Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Hausarbeit

Informationsrecherche im Internet

Alexey Wetz 404187
Maurice Molt 402042
Markus Klemm 408833
Studiengang Bachelor IT-Forensik

Aufgabenstellung

In erster Linie sollen die frei zugänglichen Informationen einer Institution im Internet (OSINT-Recherche) unter Hinzuziehung von automatisierten Tools ausgekundschaftet werden.

Des Weiteren soll eine gezielte Informationsgewinnung durch den Einsatz von Google-Hacking und Erweiterung der Recherchen bis hin zum Darknet stattfinden.

Zuletzt soll zusätzlich eine Prüfung der SEO-basierenden Eigenschaften sowie ggf. eine darauffolgende Ausarbeitung von Optimierungsmöglichkeiten stattfinden.

Inhalt

1 Einleitung

Gut vorbereitet ist halb gehacked – so könnte eines der Sprichwörter aus der deutschen Sprache für das digitale Zeitalter umgedichtet werden.

In der Tat besteht ein gut geplanter Hacking-Angriff zum Großteil aus der vorhergehenden Informationsgewinnung zum entsprechenden Zielobjekt. Der Angriff selbst ist nur das Resultat einer zielgerichteten, nachhaltigen und umfassenden Informationsrecherche, teilweise bis über die Grenzen des Surface Webs hinaus.

In dieser Ausarbeitung werden Mittel und Wege dargestellt, wie man eine solche Recherche zielgerichtet realisiert.

Für die Durchführung der Recherchen wird die Webseite des Sportvereins *‚VTV Mundenheim 1883 e.V.‘* (https://vtv-mundenheim.de) verwendet.

2 OSINT (Footprints-Recherche)

Das Internet vergisst nichts – ein Satz, der oft im Zusammenhang mit den im Internet veröffentlichten Inhalten verwendet wird. In erster Linie wird dabei der Bezug zum Datenschutz hergestellt, wobei man zwangsläufig an diverse Social-Media-Plattformen denken muss. Allerdings sind die Gefahren des „Nichtvergessens“ genauso gut auf Webseiten übertragen werden, bei denen man nicht direkt an personenbezogene Daten oder vom User unbeabsichtigt verbreiteten Informationen denkt.

Die sog. „Footprints“ (engl. Fußstapfen) helfen dabei in der Gesamtheit aller einzeln gewonnen Erkenntnisse ein gewisses Profil der betroffenen Infrastruktur (z.B. Webseite/Webserver) zu erstellen. Diese Informationen können, zusammen mit evtl. aus der SOCMINT-Recherche oder durch Social Engineering gewonnen Erkenntnissen, anschließend verwendet werden, um den Eigentümern der Webseite zu schaden (bspw. Hacking-Angriff).

Nachfolgend werden einige Tools für eine zielgerichtete OSINT-Recherche, sowie die Ergebnisse nach der Ausführung dieser, vorgestellt. Die entsprechenden Informationen könnten theoretisch auch durch eine manuelle Suche ermittelt werden, was allerdings einen zeitlichen Mehraufwand nach sich ziehen würde, so dass die automatisierte Informationsgewinnung den Vorzug erhält.

2.1 Konzeption

Im Internet kann eine Vielzahl von OSINT-Tools, kostenlos und kommerziell, vorgefunden werden. Das liegt v.a. daran, dass die meisten Tools auf dem Betriebssystem Linux basieren und dessen Code somit auch als „Open Source“ gehandelt wird.

Bevor die OSINT-Tools ausgewählt werden, wird erörtert, welche Informationen von der Webseite zielführend wären. Zielführend bedeutet hierbei, dass man unter der Verwendung dieser Informationen einen möglichen Hacking/Phishing-Versuch unternehmen können sollte.

Um die Vorgehensweise besser darstellen zu können soll ein Vergleich von einem Hacker zu einem „analogen“ Einbrecher gezogen werden.

Bei der Planung des Einbruchs sind u.a. folgende Informationen von Nöten:

Einbrecher	Hacker
Hausanschrift/-adresse	IP-Adresse(n)
Zugangswege	Subdomains
Schlüssel	Ports/Passwörter
Gekippte Fenster/Türen	Software-Schwachstellen
Kenntnisse über Bewohner(-routinen)	Namen, Mailadressen, Verwendung Software

Tabelle 1 Vergleich Einbrecher – Hacker

2.2 Auswahl der Tools

Unter der Berücksichtigung der o.g. Kriterien wurden die folgenden Tools ausgesucht. Es wurde dabei bewusst auf Hinzuziehung von SOCMINT-Tools verzichtet, weil sich dadurch der Umfang dieser Ausarbeitung deutlich vergrößern würde.

2.2.1 Wappalyzer

Bei dem Firefox-Addon ‚Wappalyzer‘ handelt es sich um ein API-basierendes Tool zum Durchführen von „Webseiten-Profiling“. Damit kann man sich direkt beim Aufrufen der Webseite einen Überblick über das Backend und ggf. die verwendete Software, inkl. Softwareversion, verschaffen.

Einsatz

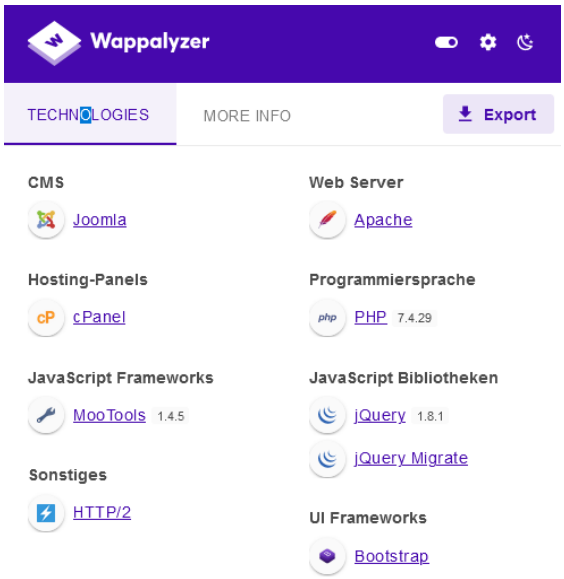


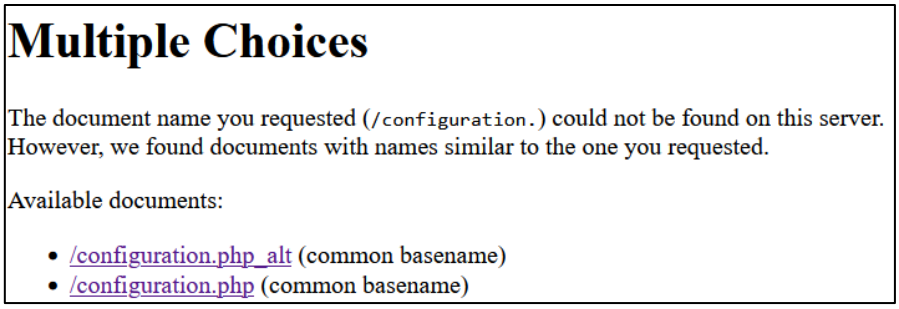
Abbildung 1 Wappalyzer auf vtv-mundenheim.de

Erkenntnis

Die Haupterkenntnis kann hier auf das verwendete CMS ‚Joomla' und die verwendete Programmiersprache PHP zurückgeführt werden.

Immer öfter werden unter ‚Joomla' Sicherheitslücken und Schwachstellen bekannt, die für einen gezielten Angriff benutzt werden können. Zusammen mit dem Wissen, wie die Ordner-/Dateistruktur auf dem Webserver im Normalfall auszusehen hat wurde diese Erkenntnis wie folgt eingesetzt.

Aufrufen von https://vtv-mundenheim.de/configuration. im Internetbrowser liefert folgende Ausgabe:



Multiple Choices

The document name you requested (`/configuration.`) could not be found on this server. However, we found documents with names similar to the one you requested.

Available documents:

- /configuration.php_alt (common basename)
- /configuration.php (common basename)

Abbildung 2 Multiple Choices in Joomla

Da die entsprechende Datei auf dem Webserver nicht vorgefunden wurde, wird man durch ‚Joomla' darauf hingewiesen, dass man ähnliche Dateinamen vorliegen hat.

Aufruf von *configuration.php* liefert eine weiße Seite.

Aufruf von *configuration.php_alt* ruft den kompletten Quellcode der Konfigurationsdatei auf. Um nicht auf den kompletten Inhalt der Datei einzugehen werden die drei relevantesten Erkenntnisse aus dieser beispielhaft dargestellt.

```
public $host = 'db446673090.db.1and1.com';
public $lifetime = '15';
public $list_limit = '20';
public $live_site = '';
public $log_path = '/homepages/42/d17324383/htdocs/VTV2014/logs';
```

Abbildung 3 Datenbank Host + Ordnerstruktur

```
public $session_redis_server_host = 'localhost';
public $session_redis_server_port = '6379';
public $session_redis_server_auth = '';
public $session_redis_server_db = '0';
public $shared_session = '0';
```

Abbildung 4 Intern genutzter Port

```
public $password = 'munnerem1883';
public $robots = '';
public $secret = 'CPa35ZGXkqKPeYpzO6VqepYxDgfyNHXO';
```

Abbildung 5 Passwort in Klartext

Auch wenn es sich hierbei offensichtlich um eine veraltete Konfigurationsdatei handelt, besteht eine hohe Wahrscheinlichkeit, dass das Passwort unverändert in der neuen Konfiguration übernommen wurde.

2.2.2 host.io

Hierbei handelt es sich um einen kommerziellen Dienstleister, der Abfragen zu Domains/Webhosts sehr übersichtlich aufarbeitet. Da es möglich ist eine kostenlose Abfrage pro Tag zu machen, wurde diese Tool für eine Art „qualifizierte" WHOIS-Abfrage verwendet.

Einsatz

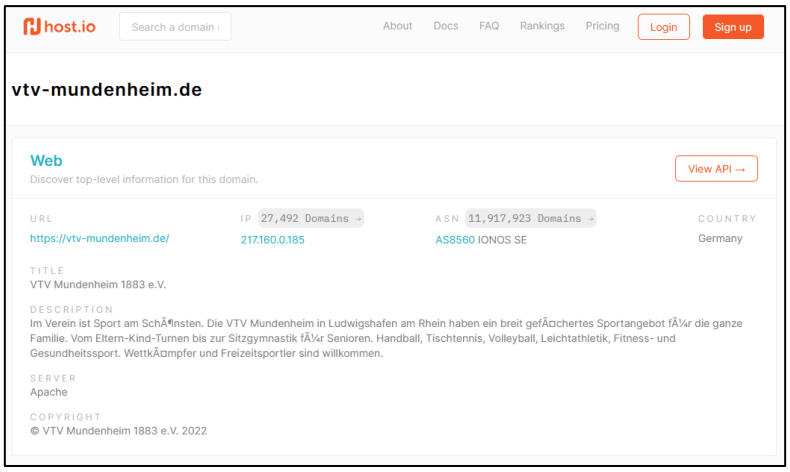


Abbildung 6 host.io Web-Infos

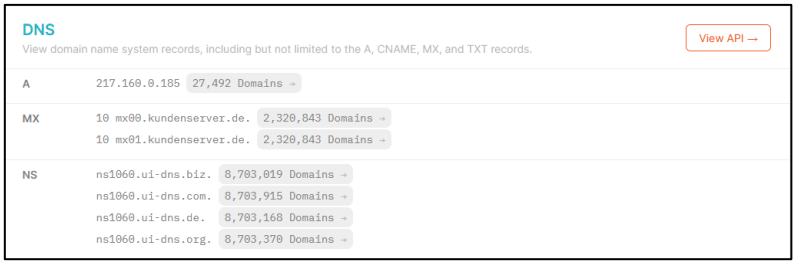


Abbildung 7 host.io DNS-Infos

Abbildung 8 host.io Co-Hosted

Abbildung 9 host.io Links

Erkenntnis

Anhand der gelieferten Informationen lässt sich ableiten, dass die Domain vtv-mundenheim.de bei einem großen Anbieter gehosted wird. Ein Übergriff auf die anderen Co-Hosted Webserver gilt deshalb als unwahrscheinlich.

Eine interessente Erkenntnis liefern dabei die auf der Webseite verfügbaren Weiterleitungen/Verlinkungen (*s. ‚Abbildung 9 host.io Links'*). Die Links könnten als solche missbraucht bzw. verändert werden und den User auf eine gefälschte Webseite zu locken, um seine Daten abzufangen.

2.2.3 Knockpy

Dieses Linux-basierte Tool prüft die TLD auf mögliche Subdomains mit einem „Wörterbuchangriff". Dabei werden alle bekannten Subdomains in alphabetischer Reihenfolge abgefragt und bei einer erfolgreichen Antwort des Hosts protokolliert.

Einsatz

Abbildung 10 Ausführung Knockpy

Erkenntnis

IP	Status	Typ	Subdomain	Server
217.160.0.159	302 (Found)	host	email.vtv-mundenheim.de	Apache
212.227.247.139	403 (Forbidden)	host	ftp.vtv-mundenheim.de	Apache
217.160.0.159	302 (Found)	host	sanantonio.vtv-mundenheim.de	Apache
217.160.0.185	301 (Moved Permanently)	host	www.vtv-mundenheim.de	Apache

Tabelle 2 Subdomain-Analyse

2.2.4 GetIPInfo

Aus der vorhergehenden Subdomain-Analyse wurde bekannt, dass zwei weitere IP-Adressen mit der eigentlichen TLD vtv-mundenheim.de in Verbindung gebracht werden können. Mit dem Tool ‚GetIPInfo' können mehrere, in einer Liste aufgeführten, IP-Adressen gleichzeitig abgefragt werden.

Einsatz

Hierfür wird eine CSV-Datei mit den vorliegenden IP-Adressen angelegt und beim Ausführen des Tools adressiert.

Erkenntnis

Die kombinierte WHOIS-Abfrage lieferte keine neuen, relevanten Erkenntnisse. Bei allen drei IP-Adresse erhält man folgende Informationen (am Beispiel für die IP-Adresse 217.160.0.159) zum Host:

success, Germany, DE, NW, North Rhine-Westphalia, Essen, 45127, 51.4556,7.01156, Europe/Berlin, IONOS SE, Ionos, AS8560 IONOS SE, "217.160.0.159

2.2.5 Tekdefense

Mit Hilfe des Linux-Tools ‚Tekdefense' lässt sich eine Übersicht über potenzielle Schwachstellen erstellen, die durch Software-Installationen auf dem Host verursacht werden.

Einsatz

Ausführen den Scripts/Tools unter Linux mit der Eingabe der Domain.

Erkenntnis

```
_____________________          Results found for: vtv-mundenheim.de
No results found in the FNet URL
No results found in the Un Redirect
[+] IP from URLVoid: No results found
[+] Blacklist from URLVoid: No results found
[+] Domain Age from URLVoid: No results found
[+] Geo Coordinates from URLVoid: No results found
[+] Country from URLVoid: No results found
[+] pDNS data from VirusTotal: No results found
[+] pDNS malicious URLs from VirusTotal: No results found
[+] Malc0de Date: No results found
[+] Malc0de IP: No results found
[+] Malc0de Country: No results found
[+] Malc0de ASN: No results found
[+] Malc0de ASN Name: No results found
[+] Malc0de MD5: No results found
No results found in the THIP
[+] McAfee Web Risk: No results found
[+] McAfee Web Category: No results found
[+] McAfee Last Seen: No results found
```

Abbildung 11 Tekdefense - no results

Bei dem durchgeführten Scan konnten keine Software-Schwachstellen festgestellt werden.

2.2.6 Nmap

‚Nmap' ist ein weitverbreitetes Linux-Tool zum Durchführen von automatisierten Portscans in einem Netzwerk.

Einsatz

Die Ausführung findet in der Linux-Konsole mit root-Rechten statt. Neben den Ports wird die Antwortzeit (Latenz) sowie der rDNS ermittelt.

```
[redacted]$ sudo nmap -sSV -T4 vtv-mundenheim.de
[sudo] Passwort für [redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-15 13:57 CEST
Nmap scan report for vtv-mundenheim.de (217.160.0.185)
Host is up (0.013s latency).
rDNS record for 217.160.0.185: 217-160-0-185.elastic-ssl.ui-r.com
Not shown: 996 filtered ports
PORT      STATE  SERVICE  VERSION
80/tcp    open   http     nginx
81/tcp    open   http     nginx
443/tcp   open   ssl/http nginx
50001/tcp closed unknown
```

Abbildung 12 nmap

<u>Erkenntnis</u>

Erwartungsgemäß befinden sich in der Liste der geöffneten Ports die klassischen HTTP (80; 81) und HTTPS (443) Ports.

Des Weiteren wurde ein geschlossener Port (50001) identifiziert. Dieser könnte eine zusätzliche Angriffsfläche bieten.

2.2.7 Metagoofil

Eine weitere Quelle der Informationen bieten die auf den Servern hinterlegten Dokument-Dateien (.pdf; .docx; …). Die daraus gewonnenen Erkenntnisse bieten v.a. eine gute Vorlage für die, theoretisch, weitergehenden SOCMINT-Recherchen und Social-Engineering „Attacken“.

<u>Einsatz</u>

Durch den Einsatz von ‚Metagoofil‘ wird die gesamte Webseite nach den vorhandenen Dateien gescannt und die dort gespeicherten Information (z.B. Erfasser des Dokuments) protokolliert.

<u>Erkenntnis</u>

Nachfolgend werden drei ausgewählte Ausschnitte aus der Gesamtliste vorgestellt.

```
Dateiname                          : Datenschutz fuer Mitglieder.pdf
Verzeichnis                        : [redacted]
Dateigröße                         : 79 kB
Datum/Uhrzeit der Dateiänderung    : 2022:06:01 10:01:50+02:00
Datum/Uhrzeit des letzten Dateizugriffs: 2022:06:01 10:01:50+02:00
Datum/Uhrzeit der letzten Inode Änderung: 2022:06:01 10:01:50+02:00
Dateiberechtigungen                : rw-r--r--
Dateityp                           : PDF
File Type Extension                : pdf
MIME-Typ                           : application/pdf
PDF Version                        : 1.7
Linearized                         : No
Page Count                         : 5
Sprache                            : de-DE
Tagged PDF                         : Yes
XMP Toolkit                        : 3.1-701
Produzent                          : Microsoft® Word für Microsoft 365
Ersteller                          : [redacted]
Erstellertool                      : Microsoft® Word für Microsoft 365
Digitalisierungsdatum/-uhrzeit     : 2020:11:14 14:15:19+01:00
Änderungsdatum                     : 2020:11:14 14:15:19+01:00
Document ID                        : uuid:7BAF9689-BA7B-4B1B-ACC2-DB35405990ED
Instance ID                        : uuid:7BAF9689-BA7B-4B1B-ACC2-DB35405990ED
Autor                              : [redacted]
```

Abbildung 13 Metagoofil 1

```
Erstellertool                      : PDFCreator 3.3.2.3528
Document ID                        : uuid:2846eaf3-fc28-11ea-0000-ebb83aa65b74
Format                             : application/pdf
Titel                              : Hygienekonzept TT2020 erkärung neu
Ersteller                          : [redacted]
Beschreibung                       :
Autor                              : [redacted]
```

Abbildung 14 Metagoofil 2

```
Enabled: True
Site Id: e4e1abd9-eac7-4a71-ab52-da5c998aa7ba
Owner: [redacted]
Set Date: 2020-08-27T15:20:40.6162302Z
Name: C1 - Internal use
Application: Microsoft Azure Information Protection
Action Id: 7a5f2ad3-dd0e-4f74-bbeb-dff20941c39c
Extended MSFT Method: Automatic
```

Abbildung 15 Metagoofil 3

Allein anhand der o.g. Beispiele konnten drei Klarpersonalien festgestellt werden, die für die SOCMINT-Recherche verwendet werden können. Beim dritten Beispiel ist sogar die, vermutlich, Arbeitsmailadresse des Erstellers einsehbar.

Des Weiteren können Rückschlüsse auf die Benutzung von Software/Apps der jeweiligen Ersteller gezogen werden.

2.2.8 Spiderfoot

Zuletzt wird ein kleiner Einblick in das wohl „mächtigste“ Tool dieser Ausarbeitung gegeben. Bei ‚Spiderfoot‘ handelt es sich um eine großflächige Informationssammlung bis hin ins Darknet. Aufgrund des großen Umfangs der Ergebnisse werden hier nur die angelieferten E-Mail-Adressen vorgestellt.

Einsatz

Folgende Syntax steht für die Recherche mit ‚Spiderfoot‘ zur Auswahl:

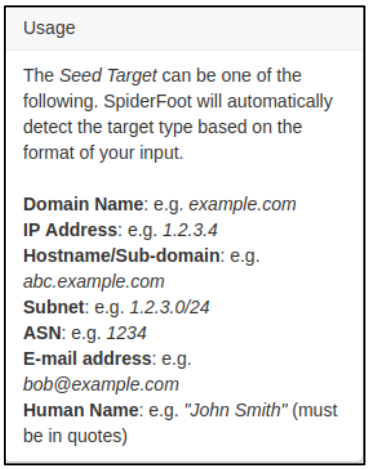


Abbildung 16 Syntax Spiderfoot – Seed Target

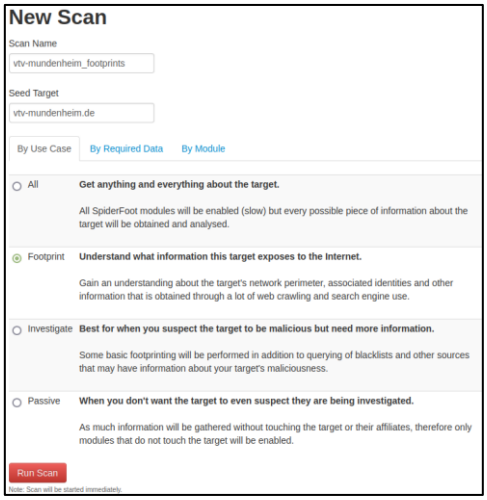


Abbildung 17 Syntax Spiderfoot – Footprints

Erkenntnis

Standard
Data
Volleyball@vtv-mundenheim.de
fit-in@vtv-mundenheim.de
handball@vtv-mundenheim.de
info@vtv-mundenheim.de
info@vtv-mundenheim.de
[redacted]@vtv-mundenheim.de
verwaltung@vtv-mundenheim.de

Abbildung 18 Spiderfoot – Mails

Die aufgelisteten E-Mailadressen bieten eine gute Grundlage um potenzielle Phishing-Angriffe o.Ä. durchzuführen.

3 Der Johnny Long Google Hacking Guide

Nachfolgend werden einige Anfragen aus dem ‚Johnny Long Google Hacking Guide' vorgestellt und unter Berücksichtigung der Personalisierungs- sowie Technischen-Aspekte in Bezug auf die Webseite vtv-mundenheim.de vorgeführt.

3.1 Einleitung und Vorgehensweise

Johnny Long ist ein Computer-Sicherheitsexperte und unter anderem bekannt für sein Buch „Google Hacking for Penetration Testers" was im Jahr 2004 veröffentlicht wurde. Google Hacking ist demnach keine direkte Hacking-Methode, sondern bedient sich einfacher erweiterter Google-Operatoren, die mit in die Google-Suche eingebunden werden und die Suche verfeinern bzw. steuern. Hierbei wird eine einfache Syntax verwendet, welche im Nachfolgenden genauer erläutert und beispielhaft erklärt wird. Ziel des Google Hackings ist es, durch Google-Operatoren relevante Informationen und Daten, die unverschlüsselt hochgeladen oder versehentlich indiziert wurden, zu beschaffen. Oft werden sensible Daten nicht gelöscht oder de-indiziert. Hierbei handelt es sich um Informationsbeschaffung auf legalem Gebiet, sofern diese Daten nicht weiterverwendet werden.

Im folgenden Sachverhalt wird die Internetseite https://vtv-mundenheim.de/ untersucht und versucht durch die Operatoren des Google Hacking Guides so viele sensible und relevante Daten bzw. Informationen zu beschaffen wie möglich. Hierbei werden zuerst einzelne Operatoren verwendet, um im späteren Verlauf mehrere miteinander zu kombinieren. Im zweiten Teil der Recherche werden wir mit Hilfe der gewonnenen Informationen unsere Suche personalisieren bzw. technische Aspekte spezifizieren.

3.2 Google Hacking VTV Mundenheim 1883 e.V.

Das folgende Bild zeigt die wesentlichen Google Operatoren auf einen Blick und erklärt, wie diese funktionieren und ob Kombinationen mit anderen Operatoren möglich sind:

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Abbildung 19 Google Operatoren

Die Tabelle zeigt auf, dass der Operator „site:“ nach Ergebnissen zu einer spezifischen Website sucht. Im vorliegenden Fall findet Operator „site:vtv-mundenheim.de“ folgendes Ergebnis:

Abbildung 20 site:vtv-mundenheim.de

Das ist der erste Schritt, um diese Website gründlicher zu durchsuchen. Planende Hacker sammeln so viele Informationen wie möglich. In diesem Beispiel wird mit der Suche nach Informationen zu Personen begonnen, es wird zusätzlich zum Operator „site:“ der Operator „intext:name“ verwendet, welcher nach dem Wort „name“ in der angegebenen Website sucht.

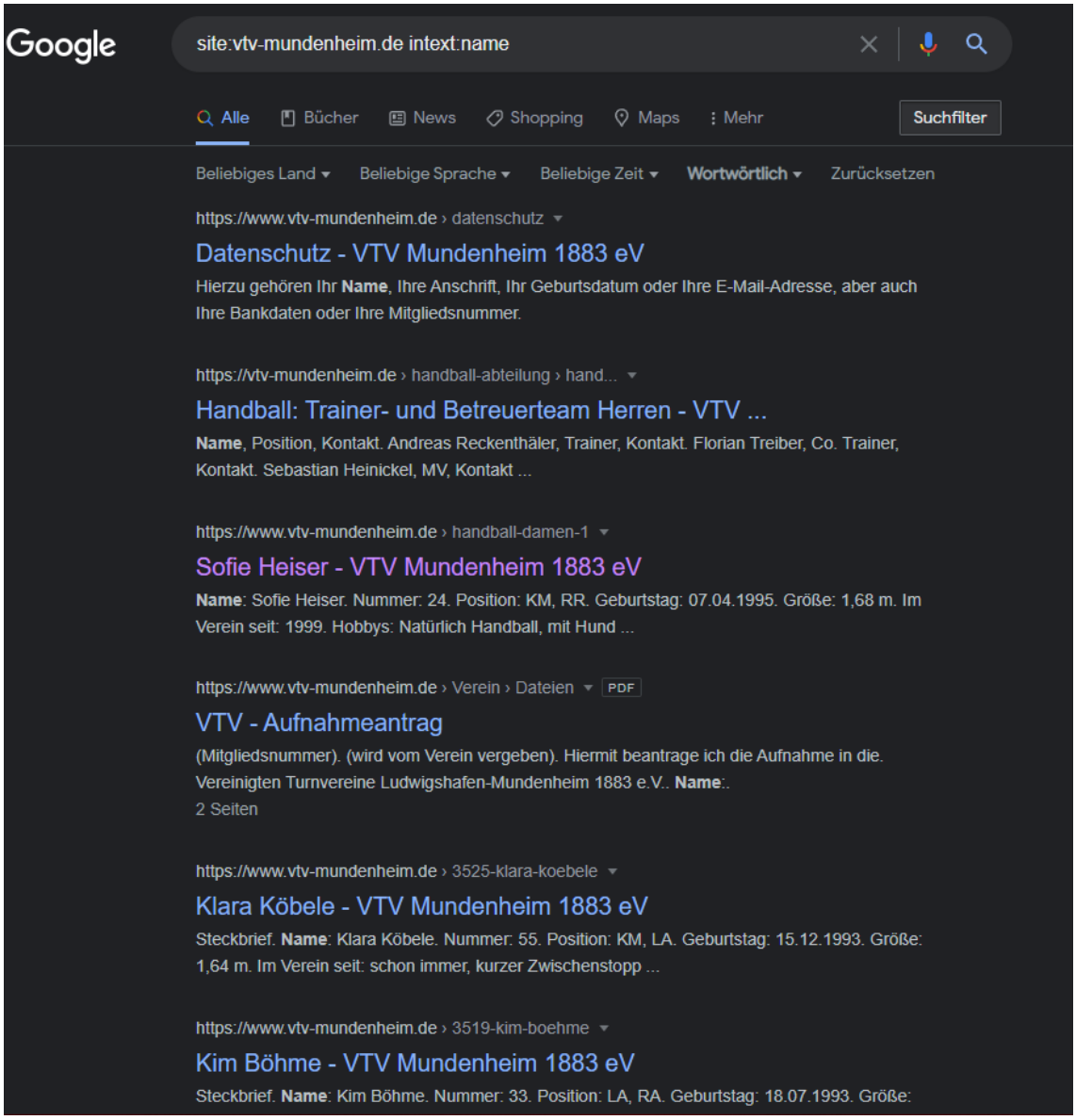


Abbildung 21 site:vtv-mundenheim.de intext:name

Allein durch diese einfache Syntax wurden Daten zu Namen, Geburtsdatum, Körpergröße, Spielernummer, Position und Vereinsbeitrittsdatum gefunden. Bei der nächsten Suchanfrage wird folgende Operatorkombination verwendet: “site:vtv-mundenheim.de intext:username | password“. Dadurch wurde die Suche so erweitert, dass auf der Website nach den Wörtern „username“ oder „password“ gesucht wird.

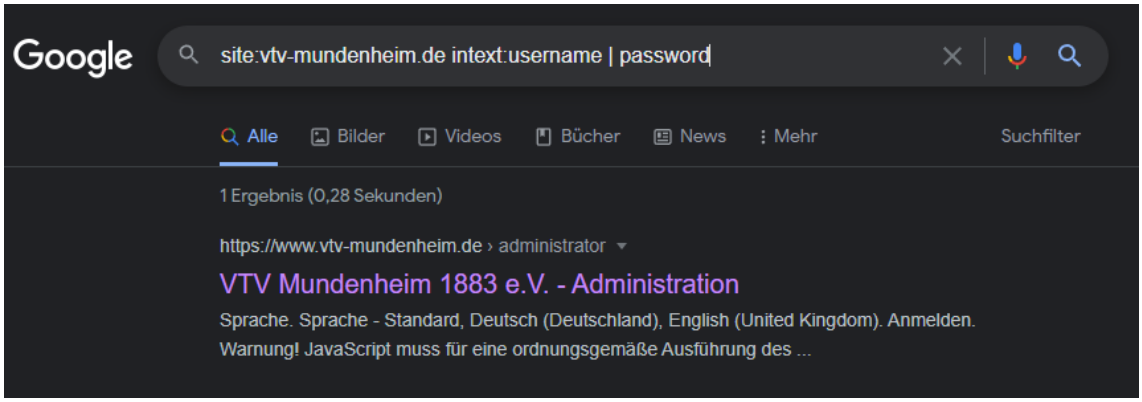


Abbildung 22 site:vtv-mundenheim.de intext:username | password

Das Ergebnis ist ein Link zur Anmeldung der Webmaster-Site von Joomla, ein Hinweis, dass die Seite des VTV Mundenheim 1883 e.V. damit programmiert wurde. Für Hacker kann diese Information z.B. für eine weitere Schwachstellensuche verwendet werden.

Abbildung 23 Joomla

Der zweite Schritt des Google Hackings beinhaltet die Personalisierung bzw. die Kontextualisierung und Überbrückung der technischen Aspekte der Google Suche. Da Google die mit Hilfe früherer Suchanfragen neue Suchvorgänge personalisiert und kontextualisiert, kann es vorkommen, dass weitere nützliche Informationen über das Suchziel nicht im Vordergrund angezeigt werden.

Über die Abfrage in Abbildung 3 wurden zur Person [redacted] folgende Daten gesammelt:

Name: [redacted]

Geburtsdatum: 15.12.[redacted]

Größe: 1,64m

Nummer: 55

Position: KM, LA

Nun wird die Suche auf diese Person weiter kontextualisiert. Die Syntax lautet „site:vtv-mundenheim.de intext:[redacted] und liefert folgende Ergebnisse:

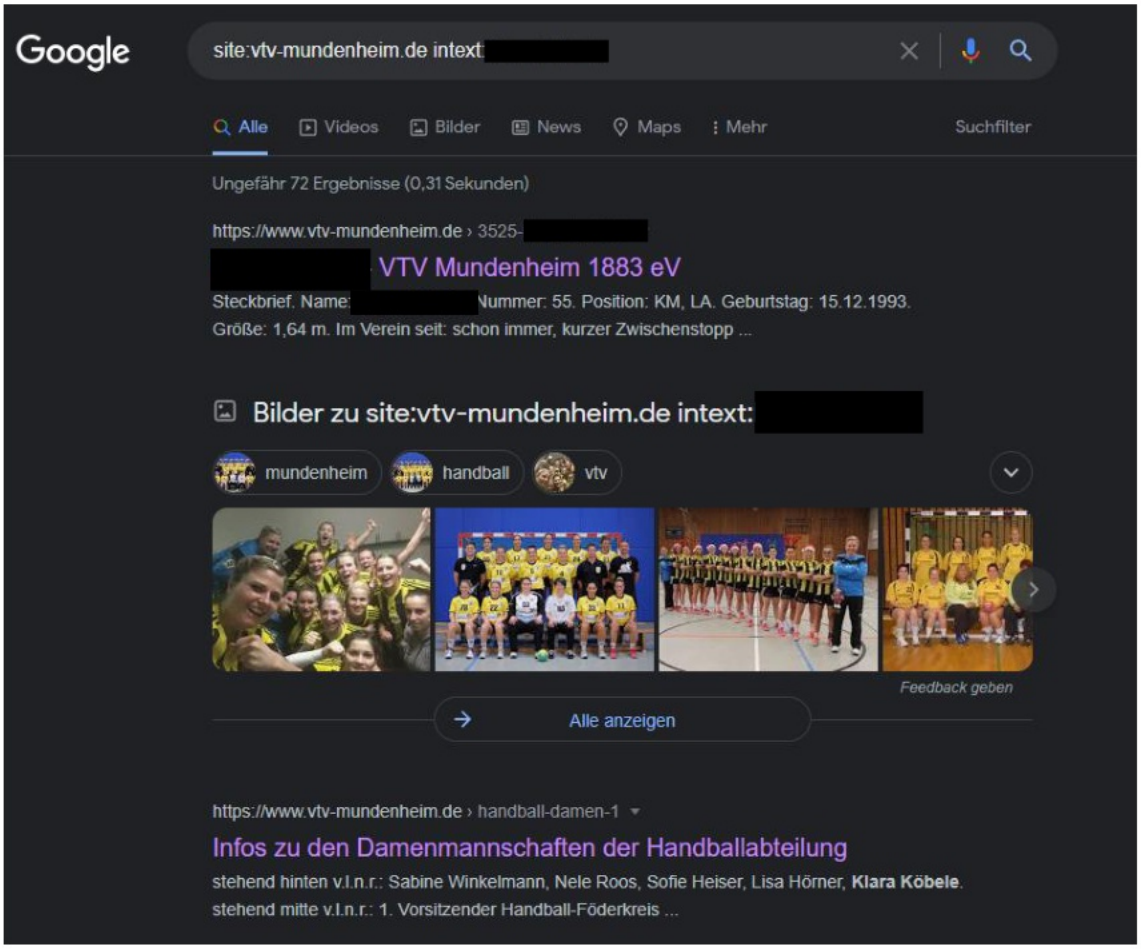


Abbildung 24 site:vtv-mundenheim.de intext:[redacted]

Auffällig hierbei ist, dass durch den Operator „intext:“ auch Bildergebnisse mit dem gesuchten Wort angezeigt werden. So kann die Person [redacted] mit Hilfe der Bildbeschreibung der Website eindeutig identifiziert werden:

Abbildung 25 [redacted]

Die Bildbeschreibung lautet wie folgt: „stehend hinten v.l.n.r.: [redacted]“.

Eine weitere Verfeinerung der Suche, um Medieninhalte (Bild-, Videodateien) zu finden, liefert keine Ergebnisse mehr:

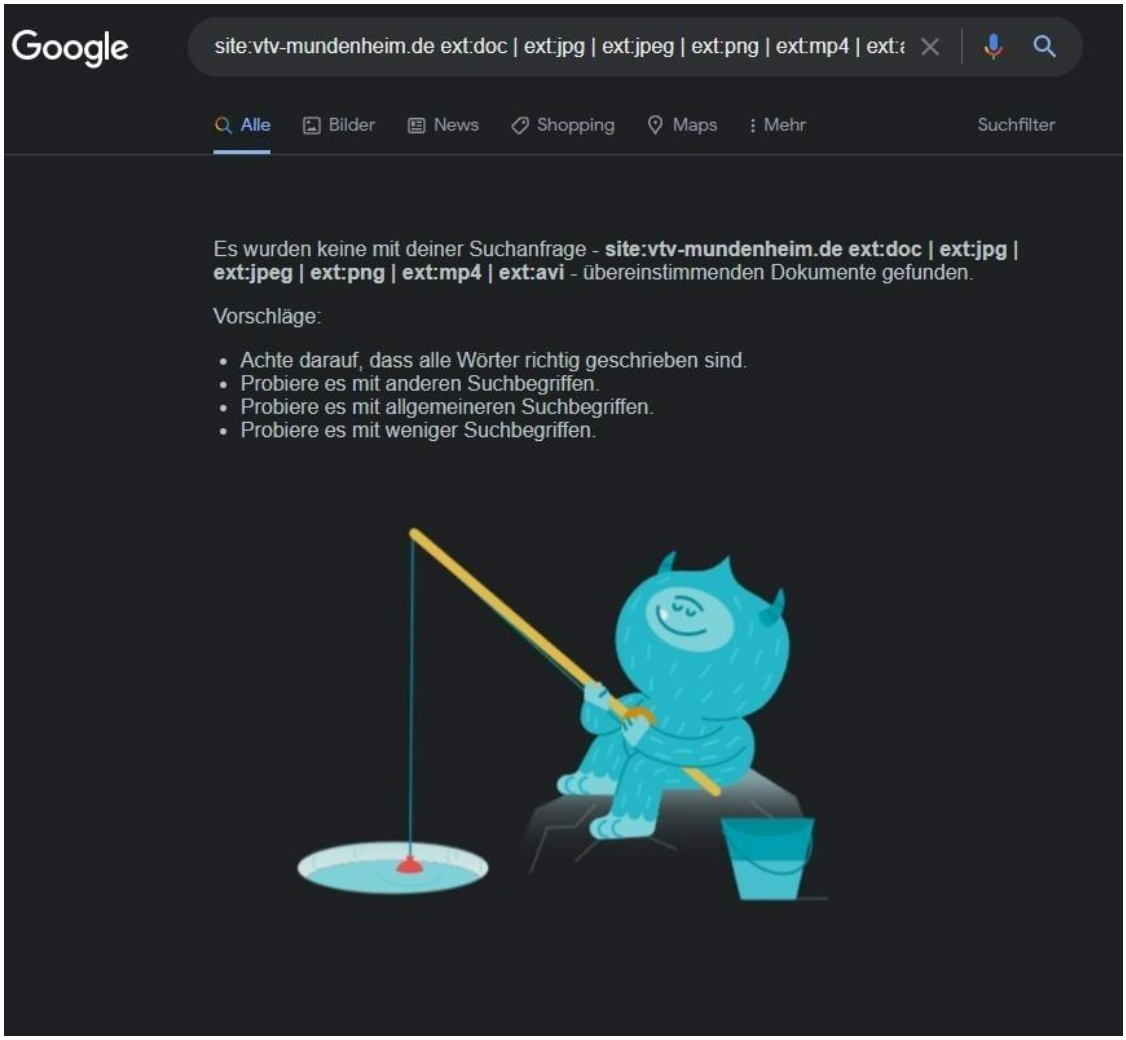


Abbildung 26 site:vtv-mundenheim.de Suche mit filetype-Parametern

4 Recherche im Dark Web mit Hilfe des TOR Browsers

Zusätzlich zu den durchgeführten Google-Hacks wird nachfolgend die Recherche auf das Darknet ausgeweitet. Damit wird gewährleistet, dass die gesamte Informationsbeschaffung etwas breitflächiger gestaltet wird.

4.1 Einleitung und Vorgehensweise

Das Dark Web oder Darknet beschreibt „[…] eine Vielzahl separater Netzwerke (Darknets), die untereinander nicht vernetzt sind.“ Es handelt sich hierbei um ein Peer-to-Peer-Overlay-Netzwerk, mit welchem sich die Teilnehmer untereinander manuell verbinden. Häufig wird der Begriff Dark Web synonym mit dem Deep Web betrachtet, allerdings handelt es sich beim Dark Web nur um einen Teil des Deep Webs:

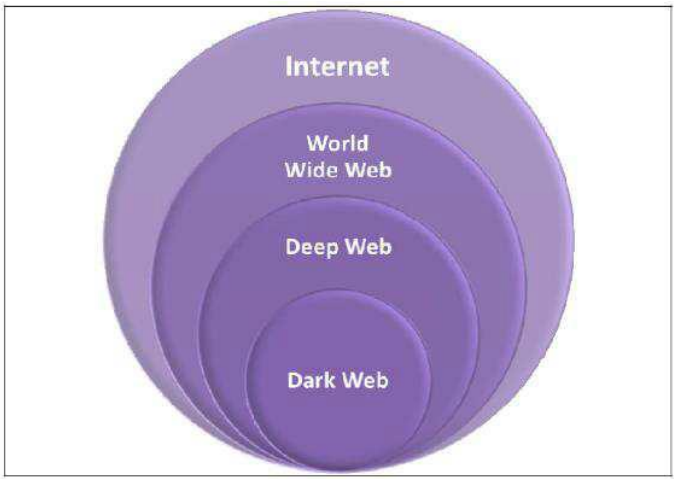


Abbildung 27 Layers of the Internet (Finklea 2015, S. 3)

Im Folgenden wird versucht weitere Informationen zum VTV Mundenheim 1883 e.V. über das Dark Web herauszufinden. Hilfreich dafür ist die Webseite https://dnstats.net/, welche verschiedene Darknet-Märkte sowie Foren zum Informationsaustausch aufführt. Diese Art von Seiten ist nur über die sogenannten Onion-Links erreichbar. Das Onion-Routing (dt. = Zwiebel) arbeitet mit mehreren Knoten, über die die Aufrufe der Webinhalte geroutet und verschlüsselt werden:

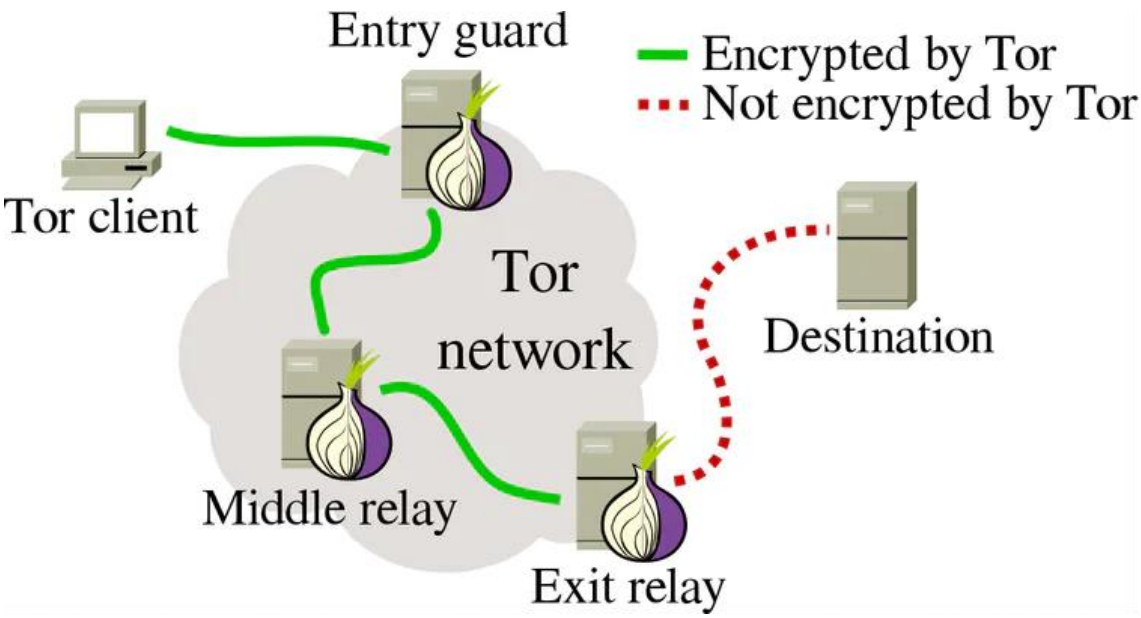


Abbildung 28 Onion-Routing des TOR-Browsers https://changelly.com/blog/tor-network/

Mit diesem „Zwiebelsystem“ ist es so gut wie unmöglich die Aufrufe noch nachverfolgen zu können, deshalb wird der TOR-Browser gerne genutzt, um anonym im Internet zu surfen.

Ziel der Recherche im Dark Web ist es, noch sensiblere Inhalte oder Informationen, die nicht im Clearweb indiziert sind, zu erhalten. Hierbei werden die auf https://dnstats.net/ aufgeführten Dark-Web-Onion-Links durchforstet.

4.2 Recherche im Dark Web VTV Mundenheim 1883 e.V.

Anhand der dnstats Webseite lassen sich zahlreiche Darknet-Marktplätze aber auch Foren finden. Im vorliegenden Fall wird zuerst die Webseite „Just Kill“ verwendet:

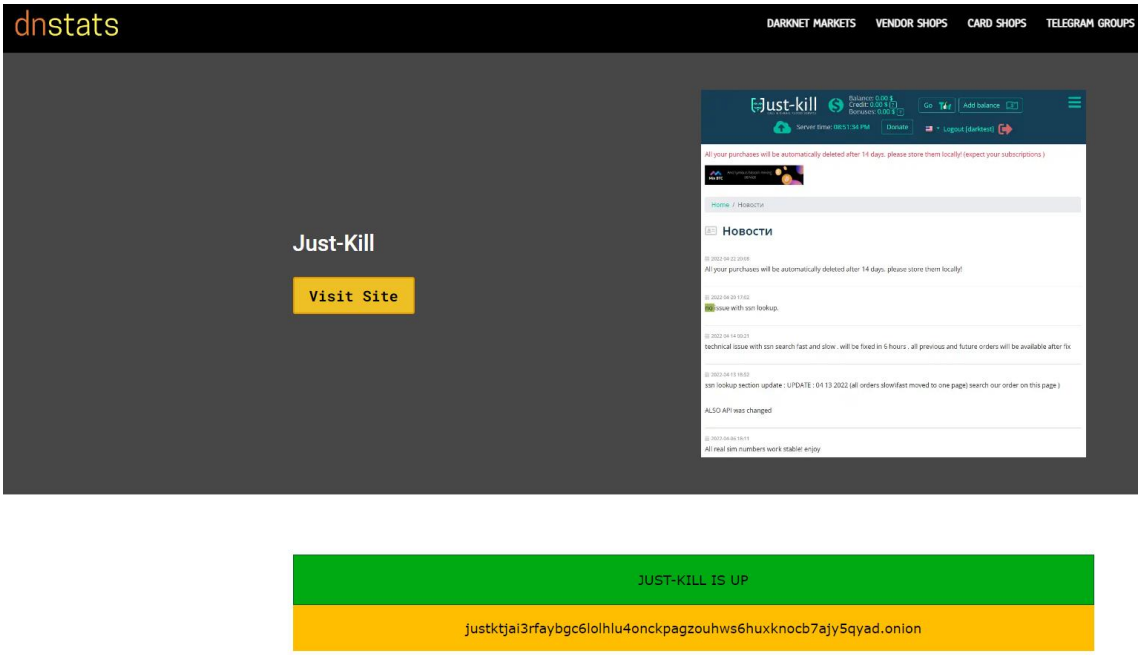


Abbildung 29 dnstats - Just Kill

Der Onion-Link, hier unten gelb hinterlegt, wird kopiert und in den TOR-Browser eingefügt:

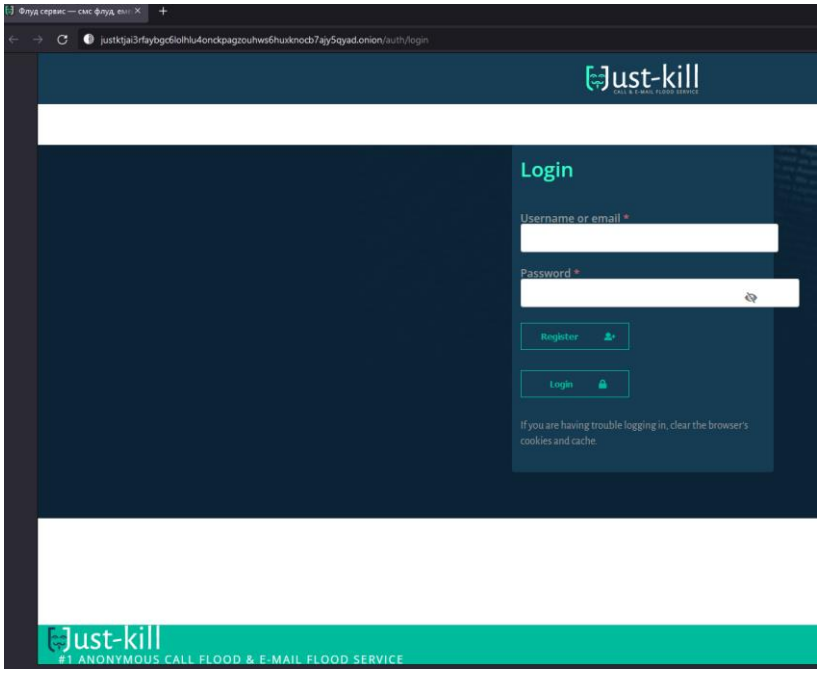


Abbildung 30 Just Kill

Wie im Screenshot ersichtlich benötigt es eine Registrierung, um weiter auf Just-kill zu recherchieren, weshalb auf die Seite „Dread“ zurückgegriffen wird:

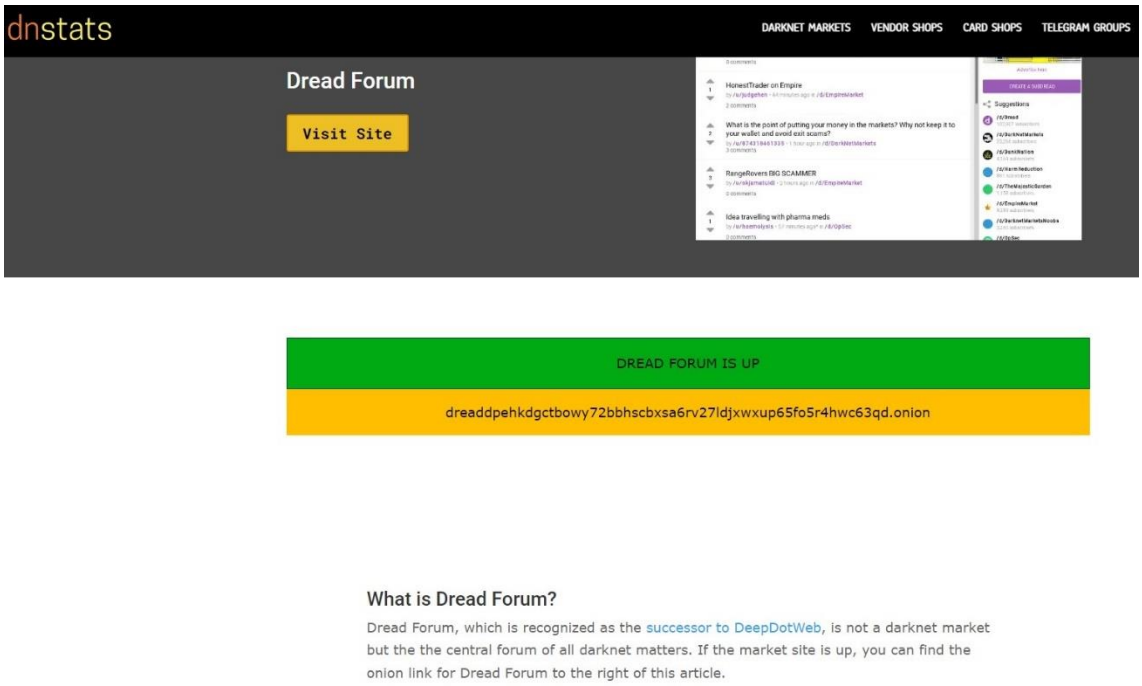


Abbildung 31 dnstats - Dread Forum

Der TOR-Browser leitet den User auf die Initialseite weiter, die das Forum durch einen 6-stelligen Zufallscode vor DDOS Attacken schützt.

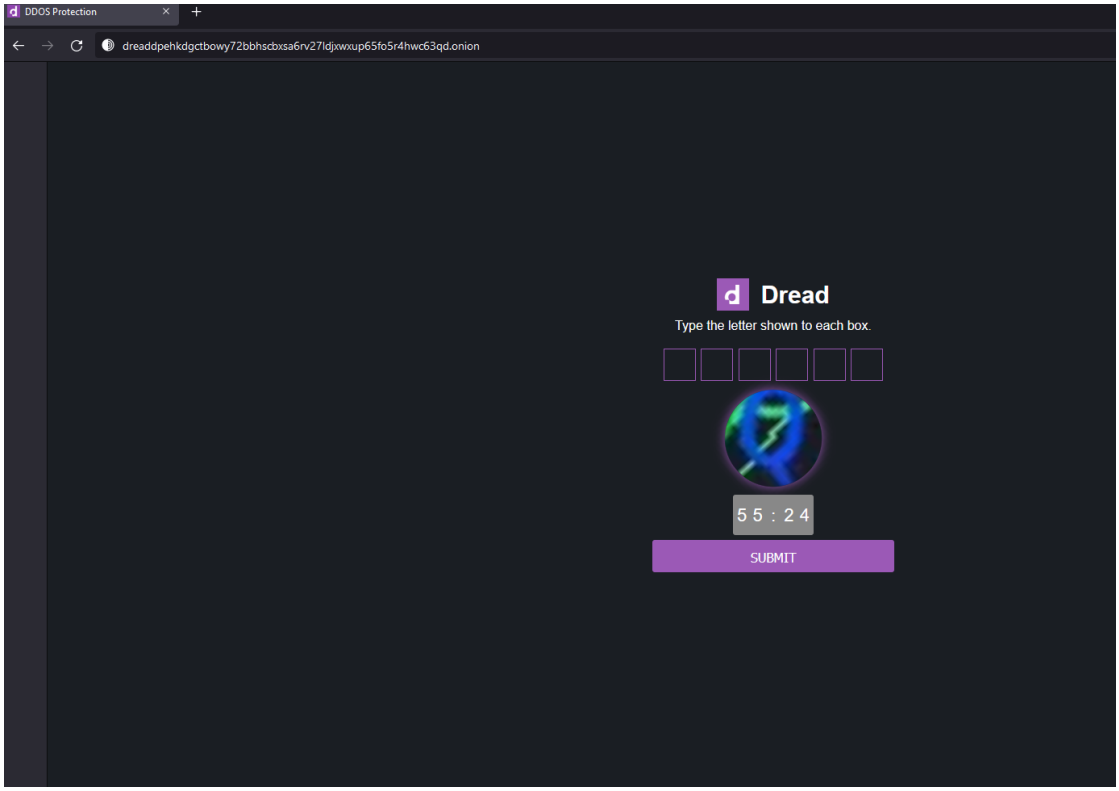


Abbildung 32 Dread Forum

Nach korrekter Eingabe des Bildcodes leitet die Webseite den User auf die Frontpage weiter. Es werden zahlreiche Beiträge mit Themen über Fake IDs oder illegalen Drogen (Edibles) direkt auf der Homepage angezeigt:

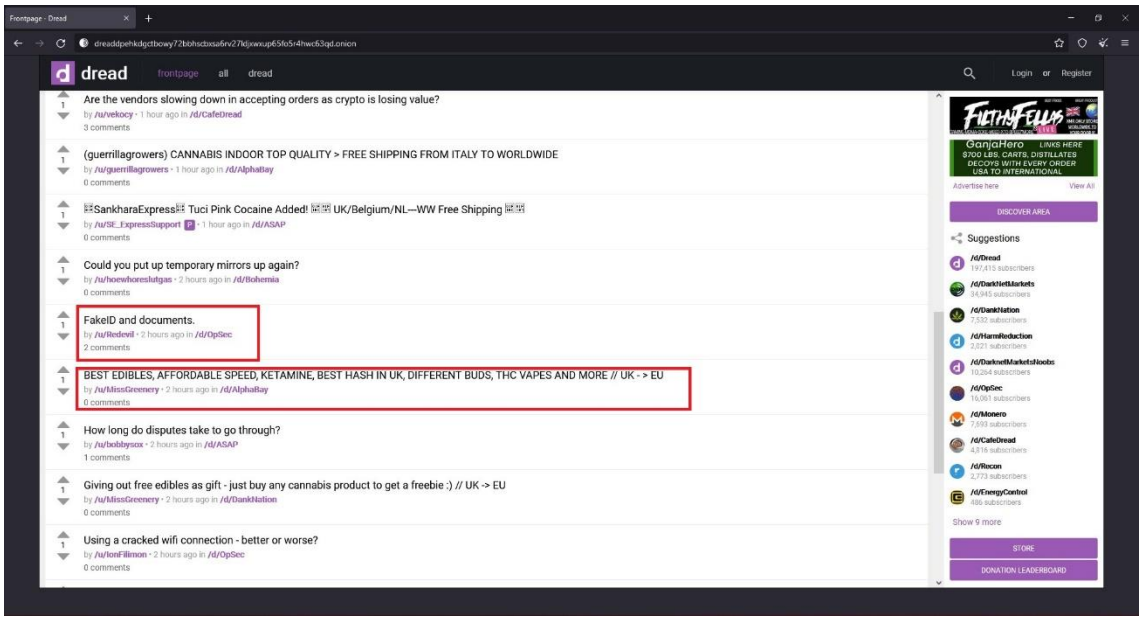


Abbildung 33 Dread Forum Frontpage

Mit der Lupe rechts oben im Screenshot kann das Forum durchsucht werden, jedoch ist es im Darknet üblich Adressen und Namen nur verschlüsselt weiterzugeben, wodurch kein Stichwort zum Thema VTV Mundenheim 1883 e.V. bzw. aus den Ergebnissen des Google Hackings ein positives Suchergebnis bringt:

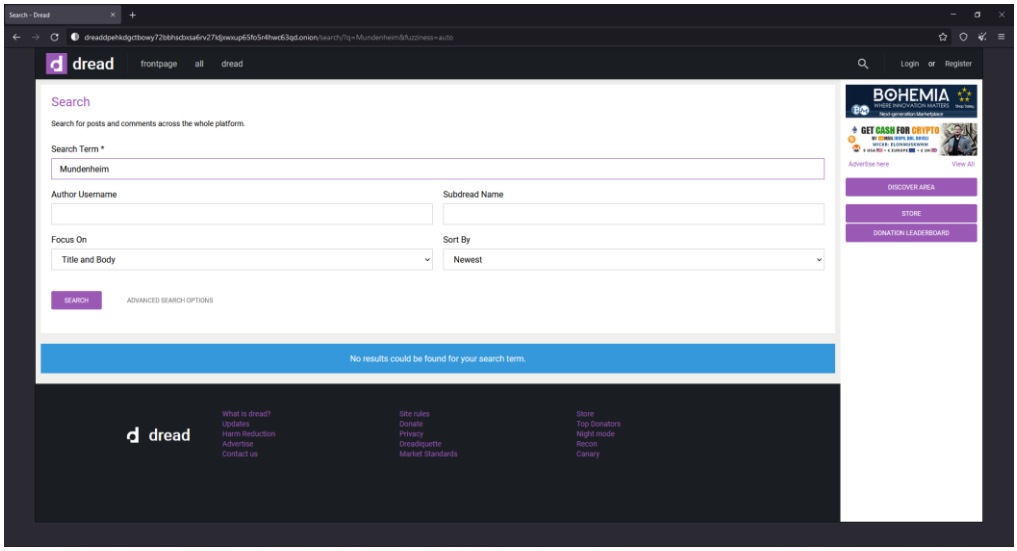


Abbildung 34 Dread Forum Suche

Andere Darknet-Webseiten sind zum Zeitpunkt der Recherche offline oder bereits ganz geschlossen:

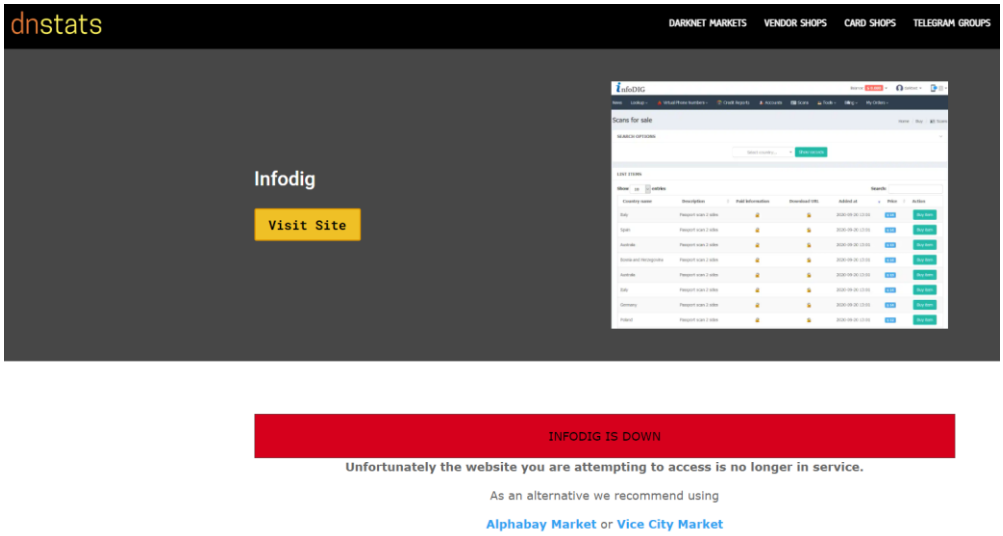


Abbildung 35 Infodig offline

Im zweiten Schritt wird versucht, Informationen über eine Dark-Web-Search-Engine zu erhalten. Hierbei wird auf die Onion Search Engine zurückgegriffen und mit dem Stichwort „mundenheim“ gesucht:

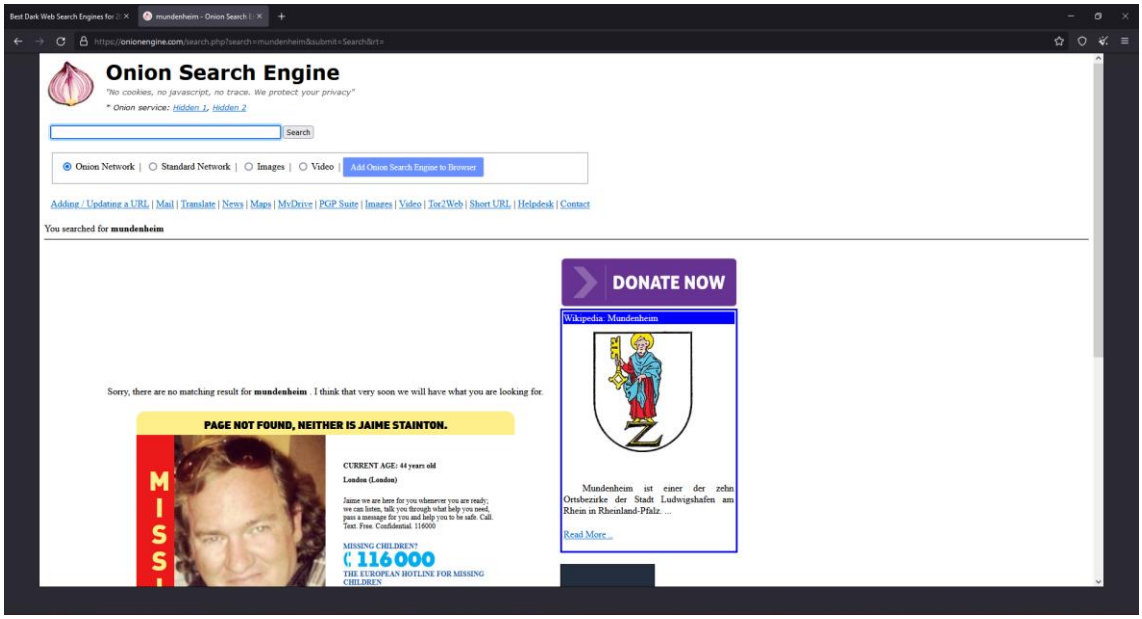


Abbildung 36 Onion Search Engine

Auch hier wurden keine Ergebnisse zur gewählten Homepage gefunden.

Dasselbe Ergebnis erhält man über die Engine torsearch:

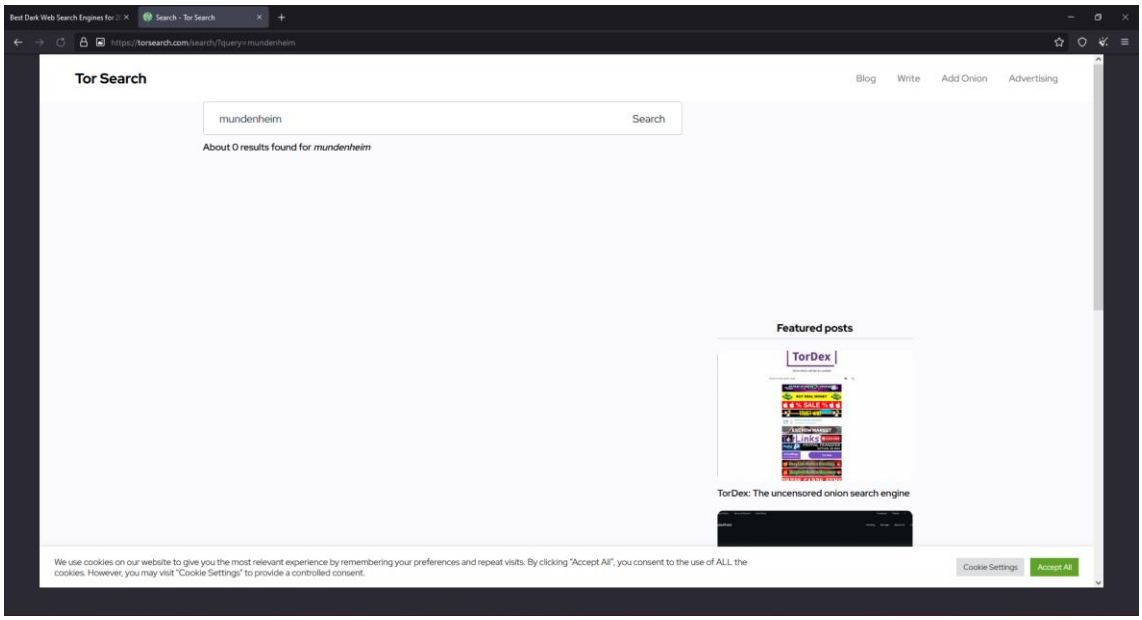


Abbildung 37 torsearch

5 Search Engine Optimization (SEO)

Um eine Homepage in den endlosen Weiten des Internets auffindbar zu machen, gibt es eine Reihe von Richtlinien und Optimierungsmöglichkeiten. SEO bedeutet Search Engine Optimization und richtet sich gezielt danach, durch Optimierung des Seiteninhalts, ein höheres Ranking bei einer Onlinesuchmaschine zu erreichen.

Zudem gibt es noch diverse Richtlinien, um es Nutzern möglichst angenehm zu gestalten die Homepage aufzusuchen.

Grundsätzlich sollte eine Webseite:

- für den Googlebot gut lesbar sein und keine Elemente ungewollt verstecken.
- thematisch gut strukturiert sein. Das Menü sollte benutzerfreundlich und selbsterklärend sein.
- nicht allzu viel Zeit benötigen, bis sie geladen ist.
- sowohl am Smartphone als auch auf dem Desktop super bedienbar sein.
- einen sauberen Quellcode besitzen (gute Überschriftenstruktur, alternative Texte und sprechende URLs, sowie notwendige Meta-Daten)

5.1 On-The-Page-SEO

Hiermit ist die Optimierung direkt auf der Webseite, bzw. im Quellcode gemeint. On-The-Page-SEO hat den wesentlich größeren Einfluss auf das Suchmaschinenranking. Durch korrekte Verwendung von Meta-Tags und Keywords zum Beispiel im Fließtext der Homepage, steigt das Ranking bei Suchmaschinen. Eine gut designte Webseite gibt nicht direkt ein besseres Ranking, allerdings geht schlechtes Design meistens einher mit unaufgeräumtem, bzw. unsauberem Quellcode.

5.2 Off-The-Page-SEO

Unter diesem Begriff versteht man den Einfluss des Suchmaschinenrankings durch Verlinkungen von anderen Domains. Dies kann sowohl positive als auch negative Auswirkungen auf das Ranking habe. Ziel ist es von Verlinkungen von großen Webverzeichnissen zu bekommen, aber auch von Webseiten wie Wikipedia. Schlecht bewertet werden hingegen Verlinkungen von bekannten Spam- oder Scam-Webseiten. Diese werden von Suchmaschinen schlechter bewertet.

Wie in einem Blogeintrag der Webseite seokratie.de geschrieben steht: „Eine gute Website bekommt viele Links von anderen guten Websites“.

5.3 Negativbeispiele

Die Webseite einer lokalen kleinen Werkstatt eignet sich hier sehr gut als Negativbeispiel für die Strukturierung einer Webseite. Da sich die Werkstatt auf den Wechsel von Autorreifen spezialisiert hat, sollte die Seite im Suchmaschinenranking weit oben sein. Bei der Suche „reifen wechseln nagold“ findet man sie an der sechsten Stelle, was für ein Unternehmen mit weniger als zehn Mitarbeitern relativ gut ist

Abbildung 38 Landingpage Reifenhaus Schwarz

Das Design ist definitiv schon veraltet und nicht sehr ansprechen für Besucher der Webseite. Ein Cookiebanner ist nicht existent, welches bei einer Webseite dieser Art aber auch nicht zwingend erforderlich ist, wenn wirklich keine Daten gesammelt werden.

Eine mobile Version existiert nicht. Die Homepage wird auf einem Smartphone exakt gleich angezeigt.

Den Onlineshop cw-mobile.de kann man als SEO-Negativbeispiel aufführen.

Beim Aufrufen des Shops sieht man, dass aktuell eine „HopfenHöhle“ im Wochenangebot ist.

Abbildung 39 Reifenhaus Schwarz Mobil

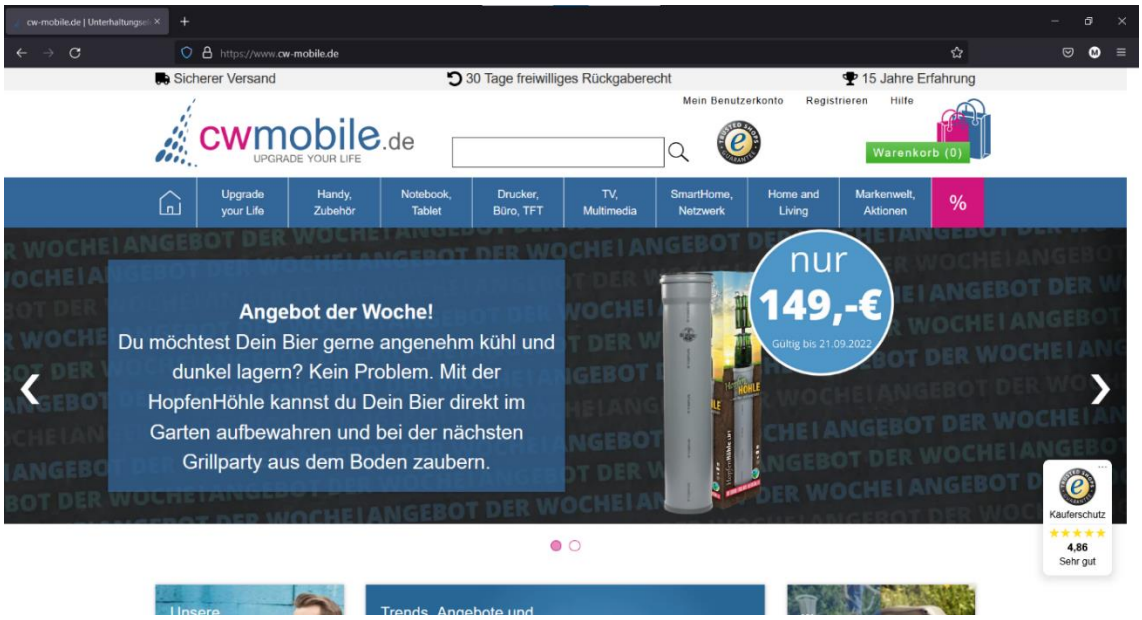


Abbildung 40 cwmobile Landingpage

Nutzt man nun eine Suchmaschine mit der Suche „Hopfenhöhle kaufen“ erscheint der Shop cw-mobile.de aber erst an neunter Stelle und ist somit schon fast nicht mehr relevant.

5.4 SEO-Bewertung für die Webseite vtv-mundenheim.de

Die Webseite des VTV-Mundenheim ist auf den ersten Blick relativ einladend aus, jedoch fallen sehr schnell diverse Logikfehler auf.

Es existiert zum Beispiel der Punkt „Datenschutz“ im Untermenü „Über den Verein“, welcher wiederum aber kein Menüpunkt in der oberen Menüleiste ist, sondern nur auf der Startseite existiert. Darunter sollte meiner Meinung nach auch der Punkt „Impressum“ existieren. Der wiederum ist aber nur sehr klein ganz am Ender der Webseite.

Abbildung 41 VTV-Mundenheim Landingpage

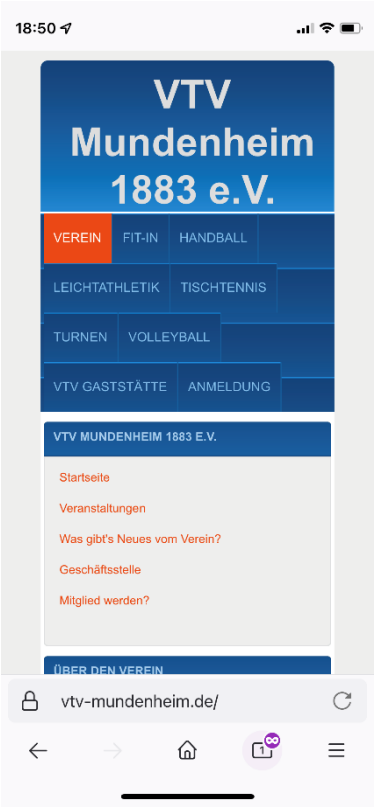


Abbildung 42 VTV-Mundenheim Mobile

Beim Aufrufen der mobilen Version der Webseite fällt sofort das übergroße Menü auf, das fast 50% des gesamten Smartphone-Bildschirms einnimmt. Im Vergleich zur Desktopversion ändert sich nur die Anordnung der Untermenüs. Beim Durchsehen der Seite stellt man diverse Optimierungsfehler im Design fest.

Abbildung 43 VTV-Mundenheim Formatfehler

Ein Cookiebanner wird beim Aufrufen der Webseite nicht eingeblendet. Wenn tatsächlich keine Trafficanalyse der Webseite existiert, wie zum Beispiel Google Analytics, dann wird auch kein Hinweis benötigt, dass Cookies verwendet werden.

Wer die Webseite des VTV-Mundenheim finden will kommt über Suchmaschinen sehr schnell an sein Ziel.

Bei dem Suchbegriff „Mundenheim“ ist schon beim zehnten Eintrag der Sportverein aufgelistet. Mit „Mundenheim Sport“ oder einer bestimmten Sportart anstatt „Sport“, findet man die Webseite schon auf dem ersten Platz.

Mit den Entwicklertools eines Browsers lassen sich die Meta-Tags der Webseite auslesen.

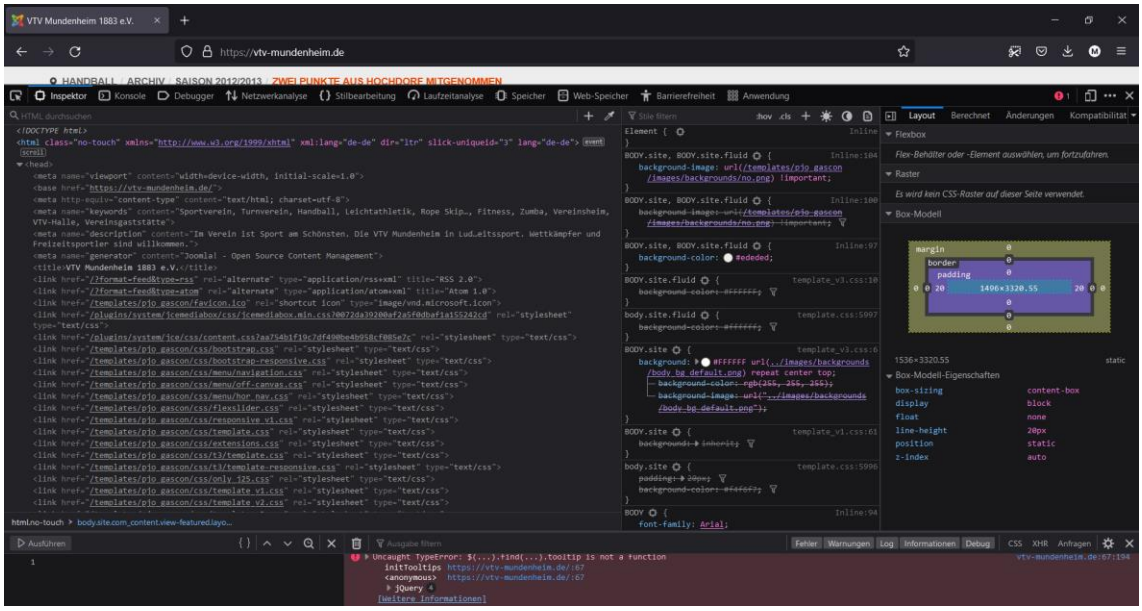


Abbildung 44 VTV-Mundenheim Quelltext

5.5 Die Metadaten der Webseite vtv-mundenheim.de:

Titel	VTV Mundenheim 1883 e.V.
Meta-Keywords	Sportverein, Turnverein, Handball, Leichtathletik, Rope Skipping, Tischtennis, Seniorensport, Turnen, Volleyball, Wirbelsäulengymnastik, Sitzgymnastik, Herzsport, Coronarsport, Eltern-Kind-Turnen, Kinderturnen, Aerobic, Fitness, Zumba, Vereinsheim, VTV-Halle, Vereinsgaststätte
Meta-Description	Im Verein ist Sport am Schönsten. Die VTV Mundenheim in Ludwigshafen am Rhein haben ein breit gefächertes Sportangebot für die ganze Familie. Vom Eltern-Kind-Turnen bis zur Sitzgymnastik für Senioren. Handball, Tischtennis, Volleyball, Leichtathletik, Fitness- und Gesundheitssport. Wettkämpfer und Freizeitsportler sind willkommen.

- Der Titel ist kurz, knapp und hat keine weitere Beschreibung.
- Die Meta-Keywords sind mit 25 Stück etwas zu viel. Empfohlen sind maximal 20 Keywords.
- Die Meta-Description übersteigt mit 333 Zeichen die empfohlene Zeichenlänge von 160 und mit 2165 Pixeln die empfohlene Pixelbreite von 1000.
- In den Metadaten wird die Sprache de-de übergeben. Dies nutzen Suchmaschinen, um Suchergebnisse in gewünschten Sprachen anzeigen zu können.

5.6 Verbesserungsmöglichkeiten für vtv-mundenheim.de

Zur beispielhaften Darstellung der Verbesserungsmöglichkeiten wird die Webseite wired.com genutzt.

5.6.1 Darstellung der mobilen Webseite:

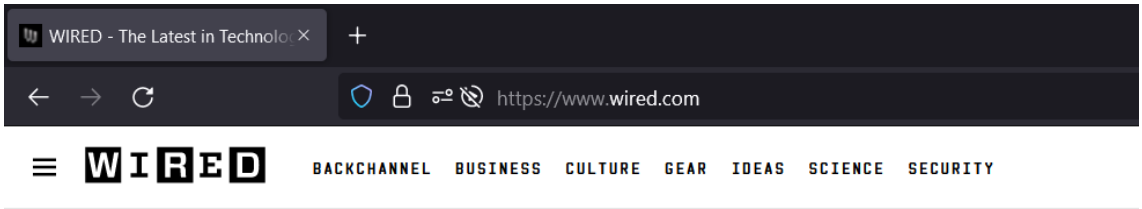


Abbildung 46 Wired Landingpage

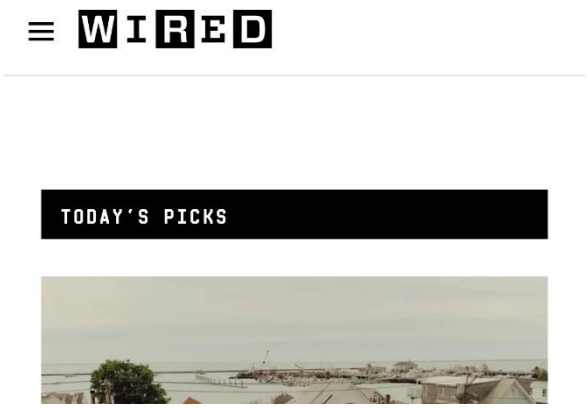


Abbildung 45 Wired Mobile

Die Menüstruktur der Desktopdarstellung ist in Ordnung, nur im mobilen Browser werden die einzelnen Menüpunkte zusammengestaucht. Im Beispiel von wired.com sieht man, dass in der mobilen Darstellung die Menüleiste verschwindet und die Navigation komplett über das ausklappbare Menü links oben funktioniert. Zudem sollten bei vtv-mundenheim.de die Untermenüs sinnvoller zusammengefasst werden.

5.6.2 Meta-Tags:

Die Meta-Description von vtv-mundenheim.de ist etwas zu lang. Diese sollte auf maximal 160 Zeichen gekürzt werden und auf den Punkt bringen, was man auf dieser Webseite, bzw. in dem Verein findet.

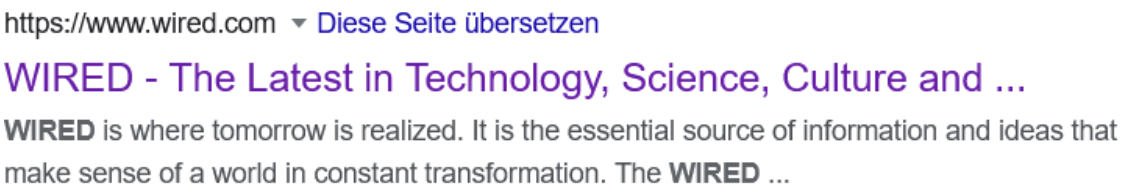


Abbildung 47 Wired Googleergebnis

Quellenverzeichnis

https://de.wikipedia.org/wiki/Darknet

https://www.seokratie.de/webdesign-und-seo/

https://www.seokratie.de/seo-kurz-check-15-min-anleitung/

https://www.seokratie.de/wie-funktioniert-seo/

https://freetools.seobility.net/de/seocheck/

https://www.screamingfrog.co.uk/seo-spider/

Literaturverzeichnis

[1] MUSTERMANN, HANS : Elektromagnetische Verträglichkeit in Verbindung mit Blitzschutzsystemen. In: *e&i, elektrotechnik und informationstechnik*, 123 (2006) 1/2. Wien und New York: Springer, 2006, S. 39 - 45.

[2] MUSTERFRAU, RITA : Messung von … Kunststoffproben. Wismar, Hochschule Wismar, Fachhochschule für Technik, Wirtschaft und Gestaltung, Fachbereich Elektrotechnik und Informatik, Diplomarbeit (FH), 2002.

Bilderverzeichnis

Tabellenverzeichnis

Verzeichnis der Abkürzungen

API	Application Programming Interface
bspw.	beispielsweise
bzw.	beziehungsweise
CMS	Content Management System
dt.	*deutsch*
engl	*englisch*
evtl.	eventuell
ggf.	gegebenfalls
inkl.	*inklusive*
o.Ä.	oder Ähnliches
o.g.	oben genannte
rDNS	reverse Domain Name Service
SEO	Search Engine Optimization
sog.	sogenannte
TLD	Top Level Domain
u.a.	unter anderem
URL	Uniform Resource Locator
v.a.	vor allem
z.B.	zum Beispiel