

13. JavaScript Attack

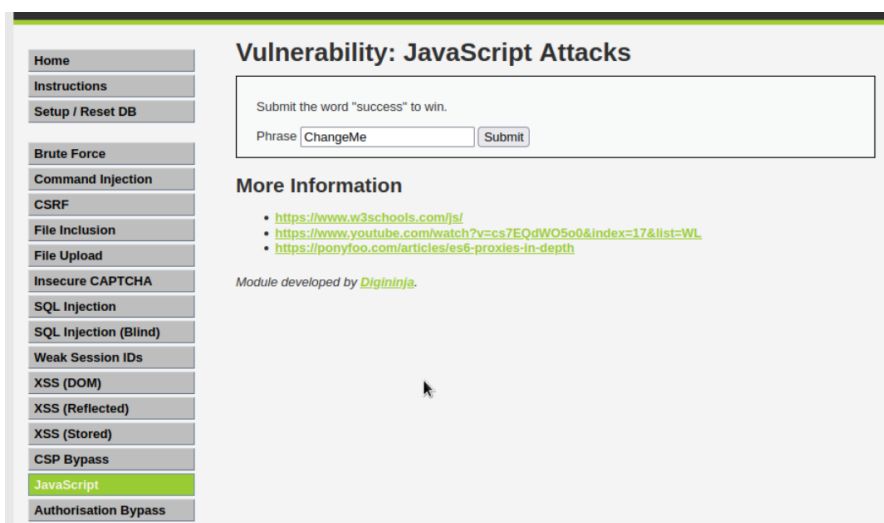
Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafidh Akbar Sya'bani (akbar@dinustek.com)

Information Gathering

Pada tampilan awal DVWA klik bagian JavaScript



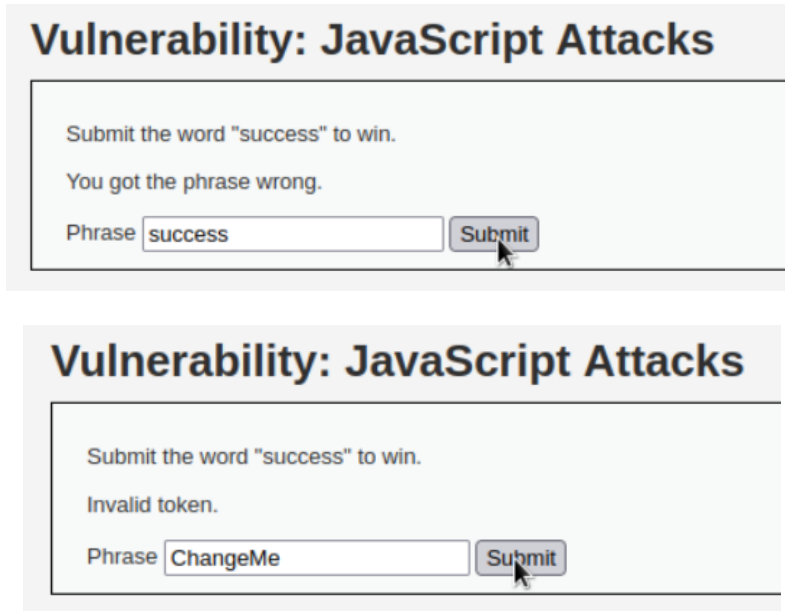
Tujuan disini adalah untuk menginputkan string yang dianggap “succes”

Menggunakan string default, coba untuk klik Submit



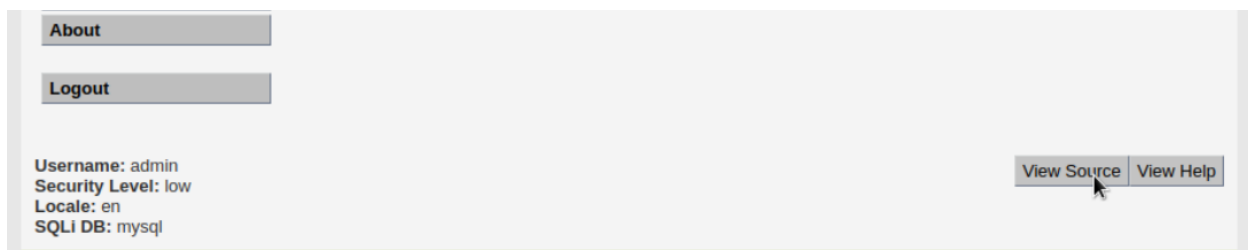
Muncul bahwa string tersebut salah, muncul status “You got the phrase wrong”

Coba untuk gunakan kata lain seperti “success”



Kata tersebut juga salah, namun status berganti menjadi "Invalid token"

Coba scroll kebawah dan klik "View Source"



Disana akan ditampilkan kode dari program JavaScript Attack, di bagian bawah akan ada fungsi seperti berikut

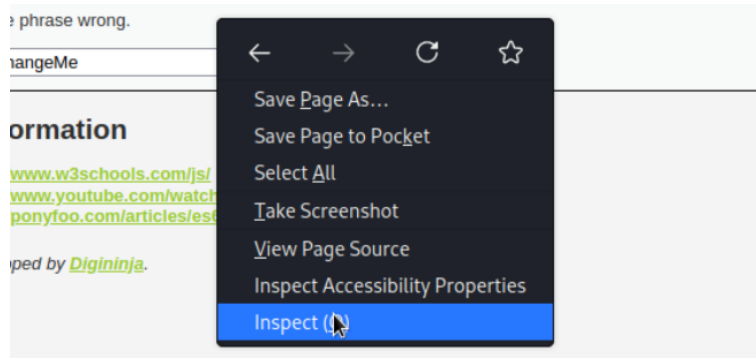
```
function rot13(inp) {
    return inp.replace(/[a-zA-Z]/g,function(c){return String.fromCharCode((c<="Z"?90:122)>=(c=c.charCodeAt(0)+13)?c:c-26)});
}

function generate_token() {
    var phrase = document.getElementById("phrase").value;
    document.getElementById("token").value = md5(rot13(phrase));
}

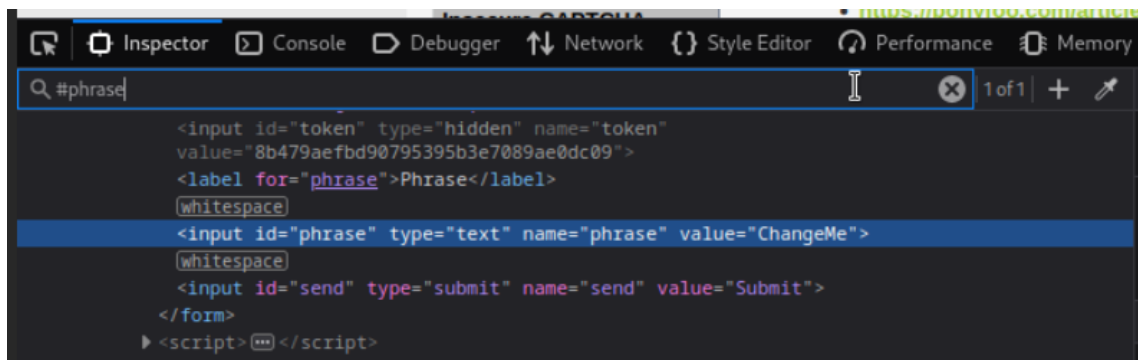
generate_token();
</script>
```

Terdapat 2 fungsi untuk melakukan encode string, fungsi pertama akan mengubah string dalam bentuk ROT13 lalu di fungsi kedua akan diubah menjadi MD5. String yang akan diubah diambil dari element dengan ID "phrase", coba lihat dimanakah element dengan ID phrase tersebut menggunakan Inspect element bawaan browser

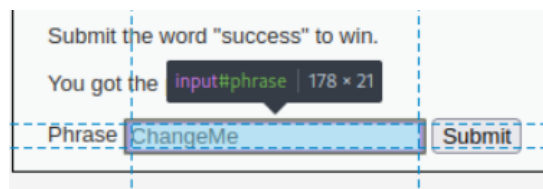
Pada browser Firefox, klik kanan dimana saja lalu pilih "Inspect"



Pada kolom pencarian, ketikkan “#phrase” lalu enter

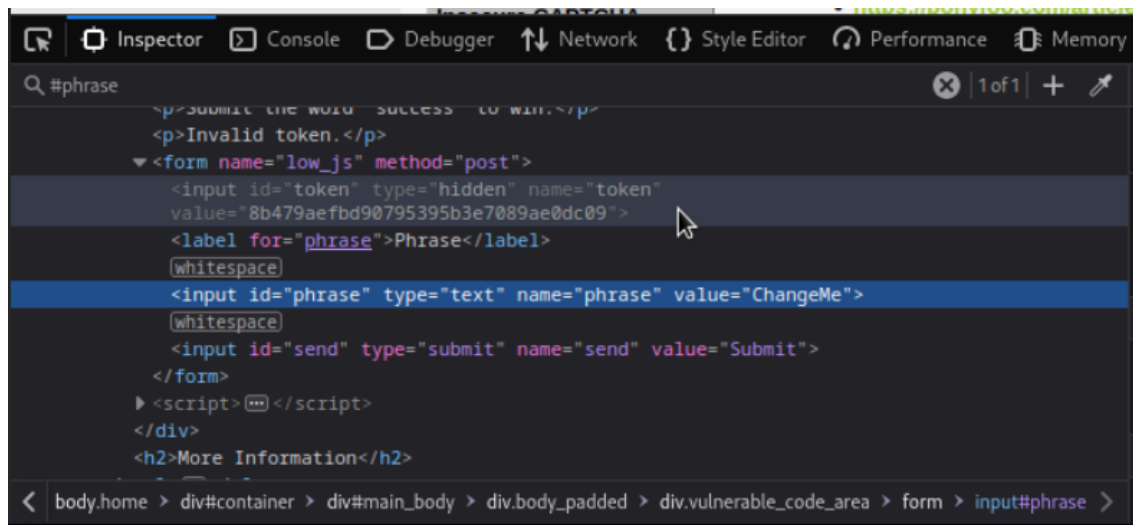


Maka akan tampak bahwa ID “phrase” digunakan pada kolom string yang diinputkan pada field Phrase



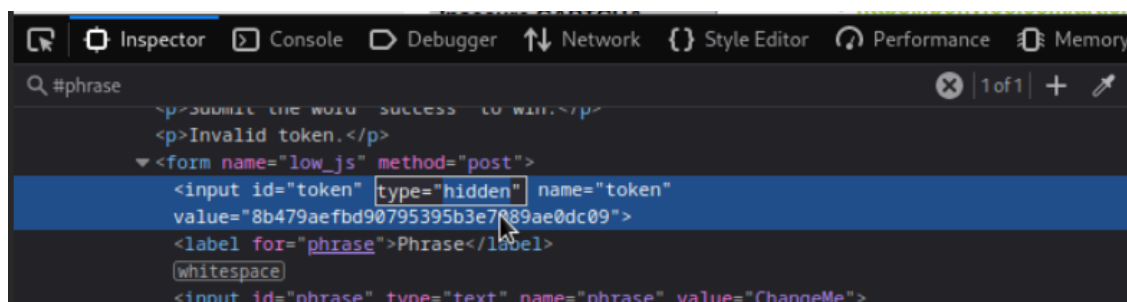
Ini berarti setiap kali string yang dimasukkan pada field Phrase akan diconvert menjadi ROT13 lalu diconvert lagi ke MD5, tetapi kenapa saat string “success” dimasukkan tetap menghasilkan output yang salah dengan status “Invalid token”?

Perhatikan kembali pada elemen input, disana terdapat attribute `value="ChangeMe"`, yang mana ini membuat string “ChangeMe” menjadi default value, jadi setiap kali halaman dibuka, yang akan diconvert pertamakali adalah string tersebut. Terlebih lagi jika diperhatikan kembali pada inspect element, terdapat element input lagi yang tersembunyi diatas element input phrase.

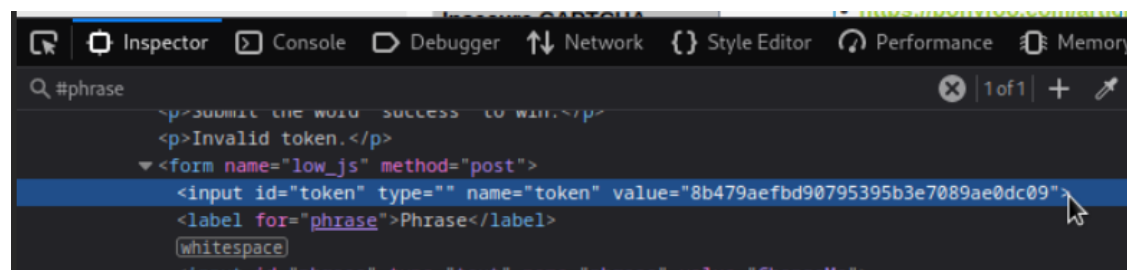


Perhatikan pada element yang diarahkan oleh cursor, element tersebut memiliki attribute `type="hidden"`, ini menyebabkan element tersebut tidak ditampilkan. Coba untuk tampilkan input tersebut dengan menghilangkan kata "hidden" pada attribute type.

Klik 2 kali pada attribute `type="hidden"`



Hapus valuenya lalu enter



Maka akan muncul input token di sebelah input phrase

Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Invalid token.

8b479aefbd90795395b3e708
Phrase
ChangeMe
Submit

Value dari token tersebut adalah sebagai berikut

```
8b479aefbd90795395b3e7089ae0dc09
```

Dari fungsi pada source code sebelumnya, phrase akan diconvert ke ROT13 lalu dienkrpsi ke MD5, maka kemungkinan token ini jika didencrypt akan menjadi phrase "ChangeMe". Buktikan dengan mengubah phrase "ChangeMe" menjadi ROT13 terlebih dahulu, bisa gunakan website encryptor online, disini akan menggunakan web <https://www.dcode.fr/rot-13-cipher>

Pada ROT13 Encoder, ketikkan phrase "ChangeMe" lalu klik "ENCRYPT WITH ROT-13"

ROT13 ENCODER

★ ROT13 PLAIN TEXT ?
↻

ChangeMe

★ APPLY ROT-5 ON NUMBERS (ROT13.5) ☐

▶ ENCRYPT WITH ROT-13

See also: [ROT Cipher](#) – [Caesar Cipher](#) – [ROT-47 Cipher](#)

Hasilnya akan muncul pada kiri atas halaman

Results

CHANGE ME

📄
📋
📄
⬇️
📌
✖️

PunatrZr

ROT-13 Cipher - [dCode](#)

Tag(s) : Substitution Cipher

ROT13 dari "ChangeMe" adalah "PunatrZr", selanjutnya encrypt string ini menggunakan MD5

Masih menggunakan web yang sama, namun pada jenis encoder yang berbeda <https://www.dcode.fr/md5-hash>

Ketikkan string ROT13 tadi lalu klik "ENCRYPT"

MD5 ENCODER

☒ FROM A CHARACTER STRING

★ MD5 PLAIN TEXT OR PASSWORD (?)

PunatrZr

☐ FROM A FILE

★ FILE NO FILE CHOSEN

Perhatikan pada kiri atas halaman, jika muncul captcha klik saja checklistnya

Results

☐ I'm not a robot

reCAPTCHA
Privacy - Terms

Pada tempat yang sama akan muncul hasil encrypt dari string ROT13 tadi menggunakan MD5

Results

MD5 (PunatrZr)

8b479aefbd90795395b3e7089ae0dc09

MD5 - [dCode](#)

Tag(s) : Hashing Function, Modern Cryptography

Perhatikan bahwa hasil encrypt tersebut sama seperti yang ada pada value token sebelumnya

8b479aefbd90795395b3e7089ae0dc09

Pada halaman JavaScript Attack DVWA, saat tombol Submit diklik, sistem akan melakukan pengecekan pada phrase dan token. Karena default value pada phrase dari halaman tersebut adalah "ChangeMe" maka token akan selalu menjadi "8b479aefbd90795395b3e7089ae0dc09".

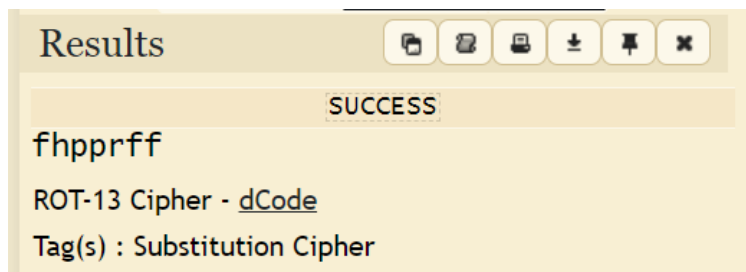
Saat phrase default "ChangeMe" disubmit, sistem akan memeriksa bahwa phrase salah dan token juga salah, sehingga memunculkan status "You got the phrase wrong". kemudian saat phrase default diganti dengan "success", sistem akan memeriksa bahwa phrase sudah benar, namun tidak dengan token, karena token yang digunakan masih menggunakan token default dari phrase "ChangeMe", sehingga memunculkan error status "Invalid token".

Terdapat 2 cara untuk mengatasi ini adalah dengan memunculkan input token melalui inspect element lalu mengganti value tokennya seperti cara sebelumnya, atau menggunakan tool lain yang salah satunya adalah Burp Suite. Sebelum melakukan serangan ini, ketahui dulu seperti apa string "success" jika diubah ke ROT13 dan diencrypt ke MD5

Buka web <https://www.dcode.fr/rot-13-cipher> lalu pada bagian ROT13 Decoder masukkan phrase “success” lalu klik “DECRYPT ROT13”



Hasil akan muncul pada bagian kiri atas



Kemudian decrypt string tersebut menggunakan MD5 melalui web <https://www.dcode.fr/md5-hash>
Masukkan string “fhpprff” ke MD5 Encoder lalu klik “ENCRYPT”



Hasil akan muncul pada kiri atas

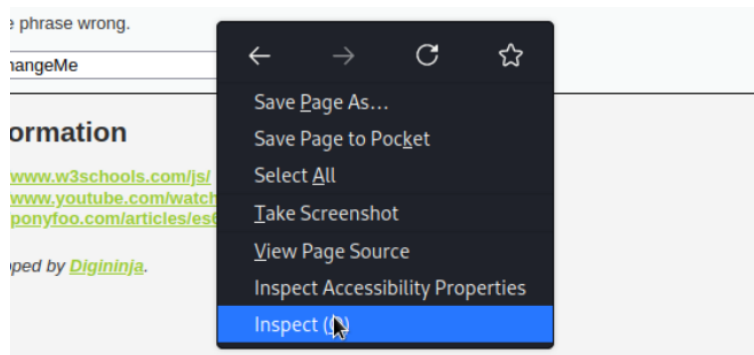


Maka dapat diketahui bahwa phrase "success" yang diubah menjadi ROT13 lalu diencrypt menggunakan MD5 adalah seperti berikut

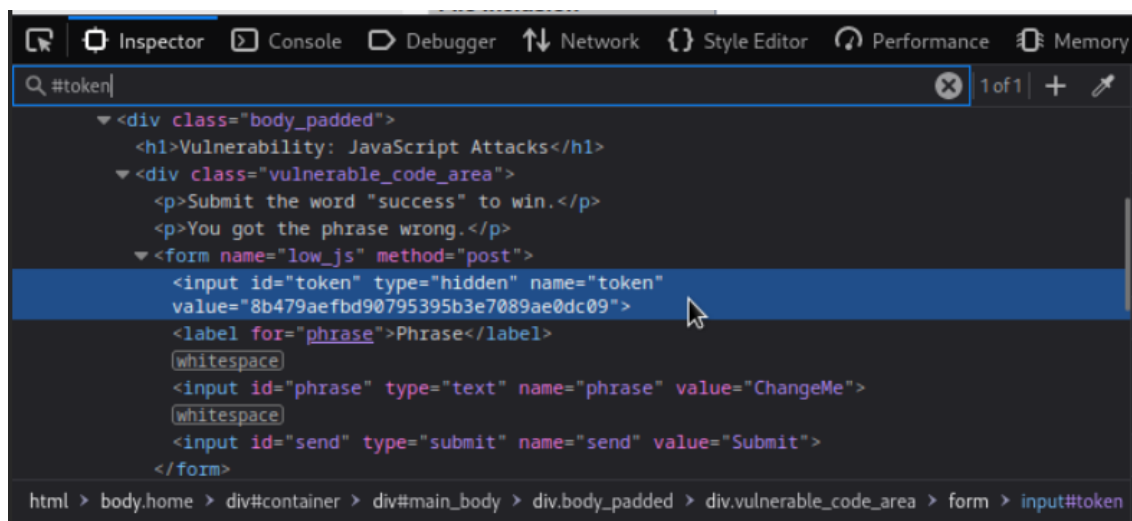
```
38581812b435834ebf84ebcc2c6424d6
```

JavaScript Attack - Inspect Element

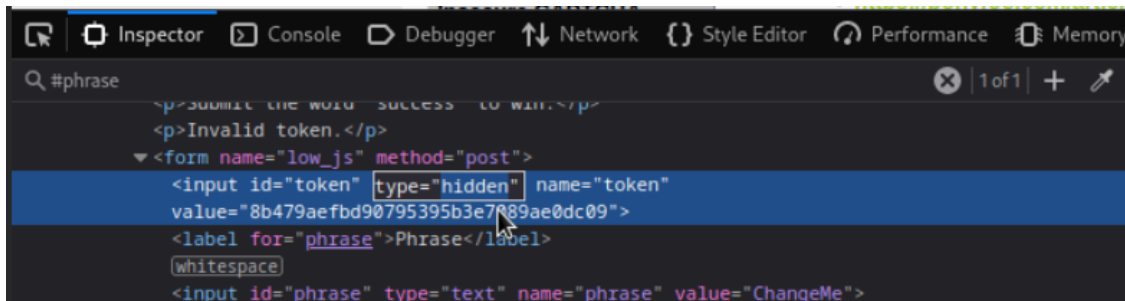
Pada browser Firefox, klik kanan dimana saja lalu pilih "Inspect"



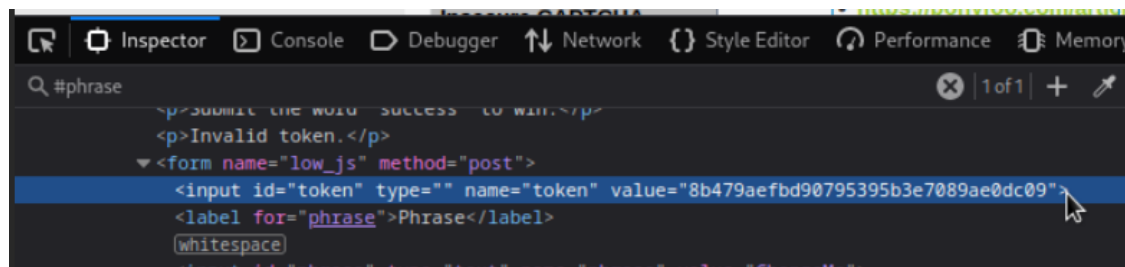
Pada kolom pencarian, ketikkan "#token" lalu enter



Klik 2 kali pada attribute `type="hidden"`



Hapus valuenya lalu enter



Maka akan muncul input token di sebelah input phrase

Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Invalid token.

8b479aefbd90795395b3e708 Phrase ChangeMe Submit

Pada tahap ini token bisa diganti, hapus token sebelumnya lalu masukkan token dari phrase "success", yaitu "38581812b435834ebf84ebcc2c6424d6" kemudian ganti phrase "ChangeMe" menjadi "success"

Vulnerability: JavaScript Attacks

Submit the word "success" to win.

You got the phrase wrong.

'b435834ebf84ebcc2c6424d6 Phrase success Submit

Klik submit, jika muncul teks "Well done!" berarti phrase dan token sudah benar

Vulnerability: JavaScript Attacks

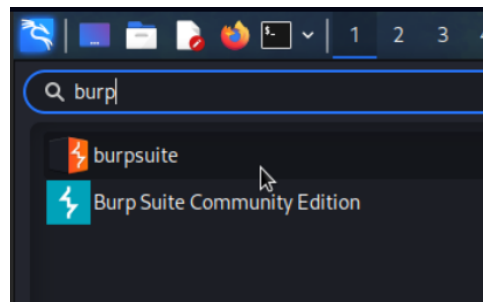
Submit the word "success" to win.

Well done!

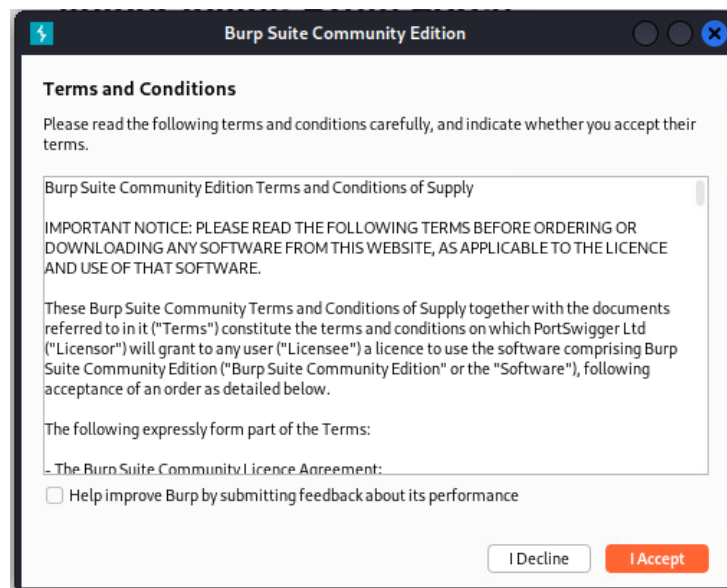
Phrase

🦴 JavaScript Attack - Burp Suite

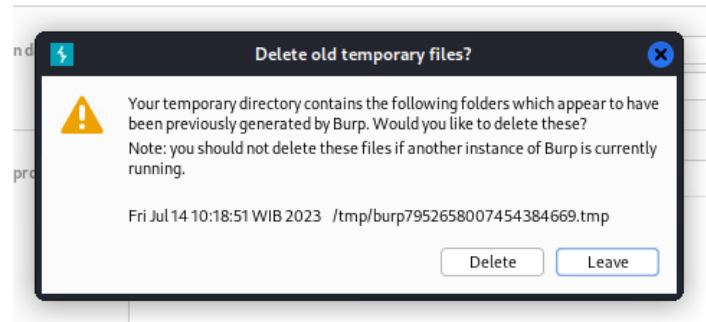
Buka Burp Suite



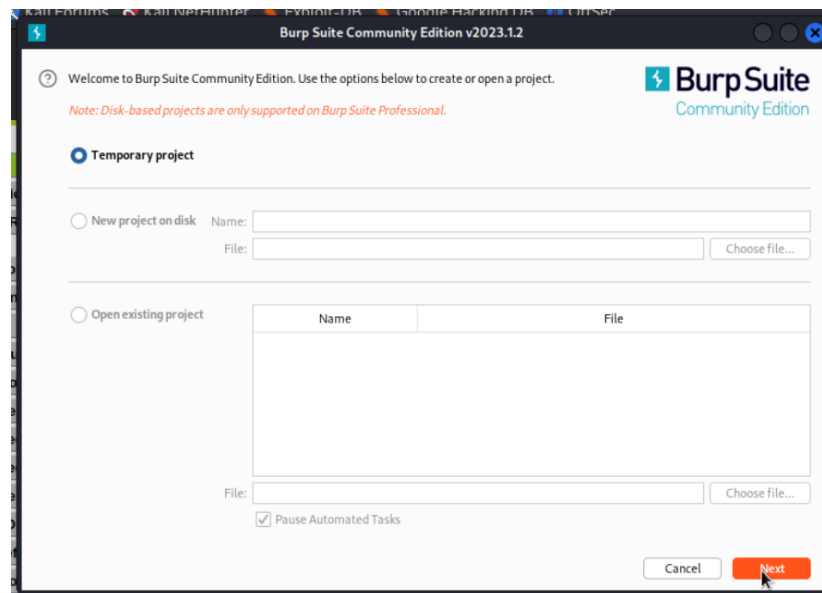
Klik I Accept



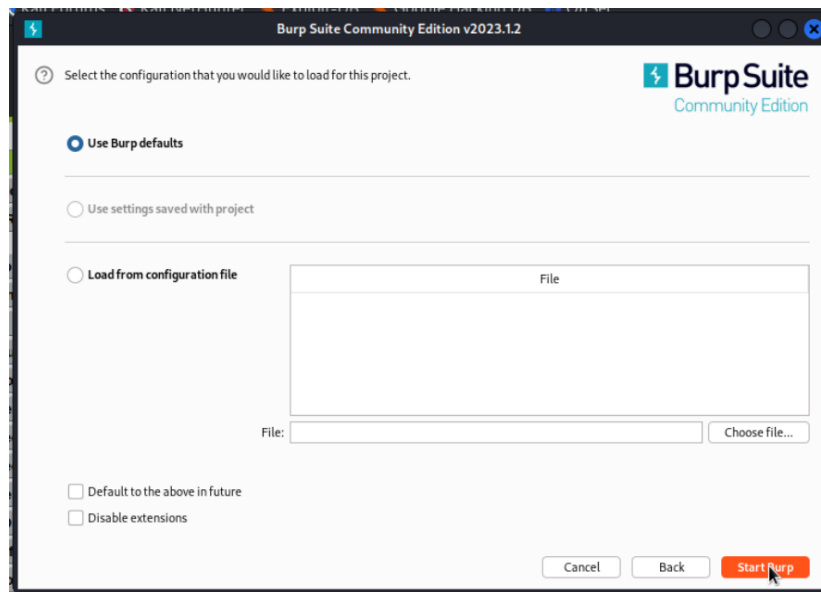
Klik Leave



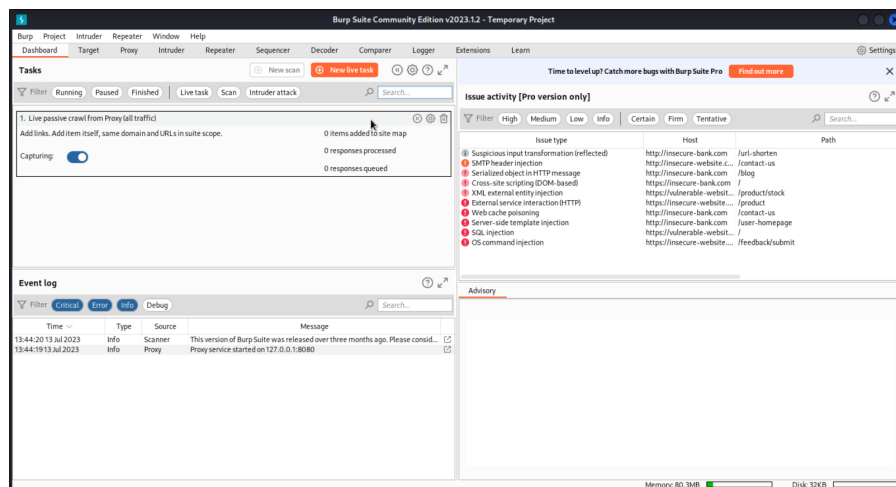
Klik next



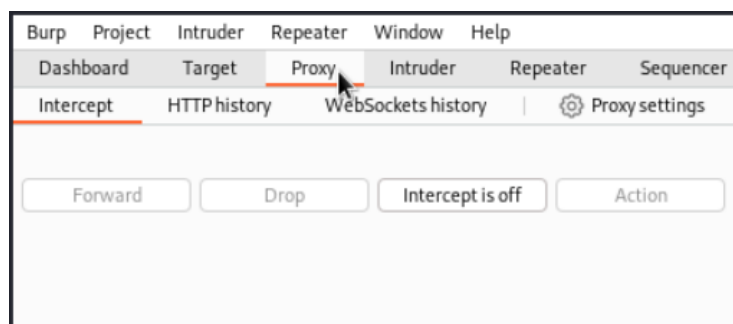
Klik Start Burp



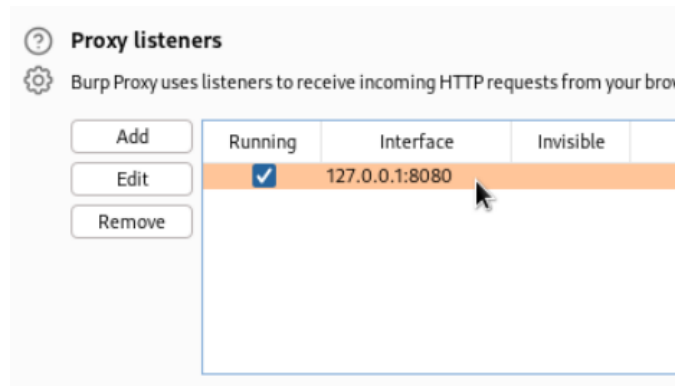
Tampilan Burp Suite



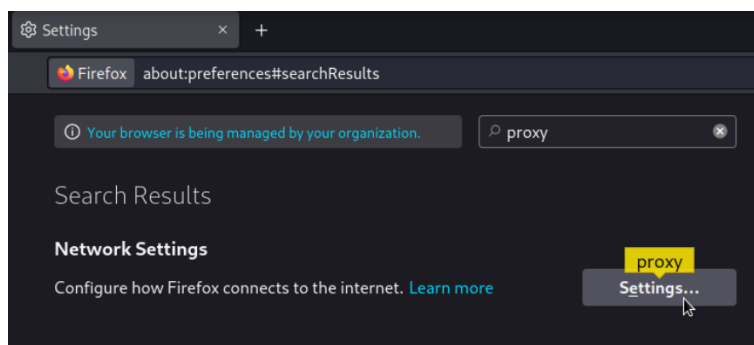
Klik tab Proxy



Klik Proxy settings dan pastikan pada Proxy listeners terdapat alamat IP dan port yang running
IP dan port ini yang nanti akan dijadikan proxy oleh browser



Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy



Didalamnya ganti "Use system proxy settings" menjadi "Manual proxy configuration"

Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK

Configure Proxy Access to the Internet

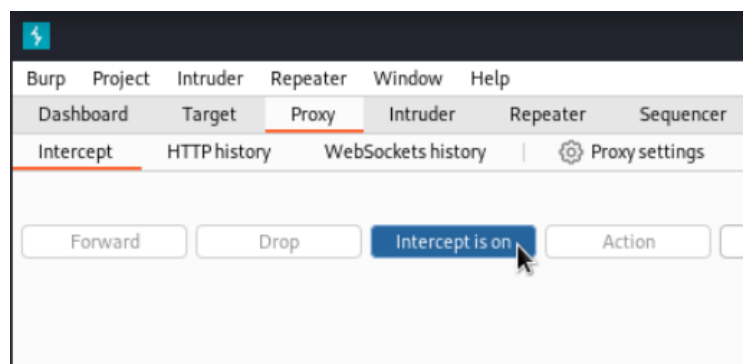
☐ No proxy
☐ Auto-detect proxy settings for this network
☐ Use system proxy settings
☒ Manual proxy configuration

HTTP Proxy Port
☒ Also use this proxy for HTTPS

HTTPS Proxy Port
 SOCKS Host Port
☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Buka Burp Suite, aktifkan intercept dengan klik tombol "Intercept is off"



Kembali ke halaman JavaScript Attack, ketikkan "success" pada phrase lalu klik submit

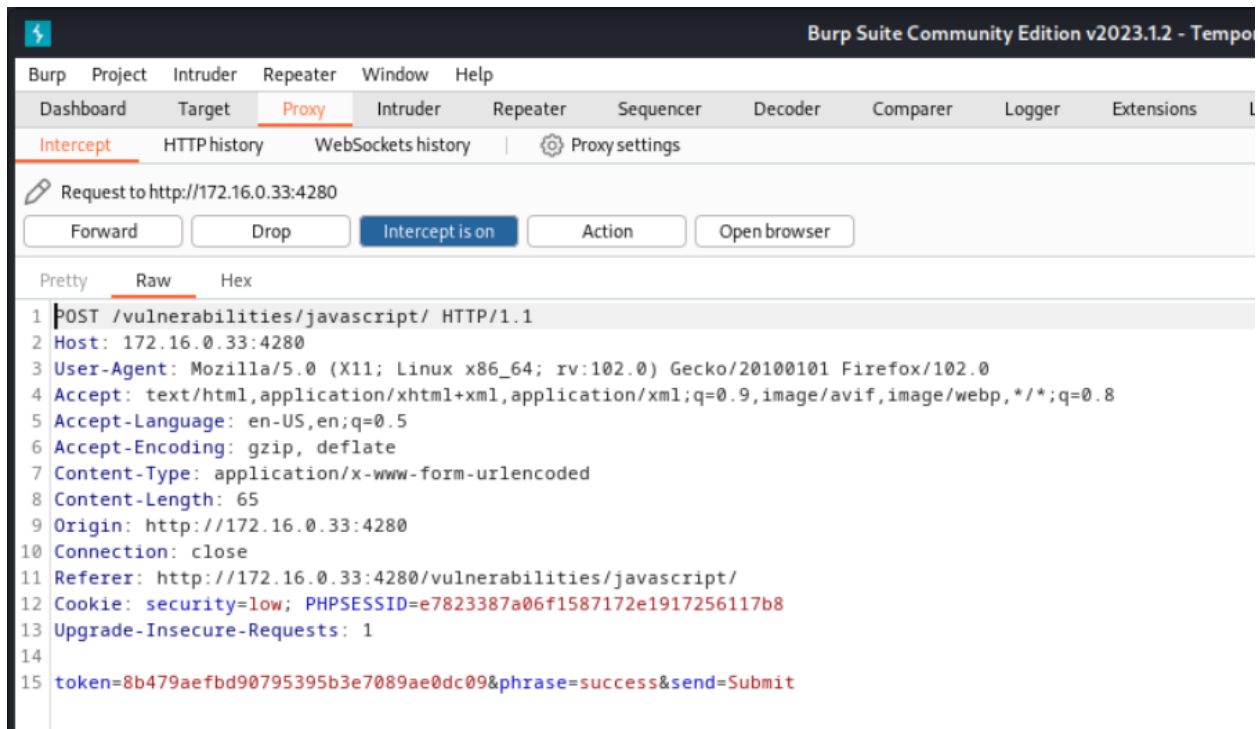
Vulnerability: JavaScript Attacks

Submit the word "success" to win.

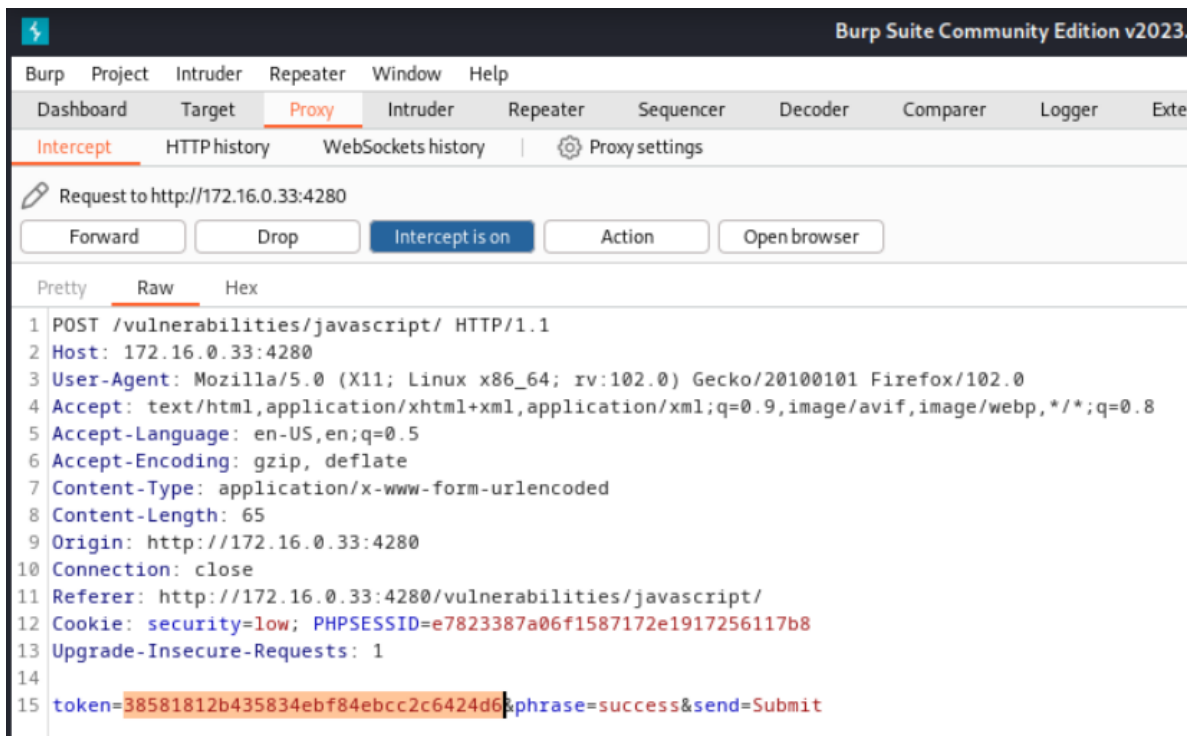
You got the phrase wrong.

Phrase

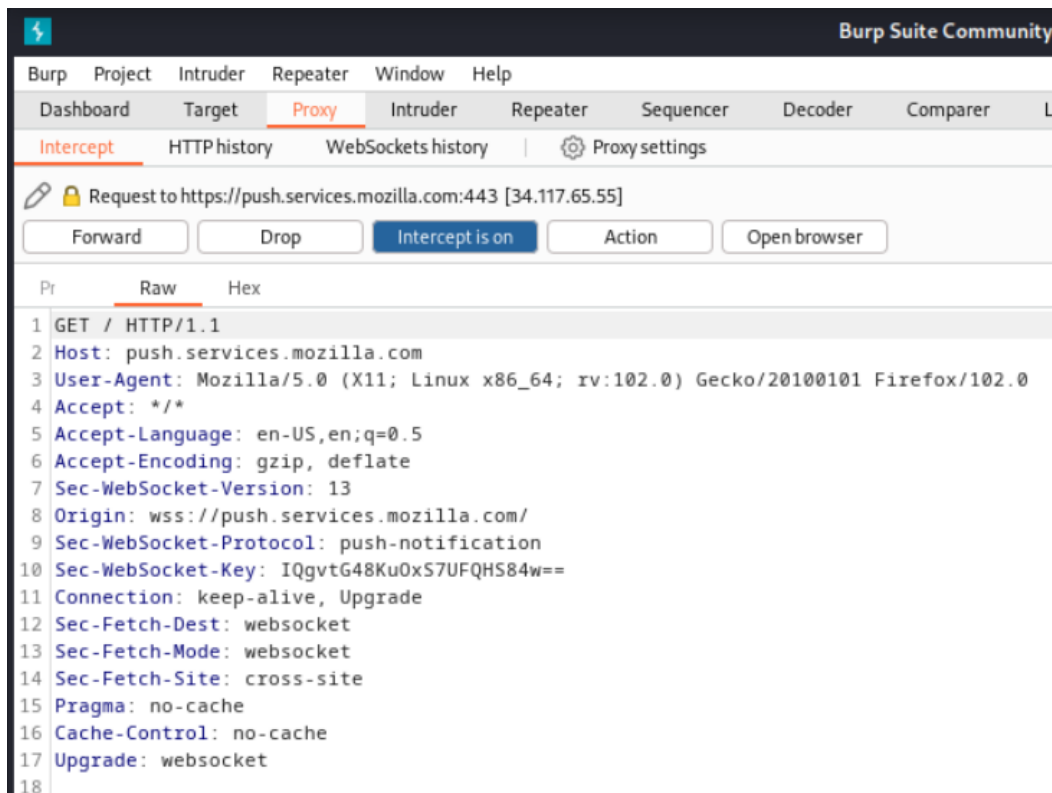
Maka akan muncul pop up dari Burp Suite



pada bagian paling bawah, ganti value pada bagian token menjadi "38581812b435834ebf84ebcc2c6424d6"



Setelah token diganti, pada kiri atas klik Forward, maka tampilan Burp Suite akan menjadi seperti berikut



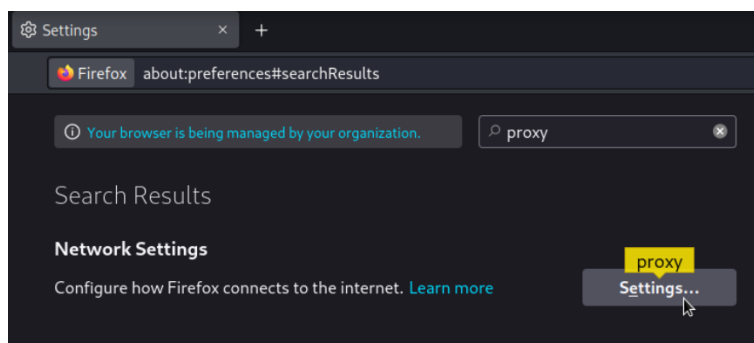
Kembali ke browser, pada halaman JavaScript Attack, jika muncul teks “Well done!” berarti phrase dan token sudah benar



🧹 Clean up

Kembalikan setting proxy seperti semula pada browser

Masuk ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy



Didalamnya ganti "Manual proxy configuration" menjadi "Use system proxy settings" lalu klik OK

