


HACKTHEBOX – babynginxatsu

Bu makinede hassas verilerin açığa çıkarılması(Sensitive data exposure) güvenlik zaafiyeti ele alınmıştır.

Öncelikle makinemizi dağıttıktan sonra karşımıza çıkan IP adresine giriş yapıyorum zaten web uygulaması olduğunu bildiğim için ekstra nmap ile port taraması yapmıyorum verilen portu direkt olarak web tarayıcıma giriyorum ve karşıma bir nginx web sunucusunda çalışan web uygulaması yükleniyor ve bir 'login' sayfası bizleri karşılıyor. Burada bir email ve şifre ile giriş yapmamız isteniyor, fakat henüz ne bir email'e ne de şifreye sahip değilim. Böyle uygulamalarda bazen google'dan varsayılan kimlik bilgilerini araştırmak işe yarayabilir, fakat bu uygulamada herhangi bir varsayılan kimlik bilgisi ile giriş yapamıyorum. Ardından 'Create A New Account' seçeneğinden yeni bir hesap ile giriş yapmayı deniyorum. Hesabı oluşturduktan sonra kendi konfigürasyon dosyamı oluşturulmak için bir sayfaya yönlendiriliyorum.

nginxatsu



Generate your own nginx config file

Server

Server Name	Port
<input type="text" value="-"/>	<input type="text" value="80"/>
Root	Default Index
<input type="text" value="/www/public"/>	<input type="text" value="index.php"/>
Nginx user	Worker Connections
<input type="text" value="www"/>	<input type="text" value="1024"/>

Turn off server tokens?

☒ Yes ☐ No

Routes

Location	Nginx directive
<input type="text" value="/storage"/>	<input type="text" value="autoindex on"/>

Add route

Generator

Generate Config

Configs

51

10:12:31

Yukarıda bize bazı bilgiler sağlanıyor bunlardan bazıları şöyle:

- `/www/public/` dizin: Uygulamanın kök dizini
- `/storage` dizin: mevcut konfigürasyon dosyalarının barındırıldığı dizin

Formu gönderdikten sonra oluşturulan konfigürasyon dısyasını temsil eden bir ikon oluşturuldu. 'Configs' altındaki bu ikona tıkladığımızda bizi konfigürasyon dosyamıza götürür ve buradan 'Raw Config' butonu ile ham şeklini ve dizini görüntüleyebiliriz.

```
Config
Raw Config

user www;
pid /run/nginx.pid;
error_log /dev/stderr info;

events {
    worker_connections 1024;
}

http {
    server_tokens off;

    charset utf-8;
    keepalive_timeout 20s;
    sendfile on;
    tcp_nopush on;
    client_max_body_size 2M;

    include /etc/nginx/mime.types;

    server {
        listen 80;
        server_name _;

        index index.php;
        root /www/public;

        # We sure hope so that we don't spill any secrets
        # within the open directory on /storage

        location /storage {
            autoindex on;
        }

        location / {
            try_files $uri $uri/ /index.php?$query_string;
            location ~ \.php$ {
                try_files $uri =404;
                fastcgi_pass unix:/run/php-fpm.sock;
                fastcgi_index index.php;
                fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
                include fastcgi_params;
            }
        }
    }
}
```

Yukarıdaki yorum satırında da görüntülüyoruz ancak 'Raw Config' butonuna tıkladığımızda da mevcut konfigürasyon dizininden de gidilebilir `/storage` dizinine gidiyoruz ve burada ilginç bir dosya dikkatimi çekiyor.

index of /storage/

94.237.59.199:30083/storage/

Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

regina_66ef8a2b0c87.conf22-Sep-2024 09:511101

regina_66ef8a2b1f81.conf22-Sep-2024 09:511101

regina_66ef8a2b1f85.conf22-Sep-2024 09:511101

regina_66ef8a2b1f89.conf22-Sep-2024 09:511101

regina_66ef8a2b1f97.conf22-Sep-2024 09:511101

regina_66ef8a2b1f9a.conf22-Sep-2024 09:511101

regina_66ef8a2b1f9d.conf22-Sep-2024 09:511101

regina_66ef8a2b1f9e.conf22-Sep-2024 09:511101

regina_66ef8a2b1f9f.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa0.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa1.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa2.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa3.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa4.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa5.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa6.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa7.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa8.conf22-Sep-2024 09:511101

regina_66ef8a2b1fa9.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-2024 09:511101

regina_66ef8a2b1faa.conf22-Sep-2024 09:511101

regina_66ef8a2b1fab.conf22-Sep-2024 09:511101

regina_66ef8a2b1fac.conf22-Sep-2024 09:511101

regina_66ef8a2b1fad.conf22-Sep-2024 09:511101

regina_66ef8a2b1fae.conf22-Sep-2024 09:511101

regina_66ef8a2b1faf.conf22-Sep-2024 09:511101

regina_66ef8a2b1fag.conf22-Sep-2024 09:511101

regina_66ef8a2b1fah.conf22-Sep-2024 09:511101

regina_66ef8a2b1fai.conf22-Sep-2024 09:511101

regina_66ef8a2b1faj.conf22-Sep-2024 09:511101

regina_66ef8a2b1fak.conf22-Sep-2024 09:511101

regina_66ef8a2b1fal.conf22-Sep-2024 09:511101

regina_66ef8a2b1fam.conf22-Sep-2024 09:511101

regina_66ef8a2b1fan.conf22-Sep-2024 09:511101

regina_66ef8a2b1fao.conf22-Sep-2024 09:511101

regina_66ef8a2b1fap.conf22-Sep-2024 09:511101

regina_66ef8a2b1faq.conf22-Sep-2024 09:511101

regina_66ef8a2b1far.conf22-Sep-2024 09:511101

regina_66ef8a2b1fas.conf22-Sep-2024 09:511101

regina_66ef8a2b1fat.conf22-Sep-20

Yukarıdaki görselde bir veri tabanı yedek dosyası barındırılıyor. Hemen bunu ``wget`` komutu ile indirip dosyayı çıkardıktan sonra içeriğini görüntülüyorum.

İçeriğinde bir adet `database` isminde bir dizin ve içerisinde `database.sqlite` adında sqlite veri tabanı dosyası çıktı bunu DB Browser veya linux terminal üzerinden `sqlite3` yardımcı programı ile inceleyebilirsiniz. Ben Parrot OS (Linux) kullandığım için `sqlite3` yardımcı programı ile bu veritabanını komut satırı arayüzünden inceliyorum.

`sqlite3 database/database.sqlite` komutu ile database dosyama giriş yaptıktan sonra aşağıdaki sorguyu çalıştırıyorum.

```
`SELECT * FROM users;`
```

Çok temel bir sorgudur ve mevcut veritabanındaki kullanıcı tablosundaki tüm kayıtları(sütunları ve değerlerini) listeler.

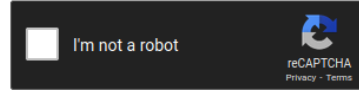
Burada görüldüğü gibi kullanıcı email ve parola bilgileri açığa çıkarılmış oldu.

Muhtemelen en üstteki kullanıcı admin kişinin email ve parola bilgileri ama parola değeri MD5 ile hash'lenmiş gibi görünüyor. Bunu crackstation gibi çevrim içi bir siteden kırıyorum. Elde ettiğim hash değerini parola olarak kullanabilirim.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e7816e9a10590b1e33b87ec2fa65e6cd



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e7816e9a10590b1e33b87ec2fa65e6cd	md5	adminadmin1

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/Desktop/babynginxatsu$ cat crackme.txt
#cat crackme.txt: [tnl_send: tnl_generic_error (-101): Network is unreachable]
e7816e9a10590b1e33b87ec2fa65e6cd -> nginxatsu-adm-01@makelarid.es -> adminadmin1
616243c128cdf340f5523bd1e68e9238a1c_gateway<UNDER
72bc85eaa06d8d28d563b64b3082a4d8 -> e tun0 opened
[root@parrot]~/Desktop/babynginxatsu$ tun0
# 2024-09-22 09:57:34 net_iface_up: set tun0 up
2024-09-22 09:57:34 net_addr_v4_add: 10.10.16.7/23 dev tun0
2024-09-22 09:57:34 net_iface_mtu_set: mtu 1500 for tun0
2024-09-22 09:57:34 net_iface_up: set tun0 up
2024-09-22 09:57:34 net_addr_v6_add: dead:beef::1005/64 dev tun0
2024-09-22 09:57:34 net_route_v4_add: 10.10.10.0/23 via 10.10.16.1 dev [NULL] ta
ble 0 metric -1
2024-09-22 09:57:34 net_route_v4_add: 10.129.0.0/16 via 10.10.16.1 dev [NULL] ta
ble 0 metric -1
2024-09-22 09:57:34 add_route_ipv6(dead:beef::/64 -> dead:beef::1 metric -1) d
ev tun0
2024-09-22 09:57:34 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 met
ric -1
2024-09-22 09:57:34 Initialization Sequence Completed
2024-09-22 09:57:34 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id:
0, compression: 'lz0'
2024-09-22 09:57:34 Timers: ping 10, pong restart 120
```

Daha sonra admin kullanıcı bilgileri ile login sayfasından giriş yapıyorum ve evet! Başarılı bir şekilde flag'i elde ederek odayı tamamlıyoruz.