



OWASP TOP 10

falk-m.de
2024

OWASP

- Open Worldwide Application Security Project (OWASP)
- Non profit organization, aiming to increase security in www
- Top 10 list of most critical security risks to web applications
- <https://owasp.org/Top10/>










A01: Broken Access Control

A01: Broken Access Control

- view or modification of data, performing functions
- out of users permissions or limits
- missing or wrong user authentication

web server directory listing

Index of /

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	README.md	2023-12-08 12:30	199	
	api/	2024-01-03 15:10	-	
	docker-compose.yml	2023-12-08 12:23	806	
	docker/	2023-06-09 07:02	-	
	www/	2024-01-03 15:10	-	

Cross-Site Request Forgery (CSRF)

interaction with user authentication, e.g., permits requests and uses the session cookie

```
<form>  
  <input type="hidden" name="_csrf" value="550e8400-e29b-11d4-a716-446655440000" />  
  <button>Delete</button>
```

- session based anti-csrf-token must be permitted for action
- reauthentication for high risk actions

Cross-Origin Resource Sharing (CORS)

- Policy to use resources in Browser
- Host: managed by '**Content-Security-***' headers
- Resource: ,**Access-Control-Allow-Origin: ***'
- Same-Origin-Policy by default



Cookie-Einstellungen

Cookies und ähnliche Tools, die erforderlich sind, um dir das Tätigen von Einkäufen zu ermöglichen, dein Einkaufserlebnis zu verbessern und unsere Dienste bereitzustellen, wie in unserem [Cookie-Hinweis](#). Wir verwenden diese Cookies auch, um zu verstehen, wie Kunden unsere Dienste nutzen (z. B. durch Messung der Websiteaufrufe), damit wir Verbesserungen vornehmen können.

Wir verwenden wir auch Cookies, um dein Einkaufserlebnis in den Onlineshops zu verbessern, wie in unseren [Cookie-Hinweis](#) beschrieben. Deine Wahl gilt für die Verwendung von Werbe-Cookies und Drittanbietern für diesen Service. Cookies speichern oder greifen auf Standardgeräteinformationen wie eine eindeutige Kennung zu. Die [103 Drittanbieter](#), die auf diesem Dienst Cookies zu ihren Zwecken, um personalisierte Werbung anzuzeigen und zu messen, Einblicke in die Zielgruppe zu gewinnen und Produkte zu entwickeln und zu verbessern. Klicke auf „Ablehnen“, um auf „Anpassen“, um detailliertere Werbeoptionen auszuwählen oder mehr zu erfahren. Du kannst deine Auswahl jederzeit ändern, indem du die [Cookie-Einstellungen](#) aufrufst, wie im Cookie-Hinweis. Um mehr darüber zu erfahren, wie und zu welchen Zwecken Amazon personenbezogene Daten verwendet (z. B. den Bestellverlauf des Amazon Store), besuche bitte unsere [Datenschutzrichtlinie](#).

Ablehnen

Anpassen

Kopfzeilen durchsuchen

Blockieren Erneut senden

content-encoding: gzip

content-language: de-DE

 content-security-policy: upgrade-insecure-requests;report-uri <https://metrics.media-amazon.com/> content-security-policy-report-only: default-src 'self' blob: https: data: mediastream: 'unsafe-eval' 'unsafe-inline';report-uri <https://metrics.media-amazon.com/>

The image shows a screenshot of a web browser window. The main content area displays a collection of various Amazon logos, including 'smile', 'amazon', 'prime', 'prime day', 'amazon.ae', 'fresh', and 'amazon smile'. Below the logos, there are several icons: a magnifying glass, a location pin, a shopping cart, a user profile, and a checkmark. The browser's address bar is empty. The bottom of the browser window shows the Chrome DevTools interface. The 'Netzwerk' (Network) tab is selected, and the 'Kopfzeilen' (Headers) sub-tab is active. The 'Kopfzeilen' tab shows a list of headers, with 'access-control-allow-origin: *' highlighted in a red box. Other headers visible include 'accept-ranges: bytes' and 'age: 6096756'. The 'Cookies' tab is also visible, showing a list of cookies. The 'Anfrage' (Request) and 'Antwort' (Response) tabs are also visible. The 'Zeilen' (Lines) tab is also visible. The 'JS' tab is also visible. The 'XHR' tab is also visible. The 'Schriften' (Fonts) tab is also visible. The 'Medien' (Media) tab is also visible. The 'WebSockets' tab is also visible. The 'Sonstiges' (Other) tab is also visible. The 'C' tab is also visible.

smile amazon prime prime prime prime day amazon amazon smile amazon.ae fresh fresh amazon smile

Stilbearbeitung Laufzeitanalyse Speicher Web-S

JS XHR Schriften **Grafiken** Medien WebSockets Sonstiges

rag... Gr... **Kopfzeilen** Cookies Anfrage Antwort Zei

ND... Kopfzeilen durchsuchen

ND... accept-ranges: bytes

access-control-allow-origin: *

age: 6096756

Content-Security-Policy: **default-src** data: blob: 'self' https://*.fbshx.com *.facebook.com *.fbcdn.net 'wasm-unsafe-eval';**script-src** *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.google.com 127.0.0.1:* blob: data: 'self' connect.facebook.net 'wasm-unsafe-eval';**style-src** fonts.googleapis.com *.fbcdn.net data: *.facebook.com 'unsafe-inline';**connect-src** *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbshx.com *.fb.com wss://web.whatsapp.com/ws/chat reg-e2ee.facebook.com api1.tenor.co media.tenor.co cdn.fbsbx.com https://api.mapbox.com https://*.tiles.mapbox.com;**font-src** data: *.gstatic.com *.facebook.com *.fbcdn.net *.fbshx.com;**img-src** *.fbcdn.net *.facebook.com data: https://*.fbshx.com *.tenor.co media.tenor.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net *.giphy.com connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: googleads.g.doubleclick.net www.googleadservices.com *.whatsapp.net *.fb.com *.oculuscdn.com;**media-src** *.cdninstagram.com blob: *.fbcdn.net *.fbshx.com www.facebook.com *.facebook.com https://*.giphy.com data:;**frame-src** *.doubleclick.net *.google.com *.facebook.com www.googleadservices.com *.fbshx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com https://sandbox.paywithmybank.com;**worker-src** *.facebook.com/static_resources/webworker_v1/init_script/ *.facebook.com/static_resources/webworker/init_script/ *.facebook.com/static_resources/sharedworker/init_script/ *.facebook.com/static_resources/webworker/map_libre/ *.facebook.com/static_resources/webworker/map_libre_rtl/ *.facebook.com/sw/ *.facebook.com/sw;block-all-mixed-content;upgrade-insecure-requests

facebook

Auf Facebook bleibst du mit Menschen in Verbindung und teilst Fotos, Videos und vieles mehr mit ihnen.

Passwort

Anmelden

[Passwort vergessen?](#)

Neues Konto erstellen

Konsole Debugger **Netzwerkanalyse** Stilbearbeitung Laufzeitanalyse Speicher Web-Speicher

thsuche || + 🔍 ⛔ Alles HTML CSS **JS** XHR Schriften Grafiken Medien WebSockets Sonstiges ☐ Cache deaktivieren

Datei	Initiator	Typ	Übertrag...	Gr...	Kopfzeilen	Cookies	Anfrage	Antwort	Zeit	Sich...
b9smUWnHJW6.js?_nc_x=lj3Wp8lg5K	script	js	101,19 kB	38...	Kopfzeilen durchsuchen					
xGzxHlbkRpC.js?_nc_x=lj3Wp8lg5K	script	js	17,96 kB	55...	DNS-Auflösung System					
NJVgMHwCLBZ.js?_nc_x=lj3Wp8lg5K	script	js	15,94 kB	50...	Antwortkopfzeilen (1,249 kB)					
bpW4eEg-2_W.js?_nc_x=lj3Wp8lg5K	script	js	Aus Cache	1,...	access-control-allow-origin: https://www.facebook.com					
Lzd-U--zeLf.js?_nc_x=lj3Wp8lg5K	b9smUW...	js	3,14 kB	6,...	alt-svc: h3=":443"; ma=86400					

TODO: access control

- Implement access control mechanisms once and re-use them throughout the application
- Log access control failures, alert admins when appropriate
- Rate limit API and controller access

TODO: File protection

- Except for public resources, deny by default
- Disable web server directory listing
- ensure file metadata (e.g., .git) and backup files are not present within web roots

TODO: session invalidation

- Stateful session identifiers should be invalidated on the server after logout.
- Stateless JWT tokens should rather be short-lived



A02: Cryptographic Failures

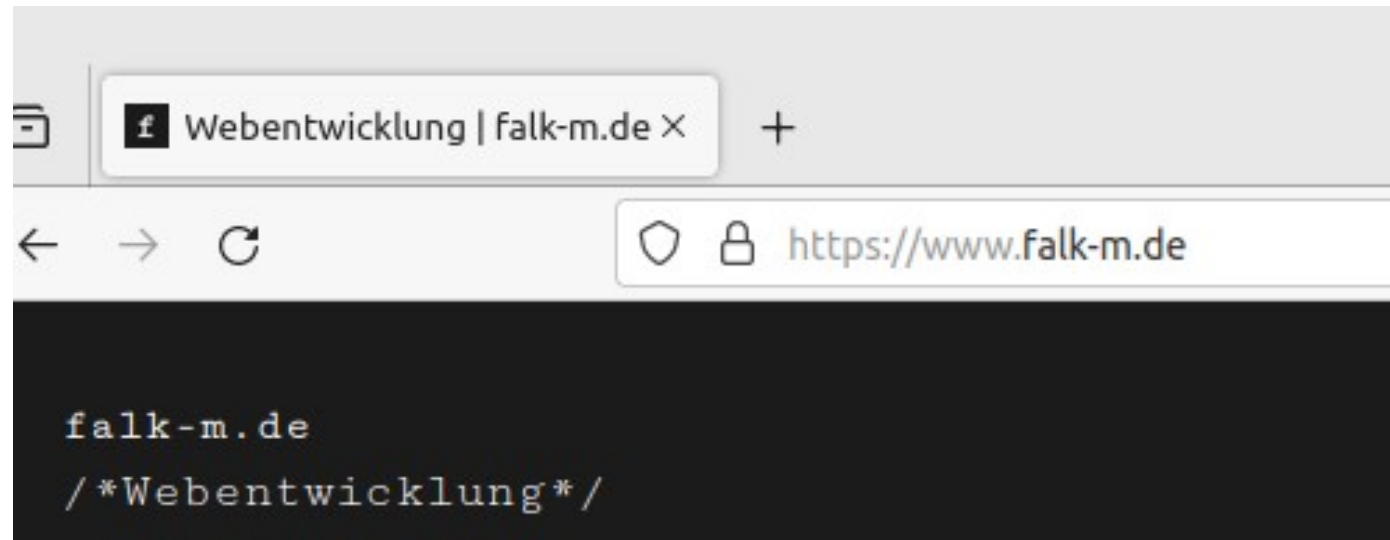
failures related to cryptography or lack of them

SFTP

The screenshot shows the interface of an SFTP client. At the top is a menu bar with the following items: Datei, Bearbeiten, Ansicht, Übertragung, Server, Lesezeichen, and Hilfe. Below the menu is a toolbar containing various icons for file operations. The main section contains input fields for connection details: 'Server:' (empty), 'Benutzername:' (xxx), 'Passwort:' (masked with three dots), and 'Port:' (22). The 'Port:' field and its value '22' are highlighted with a red rectangular box. To the right of these fields is a 'Verbinden' button and a small downward arrow. Below the input fields is a status log area with a dashed line separator. The log contains the following entries:

- Status: Verbinde mit: [redacted] ..
- Status: Verbindung hergestellt, warte auf Willkommensnachricht...
- Status: Initialisiere TLS...
- Status: Überprüfe Zertifikat...
- Status: TLS-Verbindung hergestellt.
- Status: Angemeldet

SSL/TLS



web servers, back-end systems?

TODO: transfer encryption

- Encrypt all data in transit with secure protocols such as TLS
- Do not use legacy protocols such as FTP
- Verify all internal traffic, e.g., between load balancers, web servers, or back-end systems

TODO: data encryption



- Don't store sensitive data unnecessarily. Data that is not retained cannot be stolen.
- Ensure up-to-date and strong standard algorithms, protocols, and keys
- Disable caching for response that contain sensitive data.

TODO: password encryption

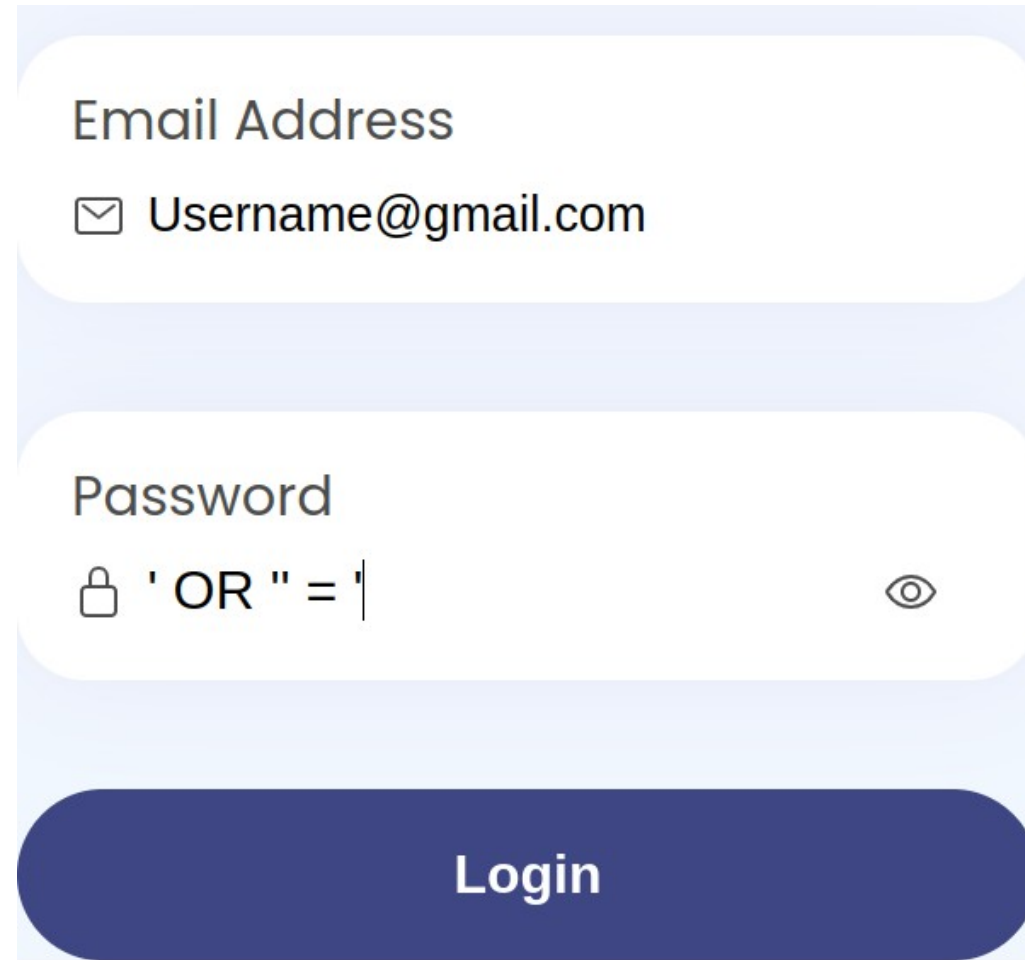


- Store passwords using strong adaptive and salted hashing functions with a work factor
 - unsalted hashes can be exposed with a rainbow table
- Avoid deprecated cryptographic functions and padding schemes, such as MD5, SHA1



A03: Injection


SQL Injection



Email Address

✉ Username@gmail.com

Password

🔒 ' OR " = ' | 

Login

WHERE Password = " **OR** " = "

TODO: use parameterized interface



Security Issue: Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.

- keeping data separate from commands and queries
- using the interpreter entirely, provides a parameterized interface
- or use escape functions

Cross-Site-Scripting

Medikament 1

Basisangaben

">pt

">pt

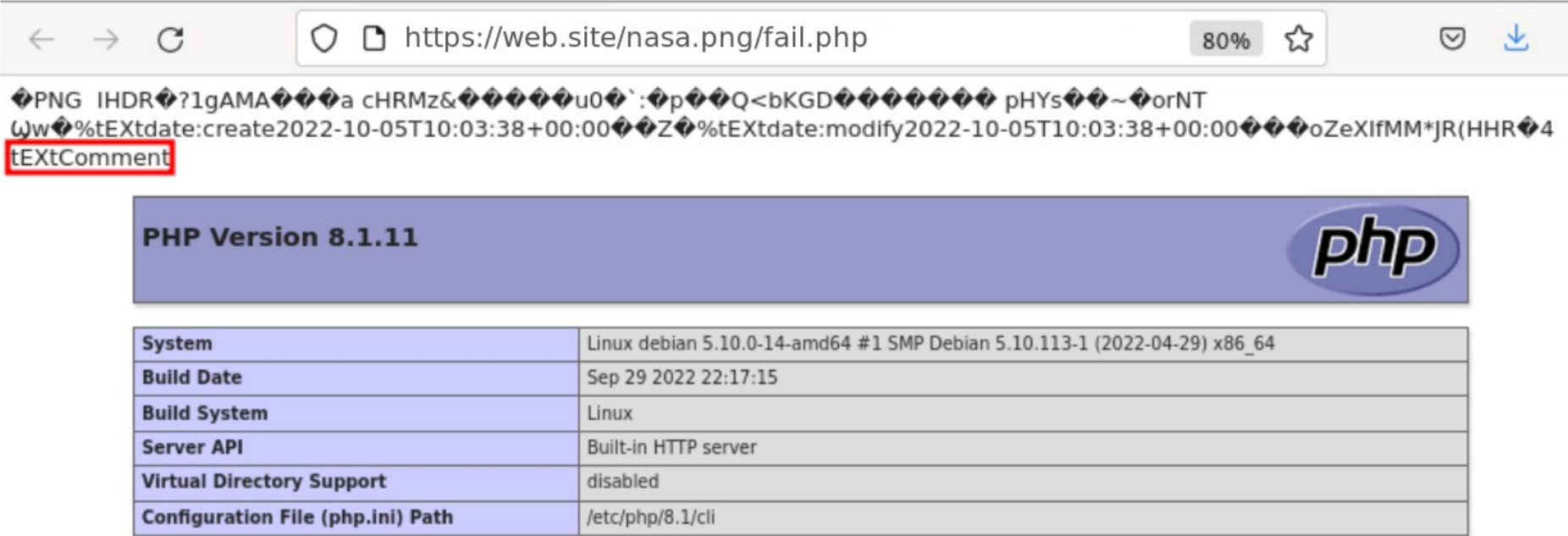
Situation

Gedanken und Gefühle

XSS_Med

OK

```
$ exiftool -comment="<?php phpinfo(); ?>" nasa.png
```



TODO: sanitize user input

Security Issue: an attack in which an attacker injects malicious executable scripts into the code of a trusted website

- Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged
- User-supplied data is validated, filtered, or sanitized by the application.



A04: Insecure Design

TODO: security by design

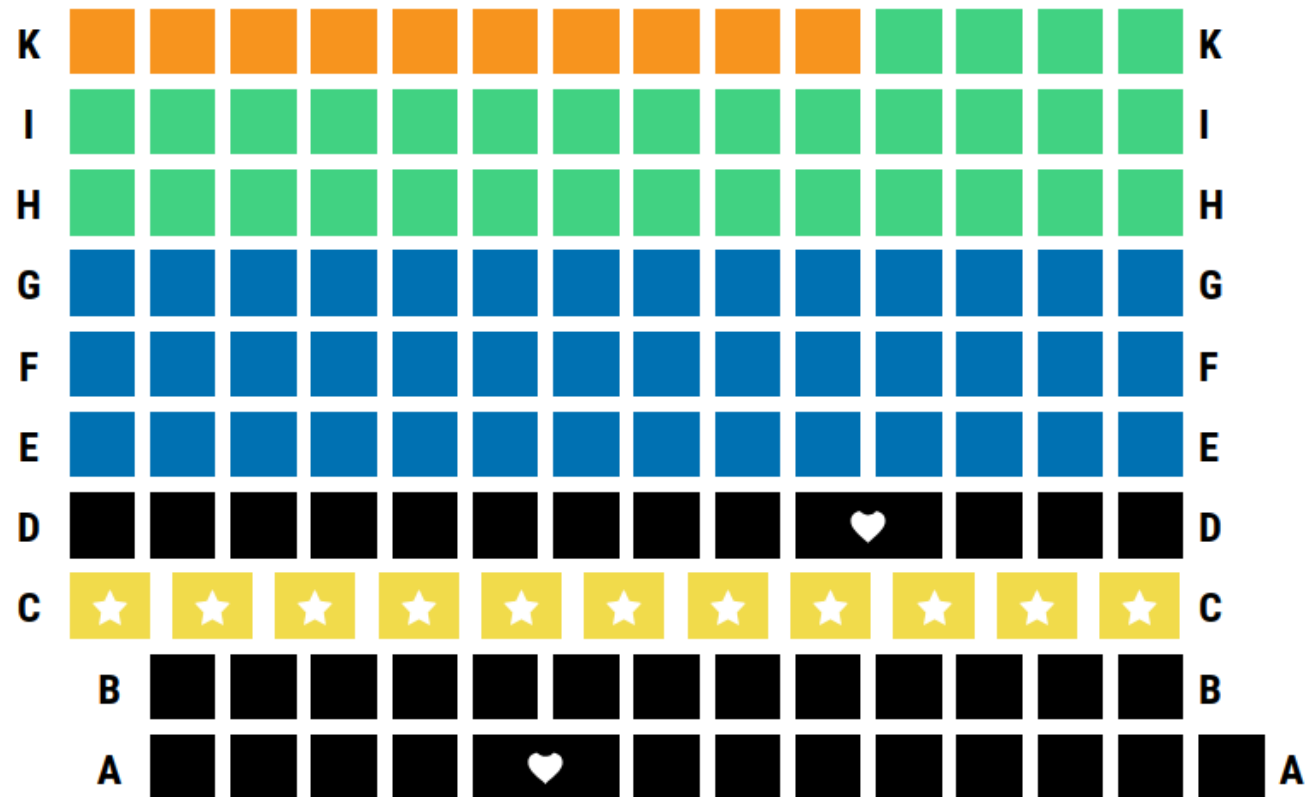
- look for changes in data flows and access control or other security controls
- In the user story, determine the correct flow and failure states


TODO: plausibility checks

- Integrate plausibility checks at each tier of your application
- Limit resource consumption by user or service

Bitte wähle maximal 10 Plätze aus

Leinwand





IHRE BESTELLUNG

PIZZA



Pizza Margarita (24 cm) -9.10€

Insgesamt für -1 Pizza Margarita: -9.10€

Gesamtbetrag inkl. MwSt.: -9.10€

BESTELLEN

TODO: few informations

Do not:

- A credential recovery workflow might include “questions and answers”, which is prohibited
- Error Message Containing Sensitive Information
- Unprotected Storage of Credentials

Error Message Containing Sensitive Information

Du hast dein Passwort vergessen?

Bitte gib hier deine E-Mail-Adresse ein. Du erhältst dann per Mail einen Link zur Erstellung eines neuen Passwortes.

Es ist kein Account zu dieser E-Mail registriert.

E-Mail-Adresse

„Sollte der Account existieren, senden wir die eine E-Mail zu.“

„Es gibt keinen Account zu dieser E-Mail oder das Passwort ist falsch“



A05: Security Misconfiguration

TODO: check configuration

Security Issues:

- Default accounts and their passwords are still enabled and unchanged.
- Error handling reveals stack traces or other overly informative error messages to users (check debug mode or environment vars)
- the latest security features are disabled or not configured securely.

No route found for "GET https://symfony.app/blog/this-page-does-not-exist"



Exceptions

2

Logs

1

Stack Traces

2

Symfony\Component\HttpKernel\Exception\

NotFoundHttpException



+ in vendor/symfony/http-kernel/EventListener/RouterListener.php (line 130)

+ in vendor/symfony/event-dispatcher/Debug/WrappedListener.php -> onKernelRequest (line 111)

+ in vendor/symfony/event-dispatcher/EventDispatcher.php -> __invoke (line 230)

+ in vendor/symfony/event-dispatcher/EventDispatcher.php -> callListeners (line 59)

+ in vendor/symfony/event-dispatcher/Debug/TraceableEventDispatcher.php -> dispatch (line 152)

+ in vendor/symfony/http-kernel/HttpKernel.php -> dispatch (line 128)

+ in vendor/symfony/http-kernel/HttpKernel.php -> handleRaw (line 74)

+ in vendor/symfony/http-kernel/Kernel.php -> handle (line 202)

+ in vendor/symfony/runtime/Runner/Symfony/HttpKernelRunner.php -> handle (line 35)

+ in vendor/autoload_runtime.php -> run (line 29)

- require_once ('/Users/antoine/Sites/demo/vendor/autoload_runtime.php')

in public/index.php (line 5)

```
1. <?php
2.
3. use App\Kernel;
```



A06: Vulnerable and Outdated Components

TODO: check features

Security issue:

- Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges)
- The software is out of date or vulnerable

Protection:

- Without a concerted, repeatable application security configuration process, systems are at a higher risk.
- Remove or do not install unused features and frameworks

TODO: hide from web



The image shows the phpMyAdmin login interface. At the top, there is a logo of a sailboat with the text "phpMyAdmin" in blue and orange. Below the logo, it says "Welcome to phpMyAdmin". There is a language selection dropdown menu set to "English". Below that is a login section with a "Log in ?" link, a "Username:" label, a password input field, and a "Go" button.

phpMyAdmin

Welcome to phpMyAdmin

Language

English

Log in ?

Username:

Password:

Go

TODO: check software

OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Only obtain components from official sources over secure links.



A07: Identification and Authentication Failures

TODO: Prevent brute Force Attacks

- Permits brute force or other automated attacks.
 - Limit or increasingly delay failed login attempts
 - Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.

TODO: Protect Sessions

- Does not expose session identifier in the URL.
- Regenerate session identifier after successful login.
- Invalidate sessions after logout or a period of inactivity.

TODO: check user passwords

- check default, weak, or well-known passwords
 - Implement weak password checks, such as testing new or changed passwords against the top 10,000 worst passwords list
- not use weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers,"
- do not use plain text, encrypted, or weakly hashed passwords data stores
- password rotation and complexity requirements encourage users to use and reuse weak passwords. Stop these practices and use multi-factor authentication.



A08 Software and Data Integrity Failures

TODO: Check components integrity

- relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs)
- Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered.
- Ensure libraries and dependencies, such as npm or Maven, are consuming trusted repositories.



A09 Security Logging and Monitoring Failures

TODO: Logging

do not:

- Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.

do:

- Ensure all login, access control, and server-side input validation failures can be logged
- log with sufficient user context to identify suspicious or malicious accounts
- NOT Insertion of Sensitive Information into Log File.

Air India Hack Exposes Credit Card and Passport Info of 4.5 Million Passengers

📅 May 22, 2021 👤 Ravie Lakshmanan



LayerX

Unveiling the Threat of Malicious Browser Extensions

Download

The Hacker News | LIVE WEBINAR

Critical SaaS Security Do's and Don'ts: Insights from 493 Companies



TODO: Escalation

do:

- Ensure that logs are generated in a format that log management solutions can easily consume.
- Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.
- use appropriate alerting thresholds, detect and alert for active attacks in real-time
- Establish or adopt an incident escalation response and recovery plan



A10 Server-Side Request Forgery (SSRF)

Paste or enter a URL

`https://falk-m.de`

No preview image
provided by website

Falk-m.de

Webentwicklung | falk-m.de

,file://' protocol, internal administration sites (mongo db, ...)

Paste or enter a URL

`file://../config.yml`

TODO: Prevent SSRF



Risk:

- a web application is fetching a remote resource without validating the user-supplied URL
- server internal requests like 'file:/' or other application internal apis

Prevent:

- Sanitize and validate all client-supplied input data
- Enforce the URL scheme, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirections



Thank you
