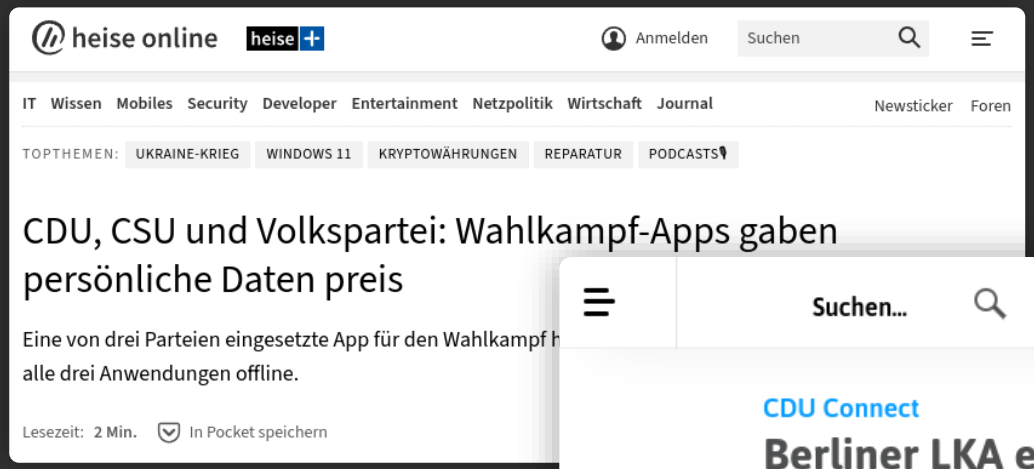
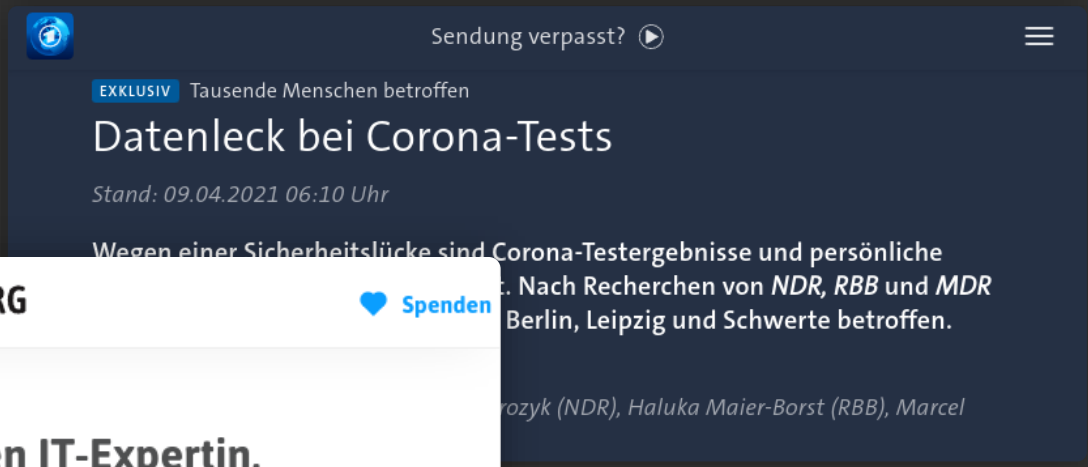
Trust nobody!

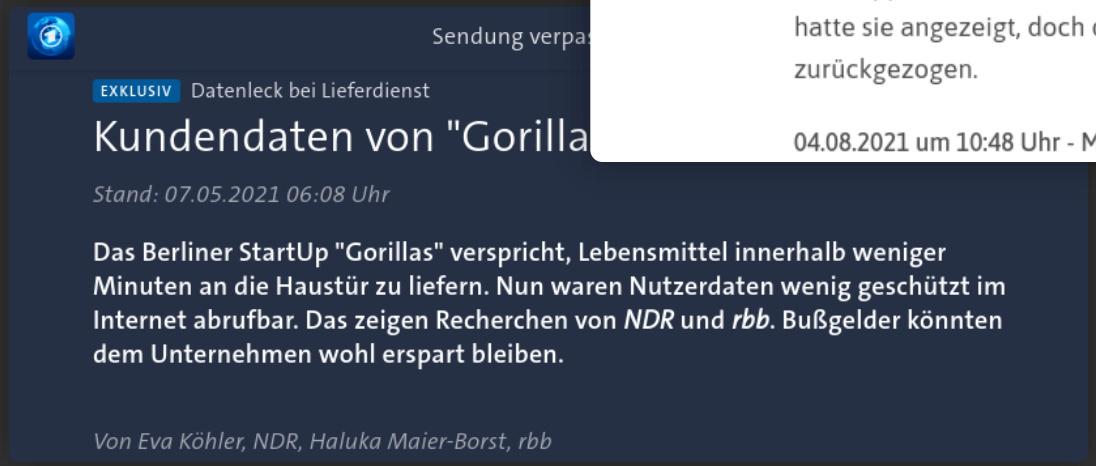
Was zum Thema Cybersecurity alles schiefgehen kann

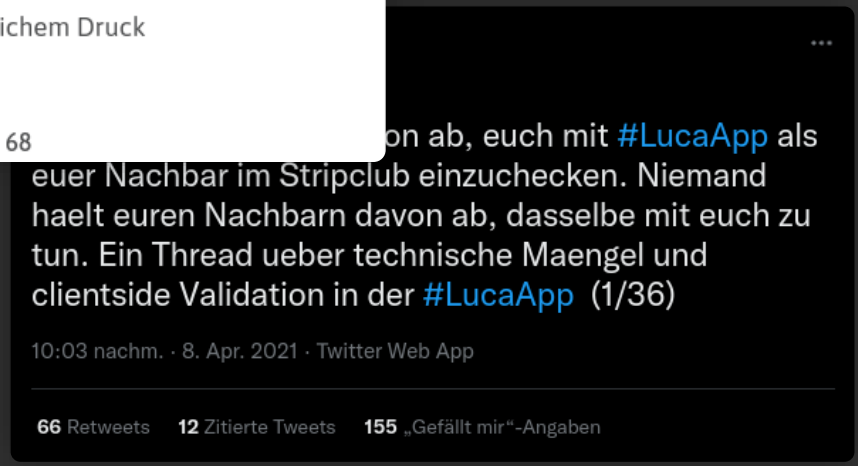
Aaron Schlitt
aaron.schlitt@student.hpi.de
aaronschlitt.de
twitter.com/aaron_sfn
chaos.social/@aaron_els


heise online
heise+
Anmelden
Suchen
IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal
Newsticker Foren
TOPTHEMEN: UKRAINE-KRIEG WINDOWS 11 KRYPTOWÄHRUNGEN REPARATUR PODCASTS
CDU, CSU und Volkspartei: Wahlkampf-Apps gaben persönliche Daten preis
Eine von drei Parteien eingesetzte App für den Wahlkampf h
alle drei Anwendungen offline.
Lesezeit: 2 Min.
In Pocket speichern


Sendung verpasst?
EXKLUSIV Tausende Menschen betroffen
Datenleck bei Corona-Tests
Stand: 09.04.2021 06:10 Uhr
Wegen einer Sicherheitslücke sind Corona-Testergebnisse und persönliche
. Nach Recherchen von NDR, RBB und MDR
Berlin, Leipzig und Schwerte betroffen.
rozyk (NDR), Haluka Maier-Borst (RBB), Marcel


Suchen...
NETZPOLITIK.ORG
Spenden
CDU Connect
Berliner LKA ermittelt gegen IT-Expertin, die Sicherheitslücken in Partei-App fand
Nachdem Lilith Wittmann eine gravierende Sicherheitslücke in einer CDU-App entdeckt hatte, ermittelt nun das LKA gegen sie. Die CDU hatte sie angezeigt, doch die Anzeige jetzt nach öffentlichem Druck zurückgezogen.
04.08.2021 um 10:48 Uhr - Markus Reuter - in Technologie - 68


Sendung verpa
EXKLUSIV Datenleck bei Lieferdienst
Kundendaten von "Gorilla
Stand: 07.05.2021 06:08 Uhr
Das Berliner StartUp "Gorillas" verspricht, Lebensmittel innerhalb weniger Minuten an die Haustür zu liefern. Nun waren Nutzerdaten wenig geschützt im Internet abrufbar. Das zeigen Recherchen von NDR und rbb. Bußgelder könnten dem Unternehmen wohl erspart bleiben.
Von Eva Köhler, NDR, Haluka Maier-Borst, rbb

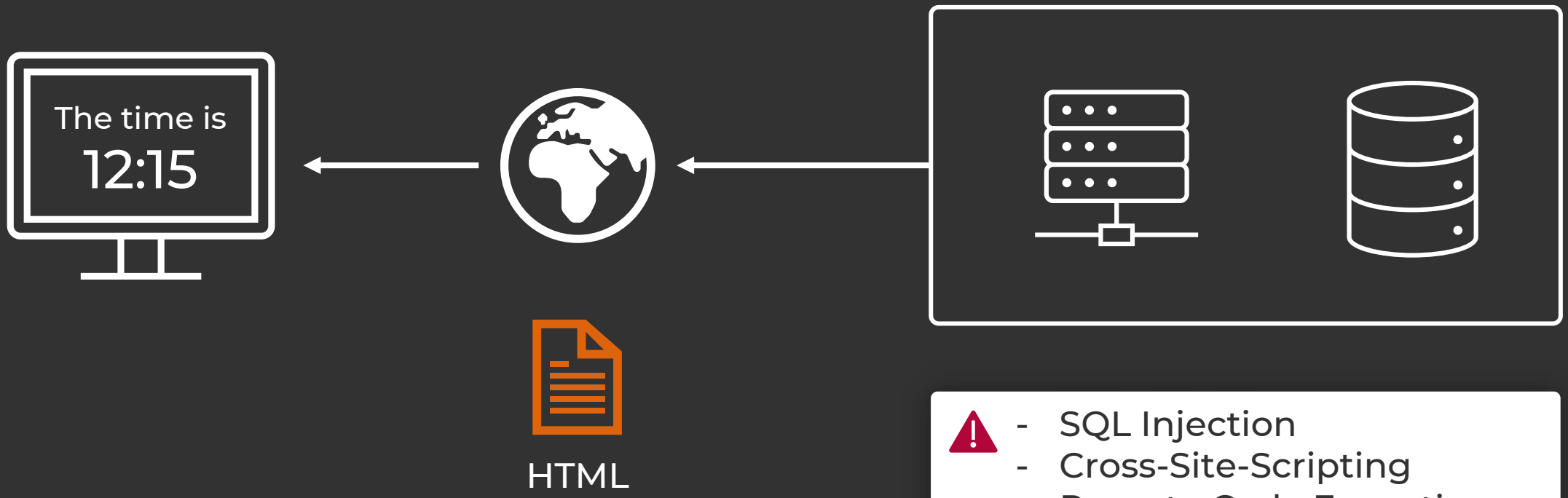

on ab, euch mit #LucaApp als
euer Nachbar im Stripclub einzuchecken. Niemand
haelt euren Nachbarn davon ab, dasselbe mit euch zu
tun. Ein Thread ueber technische Maengel und
clientside Validation in der #LucaApp (1/36)
10:03 nachm. · 8. Apr. 2021 · Twitter Web App
66 Retweets 12 Zitierte Tweets 155 „Gefällt mir"-Angaben

Was ist hier schiefgegangen?

Webanwendungen

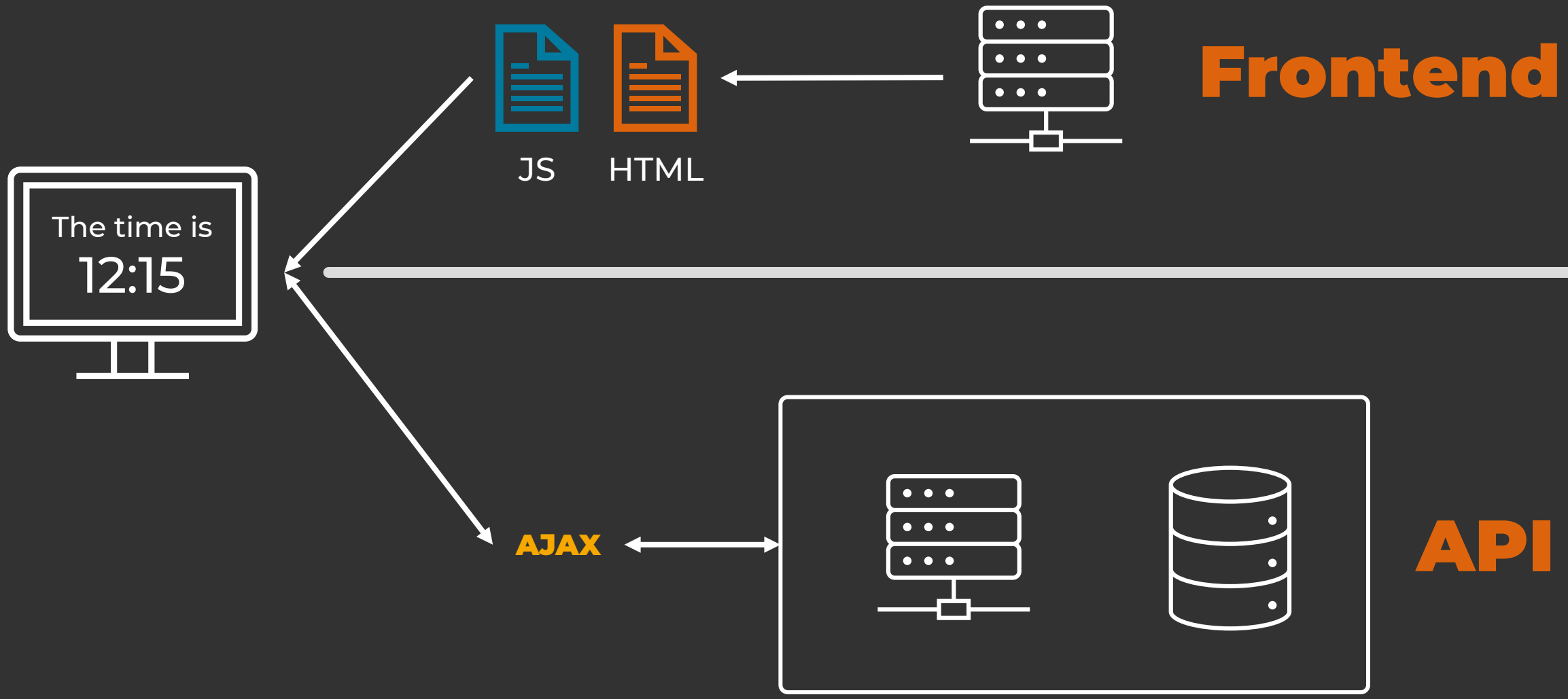
Und wie sie funktionieren

Klassische Webanwendungen



- SQL Injection
- Cross-Site-Scripting
- Remote Code Execution
- ...

Moderne Webanwendungen



Demo-Time!

https://chaos.social/web/home

Und was geht jetzt schief?


HD
tagesschau
Tagesschau, 09.04.2021

https://testzentrum.wtf/api/web/v1/results/export-patient-specific-result-file?report_id=37894

https://testzentrum.wtf/api/web/v1/results/export-patient-specific-result-file?report_id=37894

Was können wir damit machen

0001
0002
0003
0004
0005
0006
0007
0008
0009
0010
0011

- Tausende Betroffene
  - Name
  - Geschlecht
  - Adresse
  - Handynummer
  - E-Mail-Adresse
  - Testergebnis
- Extrahieren der Daten sehr einfach
- Veränderung der Daten zusätzlich möglich

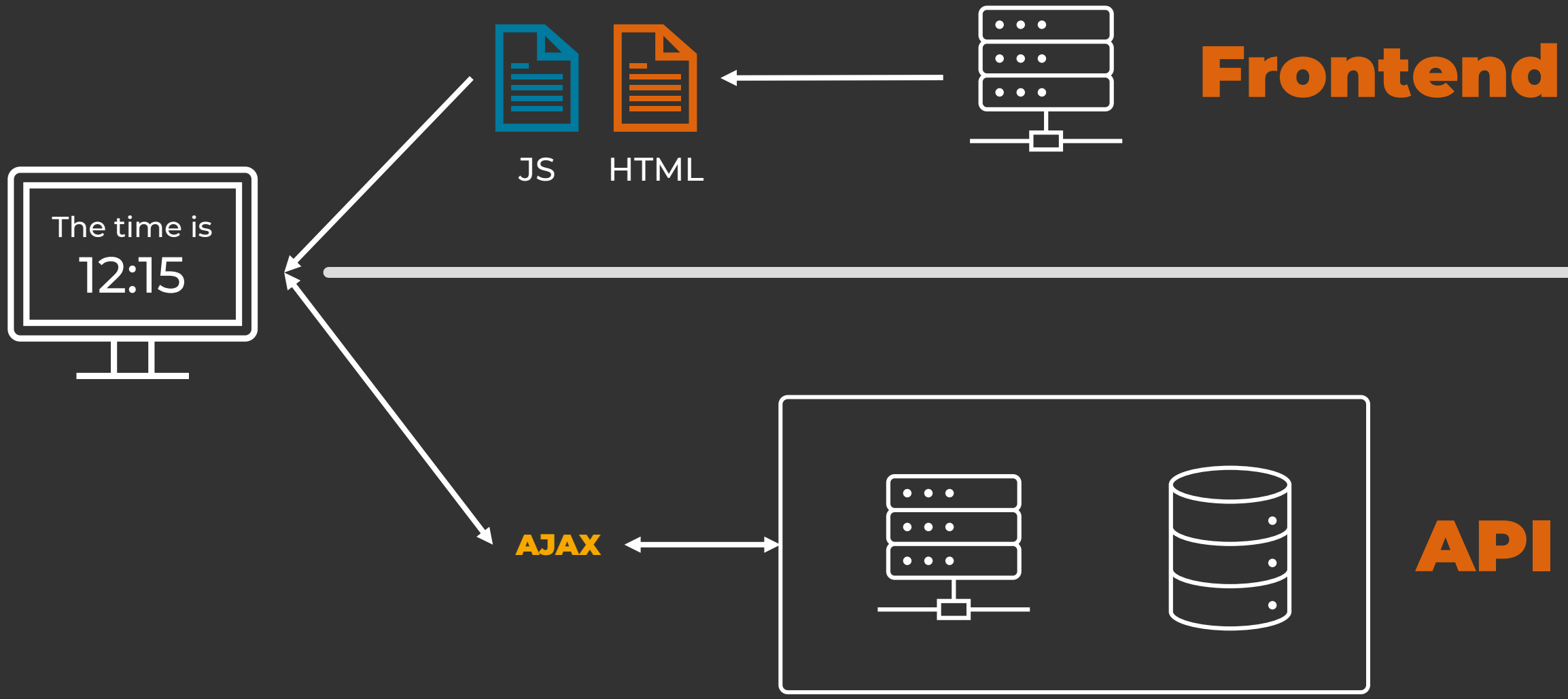
tellonym.me/notsecure

Have fun!

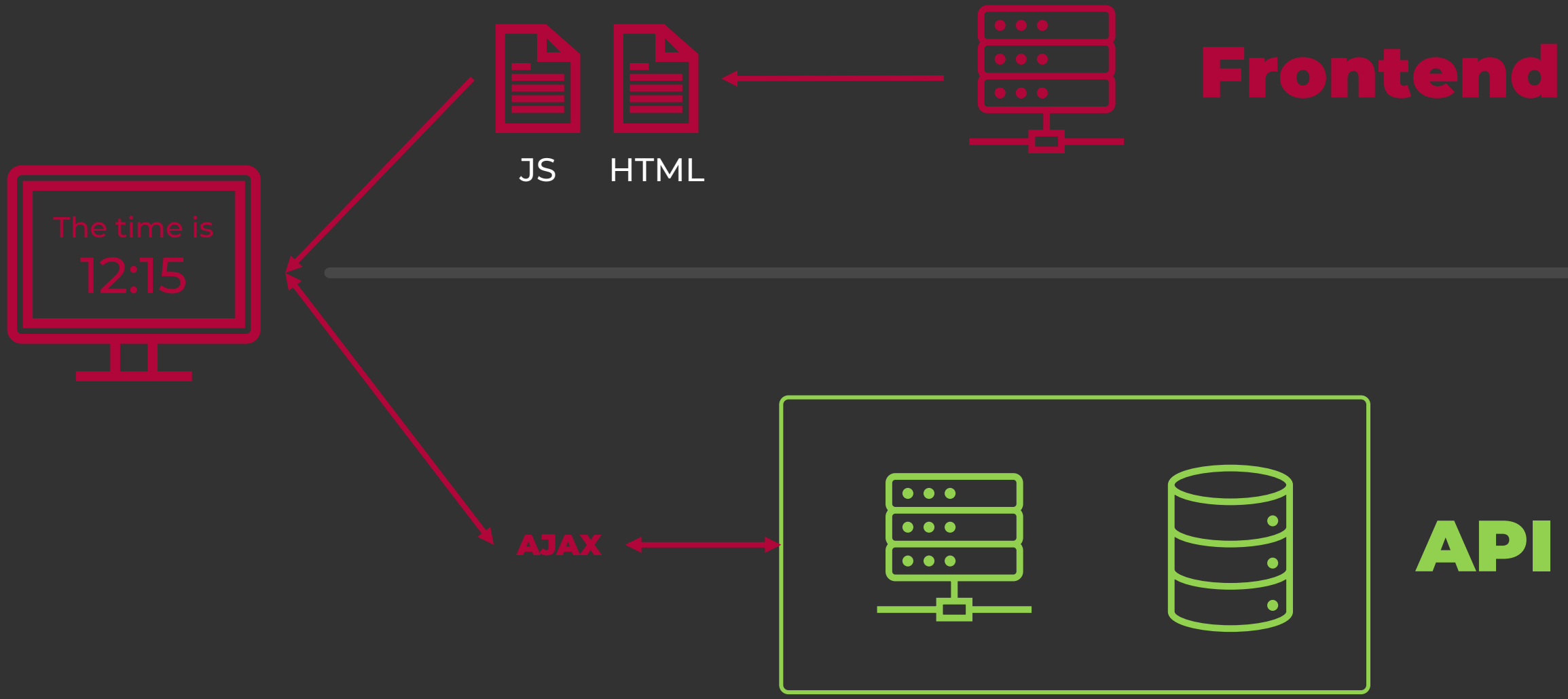
codenight{3vil_h4x0r}

Wie mache ich es besser?

Wem/was kann ich vertrauen?



Wem/was kann ich vertrauen?



Beispiel 1

https://testzentrum.wtf/result/4567

Ansatz 1

- Authentifizierung und Authentisierung

```
result = results.find(4567)
if(result.email == loggedIn.email)
    return result
else
    return "Error“
```

- Sauberste Lösung
- Übertragbar auch auf andere Daten
  - Nutzerprofile
  - Fotos
  - …

Ansatz 2

- Brute Force verhindern

https://testzentrum.wtf/result/
8ngRaLoh7mgLaF8VY3MVe4UfZe4MnJ

Ansatz 3

PLZ

Geburtsdatum

Ergebnis anzeigen

Beispiel 2: Passwort-Reset

Herausforderung: Nachweis über den Besitz einer Mailadresse

Ansatz 1
Nutzer:in schickt eine Mail an uns um zu zeigen, dass ihr die Mailadresse gehört

Ansatz 2
Mail durch unseren Server an Nutzer:in schicken und Nutzer:in einen Code eingeben lassen

Beispiel 2: Passwort-Reset

Herausforderung: Nachweis über den Besitz einer Mailadresse

Ansatz 1
Nutzer:in schickt eine Mail an uns um zu zeigen, dass ihr die Mailadresse gehört

Ansatz 2
Mail durch unseren Server an Nutzer:in schicken und Nutzer:in einen Code eingeben lassen

Beispiel 3: Callcenter

Wer ruft an?

Auch Telefonnummern sind leicht zu fälschen!

Was gibt es noch?

Verschlüsselung

SYN-Flooding

Template Injection

SQL Injection

Cookies

Cross-Site-Scripting

Hashing

DDOS

Server-Side Request Forgery

ARP-Spoofing

Denial of Service

Reverse Engineering

Broken Authentication

Remote Code Execution

Buffer Overflow

Broken Access Control

IP-Spoofing

TLS Downgrade

Phishing

Anderes Spoofing

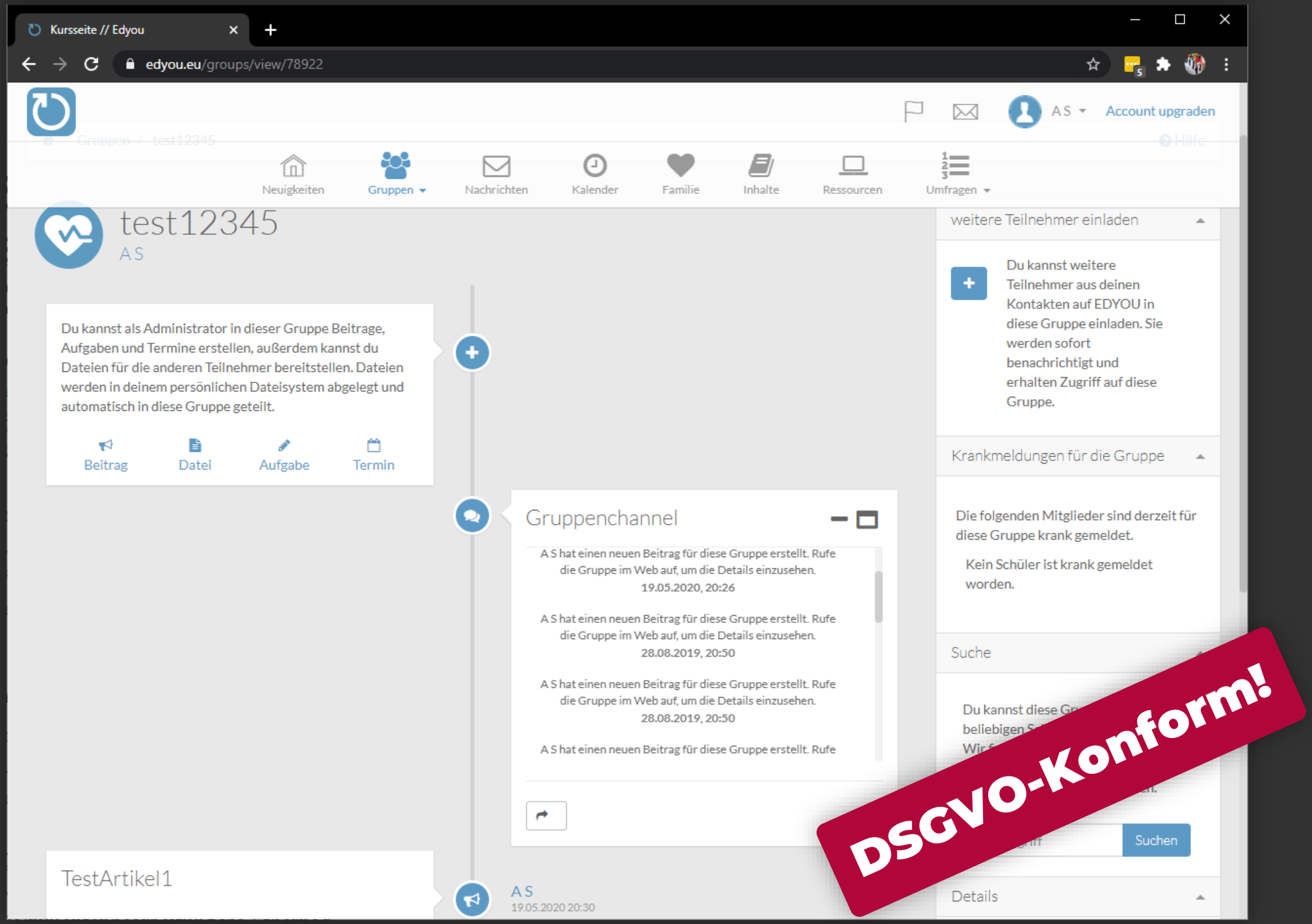
Ups, ich hab da was gefunden!?

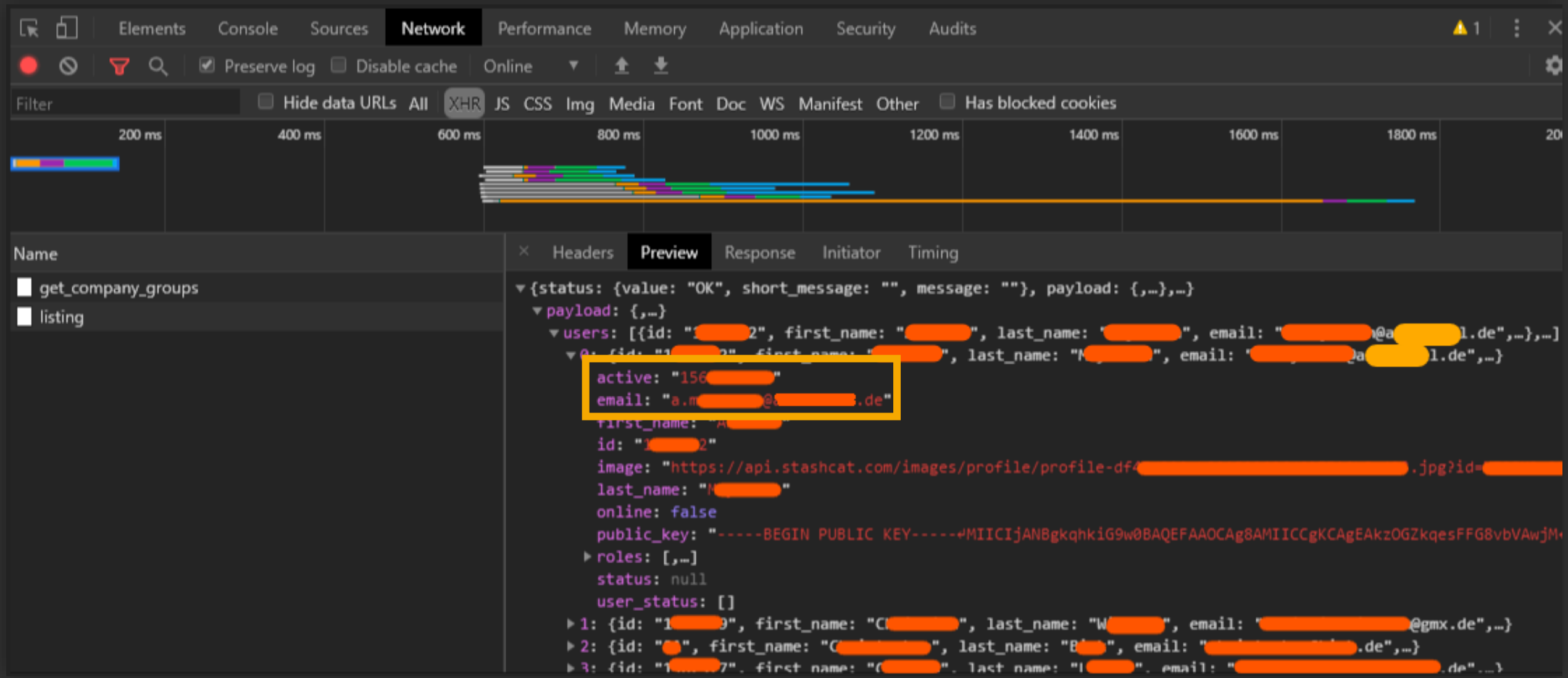
Responsible Disclosure

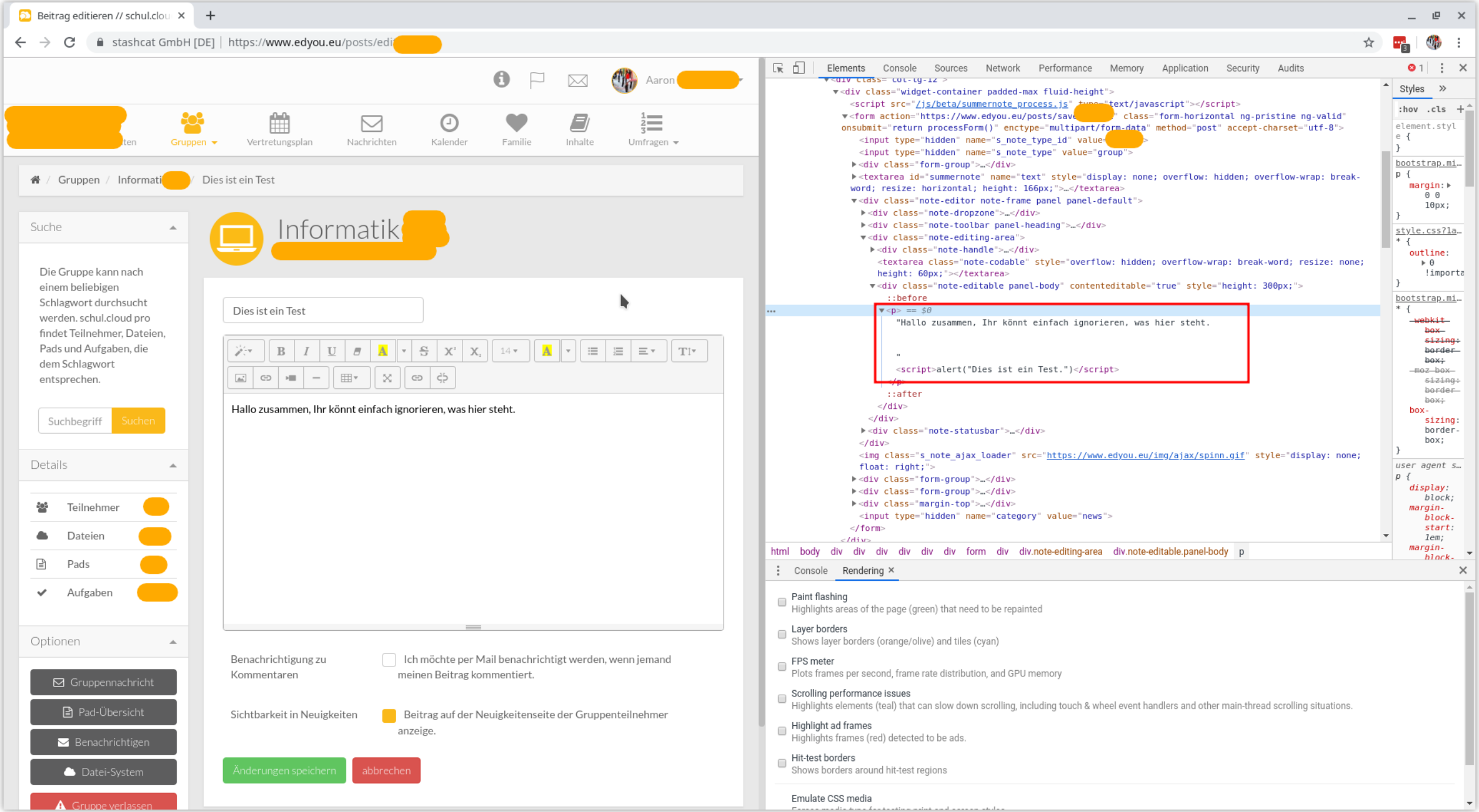
Was bisher geschah...

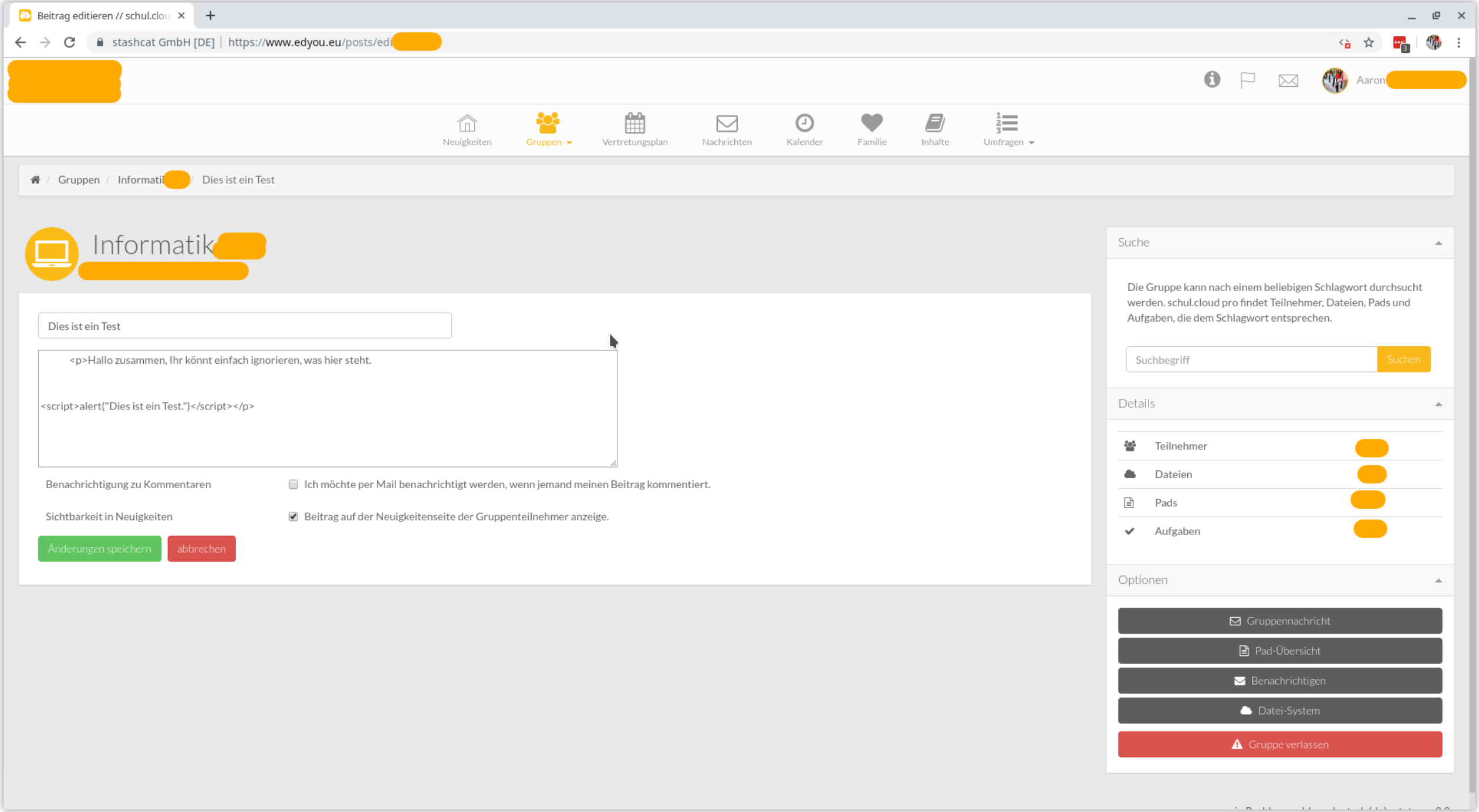
Mai 2020 – Aaron hat gerade sein Abi gemacht

und ihm ist langweilig


Kursseite // Edyou
edyou.eu/groups/view/78922
AS
Account upgraden
Neuigkeiten
Gruppen
Nachrichten
Kalender
Familie
Inhalte
Ressourcen
Umfragen
test12345
AS
Du kannst als Administrator in dieser Gruppe Beitrage, Aufgaben und Termine erstellen, außerdem kannst du Dateien für die anderen Teilnehmer bereitstellen. Dateien werden in deinem persönlichen Dateisystem abgelegt und automatisch in diese Gruppe geteilt.
Beitrag
Datei
Aufgabe
Termin
Gruppenchannel
A S hat einen neuen Beitrag für diese Gruppe erstellt. Rufe die Gruppe im Web auf, um die Details einzusehen.
19.05.2020, 20:26
A S hat einen neuen Beitrag für diese Gruppe erstellt. Rufe die Gruppe im Web auf, um die Details einzusehen.
28.08.2019, 20:50
A S hat einen neuen Beitrag für diese Gruppe erstellt. Rufe die Gruppe im Web auf, um die Details einzusehen.
28.08.2019, 20:50
A S hat einen neuen Beitrag für diese Gruppe erstellt. Rufe
TestArtikel1
AS
19.05.2020 20:30
weitere Teilnehmer einladen
Du kannst weitere Teilnehmer aus deinen Kontakten auf EDYOU in diese Gruppe einladen. Sie werden sofort benachrichtigt und erhalten Zugriff auf diese Gruppe.
Krankmeldungen für die Gruppe
Die folgenden Mitglieder sind derzeit für diese Gruppe krank gemeldet.
Kein Schüler ist krank gemeldet worden.
Suche
Suchen
Details
DSGVO-Konform!


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
200 ms
400 ms
600 ms
800 ms
1000 ms
1200 ms
1400 ms
1600 ms
1800 ms
Name
get_company_groups
listing
Headers
Preview
Response
Initiator
Timing
{status: {value: "OK", short_message: "", message: ""}, payload: {,…},…}
payload: {,…}
users: [{id: "
active: "156
email: "a.m
id: "
image: "https://api.stashcat.com/images/profile/profile-df
.jpg?id=
last_name: "
online: false
public_key: "-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkzOGZkqesFFG8vbVAwjM
roles: [,…]
status: null
user_status: []
1: {id: "
@gmx.de",…}
2: {id: "
.de",…}


Beitrag editieren // schul.clou
stashcat GmbH [DE] | https://www.edyou.eu/posts/edi
Aaron
Gruppen
Vertretungsplan
Nachrichten
Kalender
Familie
Inhalte
Umfragen
Gruppen / Informati / Dies ist ein Test
Suche
Die Gruppe kann nach einem beliebigen Schlagwort durchsucht werden. schul.cloud pro findet Teilnehmer, Dateien, Pads und Aufgaben, die dem Schlagwort entsprechen.
Suchbegriff
Suchen
Details
Teilnehmer
Dateien
Pads
Aufgaben
Optionen
Gruppennachricht
Pad-Übersicht
Benachrichtigen
Datei-System
Gruppe verlassen
Informatik
Dies ist ein Test
Hallo zusammen, Ihr könnt einfach ignorieren, was hier steht.
Benachrichtigung zu Kommentaren
Ich möchte per Mail benachrichtigt werden, wenn jemand meinen Beitrag kommentiert.
Sichtbarkeit in Neuigkeiten
Beitrag auf der Neuigkeitenseite der Gruppenteilnehmer anzeige.
Änderungen speichern
abbrechen
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
"Hallo zusammen, Ihr könnt einfach ignorieren, was hier steht.
<script>alert("Dies ist ein Test.")</script>
Styles
Console
Rendering
Paint flashing
Highlights areas of the page (green) that need to be repainted
Layer borders
Shows layer borders (orange/olive) and tiles (cyan)
FPS meter
Plots frames per second, frame rate distribution, and GPU memory
Scrolling performance issues
Highlights elements (teal) that can slow down scrolling, including touch & wheel event handlers and other main-thread scrolling situations.
Highlight ad frames
Highlights frames (red) detected to be ads.
Hit-test borders
Shows borders around hit-test regions
Emulate CSS media


Beitrag editieren // schul.clou
stashcat GmbH [DE] | https://www.edyou.eu/posts/ed
Aaron
Neuigkeiten
Gruppen
Vertretungsplan
Nachrichten
Kalender
Familie
Inhalte
Umfragen
Gruppen / Informati / Dies ist ein Test
Informatik
Dies ist ein Test
Hallo zusammen, Ihr könnt einfach ignorieren, was hier steht.
<script>alert("Dies ist ein Test.")</script>
Benachrichtigung zu Kommentaren
Ich möchte per Mail benachrichtigt werden, wenn jemand meinen Beitrag kommentiert.
Sichtbarkeit in Neuigkeiten
Beitrag auf der Neuigkeitenseite der Gruppenteilnehmer anzeige.
Änderungen speichern
abbrechen
Suche
Die Gruppe kann nach einem beliebigen Schlagwort durchsucht werden. schul.cloud pro findet Teilnehmer, Dateien, Pads und Aufgaben, die dem Schlagwort entsprechen.
Suchbegriff
Suchen
Details
Teilnehmer
Dateien
Pads
Aufgaben
Optionen
Gruppennachricht
Pad-Übersicht
Benachrichtigen
Datei-System
Gruppe verlassen

home // schul.cloud pro

stashcat GmbH [DE] | https://www.edyou.eu/dashboard

www.edyou.eu says

Dies ist ein Test.

OK

Aaron

Neuigkeiten Gruppen Inhalte Umfragen

Optionen

Wir laden deine Neuigkeiten.
Bitte hab' einen Moment Geduld.

Sollten in Kürze keine Neuigkeiten angezeigt werden, versuch einmal die Seite neu zu laden und überprüfe ob die JavaScript-Ausführung deines Browsers aktiv ist.

ein Problem melden · deutsch (du) · status · v2.0

https://edyou.eu/index.php

```
<div id="device_id" style="display:none;">Browser5xxxxxx57</div>
<div id="client_key" style="display:none;">ca8xxxxxxxxxxxxxx8q</div>
```

Joa, das sind Zugangsdaten...

Wofür?
Für alles!

Was nun?

- Wir haben Möglichkeit, ...
  - ... private E-Mail-Adressen von Schüler:innen und Lehrer:innen zu lessen
  - ... herauszufinden, wann Nutzer:innen zuletzt online waren
  - ... Mit einer Chat-Nachricht Nutzer:innen einfach auszuloggen
  - ... Zugriff auf Daten von beliebigen Nutzer:innen einer Schule zu bekommen

Responsible Disclosure!

- Finden und Dokumentieren der Sicherheitslücken
- Keine direkte Kontaktmöglichkeit für Security-Probleme
- Also: PDF per Mail an Kundensupport und allgemeine Kontaktadresse

19. Mai 2020

...

Ich frage mal an meiner Schule nach.

27. Mai 2020

- Noch immer keine Rückmeldung an mich
- Ich frage nochmal beim Hersteller nach

5. Juni 2020

- Man will mit mir telefonieren!

11. Juni 2020

- Das Telefonat!

12. Juni 2020

37 Tage!

Bis zur ersten inhaltlichen Rückmeldung

Fehlende Kontaktmöglichkeiten für Sicherheitsforschende

- Rollout erster Fixes

13. Juni 2020

Unsaubere Behebung bei vergangenen Sicherheitsmeldungen

Noch einmal zusammengefasst

Seid Euch bewusst, was **schiefgehen** kann

Kein Problem solange keine **personenbezogenen Daten**

Wenn Ihr produktive Software schreibt: Schafft eine sinnvolle **Fehlerkultur**

Vertraut bei Sicherheit nicht auf **Online-Tutorials**!

Danke fürs Zuhören!

Fragen?

Aaron Schlitt
aaron.schlitt@student.hpi.de
aaronschlitt.de
twitter.com/aaron_sfn
chaos.social/@aaron_els

Weitere Infos, Folien, …
https://aaronschlitt.de/cn22