



MAY 7, 2017 / CTF

BRAINHACK CTF WRITEUP 1.0

Welcome – Trivia 1pt

Welcome to BrainHack CTF! Format flag disini bervariasi karena sebagian challenges adalah soal-soal dari event ctf yang telah lalu. Format flag soal yang berasal dari kami adalah `noob{this_is_flag}`. Silahkan coba disini

Nothing special, tinggal masukan contoh flag.

Flag : `noob{this_is_flag}`

Mah Roboto – Trivia 25pts

Please noobies, robots is not that secure

Jadi gini, noobs.

Hint yang diberikan di soal adalah kata **robots**. Apa maksudnya robots?

Dalam web developing, kita bisa kasih instruksi ke robot saat akan mengunjungi halaman kita. Yaitu dengan cara tambahkan file **`robots.txt`** dalam direktori root web kita. Setiap robot yang akan mengunjungi halaman kita akan terlebih dahulu membaca file `robots.txt`.

Sesuai hint yang diberikan di deskripsi soal, langsung saja kita akses [robots.txt](#)

```
User-agent: *
```

```
Disallow: /dontopenthis-yourpcwillexplode
```

Line pertama mempunyai arti semua robot boleh mengunjungi web ini. Namun line kedua menunjukkan pengecualian halaman apa yang tidak boleh dikunjungi robot. Karena dalam hal ini kita bukan robot, kita bisa dengan mudah mengaksesnya

```
Noobies don't deserve the flags
```

```
The one that they deserve is explosion
```

Jika kamu melihat dengan seksama, ada flag yang dicomment dalam laman tersebut

FLAG : nooblrobots_tXt_1s_the_worst_secuurity!

Seperti yang kita lihat, robots.txt hanya akan melindungi dari robot. Namun selain itu, file ini juga dapat dengan mudah ditembus oleh berbagai web crawler dan memiliki accessibility public. Juga, menuliskan direktori rahasia kamu di robots.txt adalah hal yang nggak seharusnya dilakukan. Penulisan direktori rahasia di robots.txt bisa dianalogikan seperti : Kamu punya emas yang kamu simpan di lemari. Lalu, seseorang datang ke rumahmu untuk mencari dan mencoba mencurinya. Habis itu kamu bilang ke orang tersebut, "Di kamarku ada lemari. Jangan coba-coba buka lemari itu, disana aku nyimpen emas". So gimana noobs? robots.txt is really the worst security.

Tukang Pos – Web 100pts

Hack me if you can, NOOB Visit This : <http://10.151.32.81/hackthebrain/easy.php>

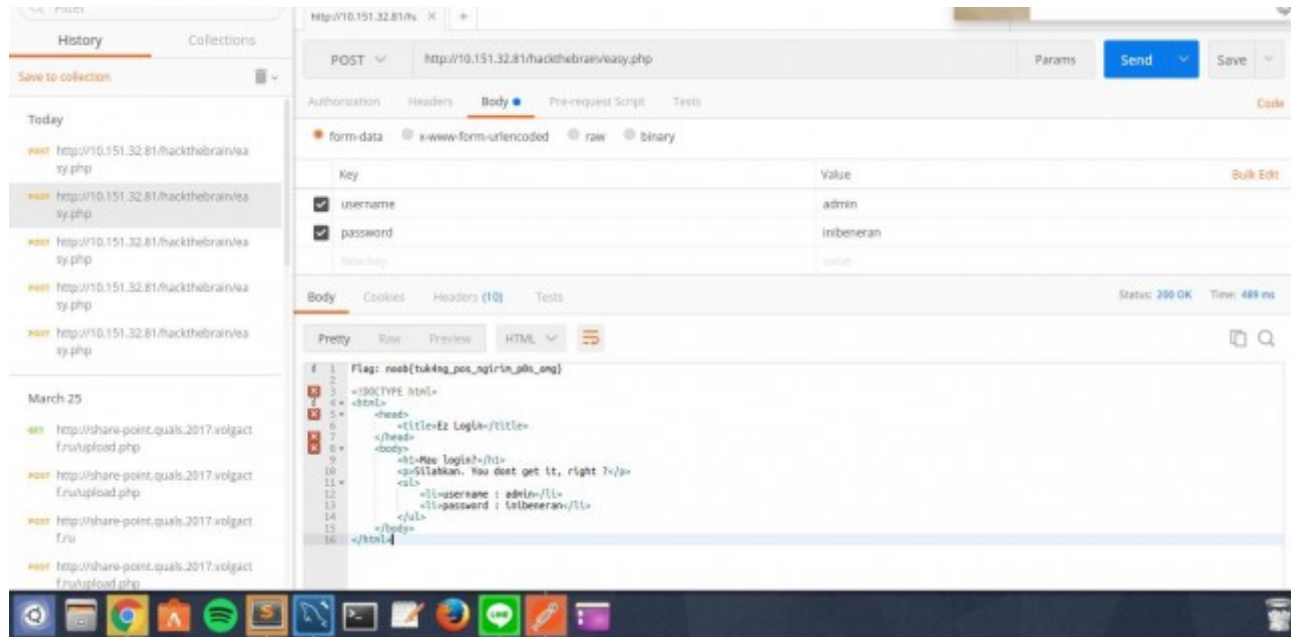
Challenge ini adalah tentang http request method. Seperti yang kita tau, http request method yang sering dipake di web itu ada **GET** sama **POST**. GET biasanya dipakai buat ngerequest data-data yang ga rahasia. Contoh dari GET adalah saat kita ngunjungi halaman web. URL itu sebenarnya dikirim ke server dengan menggunakan http request dengan method GET. Untuk ngepassing parameter, metode ini pake syntax **?lname=[value]**. Contohnya lihat aja deh di URL halaman ini, hehe. Karena requestnya telanjang gitu, gak aman buat ngirim data yang aman pake metode ini (misal username dan password). Di history juga kelihatan kan jadinya kalau pakai method ini.

Oke beranjak ke metode kedua yaitu POST. Inilah sebenarnya yang diinginkan di challenge ini.

Mau login?

Silahkan. You **dont** get it, right ?

Tapi tantangannya, kita nggak dikasih form buat ngirim request berupa Username dan Password itu ke server. Oleh karena itu kita butuh tools buat ngirim request ini. Kalo aku pakai Postman.



FLAG : noob{tuk4ng_pos_ngirim_pos_omg}

Tabur Coklat – Web 50pts

Web ini seperti biskuit bertabur bulatan coklat. Visit [This](#)

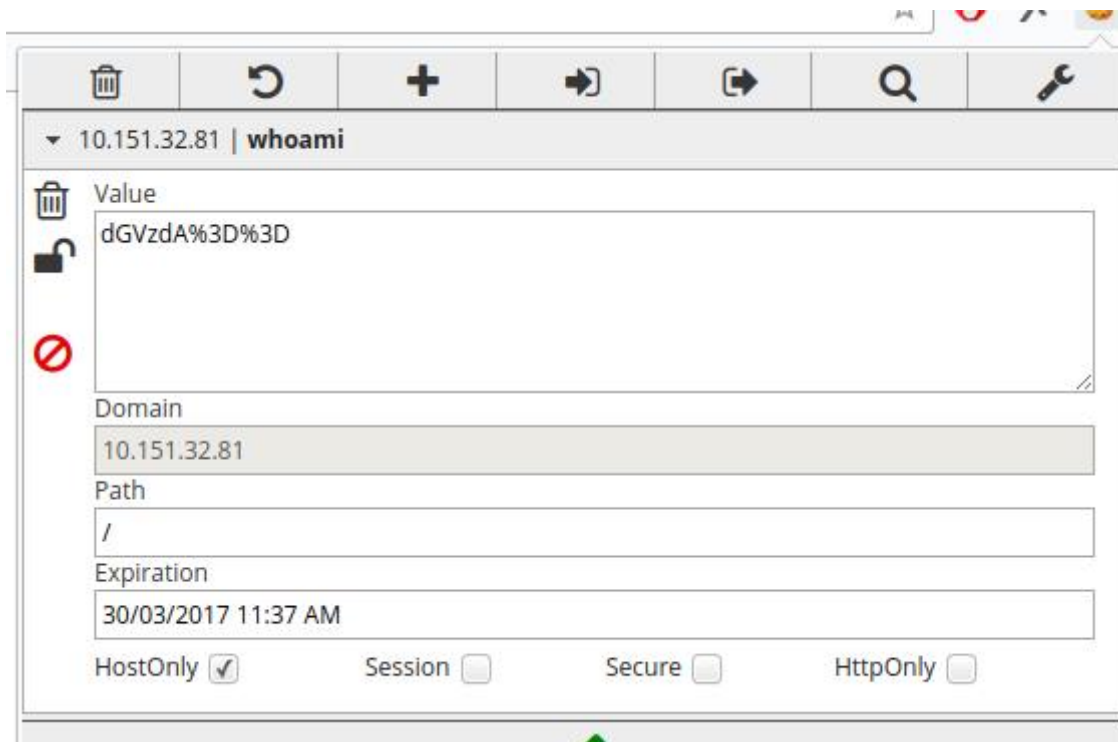
Kita diberikan challenge yang berupa form login. Pertama kita lihat dulu behaviour nya. Coba submit username : admin password : admin

Tryin hard to be admin, huh?

Ternyata di filter. Coba lagi pake username : test password : test

Hey, test

Lalu sesuai hint yang diberikan soal, biskuit bertabur bulatan coklat yang dimaksud adalah cookie. Cookie berguna untuk menyimpan sementara data yang dipunyai user untuk selanjutnya dimanfaatkan sama si web ini. Yok langsung aja kita cek cookie apa sih yang disimpan setelah login. Aku rekomendasikan pake EditThisCookie.

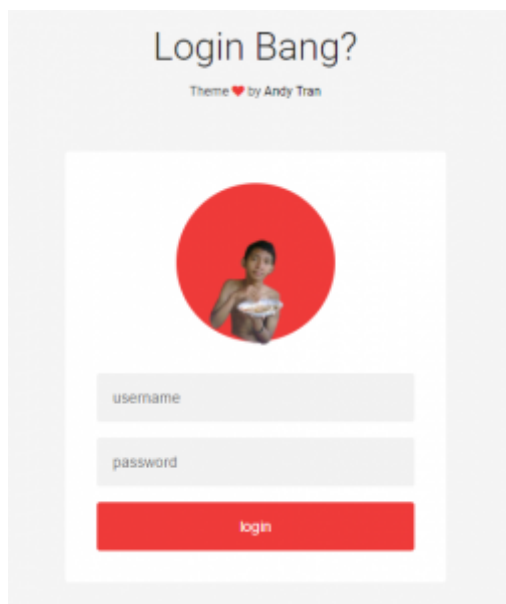


Ternyata ada cookie **whoami** yang bernilai seperti di gambar itu. Mudah saja, nilai itu telah di encrypt dengan base64 yang dimana hasilnya setelah di decrypt adalah username yang kita masukin itu sendiri. Kalo gitu yok kita encrypt ke base64 **admin** = **YWRTaW4=** terus ganti cookie nya.

FLAG : Flag: noobldonnt_encrypt_your_cook3ie_lik3_this!

Mas Alek 1.0 – Web 50pts

Mas alek memang idolaku. Dia adalah rapper Indonesia yang berjuang dari nol. Hingga akhirnya sekarang dia membuat login page yang hanya dia yang bisa login. Jadilah yonglek untuk bisa login ke sini



Melihat source code nya, no clue. Page ini hanya terdiri dari login form biasa yang akan mengirimkan request post ke dirinya sendiri. Satu-satunya jalan adalah mencoba melakukan SQL Injection. SQLI adalah teknik dimana seorang user memanfaatkan kelemahan suatu sistem untuk mendapatkan akses ke database. Ada berbagai macam tipe soal SQLI dalam CTF. Yang paling dasar adalah kita berusaha memanipulasi query pada server untuk menghasilkan nilai **TRUE**.

Asumsikan form login ini menggunakan query standar dari otentikasi login : ***SELECT * FROM user WHERE username='\$username' AND password='\$password'***. *user* adalah nama tabel pada database yang digunakan mas alek, dan memiliki setidaknya 2 kolom, yaitu *username* dan *password*. sedangkan *\$username* adalah string username yang kita kirimkan dari form login, begitupun dengan *\$password*. Query ini kemudian akan dievaluasi oleh sistem, dan jika terdapat username dan password pada tabel user yang cocok, maka sistem memberikan respon bahwa otentikasi tersebut berhasil. Maka ketika kita mengirimkan form login dengan data sebagai berikut :

Username : 'OR 1=1--

Password : <apa saja>

Query otentikasi tersebut akan dibaca oleh sistem seperti : ***SELECT * FROM user WHERE username="OR 1=1- ' AND password='\$password'***

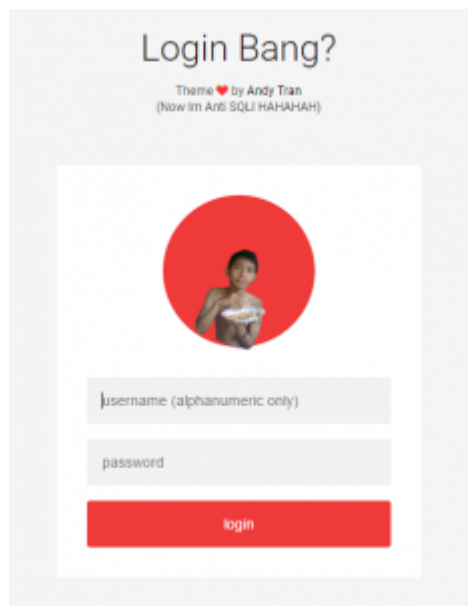
Mari kita bahas satu per satu. Tujuan diberikannya **tanda petik (')** adalah untuk sebagai tanda petik penutup, **OR 1=1** akan menghasilkan nilai **TRUE**, dan seperti yang kita tahu, – **<spasi>** adalah syntax dalam SQL yang akan menganggap semua string setelahnya

adalah komentar. Maka hasilnya, query tersebut menghasilkan nilai true, apapun yang ada dalam database.

FLAG : nooblyonglek_doing_sqlit

Mas Alek 2.0 – Web 100pts

Setelah ketahuan webnya dapat ditembus, mas alek kembali berinovasi. Kali ini di a yakin kamu gak akan bisa nyamar jadi yonglek buat login ke sini



Melihat judul soalnya, sepertinya ini challenge yang sama dengan yang sebelumnya, hanya mungkin lebih sulit (padahal gak juga sih). Yoklah langsung cus lihat sourcecodenya

```
<form class="login-form" action method="POST">
  <input type="text" name="username" placeholder="username
  (alphanumeric only)" pattern="[a-zA-Z0-9]+">
  <input type="password" name="password" placeholder="password"
  pattern="[a-zA-Z0-9]+">
  <button>login</button>
</form>
```

Ternyata kali ini inputnya di filter hanya bisa kombinasi antara huruf dan angka. Tapi you know what? This is a noob defense! HTML bersifat client-side. Artinya filter ini berjalan di browser kita, dan kita bisa dengan leluasa mengaturnya. Dengan tool hacking ternama dan tercanggih (baca: Inspect Element), kita hapus elemen pattern dari kode tersebut, lalu masukkan string yang sama dengan challenge Mas Alek 1.0

FLAG : noob!LOL_yonglek_with_client_side-defence!

Manual – Programming 50pts

Tolong bantu saya untuk menghitung ada berapa hari jumat yang ada di attachment.
Mau dihitung manual? Semangat :)

Flag : noob{jumlah_hari_jumat}

tgif

Challenge ini saya dapatkan dari ABCTF (ini keren banget contestnya gan). Jadi disini kita disediakan file yang terdiri dari 1337 baris, dimana setiap barisnya adalah suatu tanggal. Jadi yang bisa kita lakukan disini hanyalah membuka kalender online, lalu menghitung ada berapa hari jumat pada baris-baris tersebut. Iya, semuanya manual.

Wkwkwk bercanda kok. Kita bisa memanfaatkan bash programming. Berikut kodenya :

```
while read line;
do date -d"${line}" +%a;
done < tgif
```

Kita simpan sebagai file **hari.sh**, dan jalankan

```
bash hari.sh | grep Jum
```

FLAG : noob{199}

WRITEUP LAINNYA MENYUSUL (capek juga ternyata)

NO OLDER POSTS

RETURN TO BLOG

NEXT POST

ENC BRAINHACK WRITEUP

CATEGORIES

CTF

3 COMMENTS**HAIMAX**

May 23, 2017

Reply

Buat yg problem "Manual" seharusnya jawabannya 199.

**CLAY** (author)

June 9, 2017

Reply

Wah iya benar. Terimakasih koreksinya, haimax 😊

**WWW.LINUX.ORG**

June 17, 2017

Reply

Freelancing may also lead to an enormous "plus" concerning your income. As a substitute of getting to accept the precise salary that is offered by the one regulation agency that you simply work, you will have quite a lot of leeway in setting your own pay rates. This issue may end up in significantly more money for you.

Leave a Reply

Your email address will not be published. Required fields are marked *

Enter Your Comment...

Your Name*

Your Email*

Your URL

Post Comment

CLAYDAY BLOG

ARCHIVES

JUNE 2017

MAY 2017

LIFE

