tips

Security in Node.js

Ishan Marikar

Who am I?

Ishan Marikar

Software Developer/Maker of Things

(Currently Unemployed/freelancing)

Why This Topic Though?

> I wasn't creative enough.

> Help people not get their systems hacked

Put a password on it

› Secure your database/redis instances

› Bind to localhost/Open inside a vpn.

› .. and choose complex passwords.

Shodan | Developers | Book | View All...

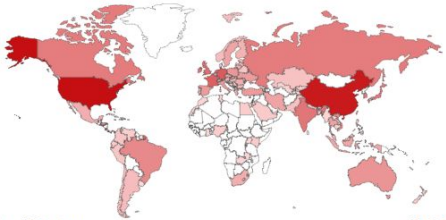
SHODAN product:"MongoDB" Explore Down

Exploits | Maps | Like 10 | Download Results | Create Report

TOTAL RESULTS

31,439

TOP COUNTRIES



United States	10,340
China	8,194
Germany	1,564
France	1,363
Netherlands	1,167

TOP ORGANIZATIONS

Amazon.com	4,180
Hangzhou Alibaba Advertising Co....	3,832
Digital Ocean	2,168
Microsoft Azure	1,496
OVH SAS	1,005

108.168.153.177

b1.99.a86c.ip4.static.sl-reverse.com

SoftLayer Technologies

Added on 2017-08-16 14:01:05 GMT

United States, Dallas

Details

database

198.204.227.3

Zhou Pizhong

Added on 2017-08-16 13:57:52 GMT

United States, Kansas City

Details

database

Don't put passwords on GIT

Use environmental variables (process.env)

If you do put them in, revoke them/change them

Rate limit your endpoints

› Use middleware to defend against brute force attacks.

› Use helmet to add the required security headers to your responses.

module	default?
contentSecurityPolicy for setting Content Security Policy	
expectCt for handling Certificate Transparency	
dnsPrefetchControl controls browser DNS prefetching	✓
frameguard to prevent clickjacking	✓
hidePoweredBy to remove the X-Powered-By header	✓
hpkp for HTTP Public Key Pinning	
hsts for HTTP Strict Transport Security	✓
ieNoOpen sets X-Download-Options for IE8+	✓
noCache to disable client-side caching	
noSniff to keep clients from sniffing the MIME type	✓
referrerPolicy to hide the Referer header	
xssFilter adds some small XSS protections	✓

Secure your cookies

› Set them as "HTTP ONLY" unless you plan to use them client-side.

› Better yet, also use signed cookies so you know they aren't tampered with.

```
app.use(session({
  secret: 'My super session secret',
  cookie: {  httpOnly: true,  secure: true  }
}));
```

Don't Root.

› Don't run your app as root. Create a separate account (deploy)

› Restrict access to Root, or disable remote logins to that user.

(maybe use docker too)

```
root@05ea8ed92224:/# useradd --user-group --create-home --shell /bin/false deploy
```

Prevent Injection Attacks

- SQL Injections, MOngoDB injections
- Obviously don't use eval()
- Escape and sanitize user data.

Yo, is there a SELECT * FROM Drunks WHERE Name="";DROP TABLE *;-- Jones" here?

Remove sensitive information

- From the urls, like Primary keys/Object ids

Thank You