LabChat

Hanna Schulze, Oliver Wagner

Cloud Computing WS 18/19

Agenda

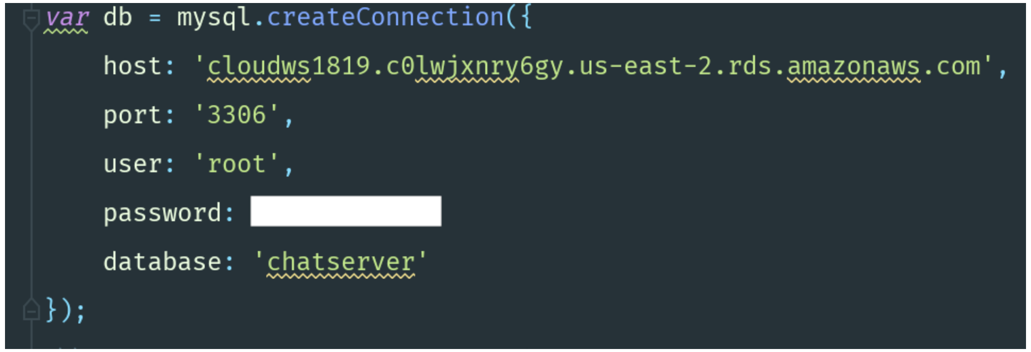
- Registering Users and Login Process
- Face Recognition
- Security aspects

- Live Demo

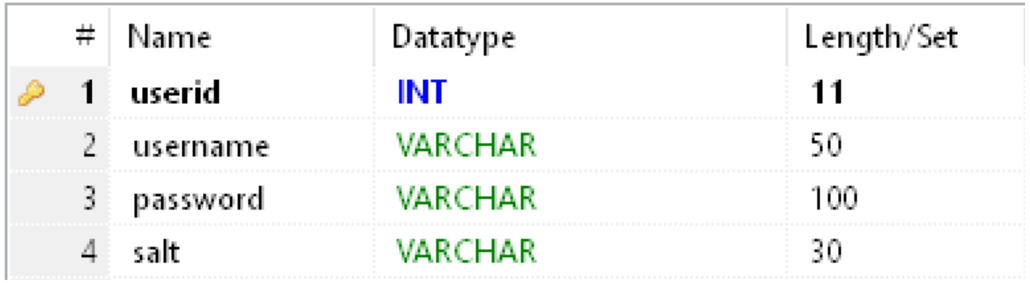
Registering Users and Login Process

- MySQL DB hosted at AWS RDS
- mysql-Node-Plugin

- Saving unique User-ID, username, salted password hash and salt

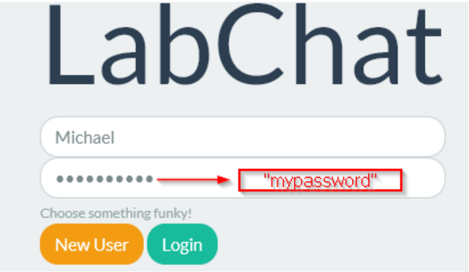


```
var db = mysql.createConnection({
    host: 'cloudws1819.c0lwjxnry6gy.us-east-2.rds.amazonaws.com',
    port: '3306',
    user: 'root',
    password: [redacted]
    database: 'chatserver'
});
```



#	Name	Datatype	Length/Set
1	**userid**	INT	**11**
2	username	VARCHAR	50
3	password	VARCHAR	100
4	salt	VARCHAR	30

Registering Users Process



LabChat

Michael

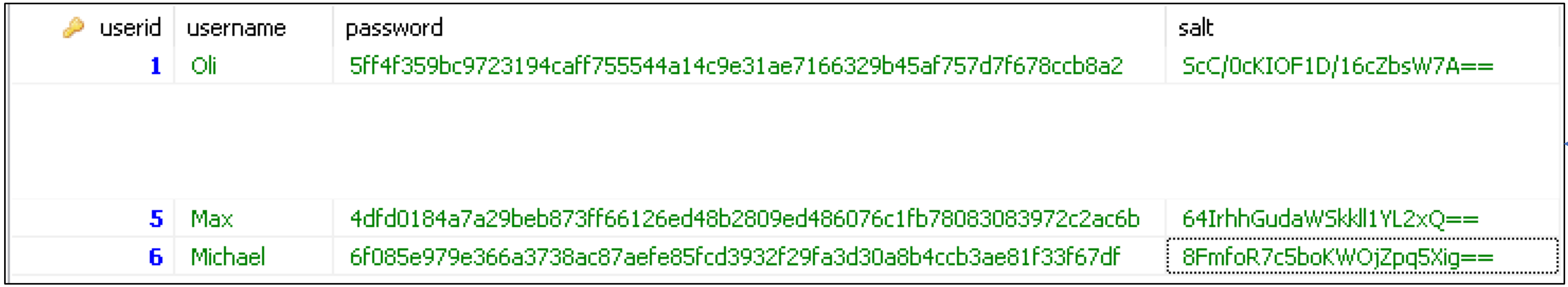
•••••••••• "mypassword"

Choose something funky!

‚New User‘

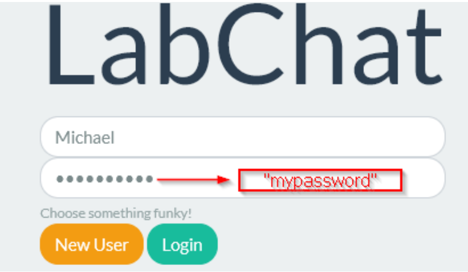
```
INSERT INTO Users … password = SHA2(?, 256)
          ? = saltedPassword
```

```
salt = 8FmfoR7c5boKWOjZpq5Xig==
saltedPassword = 8FmfoR7c5boKWOjZpq5Xig==mypassword
```



userid	username	password	salt
1	Oli	5ff4f359bc9723194caff755544a14c9e31ae7166329b45af757d7f678ccb8a2	ScC/0cKIOF1D/16cZbsW7A==
5	Max	4dfd0184a7a29beb873ff66126ed48b2809ed486076c1fb78083083972c2ac6b	64IrhhGudaWSkkll1YL2xQ==
6	Michael	6f085e979e366a3738ac87aefe85fcd3932f29fa3d30a8b4ccb3ae81f33f67df	8FmfoR7c5boKWOjZpq5Xig==

Login Users Process



Michael

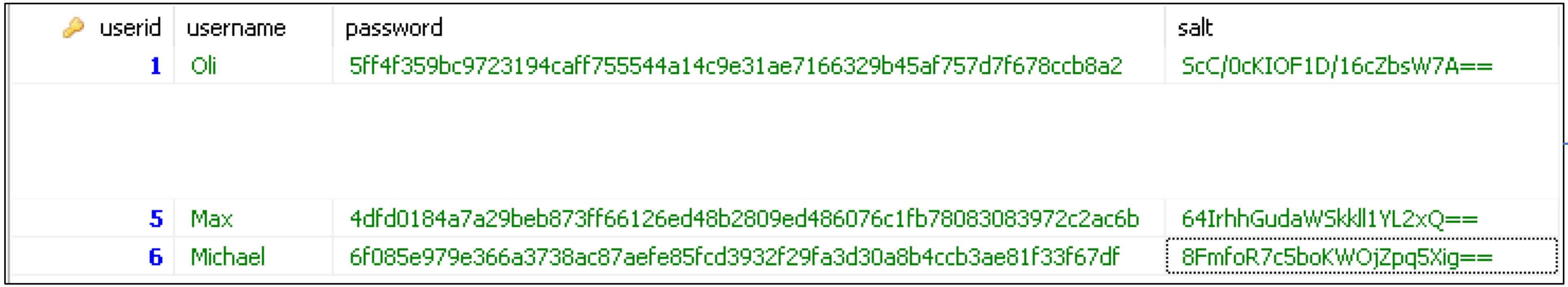
•••••••••• → "mypassword"

‚Login'

```
SELECT COUNT (*) FROM Users WHERE … password=SHA(?,256)
         ? = saltedPassword
```

count > 0

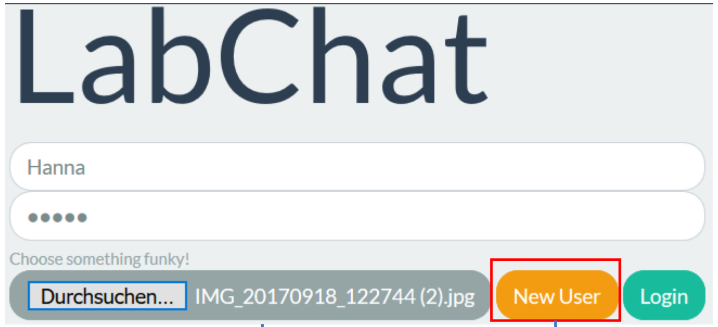
```
salt = 8FmfoR7c5boKWOjZpq5Xig==
saltedPassword = 8FmfoR7c5boKWOjZpq5Xig==mypassword
```



userid	username	password	salt
1	Oli	5ff4f359bc9723194caff755544a14c9e31ae7166329b45af757d7f678ccb8a2	ScC/0cKIOF1D/16cZbsW7A==
5	Max	4dfd0184a7a29beb873ff66126ed48b2809ed486076c1fb78083083972c2ac6b	64IrhhGudaWSkkll1YL2xQ==
6	Michael	6f085e979e366a3738ac87aefe85fcd3932f29fa3d30a8b4ccb3ae81f33f67df	8FmfoR7c5boKWOjZpq5Xig==

09:56 Michael -- Nice to meet you! -

Face Recognition

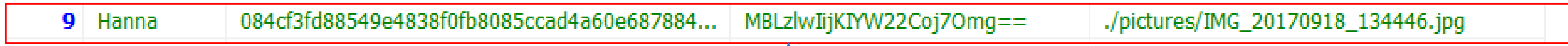


LabChat

Hanna

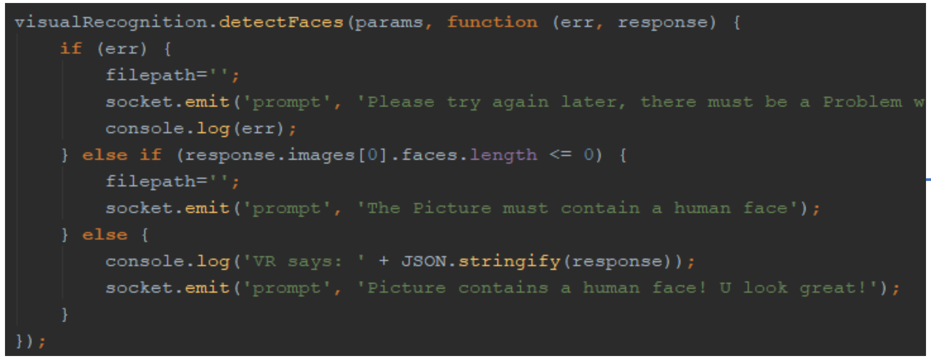
●●●●●

Choose something funky!



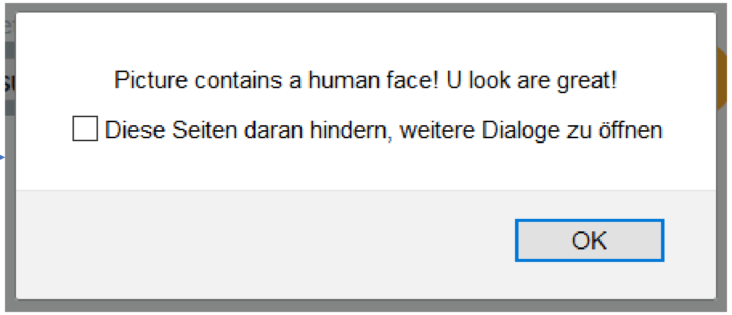
9	Hanna	084cf3fd88549e4838f0fb8085ccad4a60e687884...	MBLzlwIijKIYW22Coj7Omg==	./pictures/IMG_20170918_134446.jpg

Visual Recognition



```
visualRecognition.detectFaces(params, function (err, response) {
    if (err) {
        filepath='';
        socket.emit('prompt', 'Please try again later, there must be a Problem w
        console.log(err);
    } else if (response.images[0].faces.length <= 0) {
        filepath='';
        socket.emit('prompt', 'The Picture must contain a human face');
    } else {
        console.log('VR says: ' + JSON.stringify(response));
        socket.emit('prompt', 'Picture contains a human face! U look great!');
    }
});
```

if (response.image[0]faces.lenght >= 0)

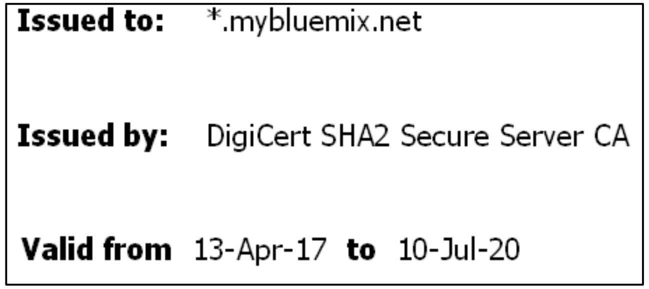


Picture contains a human face! U look are great!

☐ Diese Seiten daran hindern, weitere Dialoge zu öffnen

Security aspects: TLS

- Before: Node server speaking HTTPS with self-signed certs / Lets Encrypt
- But: Bluemix-Proxy only talking HTTP to applications, while speaking itself HTTPS to the outside world

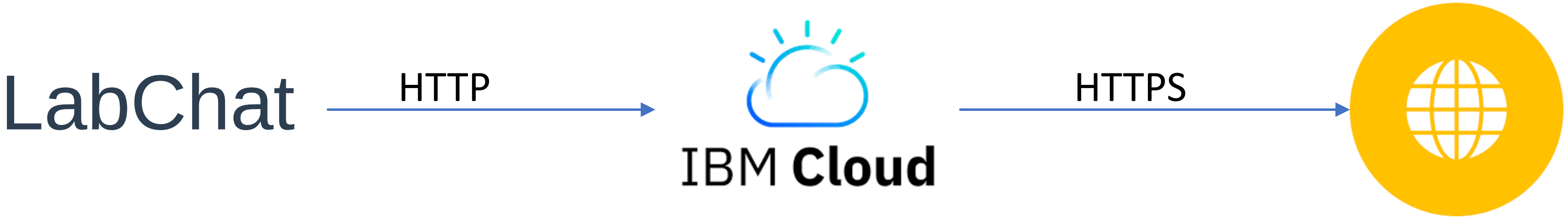


Issued to: *.mybluemix.net

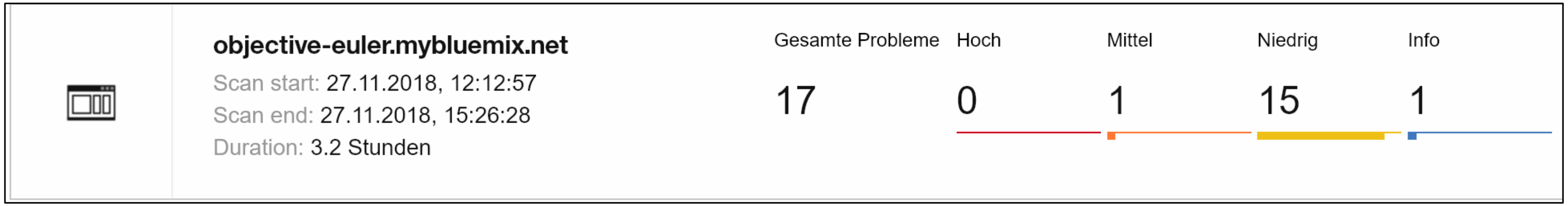
Issued by: DigiCert SHA2 Secure Server CA

Valid from 13-Apr-17 **to** 10-Jul-20

- Therefore
  - Making Node server speak HTTP again to the Bluemix-proxy
  - Make Node server trust proxies
  - On HTTP request, redirect to HTTPS



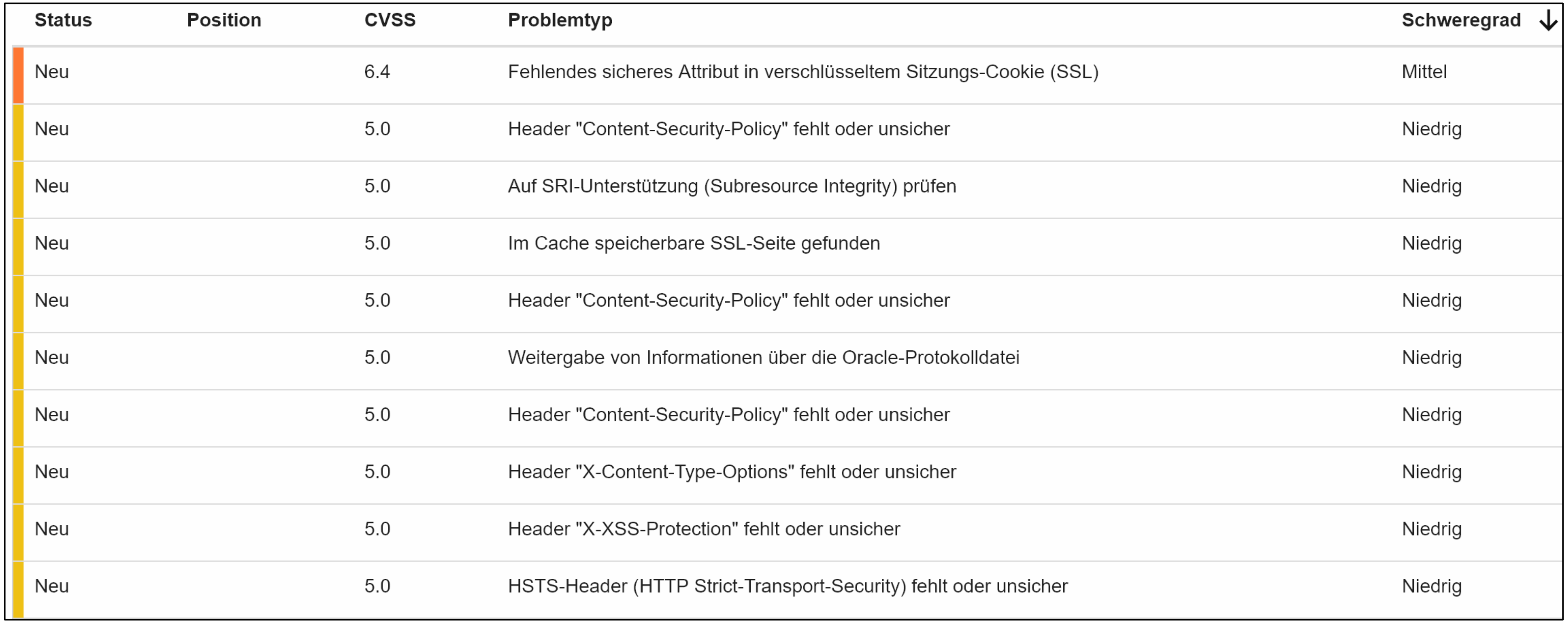
Security aspects: IBM AppScan



objective-euler.mybluemix.net

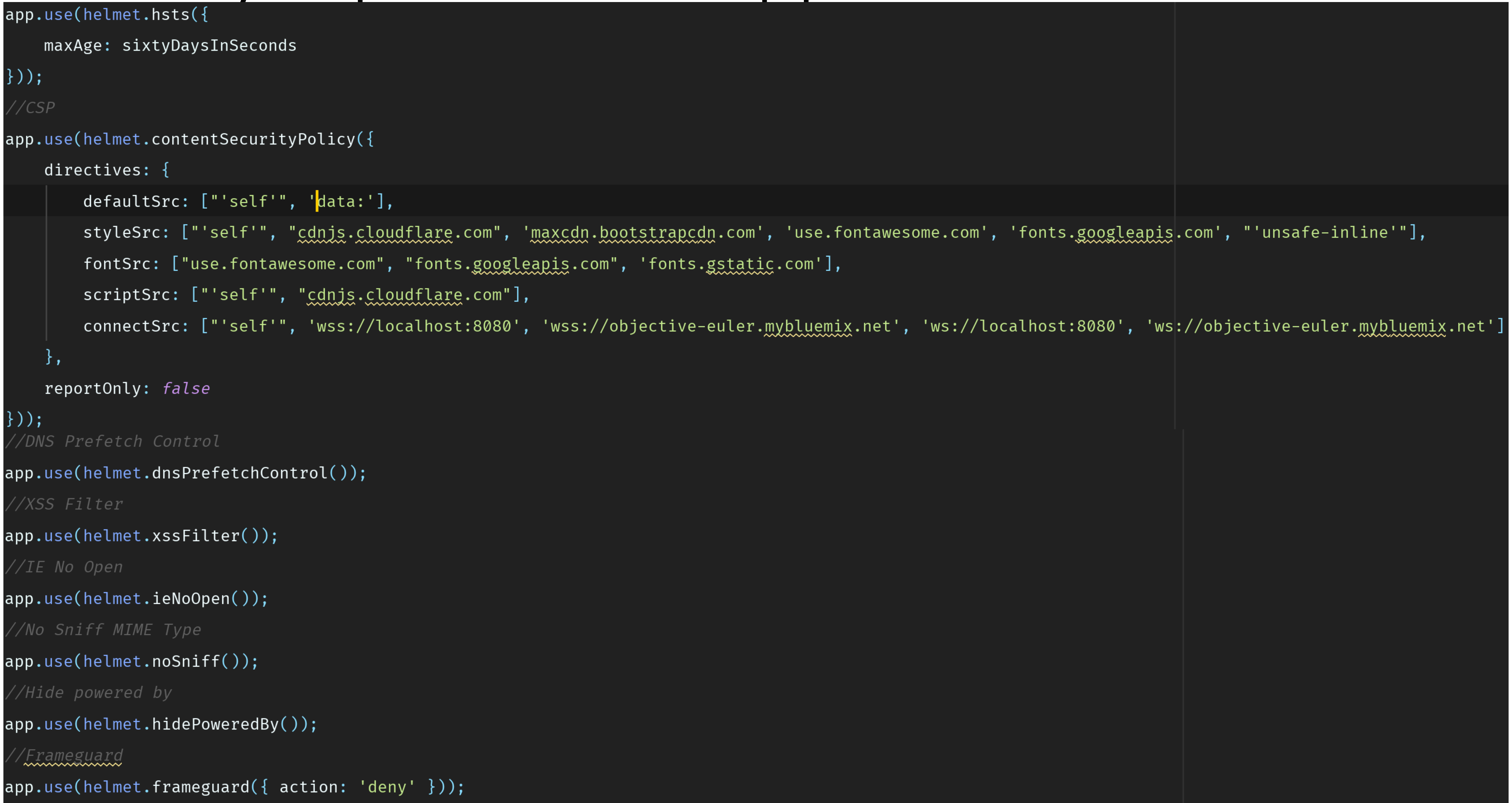
Scan start: 27.11.2018, 12:12:57
Scan end: 27.11.2018, 15:26:28
Duration: 3.2 Stunden

Gesamte Probleme	Hoch	Mittel	Niedrig	Info
17	0	1	15	1



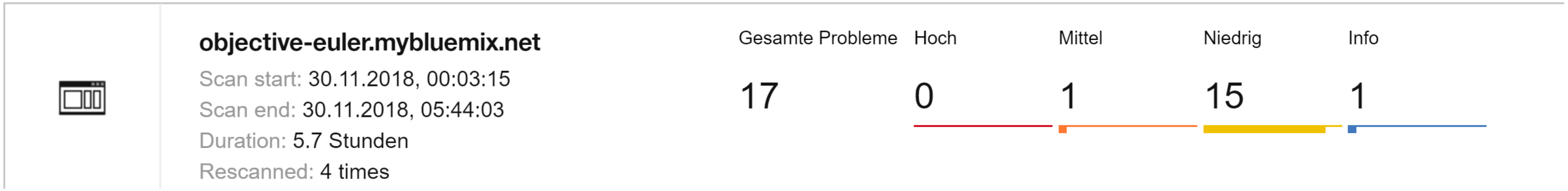
Status	Position	CVSS	Problemtyp	Schweregrad ↓
Neu		6.4	Fehlendes sicheres Attribut in verschlüsseltem Sitzungs-Cookie (SSL)	Mittel
Neu		5.0	Header "Content-Security-Policy" fehlt oder unsicher	Niedrig
Neu		5.0	Auf SRI-Unterstützung (Subresource Integrity) prüfen	Niedrig
Neu		5.0	Im Cache speicherbare SSL-Seite gefunden	Niedrig
Neu		5.0	Header "Content-Security-Policy" fehlt oder unsicher	Niedrig
Neu		5.0	Weitergabe von Informationen über die Oracle-Protokolldatei	Niedrig
Neu		5.0	Header "Content-Security-Policy" fehlt oder unsicher	Niedrig
Neu		5.0	Header "X-Content-Type-Options" fehlt oder unsicher	Niedrig
Neu		5.0	Header "X-XSS-Protection" fehlt oder unsicher	Niedrig
Neu		5.0	HSTS-Header (HTTP Strict-Transport-Security) fehlt oder unsicher	Niedrig

Security aspects: IBM AppScan



```
app.use(helmet.hsts({
    maxAge: sixtyDaysInSeconds
}));
//CSP
app.use(helmet.contentSecurityPolicy({
    directives: {
        defaultSrc: ["'self'", 'data:'],
        styleSrc: ["'self'", "cdnjs.cloudflare.com", 'maxcdn.bootstrapcdn.com', 'use.fontawesome.com', 'fonts.googleapis.com', "'unsafe-inline'"],
        fontSrc: ["use.fontawesome.com", "fonts.googleapis.com", 'fonts.gstatic.com'],
        scriptSrc: ["'self'", "cdnjs.cloudflare.com"],
        connectSrc: ["'self'", 'wss://localhost:8080', 'wss://objective-euler.mybluemix.net', 'ws://localhost:8080', 'ws://objective-euler.mybluemix.net']
    },
    reportOnly: false
}));
//DNS Prefetch Control
app.use(helmet.dnsPrefetchControl());
//XSS Filter
app.use(helmet.xssFilter());
//IE No Open
app.use(helmet.ieNoOpen());
//No Sniff MIME Type
app.use(helmet.noSniff());
//Hide powered by
app.use(helmet.hidePoweredBy());
//Frameguard
app.use(helmet.frameguard({ action: 'deny' }));
```

Security aspects: IBM AppScan



objective-euler.mybluemix.net

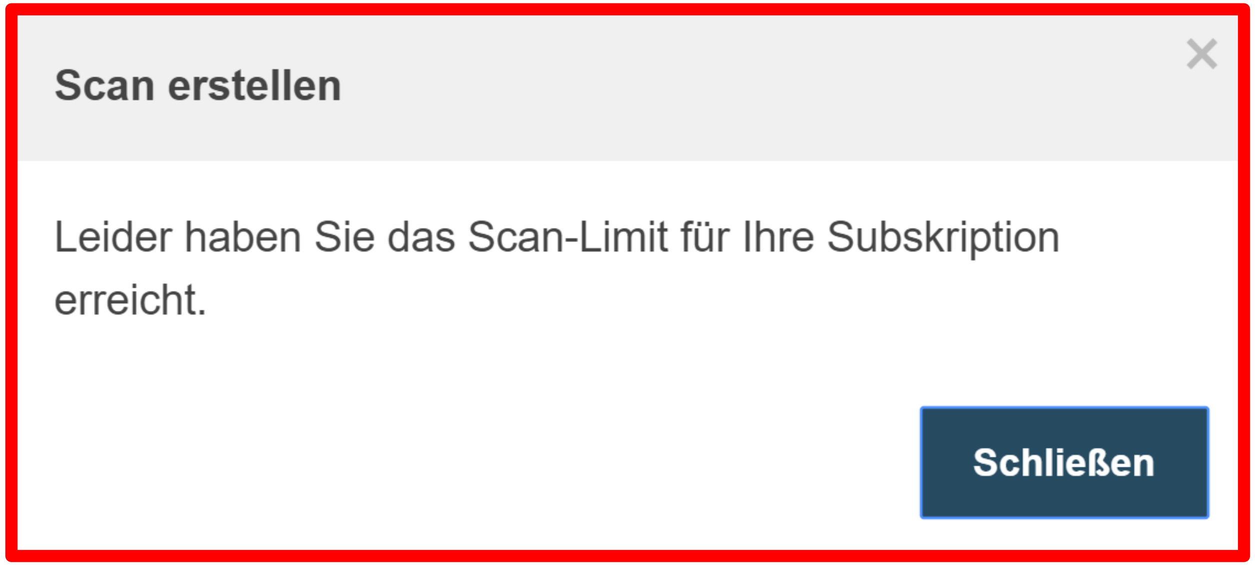
Scan start: 30.11.2018, 00:03:15

Scan end: 30.11.2018, 05:44:03

Duration: 5.7 Stunden

Rescanned: 4 times

Gesamte Probleme	Hoch	Mittel	Niedrig	Info
17	0	1	15	1



Scan erstellen

Leider haben Sie das Scan-Limit für Ihre Subskription erreicht.

Lesson learnt

- Connecting cloud services
- Connecting a CloudSQL database with a Node application, sending and receiving data from and to the database
- Using deprecated cloud services can be tricky
- Security flags and headers are crucial for running a web applications safely

Live Demo

https://objective-euler.mybluemix.net/