zurück

Zugriffsschutz – Bewerbungsnachweis

Ziel des Zugriffsschutzes

Die Anwendung zur Bewerbungsverwaltung enthält **personenbezogene Daten**, interne Notizen sowie vertrauliche Dokumente (Anschreiben, Rückmeldungen, Absagen).

Ziel des Zugriffsschutzes ist es:

- unbefugten Zugriff zu verhindern
- die Anwendung ohne zusätzliche Login-Logik abzusichern
- eine robuste, wartungsarme Lösung einzusetzen

Es wurde bewusst **keine eigene Anmeldeseite** implementiert.

Gewählte Lösung

Der Zugriffsschutz erfolgt über **HTTP Basic Authentication** mittels Apache `.htaccess`.

Gründe für diese Entscheidung

- bewährte, seit Jahrzehnten eingesetzte Technik
- keine Abhängigkeit von PHP oder Datenbank
- Schutz greift bereits vor der Anwendung
- auch bei PHP-Fehlern oder Wartung aktiv
- sehr geringer Wartungsaufwand

Für eine private Eigenanwendung ist diese Lösung **angemessen, stabil und ausreichend**.

Technische Umsetzung

1. Passwortdatei

Die Zugangsdaten werden in einer Passwortdatei gespeichert, die **außerhalb des Webroots** liegt:

snippet.text

```
/etc/apache2/htpasswd/bewerbungen.htpasswd
```

Die Datei enthält gehashte Passwörter (bcrypt/MD5 je nach Apache-Version).

Benutzer anlegen

snippet.bash

```
sudo htpasswd -c /etc/apache2/htpasswd/bewerbungen.htpasswd lars
```

Weitere Benutzer können später ergänzt werden:

snippet.bash

```
sudo htpasswd /etc/apache2/htpasswd/bewerbungen.htpasswd weitereruser
```

---

2. .htaccess-Datei

Im Wurzelverzeichnis der Anwendung:

snippet.text

```
/var/www/html/bewerbungen/.htaccess
```

befindet sich folgende Konfiguration:

snippet.apache

```
AuthType Basic
AuthName "Geschuetzter Bereich – Bewerbungsnachweise"
AuthUserFile /etc/apache2/htpasswd/bewerbungen.htpasswd
Require valid-user
```

Diese Regel schützt **alle Unterverzeichnisse**:

- /public/
- /app/
- /storage/

---

3. Apache-Konfiguration

Damit `.htaccess` ausgewertet wird, ist in der Apache-Konfiguration folgendes erlaubt:

snippet.apache

```
<Directory /var/www/html/bewerbungen>
    AllowOverride All
</Directory>
```

Nach Änderungen erfolgt ein Reload des Webservers:

snippet.bash

```
sudo systemctl reload apache2
```

Verhalten im Betrieb

- Beim Aufruf der Anwendung fordert der Browser Benutzername und Passwort an
- Ohne gültige Zugangsdaten kein Zugriff
- Nach erfolgreicher Anmeldung funktioniert die Anwendung unverändert
- Druckansicht und PDF-Erstellung bleiben möglich

Die Zugangsdaten werden vom Browser zwischengespeichert, bis dieser geschlossen wird.

Sicherheitsbewertung

Vorteile

- sehr geringer Angriffsvektor
- kein Login-Code in PHP
- kein Session-Handling notwendig
- Schutz auch für hochgeladene Dokumente
- kompatibel mit Reverse Proxies (Traefik)

Einschränkungen

- kein Rollen- oder Rechtemodell
- kein Protokoll über Benutzeraktivitäten
- Zugangsdaten werden vom Browser verwaltet

Diese Einschränkungen sind für den vorgesehenen Einsatzzweck **akzeptabel**.

Erweiterungsmöglichkeiten (optional)

Bei Bedarf kann der Zugriffsschutz erweitert werden, z. B.:

- Kombination aus Benutzer **oder** internem Netzwerk
- zeitweise Deaktivierung für Wartung
- spätere Ablösung durch eine Applikationsanmeldung

Beispiel für Zugriff aus internem Netz **oder** mit Passwort:

snippet.apache

```
<RequireAny>
    Require ip 192.168.0.0/16
    Require valid-user
</RequireAny>
```

Zusammenfassung

Der Zugriffsschutz:

- schützt alle Inhalte zuverlässig
- ist unabhängig von der Anwendung
- erfordert keine zusätzliche Logik
- ist wartungsarm und transparent

Er erfüllt die Anforderungen an Datenschutz und Zugriffskontrolle für eine **private Bewerbungsverwaltung** vollständig.