: https://youtu.be/G9Y5Dhzciyc');
            break;
    }
}
?>
```

Untuk mengakses halaman admin kita dapat menggunakan 'adm1n!strator' sebagai parameter page.

Dan Hasilnya kita bertemu dengan “Penjaga” Admin Page



Hello, My Name is MathLover, and I'm is The Admin Page Guardian. Beat me and I will give you administrator Access!

You Have to Solve 100 Questions in less than 1 second for each Question.

Question 1

6408-2855-2045+8794

Welcome

Answer

Submit

Untuk masuk kedalam admin page kita harus mengalikan penjaga terlebih dahulu. Penjaga memberikan 100 pertanyaan aritmatika yang harus kita selesaikan kurang dari 1 detik. Solusinya adalah menggunakan Automation menggunakan bantuan [Tampermonkey](#) Extension

Dengan Javascript sederhana / tambahan JQuery yang telah kita pelajari, maka kita dapat mengakses dan memodifikasi Element pada Robot Penjaga dengan DOM Html.

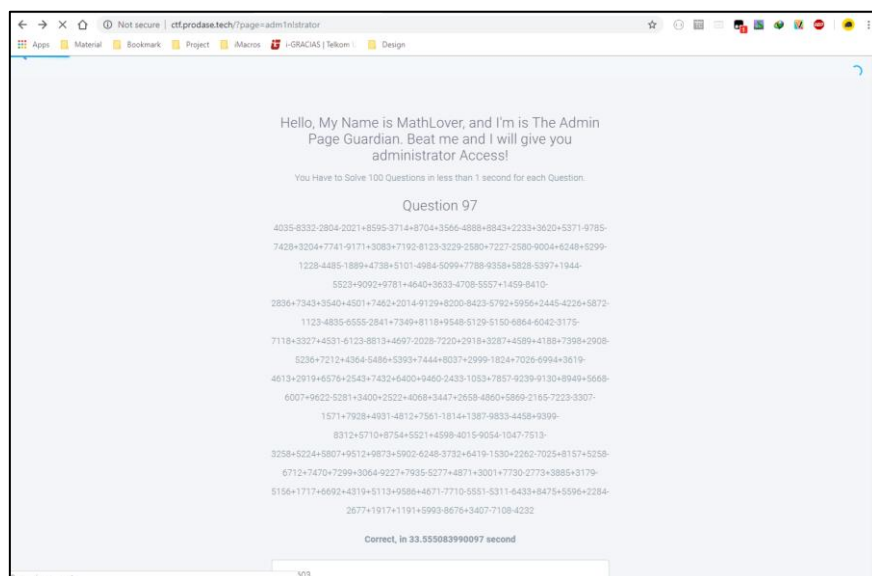
Pertama kita ambil soal aritmatika, lalu kita selesaikan dengan menggunakan fungsi eval() misalkan 1+2+3 dengan eval('1+2+3') maka hasilnya 6. Lalu hasil fungsi eval kita masukkan kedalam Field Input dan submit Formnya.

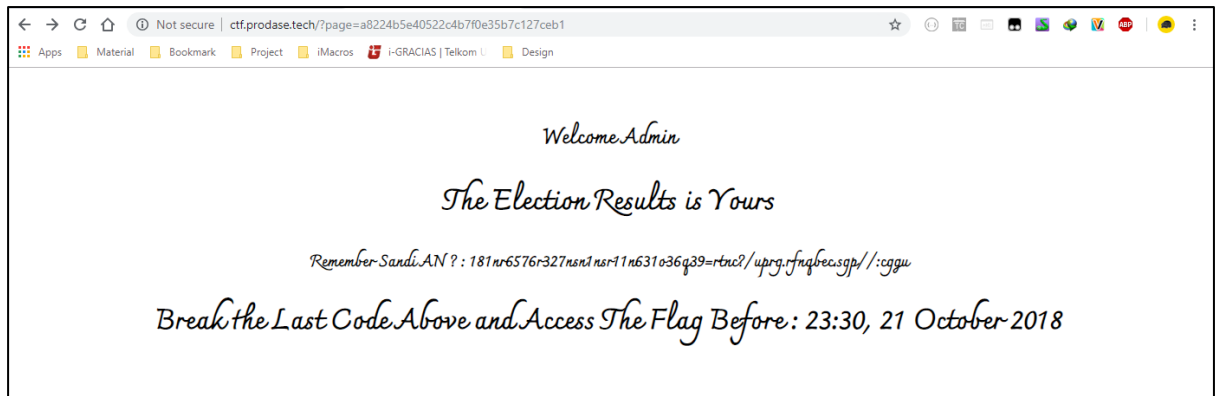
```
// ==UserScript==
// @name      MathLover
// @namespace  http://tampermonkey.net/
// @version    0.1
// @description try to take over the world!
// @author     You
// @match      http://ctf.prodase.tech/?page=admin!strator
// @grant      none
// @require    http://code.jquery.com/jquery-3.3.1.min.js
// ==/UserScript==

(function() {
    'use strict';

    $('input[name=ans]').val(eval($('#question').text()));
    'form').submit();
})();
```

Setelah 100 Pertanyaan kita jawab, kita akan dialihkan ke halaman sementara (yang menghilang setelah 30menit) yang berisi tentang clue selanjutnya





Remember Sandi AN ? :

181nr6576r327nsn1nsr11n631o36q39=rtnc?/uprg.rfnqbec.sgp//:cggu

Sandi AN adalah sandi yang mengubah $A \Rightarrow N$ (dan sebaliknya) $B \Rightarrow M$ dan seterusnya. Atau dalam istilah Cryptography sederhana sering disebut dengan ROT13.

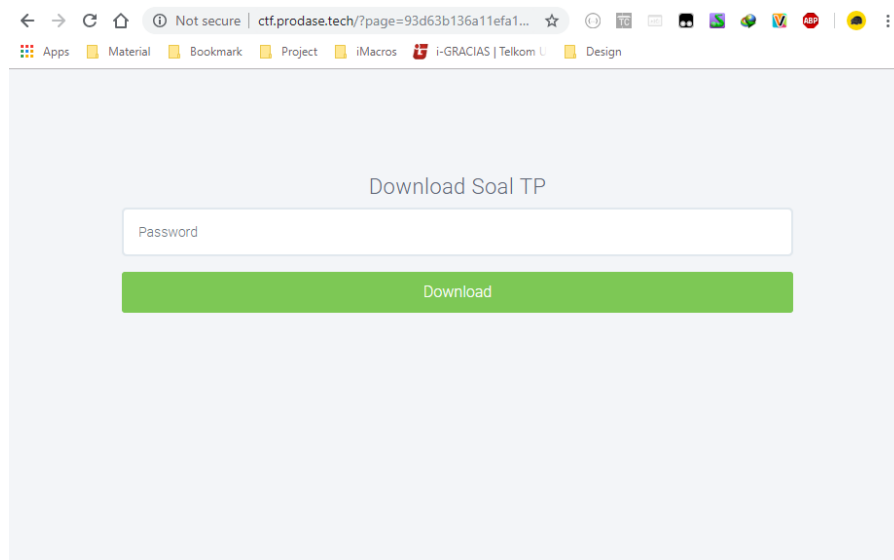
Maka hasilnya adalah:

"181ae6576e327afa1afe11a631b36d39=egap?/hcet.esadorp.ftc//:ptth"

Jika dibaca dari belakang akan terlihat lebih jelas :

<http://ctf.prodase.tech/?page=93d63b136a11efa1afa723e6756ea181>

Ketika dikunjungi isinya adalah Download Soal TP dengan Password



[illegible]

~ SEKIAN ~