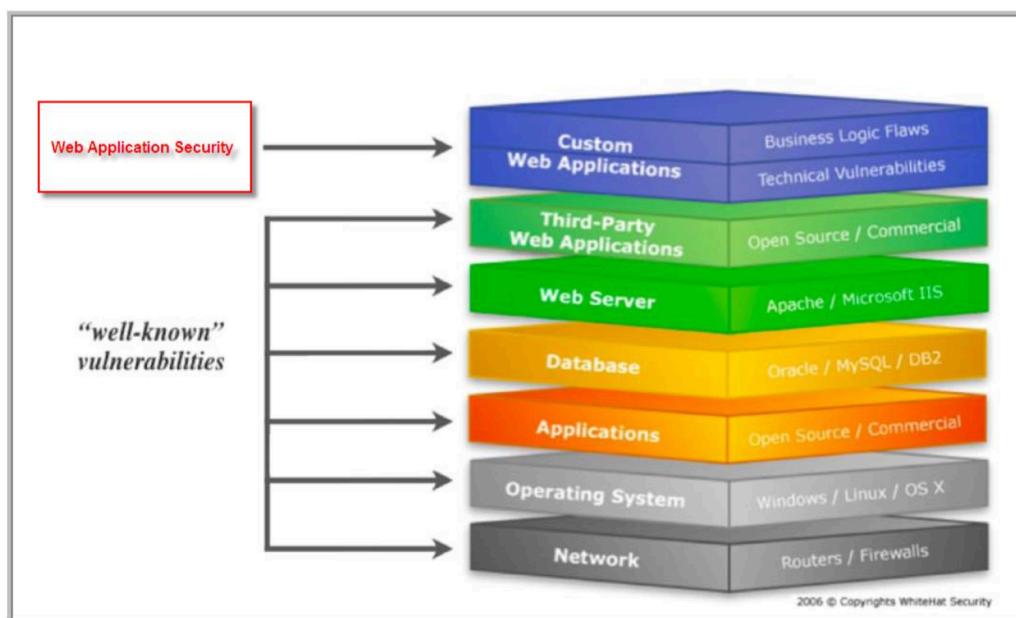


## WebSecurity SEO Accessibility

WEBSECURITY:  
Hacking evolution

### Hacking Evolution



OWASP:  
Open Web Application Security Project

### OWASP Top Ten

#### Topics 2017

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Sensitive Data Exposure
- A4 XML External Entity Attack
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 Cross-Site Scripting (XSS)
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring

SQL Injection:

## Threat: Bypass Authentication

Attacker uses following input:

- Login: meier
- Password: '' OR '='

```
SELECT Username FROM Users  
WHERE Username='meier' AND Password=''' OR '=''
```

WHERE clause evaluates to TRUE

- All rows of table get select
- Result Set will not be empty!!!

User gets authenticated!

how to prevent:

Sanitizer Parsing using Regex and filters before send to db:

mysqljs:

Use

```
.escapeId() .query() .escape()
```

Examples

```
var q = 'SELECT * FROM tbl ORDER BY  
' +
```

```
connection.escapeId(sorter);  
connection.query ('SELECT * FROM tbl  
WHERE id=?', [userId], function  
(error, results, fields) {  
  
    if (error) throw error;  
// ...});
```

## Hashed and Salted User Passwords

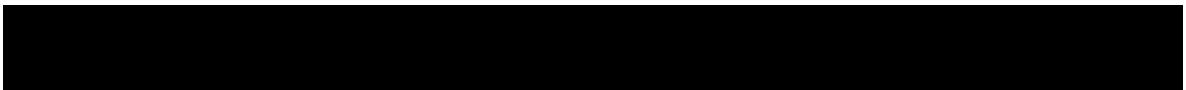
Do not store passwords in plaintext to the table

```
mysql> select username, password from users;
+-----+-----+
| username | password |
+-----+-----+
| hacker10 | compass |
```

One-way-hashed and salted passwords using bcrypt.

```
var salt = bcrypt.genSaltSync();
var hash = bcrypt.hashSync(password, salt);
```

NoSQL injection:



# NoSQL Authentication

```
app.post(''/'', function (req, res)
{
    db.users.find({
        username: req.body.username,
        password: req.body.password},
        function (err, users) {
            // login success
        }) ; }) ;
```

What if?

```
{ "username": "admin", "password":  
{"$gt": ""} }
```

**Results in login of admin because  
every password  
greater than an empty string evaluates  
to true.**

how to prevent:

```
escape("$") => %24 (deprecated  
since JS 1.5)
```

**encodeURI("\$") => \$**

```
encodeURIComponent("$") => %24
```

```
function validate(req, res,
```

```
next) {  
if  
((typeof(req.body.username)=="s  
tring") &&  
(typeof(req.body.password)=="st  
ring")) {  
next(); } else {  
res.send("Hey  
cheater!");  
}  
}  
app.post('/', validate,  
function (req, res) {  
// validation okay  
});
```

## Server Side JS Injections

Beware of the evil

- eval(), setTimeout(), setInterval(), Function()

Calculator Example

```
var result = eval(req.body.calc); // do mathz  
http://fun.stu.ff/?calc=2+3  
Returns 5
```

Exploit

```
http://fun.stu.ff/app?calc=process.exit()  
...  
while(1)  
require('fs').readFileSync(filename)
```

```
res.end(require('fs').readFileSync('/etc/password'))
```



## SSJS Prevention

### Recommendations

- Input validation
- Avoid the Big Four ;)
  - eval(),
  - setTimeout(),
  - setInterval(),
  - Function()
- Use JSON.parse() and parseXyz()
- Include 'use strict'; at the beginning of functions

## Terms

- Authentication
  - Who requires access to the application
- Authorization
  - What is the user allowed to do in the application

## Authentication

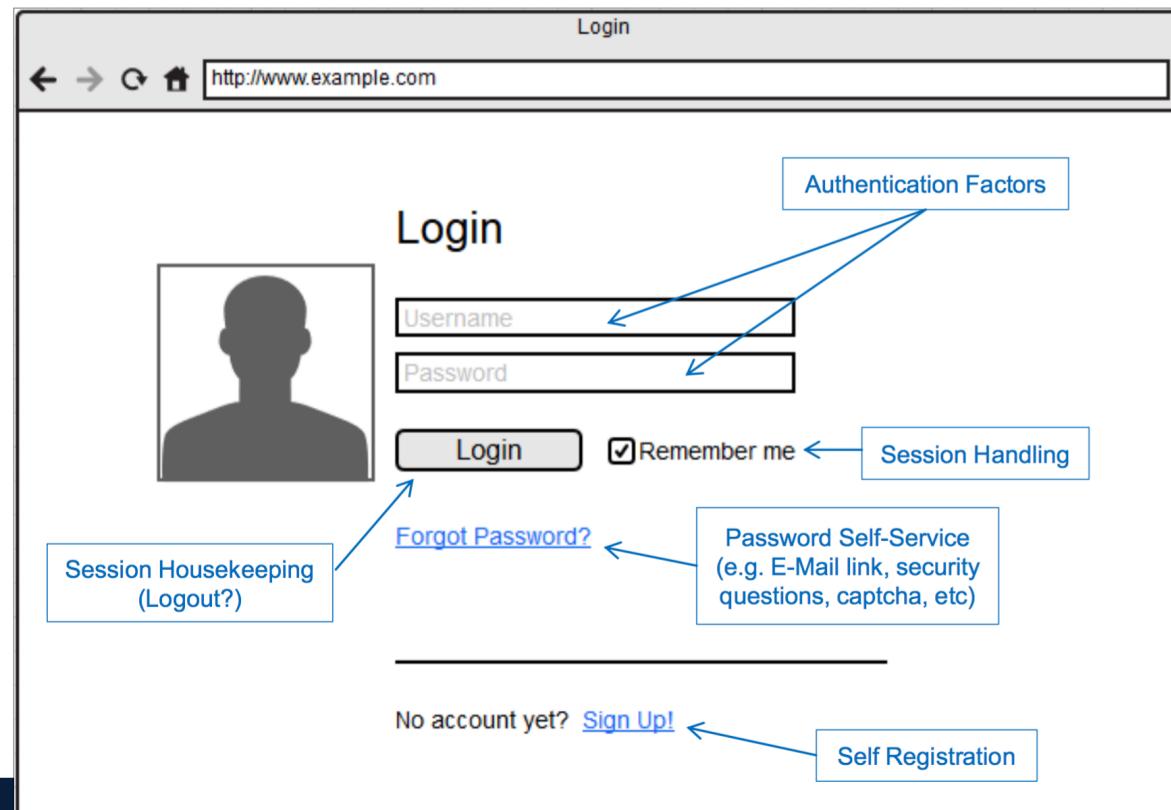
Definition (incl. Strong Authentication)

### Factors of Authentication (3 variants)

- To **KNOW** something
  - Password, PIN
- To **OWN** something
  - Smartcard, SecurId, Safeword, Vasco, OTP
- To **BE** something
  - Fingerprint, Iris, Voice, Face

Definition of “Strong authentication”

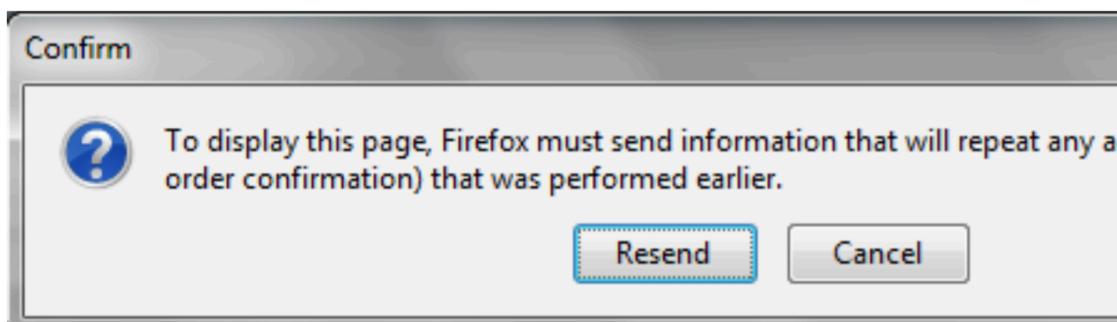
- Combination of at least 2 factors



## Back Button Relogin Vulnerability

### Szenario

- Logout of the application
- Hit the back-button until you reach the login page
- Then you may get following screen



- After pressing the button Resend you are logged in again!

expirydate of cookie only for session? - ist nicht gesetzt.

## Session Handling: Cookie based

...google.com ist

accounts.google.com (cookie geht nur dort hin)

- How does the browser receive the session-id?

20 Anwendungen... die Sicherheitslücke definiert sich durch die schwächste

Via „Set-Cookie“ HTTP response header from the server

- When does the browser send cookies along with an HTTP request?

Secure: true = cookie wird nur an server geschickt wenn TLS (SSL ist veraltet -

SSL war teuer viele Performance hotog)

▪ Depends on the cookie attributes

TLS ist außer wichtig fürs Google-Ranking

▪ Domain Achtung Secure Flag (mal unverschlüsselt) dann wirds cookie nicht geschickt

▪ Path wenn secure: true

httpOnly: clientseitig kann man nicht auf cookie zugreifen (Browser schützt)

sameSiteFlag: noch nicht überall unterstützt. Cookie GitHub einloggen

sameSite... hackerforum Inhalte heikel.. Posts nehmen dann nicht das cookie

sondern GitHub - cookie

Name	Domain	Path	Expires on	Last accessed on	Value	Secure	HttpOnly
IP_JAR	.google.com	/	Wed, 27 Dec 2017 09:08:1...	Mon, 27 Nov 2017 09:09:...	2017-11-27-9	false	false
ACCOUNT_CH...	accounts.googl...	/	Wed, 27 Nov 2019 09:08:...	Mon, 27 Nov 2017 09:08:...	AFx_ql6a00zU_u...	true	true
APISID	.google.com	/	Wed, 27 Nov 2019 09:08:...	Mon, 27 Nov 2017 09:09:...	Pgoj1s3V6Kr83V...	false	false

## Set-Cookie: Examples

- Temporary cookie (non-persistent) transmittable only via HTTPS to originating site only

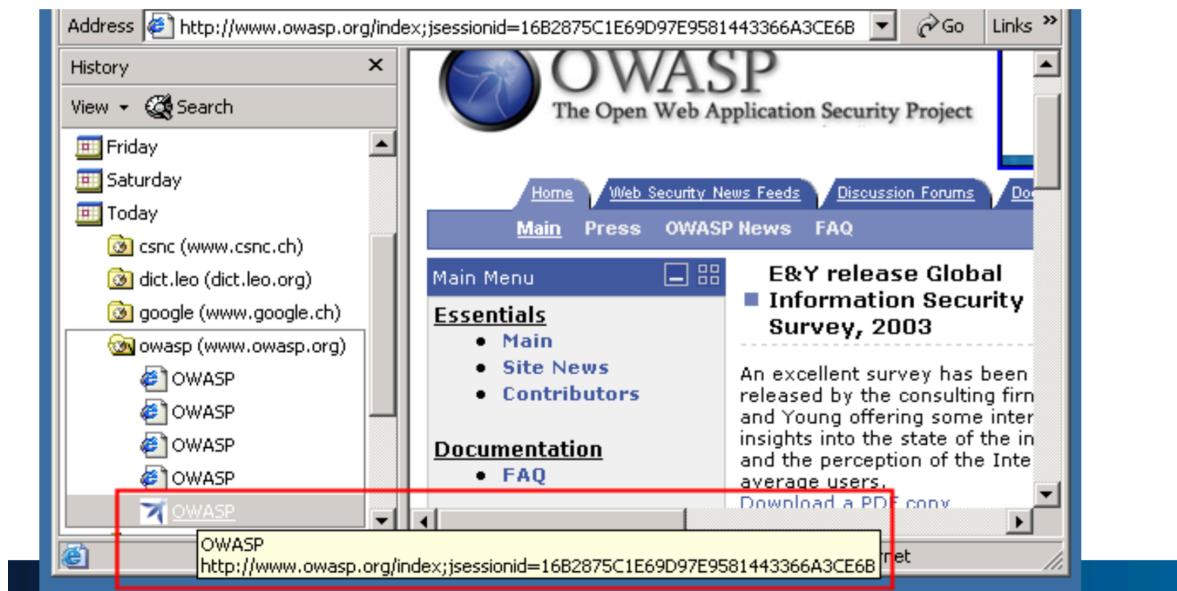
```
Set-Cookie: SESSION=123; path=/app; Secure; HttpOnly
```

- Persistent cookie which is sent to all sites belonging to domain google.ch

```
Set-Cookie: PREF=ID=2744d38c32b2ec68:LD=de:TM=1094031009  
expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.ch
```

## Remember me: Browser History

- URL with session ID is stored in browser history and cache



## War Googling: Public Access Logs

- URLs stored in server access and referrer logs

einfach mal googlen ev. kriegt man session

```
http://www.firewall-
net.com/link/index.php?LANG=french&categories_parents_id=5&PHPSESSID=761b560f16
72358d59e11cc31a52e323 -> /onlinetests/index_e.html

http://www.firewall-
net.com/link/index.php?LANG=french&categories_parents_id=5&PHPSESSID=761b560f16
72358d59e11cc31a52e323 -> /new.html

http://www.fiction.al/(fkw4n0ymyzrfsdrh1pcfykmj)/login.ashx
```

Session Fixation (hacker hat zugriff zur Sitzung bevor User angemeldet ist ... hacker ist man in the middle)

User loggt sich ein und hacker kann miederselben session alles dazwischen selber weiter bearbeiten und weiterschicken:

Prevention:

## Session Fixation

### Prevention

- Change Session after successful authentication

Session prevention stealing:

## Session Stealing Prevention

- Send session ID over HTTPS only
  - Use TLS encryption
  - Set Cookie “secure” flag
- Use restrictive Cookie parameters
  - Set HttpOnly flag
  - Do NOT set domain
  - Do NOT set expiration date
- Non-guessable session IDs
- Provide a logout button for users
- Change session ID after a successfull authentication or role change

beim abmelden session löschen auf dem server

Same Origin Followers:

## Same Origin Policy

Superwichtig: Cross Domain Probleme -  
daten von einer domain auf eine andere domain schicken  
Das rettet die welt.. Googlen und gleichzeitig ebanking macht.

WEbcontext von einander zu isolieren. Seite A und Seite B inselben Browser dürfen nicht voneinadner häcken

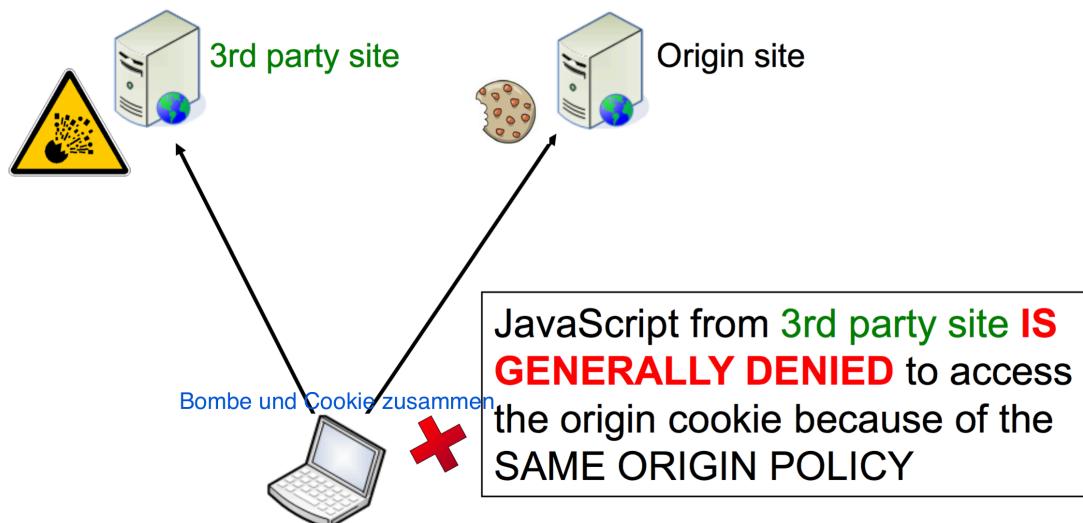
## Same Origin Followers

Restricted access to Cookies / DOM for:

- Java Script
- XMLHttpRequest (XHR)
- XDomainRequest (XDR)
- Adobe Flash
- Java Applet
- Microsoft Silverlight
- ActiveX
- Browser Extensions & Plugins

---

### Example



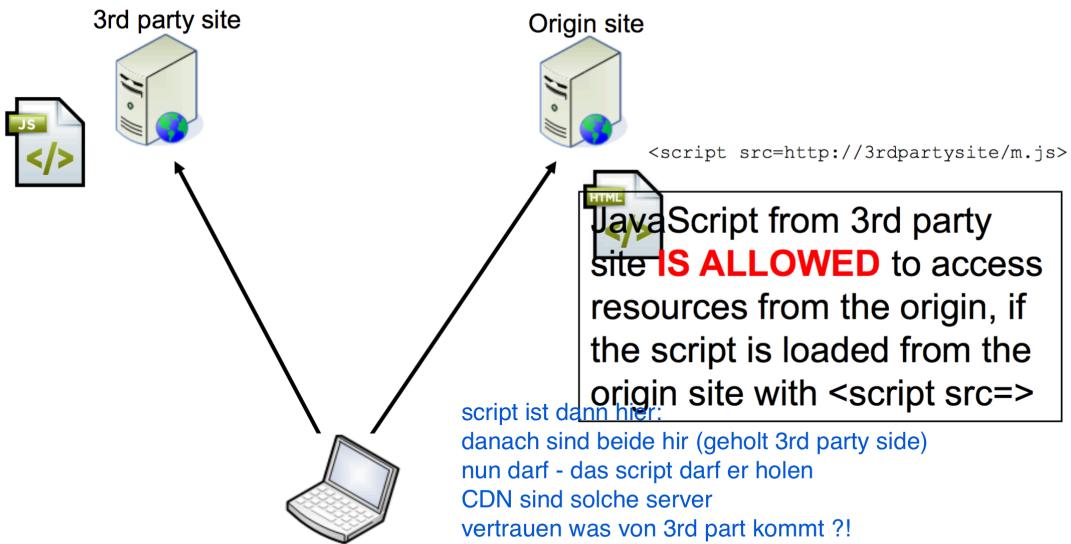
## Origin Determination Rule



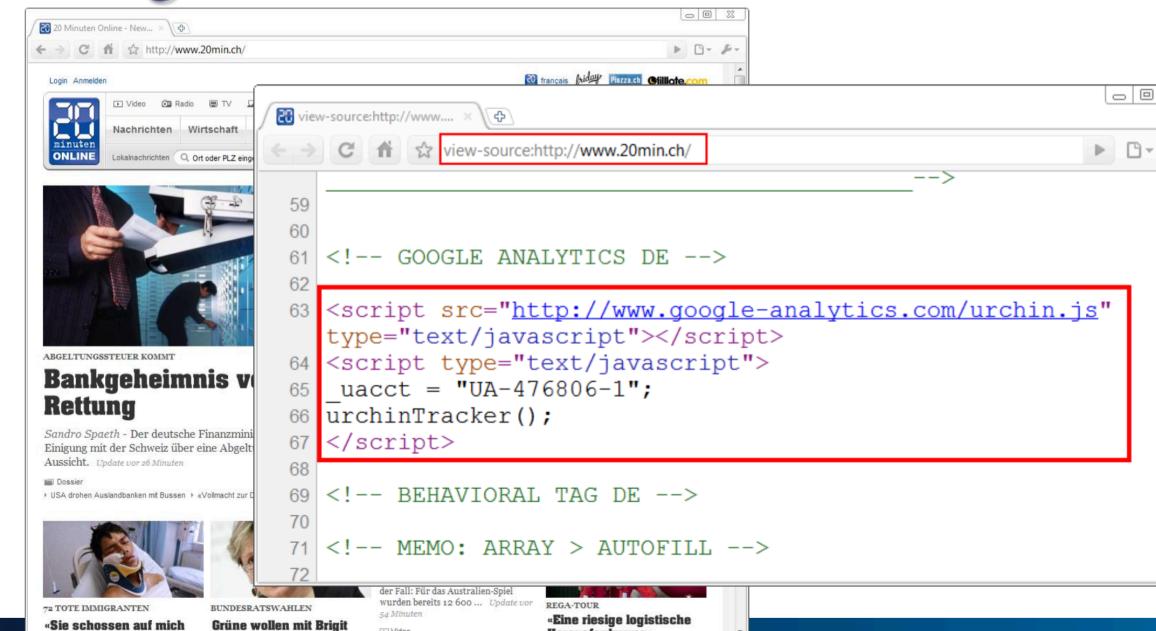
- = Protocol (http/https)
- + Host (www.csnc.ch)
- + Port (:80)

port kann implizit sein

## Solution: Include Scripts from 3rd Party



# Google Analytics



The screenshot shows a web browser window with two tabs. The left tab displays a news article from '20 Minuten ONLINE' about Sandro Spaeth. The right tab shows the source code of the same page. A red box highlights a portion of the JavaScript code:

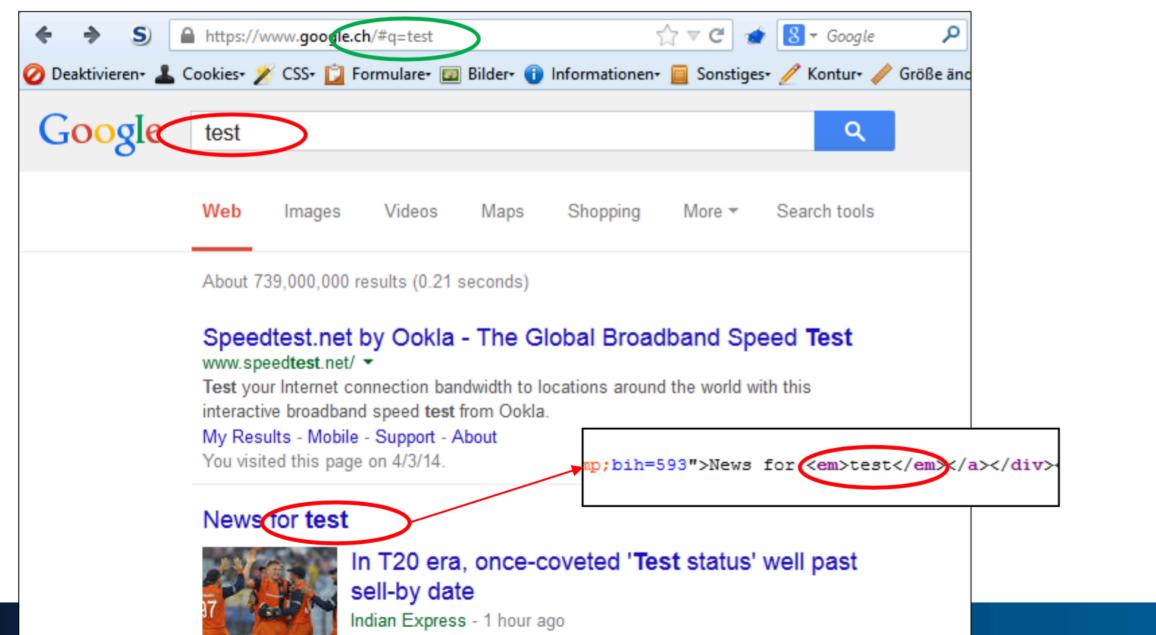
```
59
60
61 <!-- GOOGLE ANALYTICS DE -->
62
63 <script src="http://www.google-analytics.com/urchin.js"
64 type="text/javascript"></script>
65 <script type="text/javascript">
66 _uacct = "UA-476806-1";
67 urchinTracker();
68
69 <!-- BEHAVIORAL TAG DE -->
70
71 <!-- MEMO: ARRAY > AUTOFILL -->
72
```

Cross Site Scripting (ist eigentlich html injection)

Basic Problem: (folgendes Beispiel ist noch kein hackerangriff):  
Aber es zeigt, dass der UserInput mit der Antwort wieder zurückkommt (userInput macht also einen Serverroundtrip)

## Basic problem

Dynamic websites use inputs from users in the output:



The screenshot shows a Google search results page for the query 'test'. A red box highlights the search term 'test' in the search bar. Below the search bar, a news snippet from Indian Express is shown, with a red box highlighting the HTML code: `<span>bih=593">News for <em>test</em></a></div>`. A red arrow points from the highlighted code in the snippet to the highlighted 'test' in the search bar.

## Basic problem

What happens if we enter things like:

```
<blink>Hello</blink>?  
<h1>Title</h1>?  
?  
<script>alert(1)</script>?
```

hackerserver is im internet  
website in internet  
The content and/or behavior of the website in the browser can be controlled by inserting arbitrary  
benutzer in firma mit firewall und geht nach drausen auf website  
HTML code or JavaScript.

böser häcker  
port 80 auf häckerserer evil.js prox yport offen 1337 inkl. monitor  
liest mite session von opfern  
schaut auf W nach schwachstelle . <script src = evil.js > das geht dann in die db vom W-system  
evil.js holt er vom Hackerserver. und das evil.js kommuniziert zum H-Server Monitor hat session  
so sieht hacker ganzes DOM - er kann auch wieder was klicken und führt das aus -.. benutzer  
merkt nüt aber er führt sachen aus im Namen vom User.

problem dort wo daten auf den beschreibungskontext greifen

## XSS Prevention

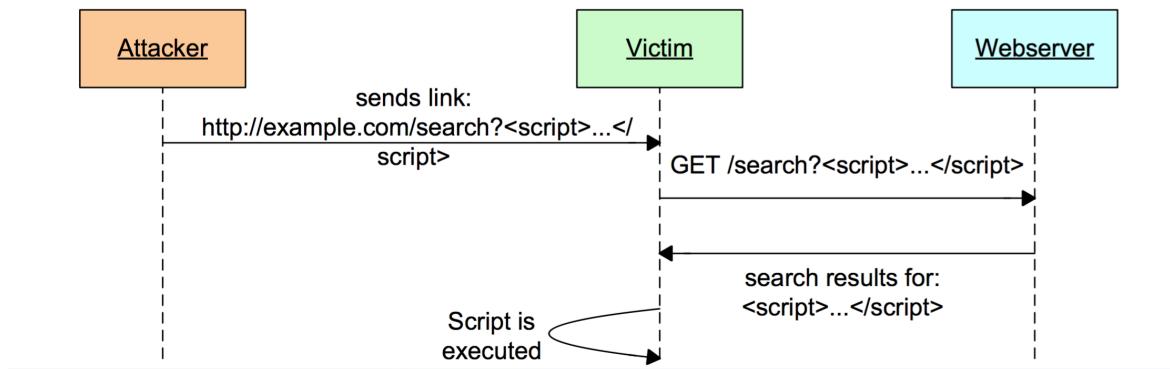
Brwoser und Server Request/Response... Injection passiert auf dem Server - da muss  
ich filtern/prüfen  
HTML Entities macht.. ich schicke script &lt;script;&gt und dann in DB speichern... in  
DB kanns gar nicht böses anrichten. Aber wenns zurückkommt:  
html - seite wird zwischenrein gebaut! Also erst dann brauchs prüfung &lg;script&gt  
(wo mach ich das rendering?)  
Angular-Client kann aber bspweise der macht nichts anfange mit &lt etc.

## Reflected XSS

über Suchfeld injection  
 Es gibt beim Seearch wieder einbetten beim rückantwort  
 Link konstruieren und z.B. auch per email an opfer (reflected -  
 get genau einmal)

- What is reflected XSS?

- Data provided by a web client is used immediately by server-side code to generate a page of results for that user
- Attacker has to send a crafted link to the victim
- Typical example: search form



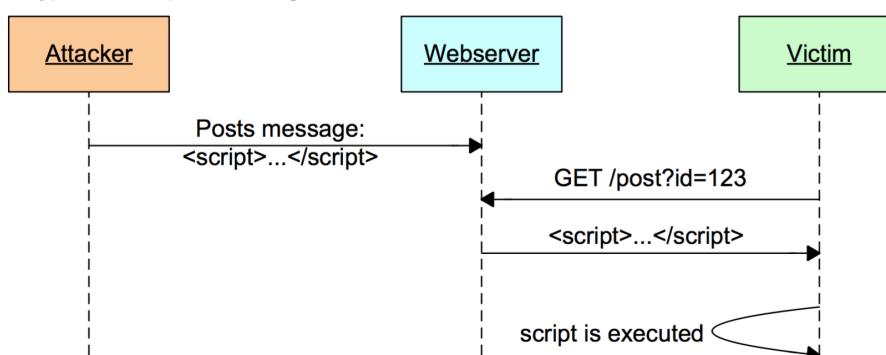
## Stored XSS

Klassischer Fall: Guestbook (offen für alle)

- What is stored XSS?

- Data provided by a web client is stored in a database. This data is then presented to the user unencoded
- Malicious script is rendered more than once
- XSS worms are based on stored XSS vulnerabilities
- Typical example: message board

HttpOnly z.B. beim cookie zum absichern

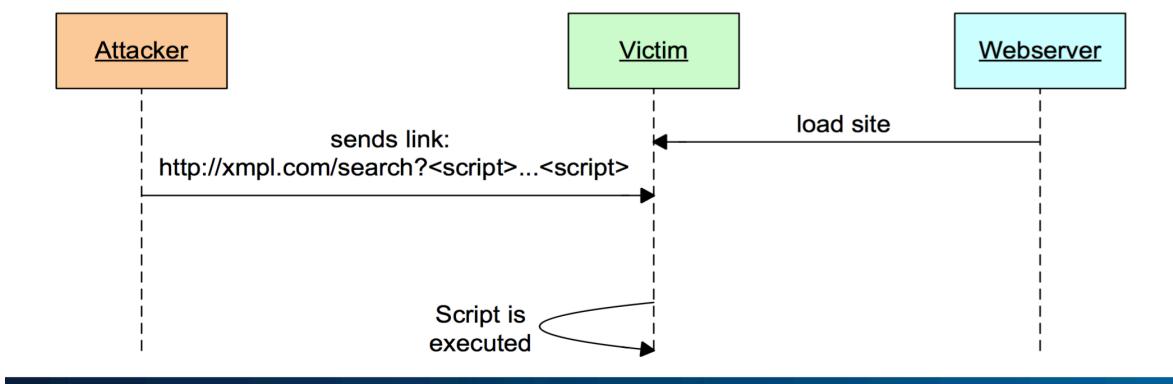


## DOM Injection

What is DOM Injection?

nur clientseitig

- Data provided by the attacker gets included in JS application
- Typical examples
  - JS application relies on URL params
  - JS application queries service data and embeds contents



problem dort wo daten auf den beschreibungskontext greifen

## XSS Prevention

Browser und Server Request/Response... Injection passiert auf dem Server - da muss ich filtern/prüfen

HTML Entities macht.. ich schicke script &lt;script&gt; und dann in DB speichern... in DB kann gar nicht böses anrichten. Aber wenns zurückkommt:

html - Seite wird zwischenrein gebaut! Also erst dann braucht Prüfung &lt;script&gt; (wo mach ich das rendering?)

Angular-Client kann aber bspweise der macht nichts anfangen mit &lt; etc.

## XSS Prevention in Node.js

Enable Template Engine Auto Escape (server.js)

Du filterst scripttag

```
swig.init({
  root: __dirname + "/app/views",
  autoescape: true // default value
});
Escape Output using "sanitizer" based on Google Caja
sanitizer.escape(poisonous_var) er macht html entnties -  
immer die welche contextwechsel zusammen
```

Escape Output using "sanitizer" based on Google Caja

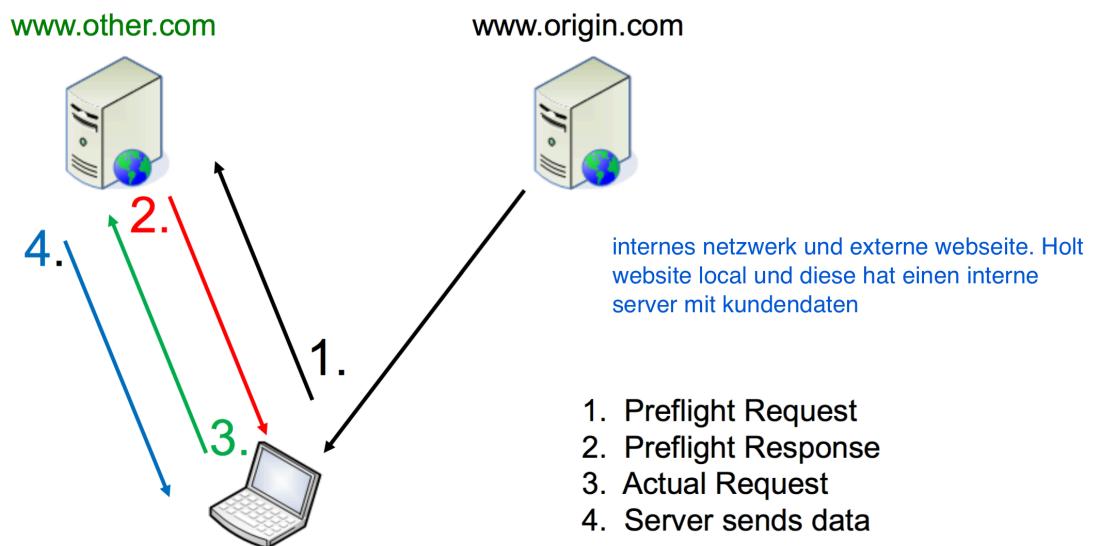
```
sanitizer.escape(poisonous_var);
< => &lt;
> => &gt;
...
```

Input Validation: Check incoming data for valid contents.

CORS:

Preflight - Request:

### CORS Preflight Request



## Conclusion

- Not adding the CORS Header «Access-Control-Allow-Origin» will stop cross origin communication (e.g. for e-banking applications)
- But if your application must be called from foreign domains, this is the way how to do it (e.g. authorizing your partners)
- If you serve non-public data, set the Access-Control-Allow-Origin according to least privileges (i.e. avoid setting header to \*)
- Preflight requests are not a security mechanism, they will not protect your server from malicious clients
- **Do NOT use the CORS headers as a method of authentication/authorization!**

## CORS Countermeasures

- Use the Access-Control-Allow-Origin header to restrict the allowed domains.
- Never set the header to \*.
- Do not base access control on the origin header.
- To mitigate DDoS attacks the Web Application Firewall (WAF) needs to block CORS requests if they arrive in a high frequency.

SEO:

## Das Ziel von Suchmaschinen: relevante Ergebnisse

The screenshot shows the Credit Suisse homepage with a search bar at the top. Below it, a navigation menu includes 'Produkte und Dienstleistungen', 'News und Expertise', 'Karriere', 'Wir über uns', and 'Suchen: Schweiz'. A sidebar on the right provides contact information: 'Beratungsgespräch vereinbar', 'Rufen Sie uns an: 0844 100 111', and 'Finanzierung anfragen'. The main content area displays search results for 'Variable Hypothek', with a snippet from a page about variable mortgages.

Relevanz: Bank Angebot oder Tagi Artikel - was ist wichtiger?!

<https://www.credit-suisse.com/ch/de/privatkunden/hypotheken/hypothekenmodelle/variable-hypothek.html> (1. Suchresultatseite für «variable Hypothek»)

The screenshot shows the TagesAnzeiger website's search results for 'variable Hypothek'. It features a header with 'TagesAnzeiger' and 'WIRTSCHAFT'. Below the header, there are news categories like 'ZÜRICH', 'SCHWEIZ', 'AUSLAND', 'WIRTSCHAFT', 'BÖRSE', 'SPORT', 'KULTUR', and 'PANORAMA'. The main content area shows a news article titled 'Die UBS trennt sich von einem alten Zopf'.

<http://www.tagesanzeiger.ch/wirtschaft/geld/Die-UBS-trennt-sich-von-einem-alten-Zopf/story/11796652> (13. Suchresultatseite für «variable Hypothek»)

## Relevanz = was steht auf der Seite?

The screenshot shows a real estate website for Hausinfo.ch. Several elements are highlighted with red arrows:

- 1. Titel (<title>-Tag)**: Points to the title bar of the browser.
- 2. Hauptüberschrift (<h1>-Tag)**: Points to the main heading 'Nebenkosten beim Stockwerkeigentum'.
- 3. Navigation**: Points to the navigation bar.
- 4. URL**: Points to the URL in the browser's address bar.
- 5. Fließtext**: Points to the main text content about additional costs for apartment owners.
- 6. Linktexte**: Points to internal links within the page.
- 7. Meta Description**: Points to the meta description tag in the page's code.

Annotations in blue text provide additional context:

- Konsistenz mit Title Fliesstext..etc.
- Auch Links zum Thema
- Einzigartigkeit der URL (unique)
- Keywords sind weniger wichtig

© Unic - Seite 12

## schema.org

- schema.org bietet zusätzliche Informationen, damit Suchmaschinen die Semantik erkennen können.
- Beispiel: [www.mondovino.ch](http://www.mondovino.ch)
- Details auf <http://schema.org>
- Einbindung im HTML-Code oder über JSON-LD (<https://developers.google.com/schemas/format/json-lld?hl=de>)
- Testing über das Test-Tool für strukturierte Daten: <http://www.google.ch/webmasters/tools/richsnippets>

MEine HTML mit Schema.org Informationen  
z.B. Ratings gleich anzeigen  
Schema.org/Rating ... dann wird das ausgelesen  
inkl. Test-Tool

**Vorschau**

Aigle Les Murailles H. Badoux Chablais AOC - Waadt - Schweiz ...  
https://www.mondovino.ch/Weisswein/\_Les.../P1000009107s...  
★★★★★ Bewertung: 4,5 - 173 Abstimmungsergebnisse - 16,80 CHF  
Der Ausschnitt der Seite wird hier erscheinen. Momentan kann kein Text von Ihrer Webseite angezeigt werden, da der Text von der Suchanfrage des Nutzers abhängt.

**z.B. auch wichtig bei Rezept plattform mondovino - explizites PRodukt**

**Publisher**

Die Seite enthält kein Publisher-Markup. Weitere Informationen

**Extrahierte strukturierte Daten**

rdfa-node	property:
	title: Aigle Les Murailles H. Badoux Chablais AOC - Waadt - Schweiz - Mondovino
	site_name: Mondovino

## Machine Learning: RankBrain

- Google setzt die Machine Learning-Technologie RankBrain als Teiles Kernalgorithmus ein, um relevante Inhalte im Index zu finden.
- RankBrain ist bereits das dritt wichtigste Rankingsignal
- Eine Frage, bei der RankBrain weiterhelfen kann (Verfeinerung des Queries):  
*What's the title of the consumer at the highest level of a food chain?*

What's the title of the consumer at the highest level of a food chain

google macht vieles. Google-KI: Google-Schlagzeilen

Voice-Search und komplexe Fragen Images News Videos Shopping More ▾ Search tools

Food Chain (keine Kette sondern Food-Chain)  
Auch werden dann relevante Teaser Infos

About 34,500,000 results (0.38 seconds)

15% der \*\*\* hat google noch nie gesehen! **Food Chain Glossary: EnchantedLearning.com**  
Google weiss auch nicht mehr [www.enchantedlearning.com/subjects/foodchain/glossary.shtml](http://www.enchantedlearning.com/subjects/foodchain/glossary.shtml) ▾  
It cannot make its own food (unlike most plants, which are producers). ... Trophic level 4 is predators that eat secondary consumers - organisms at this level are ...

**Consumer (food chain) - Wikipedia, the free encyclopedia**  
https://en.wikipedia.org/wiki/Consumer\_(food\_chain) ▾ Wikipedia ▾  
Consumers are organisms of an ecological food chain that receive energy by ... 1 Classification; 2 Levels; 3 Importance to the ecosystem; 4 See also ... at the top of food chains, capable of feeding on secondary consumers and primary consumers. ....  
Retrieved from "https://en.wikipedia.org/w/index.php?title=Consumer\_(...)"

**Who eats what in the food chain? Trophic levels of food chains**  
schooltoday.com/ecosystems/ecosystem-trophic-levels.html ▾  
The levels of a food chain (food pyramid) is called Trophic levels. The trophic level of an ... These usually eat up the primary consumers and other animal matter. They are commonly ... At the top of the levels are Predators. They are animals that ...

Mehr zu RankBrain bei Searchengineland: <http://searchengineland.com/faq-all-about-the-new-google-rankbrain-algorithm-234440> (Juni 2016)

## Gute URLs sind eine wichtige Grundlage für SEO

- In einem CMS sind Inhalte z.B. in Baum-Strukturen angeordnet. Diese Information ist für Suchmaschinen nicht einsehbar.
- Die Suchmaschine crawlt Websites auf URL-Basis und «strukturiert» Websites auf Struktur Baumstruktur ... SEO sieht diese aber nicht einfach so URLs sind wichtig...  
1 URL 1 Suchres. Gleicher 1 Inhalt auf verschiedenen URLUnter der URL Nicht zuviele URL nicht zuwenige URLs  
Dynamische WEBSITE : es wird immer wichtiger
- 1 URL ergibt 1 Suchresultat bei Google

➔ Nicht zu viele, aber auch nicht zu wenige URLs generieren

## Zu viele URLs

The screenshot shows a Google search results page for the query "site:coopathome.ch "pro montagna"". The results list several URLs from the Coop Pro Montagna website, including:

- Coop Pro Montagna - Für unsere Berge - coop.ch
- Labels - Pro Montagna - coop@home

Each result link points to a different product page or category on the website, such as 'www.coopathome.ch/...do?...', 'Pro Montagna', and 'Labels - Pro Montagna'. The page also shows navigation links like 'Projekte', 'Sortiment', 'Pro Montagna coop@home Standards', and 'Labels - Pro Montagna - coop@home'. The overall layout is typical of a Google search result with snippets of the page content and small thumbnail images.

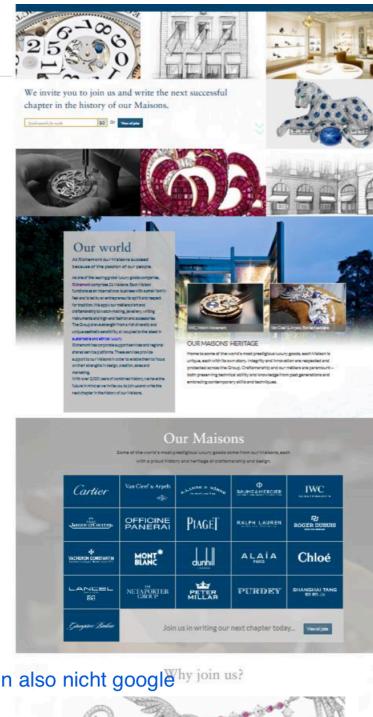
Es entsteht «Duplicate Content»:  
<http://moz.com/learn/seo/duplicate-content>

LAbel Seite für Pro Montagna ist x-mal drin . .... schlecht (performance unnötig verbraucht).

# Onepager: Eine URL für alle Inhalte

## Storytelling Ansatz

- Beispiel: Richemont Careers:  
<https://careers.richemont.com/content/careers/com/international/en.html>
  - Der Onepager von Richemont Careers erzählt eine Geschichte.
  - Er beinhaltet eine Menge Text / Keywords
  - Der ganze Inhalt ist crawlbar
  - Die Seite ist für einzelne Keywords (z.B. Brand Management) eventuell zu wenig relevant.
- ➔ Onepager sind manchmal nicht ideal, wenn man organischen Search Traffic generieren will.



wenn meine Usergruppe über Facebook aktiv ist dann also nicht google

Why join us?

## 3½ Möglichkeiten, dynamische Inhalte zur Verfügung zu stellen

- Templates zweimal bauen: clientseitig und serverseitig
- Isomorpher Ansatz (Universal-Ansatz): clientseitig und serverseitig gleicher Code
- HTML generieren mit Headless Browsers (z.B. phantomJS, casperJS, Puppeteer / Chrome im Headless-Mode etc.)
- (Warten, bis Google vollumfänglich mit Javascript und AJAX umgehen kann)  
[HTML kann man einfach korrigieren, JS kann man nicht korrigieren, Aber Dynamische Sachen kann Google nicht korrigieren](#)

## von dynamischen Inhalten

---

### “Best Practice:

- Use server-side or hybrid rendering so users receive the content in the initial payload of their web request.
- Always ensure your URLs are independently accessible:  
<https://www.example.com/product/25/>  
The above should deep link to that particular resource.
- If you can't support server-side or hybrid rendering for your Progressive Web App and you decide to use client-side rendering, we recommend using the Google Search Console “Fetch as Google tool” to verify your content successfully renders for our search crawler.  
(...)  
• Provide an XML Sitemap  
XML-sitemap  
prioris angeben,  
google-bot macht  
das früh

<https://webmasters.googleblog.com/2016/11/building-indexable-progressive-web-apps.html> (Nov. 2016)

accelerated mobile sites: AMP:



## Zwischenfazit

---

[schnell und richtige Inhalte liefern \(anstatt fancy\)](#)

- Im Zweifelsfall lieber eher statische(re) Seiten erstellen.
- Mit dem starken Fokus auf Speed und Mobile-Nutzung wird Google weiterhin pushen, dass dynamische Webinhalte crawlbar werden.
- Wenn eine URL im Chrome 41 Fehler ausgibt, dann kann Google eventuell auch nicht damit umgehen.
- Testing, Testing, Testing

[Google Cache prüfen](#)

## Take-Away-Messages zu dynamischen Inhalten und SEO

- Die **URL** ist ein zentrales Element für SEO.
- 1 URL = 1 Suchresultat bei Google
- Wenn man organischen Traffic für viele Suchanfragen generieren will, sind Onepager und Single Page Applications manchmal nicht ideal.
- Bei dynamischen Inhalten können über **HTML5 pushState** spezifische URLs generiert werden.
- Hashbang-URLs (#!) gelten seit Oktober 2015 bei Google als **deprecated**
- Mit **phantomJS oder Puppeteer** können aus dynamischen Inhalten HTML-Seiten generiert werden.
- Der isomorphe Ansatz (**Universal-Ansatz**) wird dank Initiativen wie next.js einfacher umzusetzen
- Die Fähigkeiten von Google bei der Indexierung dynamischer Inhalte sind immer noch nicht ganz klar.  
=> **Testing** ist wichtig.
- Für Google sollte sichergestellt werden, dass **alle zum Rendering notwendigen Dateien zugänglich** sind
- Der Abruf wie durch Google kann in der **Google Search Console** (ehem. Google Webmaster Tools) getestet werden.

## Which mark-up is necessary for AMP?

Rule	Description
Start with the <code>&lt;!doctype html&gt;</code> doctype.	Standard for HTML.
Contain a top-level <code>&lt;html amp&gt;</code> tag ( <code>&lt;html amp&gt;</code> is accepted as well).	Identifies the page as AMP content.
Contain <code>&lt;head&gt;</code> and <code>&lt;body&gt;</code> tags.	Optional in HTML but not in AMP.
Contain a <code>&lt;meta charset="utf-8"&gt;</code> tag as the first child of their <code>&lt;head&gt;</code> tag.	Identifies the encoding for the page.
Contain a <code>&lt;script async src="https://cdn.ampproject.org/v0.js"&gt;&lt;/script&gt;</code> tag as the second child of their <code>&lt;head&gt;</code> tag.	Includes and loads the AMP JS library.
Contain a <code>&lt;link rel="canonical" href="\$SOME_URL\$"&gt;</code> tag inside their <code>&lt;head&gt;</code> .	Points to the regular HTML version of the AMP HTML document or to itself if no such HTML version exists. Learn more in <a href="#">Make Your Page Discoverable</a> .
Contain a <code>&lt;meta name="viewport" content="width=device-width,minimum-scale=1"&gt;</code> tag inside their <code>&lt;head&gt;</code> tag. It's also recommended to include <code>initial-scale=1</code> .	Specifies a responsive viewport. Learn more in <a href="#">Create Responsive AMP Pages</a> .
Contain the <a href="#">AMP boilerplate code</a> in their <code>&lt;head&gt;</code> tag.	CSS boilerplate to initially hide the content until AMP JS is loaded.

### AMP boilerplate code

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>Sample document</title>
    <link href="https://cdn.ampproject.org/v0/regular-html-version.html?amp">
    <meta name="viewport" content="width=device-width,minimum-scale=1,initial-scale=1">
    <style amp-custom>
      h1 {color: red}
    </style>
    <script type="application/ld+json">
    {
      "@context": "http://schema.org",
      "@type": "NewsArticle",
      "headline": "Article headline",
      "image": [
        "thumbnail1.jpg"
      ],
      "datePublished": "2015-02-05T08:00:00+00:00"
    }
    </script>
    <script async custom-element="amp-carousel" src="https://cdn.ampproject.org/v0/amp-carousel-0.1.js"></script>
    <script async src="https://cdn.ampproject.org/v0.js"></script>
  </head>
  <body>
    <h1>Sample document</h1>
    <p>Some text</p>
    <amp-img src="sample.jpg" width="300" height="300"></amp-img>
    
    <div>An ad</div>
  </body>
</html>
```

## Accessibility:

### Demo 1: Tabellen

- Take home:
  - **Verwende `<th>` für Titelzellen** (mit scope Attribut, wenn sinnvoll)
  - **Verwende `<caption>` für Beschreibung der Tabelle**

## Demo: Icon-Link

---

- Take home:
  - **Für rein visuelle Elemente immer einen versteckten alternativen Text definieren**

## Demo 2: Formular-Markup und -Validierung

---

- Take home:
  - **Verwende ein <label> für jedes Feld**
  - **Markiere obligatorische Felder mit Text innerhalb des Labels.**  
Verwende required and aria-required Attribute als *progressive enhancement*.
  - **Teile dem User mit, wenn ein Input nicht valide ist:**
    - a) Ergänze das Label mit einer Fehlermeldung und fokussiere das erste invalide Feld.  
Verwende aria-invalid zur zusätzlichen Indikation.
    - b) Verwende aria-describedby um Fehlermeldungen mit dem entsprechenden Feld zu verbinden.

## Demo 3: Seitenstruktur

---

- Take home:
  - **Verwende versteckte <hX> Elemente, um Bereiche auszuzeichnen**
  - **Verwende die semantisch korrekten Markup-Elemente in Kombination mit ARIA-Rollen. Bsp: <main role="main">...</main>**
  - **Verwende Skiplinks, um dem User zu ermöglichen, Bereiche wie die Navigation zu überspringen**

## 4. Tastaturbedienbarkeit: Demos 4 und 5

---

- Take home:
  - **Entferne die Focus-Styles nie**
    - Falls doch: Definiere alternative, gut sichtbare Styles
  - **Verwende bereits barrierefreie Elemente wie <a> oder <button>**
    - Falls nicht: Füge role="button" und tabindex="0" hinzu und definiere keydown listeners für Space- und Enter-Taste

## Skalierbarkeit

---

- Ansatz: relative Dimensionen wie em oder %
  - WCAG: 1.4.4 Resize text: Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality. (Level AA)
- Anti-Pattern:

```
<meta name="viewport" content="width=device-width,  
initial-scale=1.0, user-scalable=no" />  
<meta name="viewport" content="width=device-width,  
initial-scale=1.0, maximum-scale=1" />
```
- Okay: einige Seiten wollen auf smartphones nicht skalieren um das gefühl einer App zu

```
<meta name="viewport" content="width=device-width,  
initial-scale=1.0" />
```

## WCAG 2.0 als Basis

- WCAG: **Web Content Accessibility Guidelines**
- W3C Recommendation, <http://www.w3.org/TR/WCAG/>

# Wie die WCAG strukturiert sind

---

- **4 Prinzipien**

- *perceivable / wahrnehmbar*
- *operable / bedienbar*
- *understandable / verständlich*
- *robust*

- **12 Richtlinien**

- Testbare **Erfolgskriterien** für jede Richtlinie  
[definiert wie man das testen kann](#)
- **3 Konformitätslevels** für Erfolgskriterien: A (tiefstes), AA, AAA (höchstes)  
[Pdfs, Videos?!, Standard für CH ist AA](#)
- **Ausreichende und empfohlene Techniken** zur Erfüllung eines Kriteriums  
[Katalog anschauen](#)



## ARIA: States and Properties

---

- Schwierige Abgrenzung, teilweise unter gemeinsamem Begriff "Attribut"
- Properties ändern tendenziell seltener während «life-cycle» der Applikation
- State: aria-expanded, aria-hidden
- Property: aria-describedby, aria-live

[state: aria-expanded \(drop expanded\), oder hidden um es vom screen zu verstecken.](#)  
[eigentlich sonst egal ob state oder property](#)

## Demo 6: Auto-suggest

---

- Take home:
  - **Definiere keydown listeners für Pfeiltasten, um durch Suggestions zu navigieren**
  - **Informiere den User mit ARIA live region über dynamischen Inhalt**
  - **Verwende die Rollen listbox (Container) und option (Suggestions)**
  - **Verwende den Zustand aria-expanded je nach Sichtbarkeit der Suggestions**

Testing:  
linter, onlinetools, Tenon