



baby nginxatsu

▼ Platform	HTB
📅 Date	@July 9, 2022
▼ Operating System	Web-CTF
☰ Tags	nginx web-app

General-Information

▼ Table of Contents

- Summary
- Website
- Admin password cracked
- Information Learned

▼ Passwords

- Site administrator `nginxatsu-adm-01@makelarid.es` : `adminadmin1`

▼ Challenge Description

- Can you find a way to login as the administrator of the website and free nginxatsu?

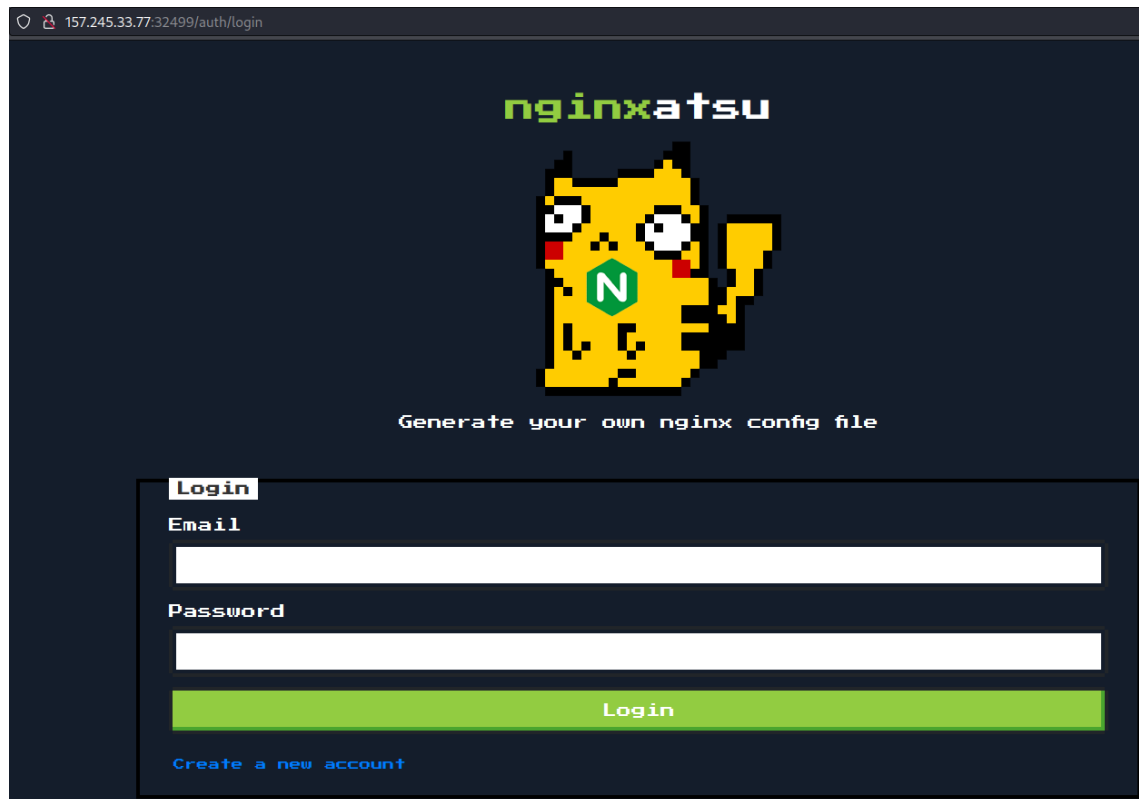
Summary

- Nginx website left a database file easily accessible and from there the administrator password can be cracked to login as them and view challenge's flag.
-

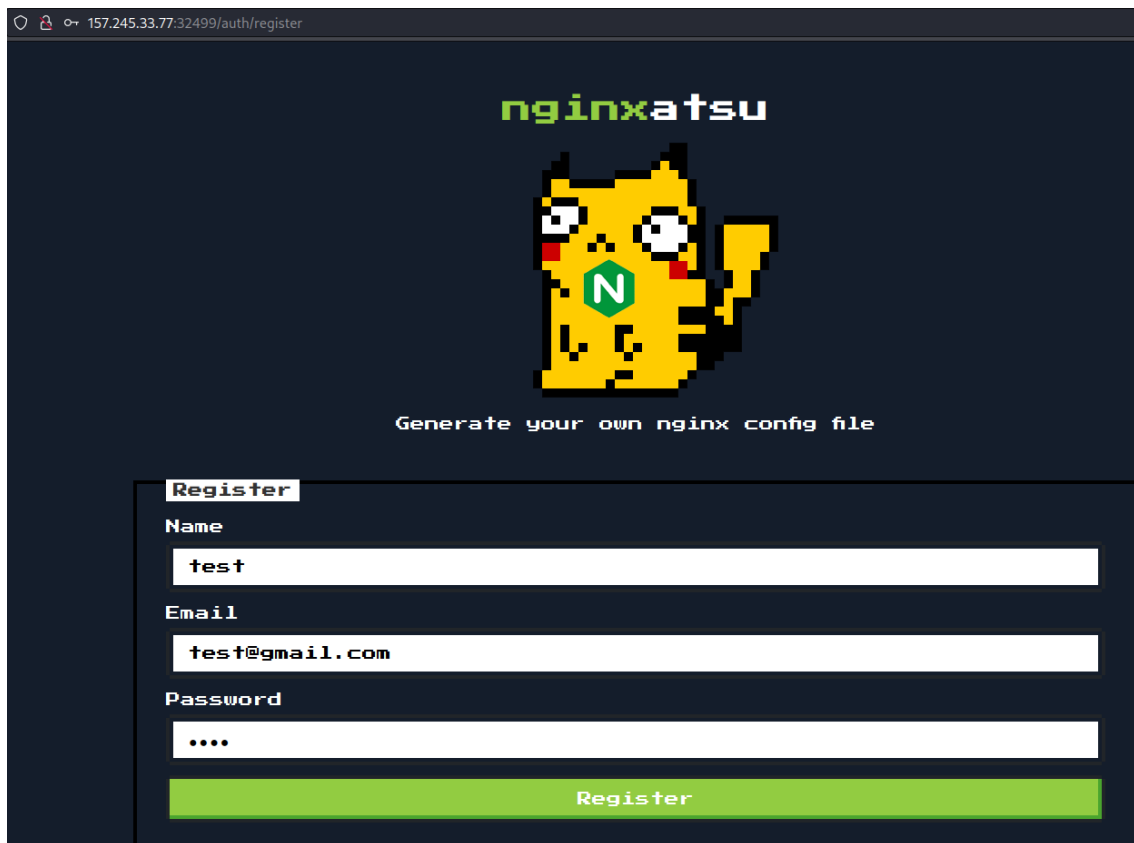
Website

▼ After starting the challenge up, I went to the IP address and was presented with a login page. I had no credentials for this site and no SQLi strings seemed to be popping. So, I went to create an account.

▼ Login portal



▼ Registering my own user



157.245.33.77:32499/auth/register

nginxatsu

Generate your own nginx config file

Register

Name

Email

Password

Register

▼ Upon logging in as my user `test`, I see that I can create my own nginx files. However, this doesn't matter in a sense. The `/storage` directory is open for auto-indexing and this is made to be an apparent misconfiguration via a comment left behind in the

▼ Creating custom nginx config files

157.245.33.77:32499

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"/>

Generator

▼ Comment talking about the `/storage` misconfiguration

```
server {  
    listen 80;  
    server_name first;  
  
    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 /uploads {  
        return 404;;  
    }  
}
```

Admin password cracked

▼ I navigated to `/storage/` and saw at the bottom a tar file called database, which when unzipped revealed a SQL file with the admin username and password

▼ `/storage/` directory

← → ↻ 🏠 46.101.78.118:31030/storage/		
Index of /storage/		
<hr/>		
../		
nginx_62c8dcc06f8b1.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0707af.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc070b2c.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc070e7c.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0711f5.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07154a.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0718bf.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc071bff.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc071f39.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0722c1.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc072626.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc072962.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc072c91.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07300a.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc073334.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07367e.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0739b4.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc073cf0.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc074092.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0743ef.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07479d.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc074bd7.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07521c.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07559e.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0758d3.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc075bf7.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0762d8.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0766ee.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc076aa4.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc076e94.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc077283.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc077662.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc077a39.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc077e3e.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc078232.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc078608.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0789bb.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc078d7d.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc079159.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc079538.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0798f8.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc079d02.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07a158.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc07a51f.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc084eab.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc085273.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc0855df.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc085974.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc085ce3.conf	09-Jul-2022 01:41	1101
nginx_62c8dcc086035.conf	09-Jul-2022 01:41	1101
nginx_62c8dd672bff5.conf	09-Jul-2022 01:44	1070
nginx_62c8dd95eeba1.conf	09-Jul-2022 01:44	1068
nginx_62c8e412132c7.conf	09-Jul-2022 02:12	1130
v1_db_backup_1604123342.tar.gz	09-Jul-2022 01:41	42496

▼ Messing with the `database.sqlite` file

▼ Downloading the file

```

(kali㉿kali)-[~/HTB/ctf/baby-ngnixatsu]
$ curl http://46.101.78.118:31030/storage/v1_db_backup_1604123342.tar.gz --output backup.tar.gz
  Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 42496 100 42496    0     0  91808      0 --:--:-- --:--:-- --:--:--  91982

(kali㉿kali)-[~/HTB/ctf/baby-ngnixatsu]
$ ls
backup.tar.gz  ferox-http_157_245_33_77:32499-1657330021.state  nikto.txt  web-enum.txt

(kali㉿kali)-[~/HTB/ctf/baby-ngnixatsu]
$ tar -xvf backup.tar.gz
database/database.sqlite

(kali㉿kali)-[~/HTB/ctf/baby-ngnixatsu]
$ ls
backup.tar.gz  database  ferox-http_157_245_33_77:32499-1657330021.state  nikto.txt  web-enum.txt

```

▼ Starting `sqlite`

```

(kali㉿kali)-[~/HTB/ctf/baby-ngnixatsu/database]
$ sqlite3 database.sqlite
SQLite version 3.38.2 2022-03-26 13:51:10
Enter ".help" for usage hints.
sqlite> .tables
failed_jobs      nginx_configs    users
migrations       password_resets
sqlite> select * from users
... > ;
1|jr|nginxatsu-adm-01@makelarid.es|e7816e9a10590b1e33b87ec2|2022-07-09 01:41:20
2|Giovanni|nginxatsu-giv@makelarid.es|b24ad2bbe3f09a3eeec9c:20|2022-07-09 01:41:20
3|me0wth|nginxatsu-me0wth@makelarid.es|9272e22bfc263d8e7f6e1:20|2022-07-09 01:41:20
sqlite> select

```

▼ Looking at the `users` file

```

sqlite> select * from users;
1|jr|nginxatsu-adm-01@makelarid.es|e7816e9a10590b1e33b87ec2fa65e6cd|r0einlUPdWYGr3R5y1Vp17SMmG1L4QEogb8h3vt83fGuM2uISjPKKg8bZhPqQViJ0GP||2022-07-09 01:41:20|2022-07-09 01:41:20
2|Giovanni|nginxatsu-giv@makelarid.es|b24ad2bbe3f09a3eeec9c001f30a06e6|14eg41yr4CSm4CWP8Vzt5mzul280Yvuul9A0wxA71o54F76slbq96StgoX1NrugF1Vfb||2022-07-09 01:20|2022-07-09 01:41:20
3|me0wth|nginxatsu-me0wth@makelarid.es|9272e22bfc263d8e7f6e2c69c60848bd|TCGVlf13RvUeSQCEBym6a4dLcyxNazA7rGYzClvFQ4WvkCDE0t0F1JjprHk7e1hUqL4M||2022-07-09 01:20|2022-07-09 01:41:20

```

▼ Sublime cleaned up output

```

jR
nginxatsu-adm-01@makelarid.es
e7816e9a10590b1e33b87ec2fa65e6cd
r0einlUPdWYGfr3R5y1Vp17SMmG1L4QEogb8h3vt83fGuM2uISjPKkG8bZhPqqVij0GP

Giovanni1
nginxatsu-giv@makelarid.es
b24ad2bbe3f09a3eeec9c001f30a06e6
i4eg4iyr4CSm4CWP8Vzt5mzul280YVuul9A0wxA71o54F76s1bq96StgoXiNrufiVfb

me0wth
nginxatsu-me0wth@makelarid.es
9272e22bfc263d8e7f6e2c69c60848bd
TCGVlf13RvUeSQCEBym6a4dLcyxNazA7rGYzClvfQ4WvkcdE0t0F1JjprHk7e1hUqL4M

```

▼ Using crackstation to crack the password

Free Password Hash Cracker

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

e7816e9a10590b1e33b87ec2fa65e6cd

I'm not a robot

reCAPTCHA
Privacy - Terms

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

▼ After successful administrator login, the flag is presented



Information Learned

- Don't forget to try a request with a `/` and without one, sometimes that's all that's need

ex. `$IP/storage` goes nowhere, but `$IP/storage/` goes where you need it to