# Cyber Insecurity in the Wild

Chris Cumming

# Who am I? (i.e. Shameless Self Promotion)

Software Consultant

https://saturdaymp.com
chris.cumming@satudaymp.com

Host of:

http://weeklydevchat.com/
https://www.legacycode.rocks/

Slacks

Chris C on
- Dev Edmonton
- Legacy Code Rocks
- YegSec

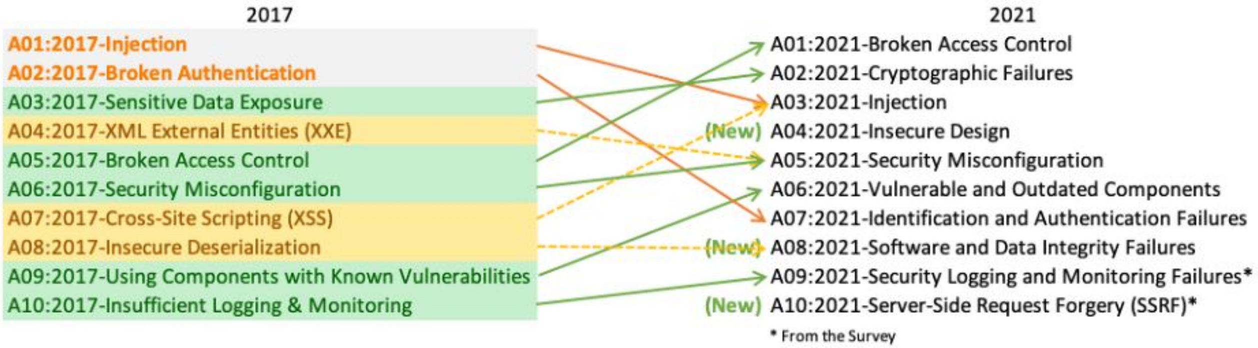
# Cyber Insecurity I’ve Witnessed (and possibly done)

- APIs with no security
- Reversible passwords
- Credentials/secrets in source code
- Publicly accessible databases
- Environments not isolated
- No rate limiting
- Password on sticky note
- Credentials in shared Excel file
- Basic auth over HTTP
- What have you seen?

# My Examples vs. OWASP

OWASP top 10:
https://owasp.org/www-project-top-ten/

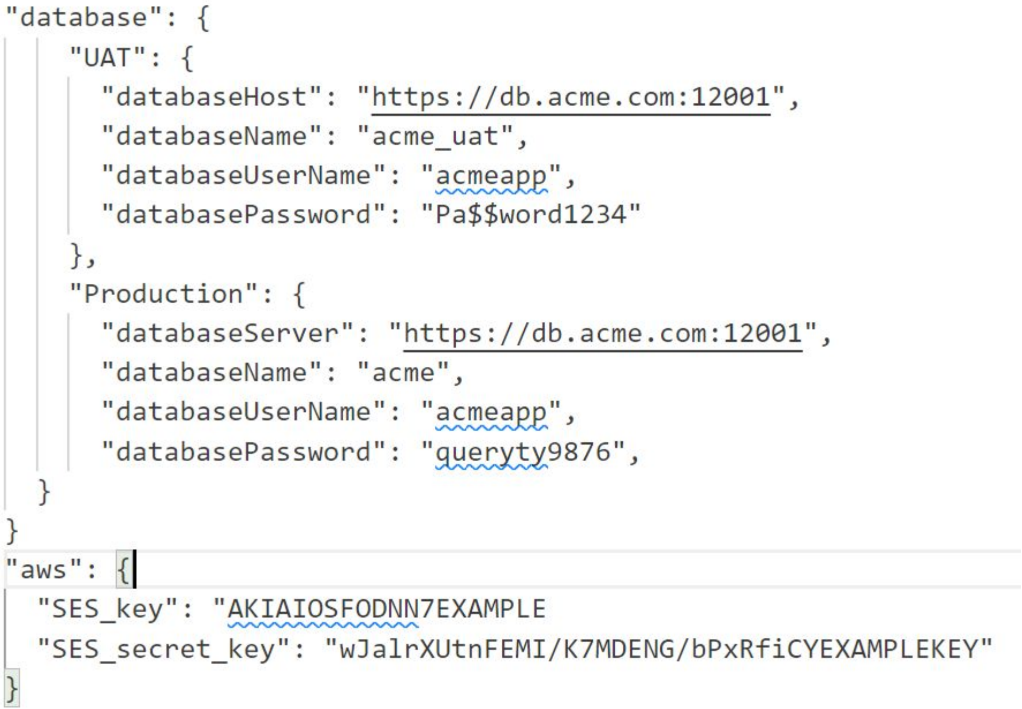
See OWASP Cheat Sheets:
https://cheatsheetseries.owasp.org/



| 2017 | 2021 |
|---|---|
| A01:2017-Injection | A01:2021-Broken Access Control |
| A02:2017-Broken Authentication | A02:2021-Cryptographic Failures |
| A03:2017-Sensitive Data Exposure | A03:2021-Injection |
| A04:2017-XML External Entities (XXE) | (New) A04:2021-Insecure Design |
| A05:2017-Broken Access Control | A05:2021-Security Misconfiguration |
| A06:2017-Security Misconfiguration | A06:2021-Vulnerable and Outdated Components |
| A07:2017-Cross-Site Scripting (XSS) | A07:2021-Identification and Authentication Failures |
| A08:2017-Insecure Deserialization | (New) A08:2021-Software and Data Integrity Failures |
| A09:2017-Using Components with Known Vulnerabilities | A09:2021-Security Logging and Monitoring Failures* |
| A10:2017-Insufficient Logging & Monitoring | (New) A10:2021-Server-Side Request Forgery (SSRF)* |

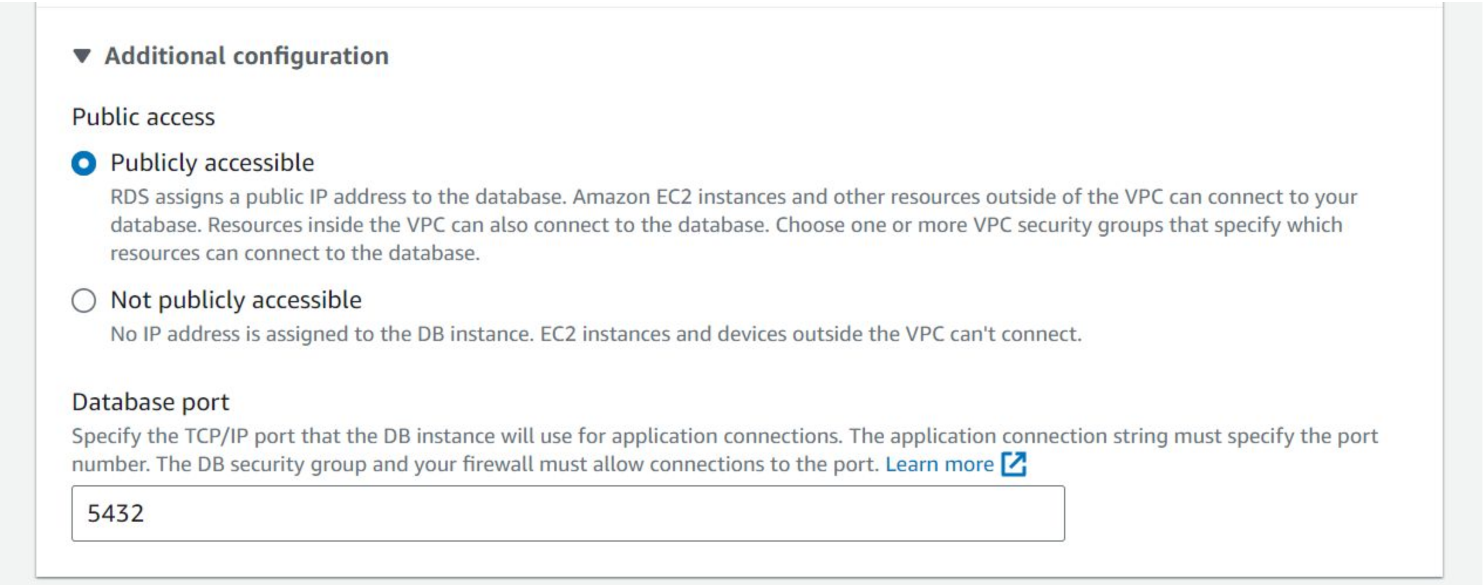
* From the Survey

# Hard Code Secrets in Source Code



```
"database": {
    "UAT": {
      "databaseHost": "https://db.acme.com:12001",
      "databaseName": "acme_uat",
      "databaseUserName": "acmeapp",
      "databasePassword": "Pa$$word1234"
    },
    "Production": {
      "databaseServer": "https://db.acme.com:12001",
      "databaseName": "acme",
      "databaseUserName": "acmeapp",
      "databasePassword": "queryty9876",
  }
}
"aws": {
  "SES_key": "AKIAIOSFODNN7EXAMPLE
  "SES_secret_key": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
}
```

# Database Publicly Accessible



▼ Additional configuration

Public access

● Publicly accessible

RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

○ Not publicly accessible

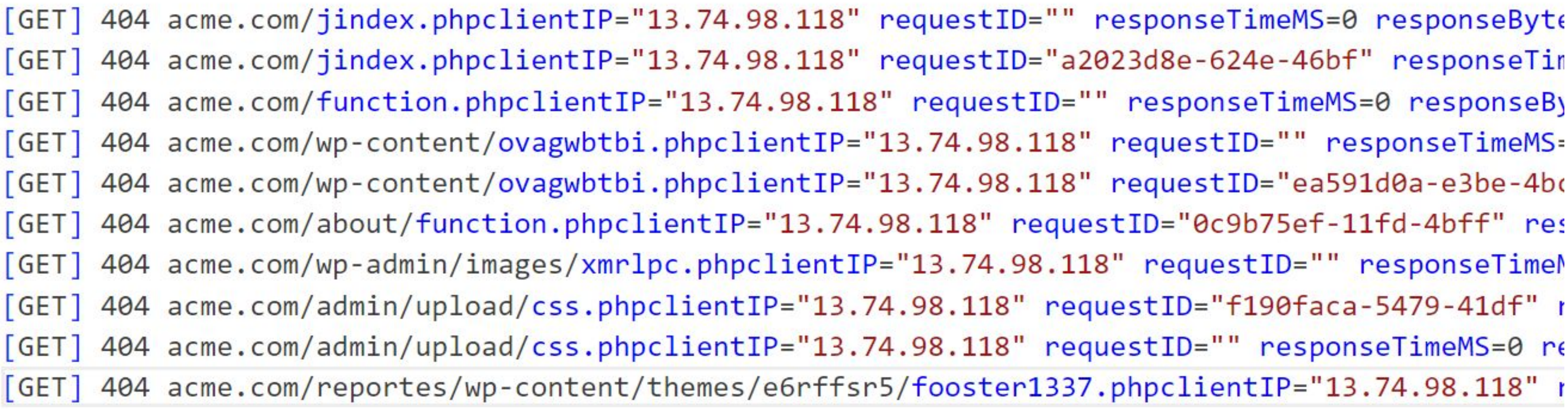
No IP address is assigned to the DB instance. EC2 instances and devices outside the VPC can't connect.

Database port

Specify the TCP/IP port that the DB instance will use for application connections. The application connection string must specify the port number. The DB security group and your firewall must allow connections to the port. Learn more

5432

# No Rate Limiting



```
[GET] 404 acme.com/jindex.phpclientIP="13.74.98.118" requestID="" responseTimeMS=0 responseByte
[GET] 404 acme.com/jindex.phpclientIP="13.74.98.118" requestID="a2023d8e-624e-46bf" responseTim
[GET] 404 acme.com/function.phpclientIP="13.74.98.118" requestID="" responseTimeMS=0 responseBy
[GET] 404 acme.com/wp-content/ovagwbtbi.phpclientIP="13.74.98.118" requestID="" responseTimeMS=
[GET] 404 acme.com/wp-content/ovagwbtbi.phpclientIP="13.74.98.118" requestID="ea591d0a-e3be-4bc
[GET] 404 acme.com/about/function.phpclientIP="13.74.98.118" requestID="0c9b75ef-11fd-4bff" res
[GET] 404 acme.com/wp-admin/images/xmrlpc.phpclientIP="13.74.98.118" requestID="" responseTime
[GET] 404 acme.com/admin/upload/css.phpclientIP="13.74.98.118" requestID="f190faca-5479-41df" r
[GET] 404 acme.com/admin/upload/css.phpclientIP="13.74.98.118" requestID="" responseTimeMS=0 re
[GET] 404 acme.com/reportes/wp-content/themes/e6rffsr5/fooster1337.phpclientIP="13.74.98.118" r
```

# Learn More

OWASP:
https://owasp.org/
https://www.meetup.com/meetup-group-opbybwve/

YegSec:
https://www.yegsec.ca/

Security Now Podcast:
https://twit.tv/shows/security-now

Rate Limiting with nginx & Fail2Ban:
https://github.com/saturdaymp-examples/rate-limiting-with-nginx-fail2ban

SaturdayMP Videos:
https://www.youtube.com/@saturdaymp

## Contact

chris.cumming@satudaymp.com

Chris C on Slack:
- Dev Edmonton
- Legacy Code Rocks
- YegSec

## Slides:

https://github.com/saturdaymp-examples/cyber-insecurity-in-the-wild