Pentest Report
“Juice Shop”

Inhaltsverzeichnis

Dokumentenhistorie

Version	Änderung	Datum	Autor
0.1	Erstellung des Dokuments	13.10.2025	Erich Geldreich
0.2	Eintragen der Findings	14.10.2025	[redacted] Erich, [redacted]
0.3	Anpassungen unter Punkt 3	16.10.2025	Erich
1.0	Finalisierung und Unterschriften	16.10.2025	[redacted] Erich, [redacted]

1 Ansprechpartner

1.1 Auftraggeber

Juice Shop Inc.
[redacted]

1.2 Auftragnehmer

ShieldSec Penetration Testing
Erich Geldreich, [redacted] Pentester
Musterstraße 456
9876 Demoort
☎ [redacted]
[redacted]

2 Projektübersicht

2.1 Einführung

ShieldSec Penetration Testing wurde mit einem Penetration Test der Web Applikation „Juice Shop" beauftragt. Das Unternehmen betreibt einen Saftladen, der unterschiedlichste Säfte online anbietet.
Die Web-App wird auf einem on premise Server des Unternehmens gehostet. Das Unternehmen möchte durch den Test einen Überblick und ein besseres Verständnis über die Sicherheitslage der selbst entwickelten App erhalten.

2.2 Rahmenbedingungen

Der Penetration Test wurde im Zeitraum 06.10.2025 bis 15.10.2025 durchgeführt und erfolgte in den Räumen der ShieldSec uncredentialed über die öffentliche Webseite durchgeführt.

2.3 Scope

Es dürfen alle im Shop angebotenen Funktionen auf ihre Sicherheit getestet werden. Einschränkungen bestehen lediglich dahingehend, dass die Funktionalität nicht unterbrochen werden darf und keine Daten verändert werden dürfen.

3 Executive Summary

Der Test wurde im Zeitraum 06.10.2025 bis 15.10.2025 durchgeführt. Dabei konnten 8 Schwachstellen identifiziert werden, die in den Findings zusammengefasst und einer Risikobewertung unterzogen wurden.

Hier die Übersicht und Risikobewertung:

Schwachstelle	**Risiko-grad**	**Pentester-in**	**Remediation (Details siehe Punkt 7)**
Login Admin Log in with the administrator's user account.	Sehr hoch	[redacted]	mittel
Forgotton Sales Backup / Poison Null Byte	Sehr hoch	[redacted]	mittel
Deluxe Fraud	Hoch	Erich	mittel
Zero Stars	Hoch	[redacted]	leicht
Weird Crypto	Hoch	[redacted]	leicht
View Basket View another user's shopping basket.	Hoch	[redacted]	leicht
Forged Coupon	Hoch	[redacted]	leicht
Empty User Registration	Normal	Erich	leicht

Die gefunden Schwachstellen sind vielfältig und nach Risikograd sortiert.
Es bestehen beispielsweise Schwachstellen, die administrativen Zugriff auf den Web-Shop ermöglichen; ebenso können gefakte Kundenbewertungen abgegeben, gefälschte Coupons eingelöst und Warenkörbe von anderen Benutzern eingesehen und modifiziert werden.

4 Methology

Der Webshop wurde auf folgende Schwachstellen untersucht:

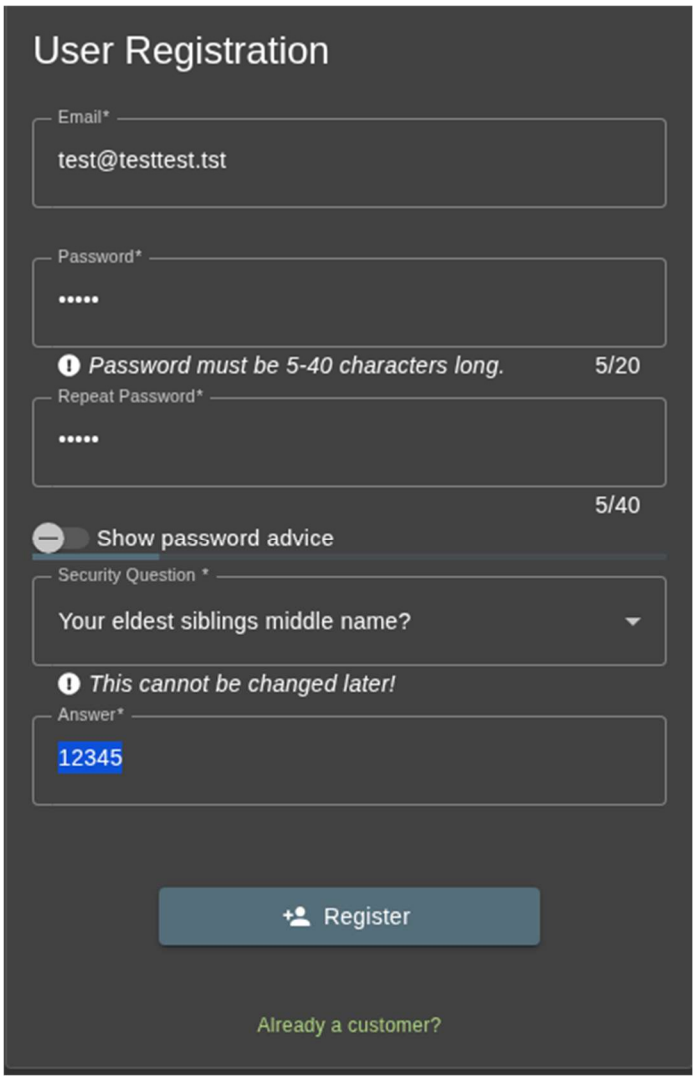
- Benutzerregistrierung
- Abfangen und umleiten von Zahlungen
- Zugangsmöglichkeit als Administrator
- Fälschen von Kundenbewertungen
- Verwendete, veraltete Bibliotheken prüfen
- Zugang zum Warenkorb anderer Benutzer
- Zugang zu gelöschten Produkten
- Einlösen von gefälschten Coupons

5 Detailed Findings

5.1 Empty User Registration

5.1.1 Ergebnis

Es wurde versucht, einen Benutzer ohne eMail-Adresse und Passwort anzulegen. Dazu wurde die Burp Suite verwendet.



Vor dem Klick auf „Register“ wurde „Intercept“ eingeschaltet.

Es konnte folgendes abgefangen werden:

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomeb
Connection: keep-alive

{
  "email":"test@testtest.tst",
  "password":"12345",
  "passwordRepeat":"12345",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2025-10-13T14:43:29.487Z",
    "updatedAt":"2025-10-13T14:43:29.487Z"
  },
  "securityAnswer":"12345"
}
```

Das Datenpaket wurde wie folgt verändert (die Mailadresse und beide Kennworteinträge wurden entfernt):

```
Connection: keep-alive

{
  "email":"",
  "password":"",
  "passwordRepeat":"",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2025-10-13T09:35:44.474Z",
    "updatedAt":"2025-10-13T09:35:44.474Z"
  },
  "securityAnswer":"123"
}
```

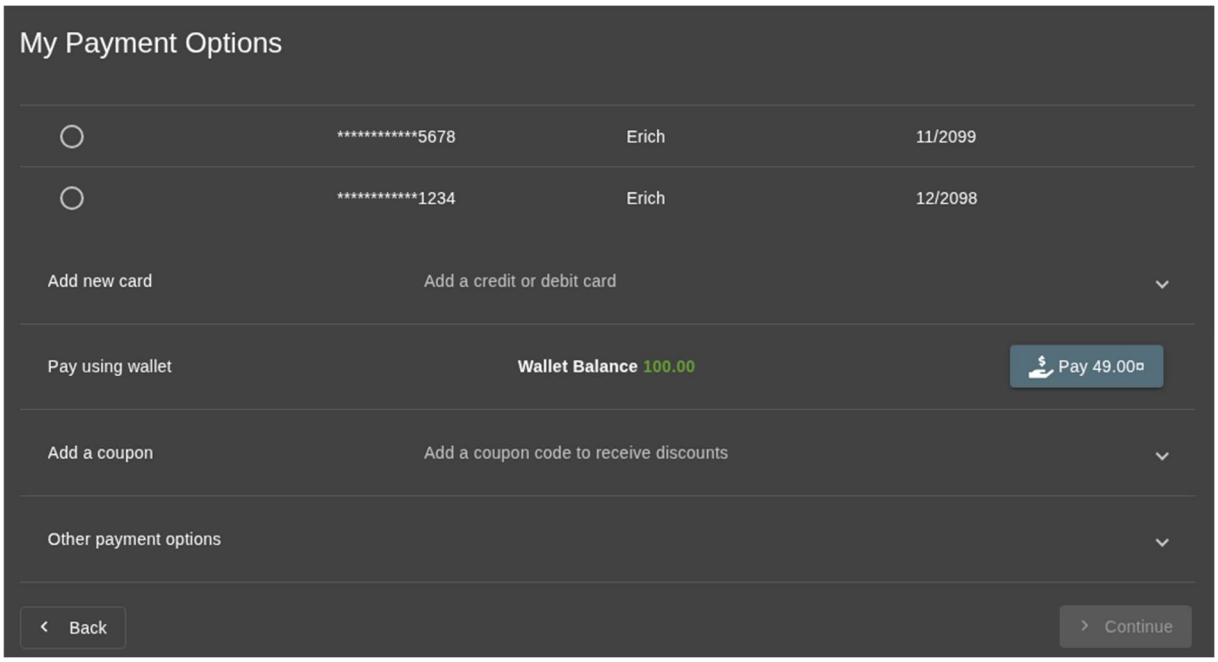
Dies wurde von der WebApp ohne Fehler akzeptiert.

5.1.2 Auswirkungen

Durch die Möglichkeit Benutzer ohne Namen / eMail Adresse und ohne Passwort zu registrieren, wird der Shop sehr verwundbar für Angriffe von außen.

5.2 Deluxe Fraud

Das Portal bietet die Möglichkeit, für USD 49.- Premium Member zu werden. Dabei kann entweder mit der Wallet oder mit Kreditkarte bezahlt werden.



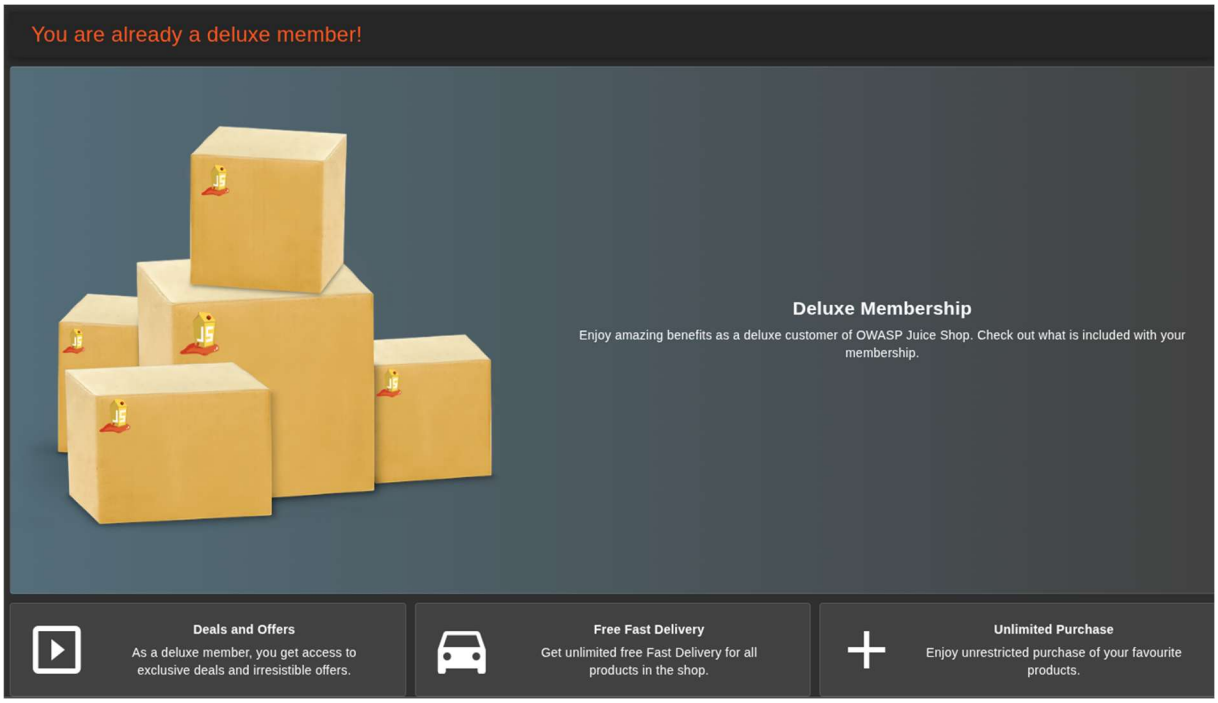
Es wurde die Bezahlung „Wallet“ ausgewählt und der Datenstrom mit Burp Suite intercepted. Das sind die Findings:

```
POST /rest/deluxe-membership HTTP/1.1
Host: 127.0.0.1:3000
Content-Length: 24
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
M3NmQ3MTNjMDdhZCIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoi
joiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTAtMTMgMTA
M30.sGa0rMIxzy4C0CNX0n3VsgtOJx7lABraDj6qnL5PIMtxWylqNpyGRXPLJH
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomebann
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
M3NmQ3MTNjMDdhZCIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoi
joiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTAtMTMgMTA
M30.sGa0rMIxzy4C0CNX0n3VsgtOJx7lABraDj6qnL5PIMtxWylqNpyGRXPLJH
vEQN8lLqvoWxPJnbrR79m1y0aOFOf7YubpI8gdzOD3Xw6kZeVpjaM25B4YKg
Connection: keep-alive

{
  "paymentMode":"wallet"
}
```

Anschließend wurde der „Payment Mode“ auf „none“ gesetzt…

```
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_s
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZ
WFkMjgzYWE0MDBhZjQ2NGM3NmQ3MTNjMDdhZCIsInJvbGUiOiJjdXN0b21lciIsImR
hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsI
CswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MDM2Njc0N30.LMECATm
Fa5N-81bHF7Jz9d2g9xXw1BBEIh7AbCgWODJWQHgELP3DmZollozlgtA
Connection: keep-alive

{
  "paymentMode":"none"
}
```

…und das Paket weitergeleitet.
Das Ergebnis:



5.2.1 Ergebnis

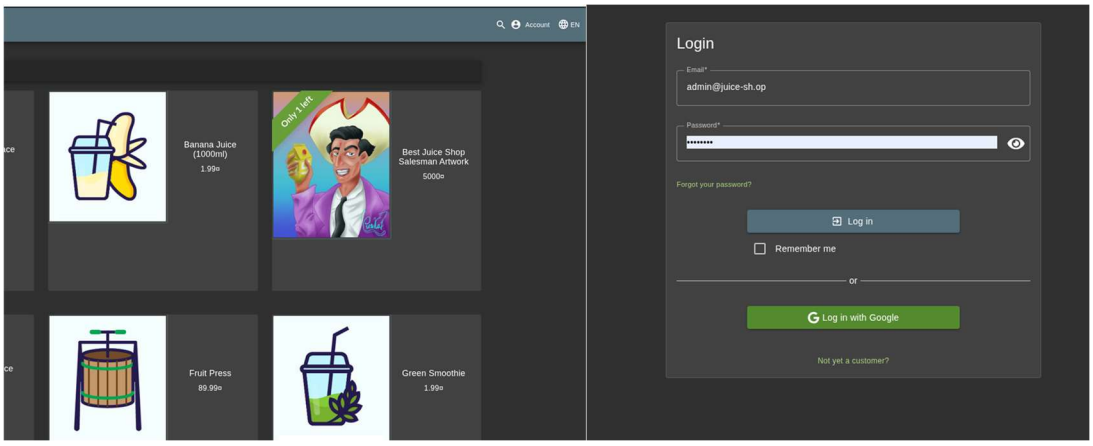
Wir sind Premium Member ohne dafür bezahlt zu haben.

5.2.2 Auswirkungen

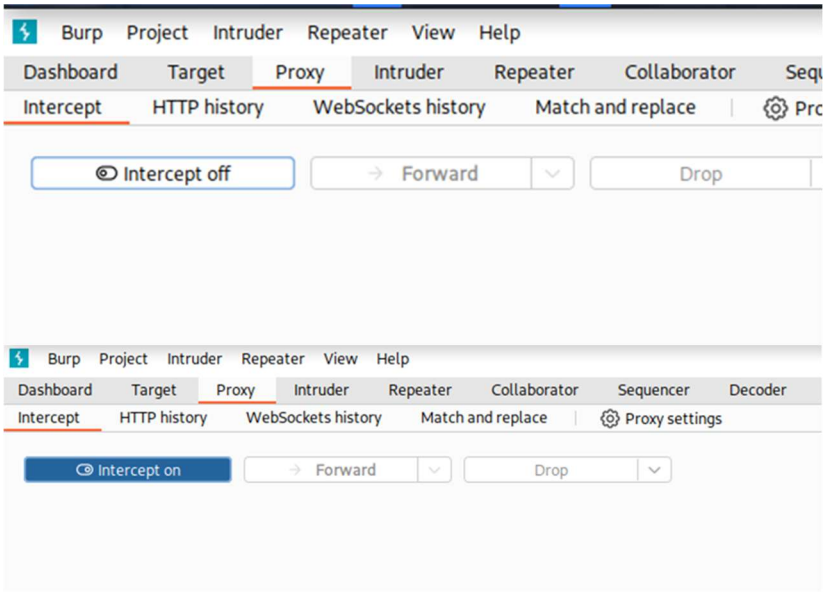
Dem Unternehmen kann durch diese Schwachstelle viel Geld verloren gehen.

5.3 Login Admin

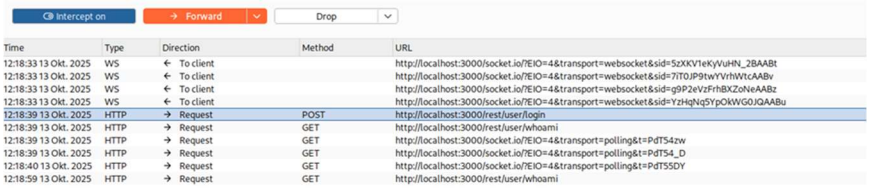
Mit dem Administrator User Account einloggen und alle Adminrechte haben.

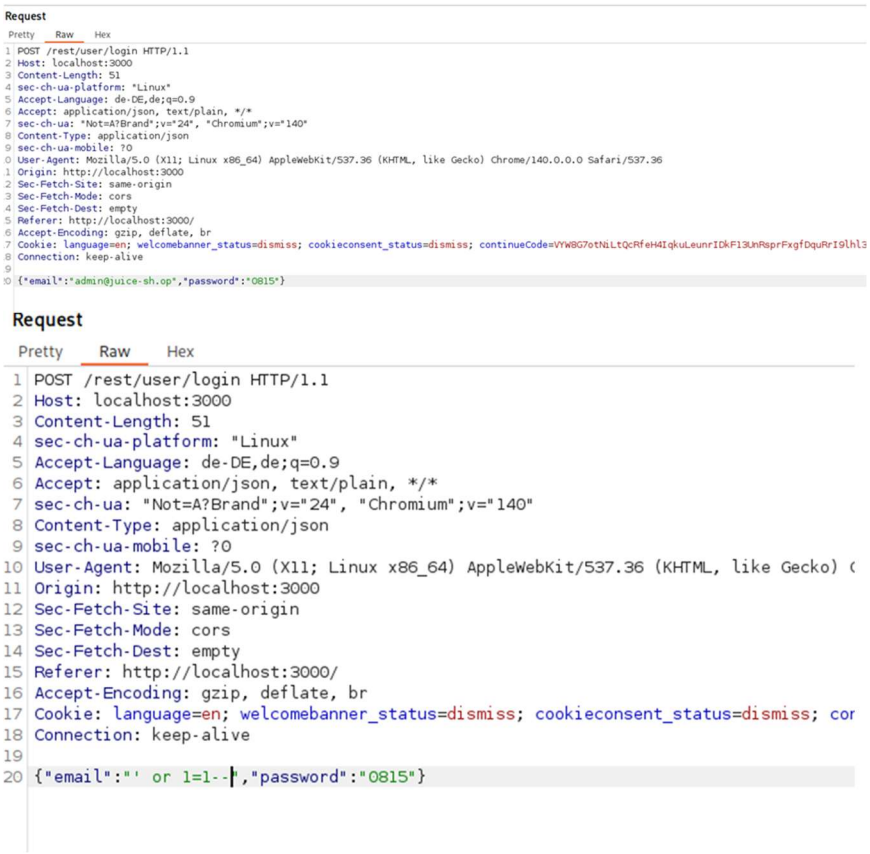


5.3.1 Ergebnis

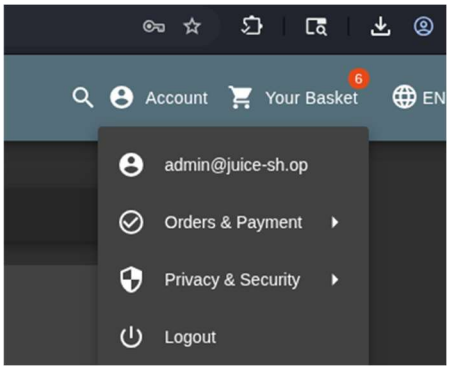


Jetzt erst auf Log-in klicken.
Nun wird der Datenstrom mit Burp Suite intercepted, also abgefangen.





Anstelle der Mailadresse:" ' OR 1=1--" eingeben. Die abgeänderte Seite forwarden und den Interccept wieder auf off stellen.



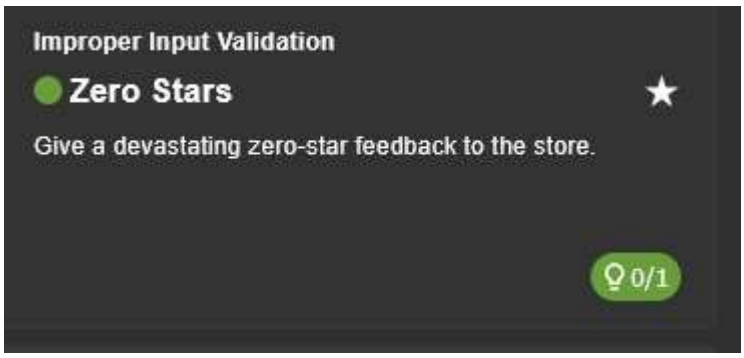
Nun ist man als Administrator und mit dessen Rechten angemeldet.

5.3.2 Auswirkungen

Vollen Administrator Zugriff auf den Saftladen.

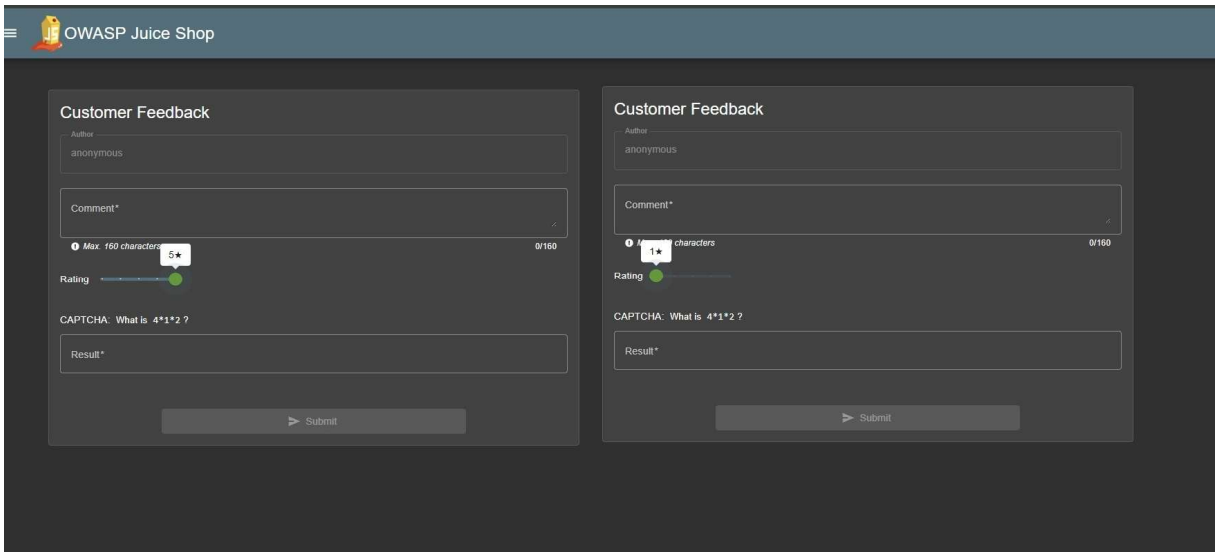
5.4 Zero Stars

Hier haben wir eine Herausforderung wo uns gesagt wird, dass wir dem Shop 0 Sterne Feedback geben sollen:

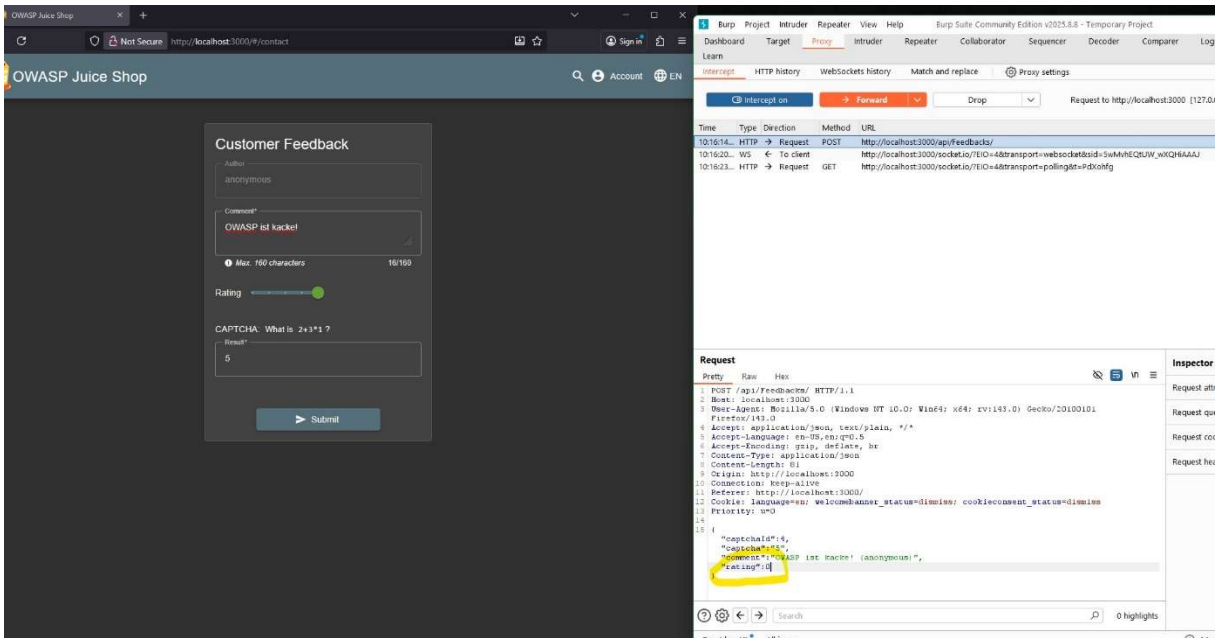


5.4.1 Ergebnis

Allerdings ist nur eine Bewertung von 1 bis 5 möglich.



Wir verwenden die Burp-Suite, um alle Daten einzugeben, drücken: „Intercept on“ und ändern dann den Standardwert auf 0. Wir müssen „Weiter“ drücken und dann „Intercept off“ und die Herausforderung ist gelöst.



5.4.2 Auswirkung

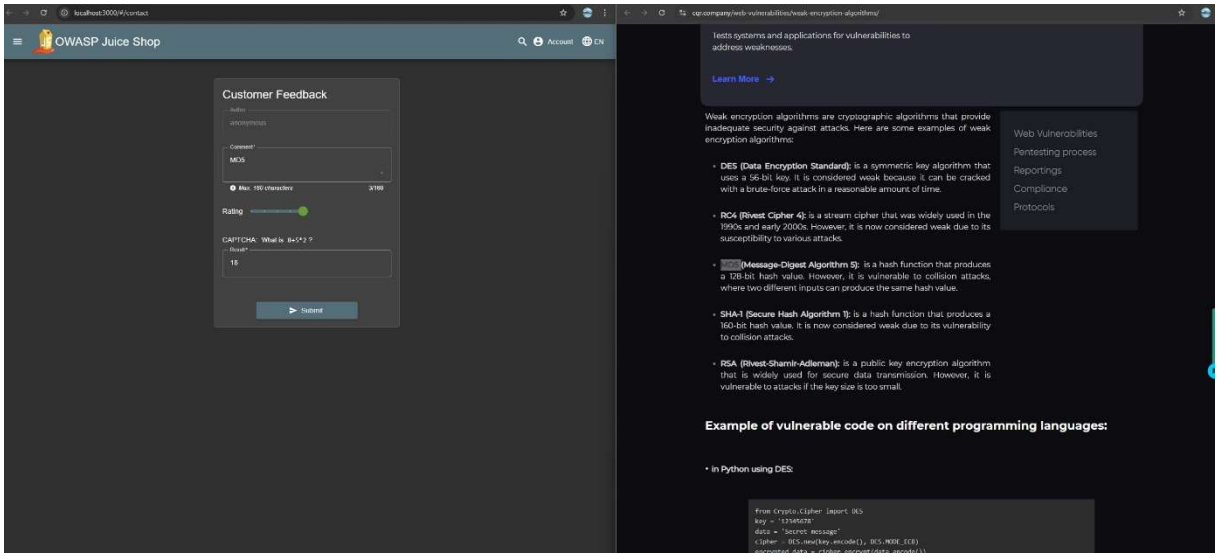
Die Möglichkeit, clientseitig ungültige Bewertungswerte (z. B. 0) zu setzen, hat reale Auswirkungen: Vertrauensverlust, verfälschte Metriken, Geschäftsentscheidungen auf falscher Datenbasis und ein Indikator für fehlende serverseitige Validierung — was wiederum weitere Angriffsflächen eröffnet. Auf der Skala: Mittelhoch bis Hoch für Reputation/Business; Hoch als Architektur-Sicherheitsmangel.

5.5 Weird Crypto

Benachrichtigen Sie in dieser Aufgabe den Store über einen Algorithmus oder eine Bibliothek, die nicht mehr verwendet werden soll.

5.5.1 Ergebnis

Deshalb haben wir gegoogelt, welche Algorithmen und/oder Bibliotheken alt oder schwach und somit unbrauchbar sind.



Danach teilen wir ihm mit, was er nicht verwenden soll. Die Herausforderung ist gelöst. Herzlichen Glückwunsch!

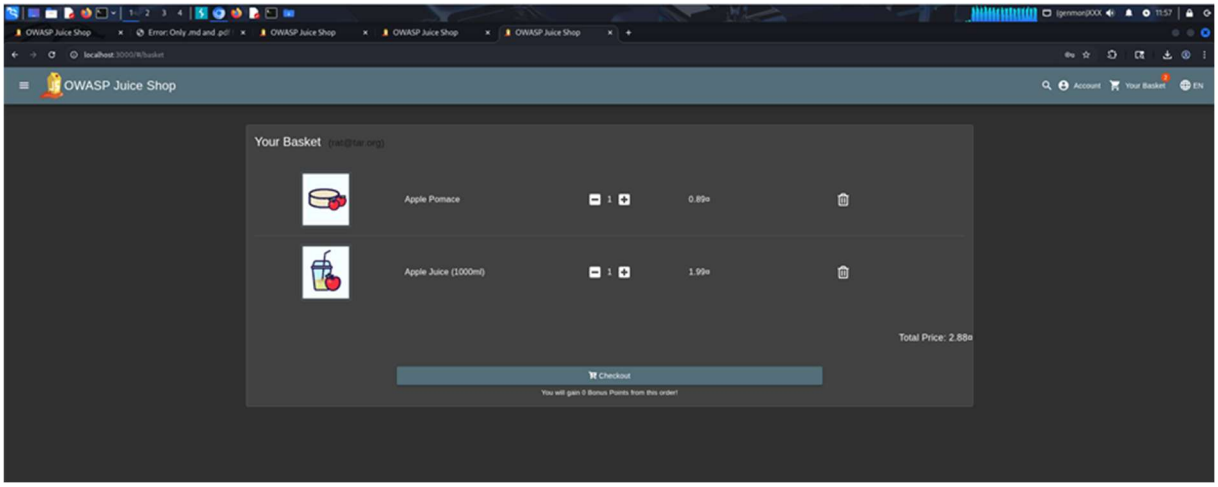
5.5.2 Auswirkung

Die Verwendung solcher Algorithmen kann zu Datenverlust, Kompromittierung von Passwörtern oder Sicherheitslücken führen. Es ist wichtig, diese nicht mehr zu verwenden und auf sichere Alternativen wie AES (GCM/CTR-Modus) oder SHA-256/512 umzusteigen.

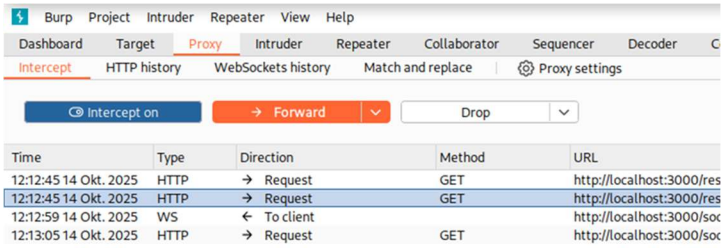
5.6 View Basket

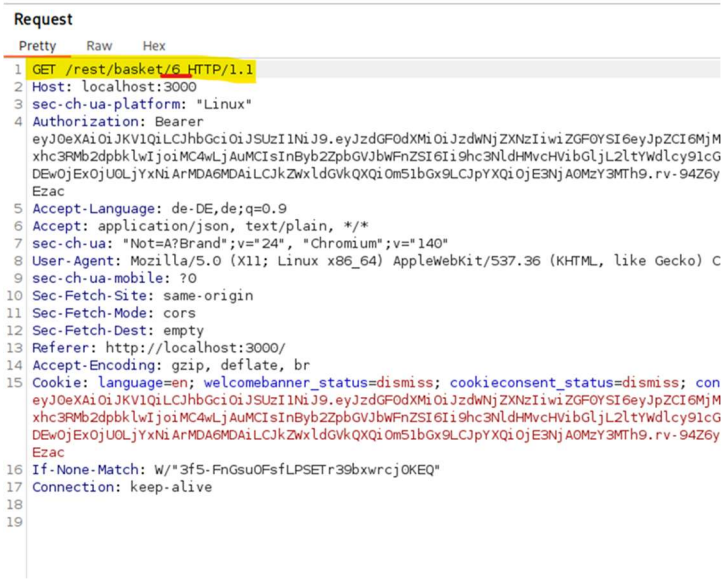
Übernahme eines anderen Warenkorbes

5.6.1 Ergebnis

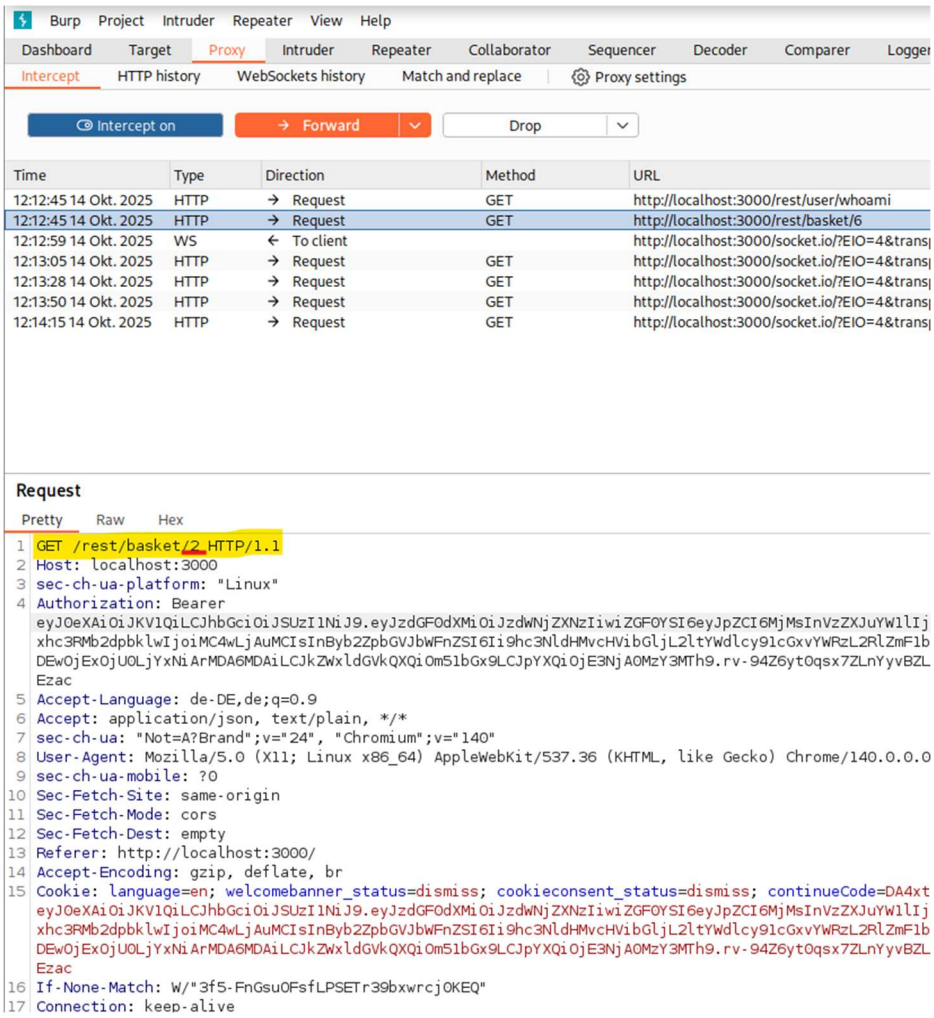


Wir öffnen die Burpsuit und darin einen Browser, wir melden uns beim Juice Shop an. Schalten in der Burpsuit Intercept auf on und öffnen unseren Warenkorb.

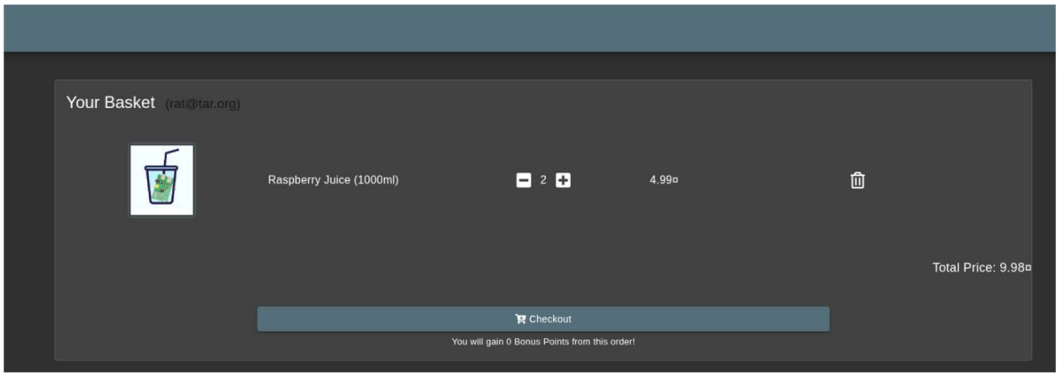




Im Request ändern wir jetzt einfach die Nummer des Basket auf eine andere Zahl (anderes Basket) um, (hier jetzt 2) -> klickt auf Forward und schaltet den Intercept auf Off.



Nun hat man ein anderes Basket übernommen:



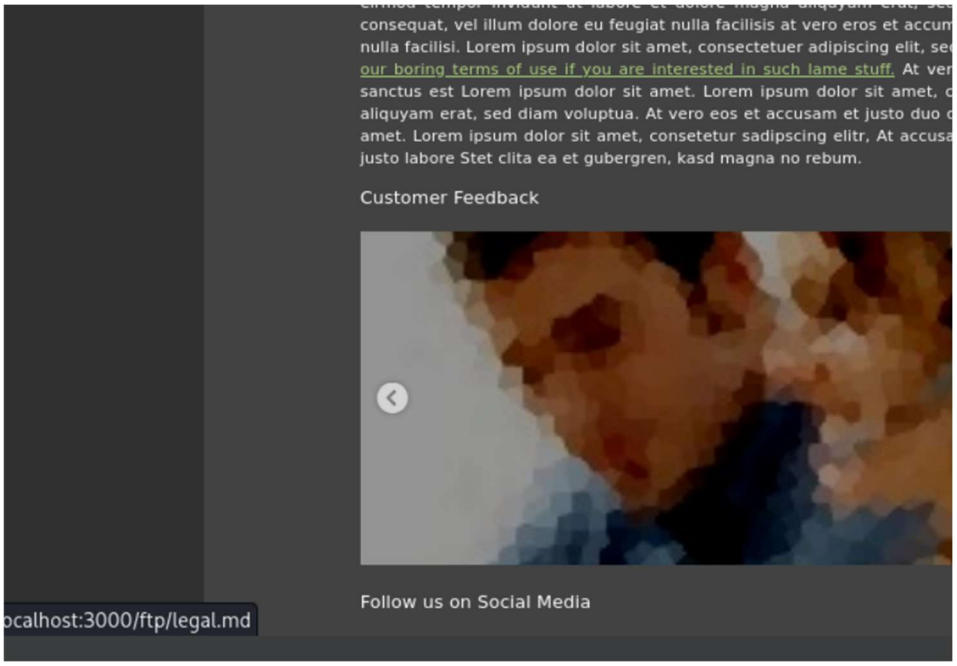
5.6.2 Auswirkungen

Man kann fremde Einkaufskörbe befüllen oder leeren.

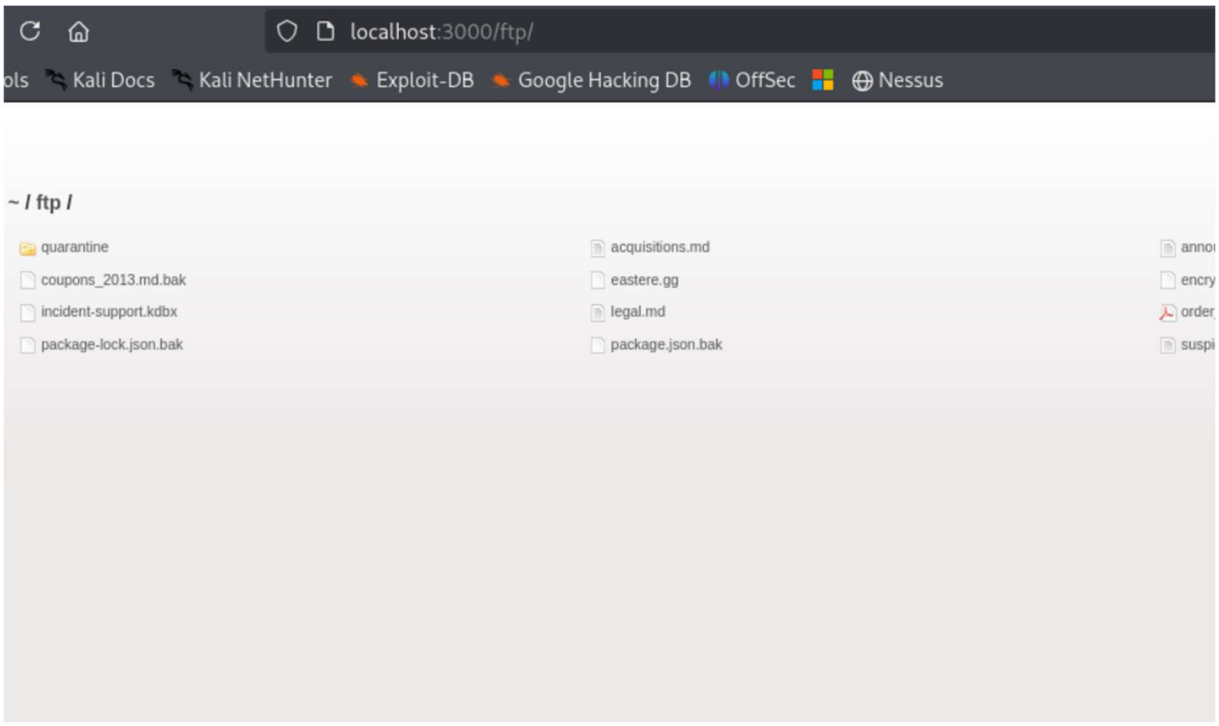
5.7 Forgotton Sales Backup / Poison Null Byte

5.7.1 Findings

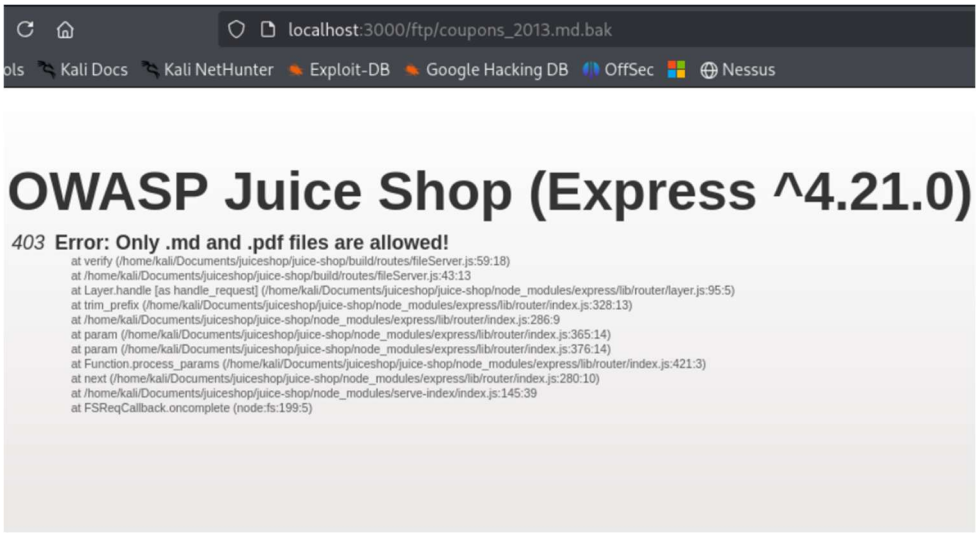
Es wird gesagt, dass irgendwo eine vergessene Datei mit einem Sales-Backup liegt, auf die man Zugriff bekommen kann.



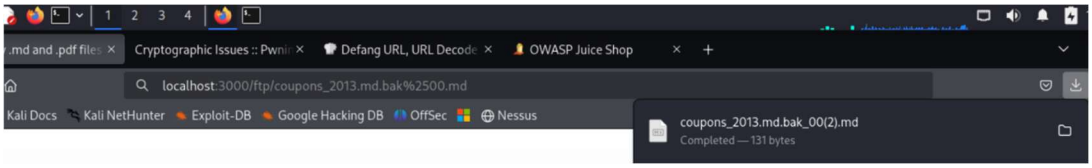
Geht man im about-Teil allerdings über den Link, sieht man, dass die Datei auf einem “ftp”-share liegt. Auf diesen kann man ohne Probleme zugreifen:



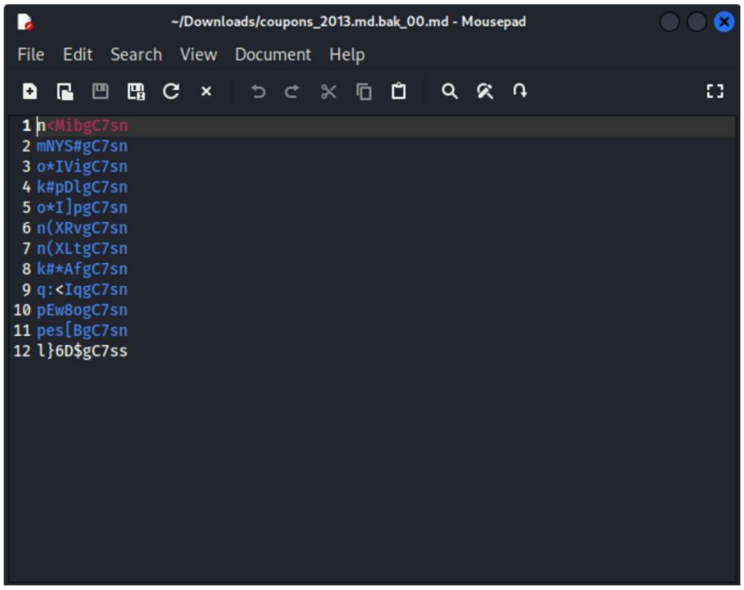
Für uns ist hier die coupon_2013.md.bak interessant. Wenn man diese herunterladen möchte, bekommt man erstmal eine Fehlermeldung:



Ein Download ist aber möglich, wenn man einen Null-Byte zum Link hinzufügt:



Dann kann man die Datei mit den alten Coupons öffnen!



5.7.2 Auswirkungen

Ungeschützter Zugriff auf einsehbare Shares - “/ftp” und den darauf liegenden Dateien. Außerdem ist die Web-Application für Null-Byte-Injections verwundbar.

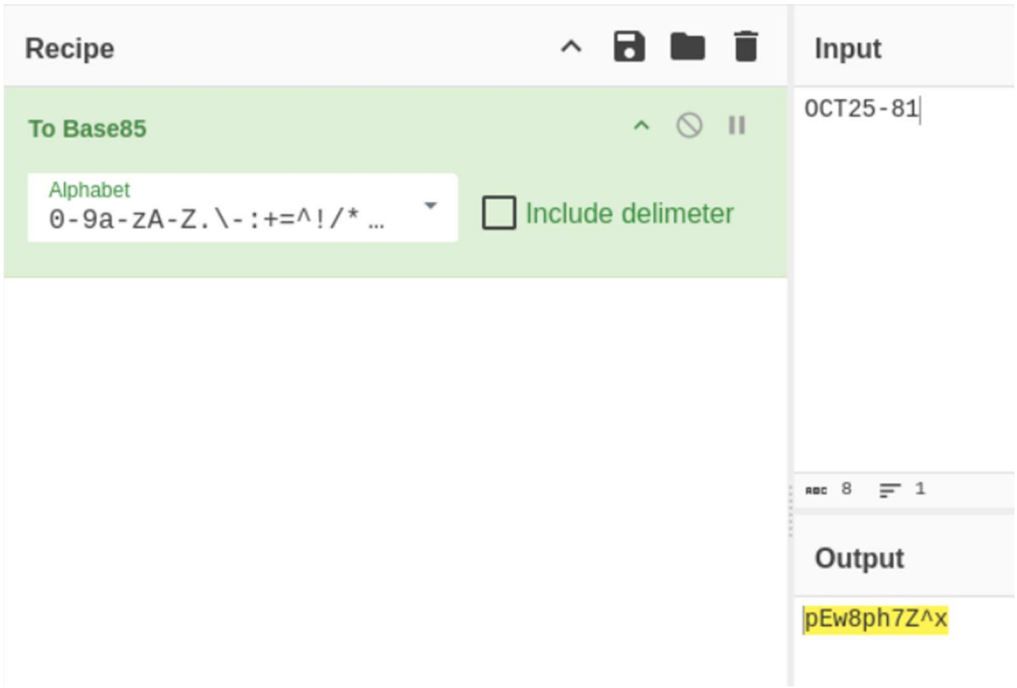
5.8 Forged Coupon

5.8.1 Findings

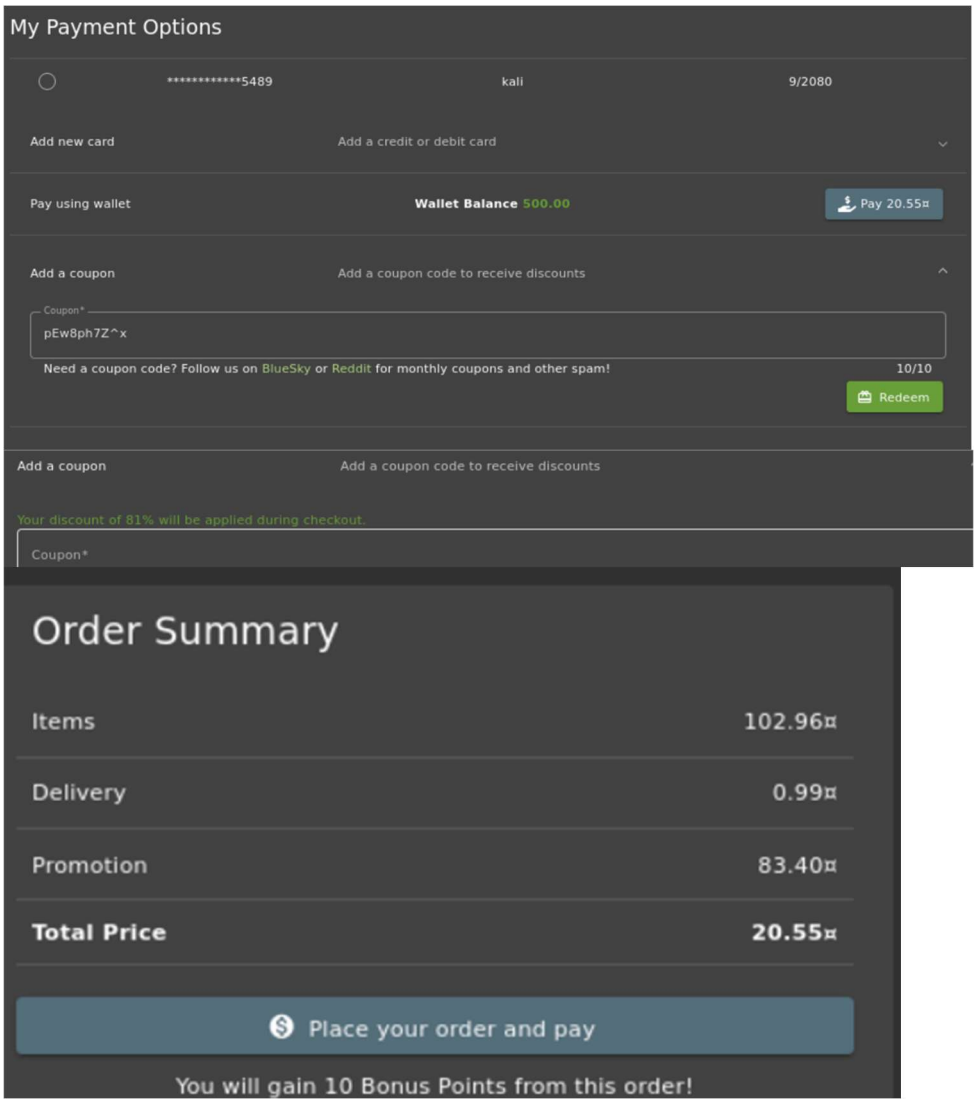
Wie kann man einen Coupon mit 80% Rabatt erstellen?

Wir haben in 5.8. erfolgreich die Liste mit den alten Coupons herunterladen können. Nach kurzer Recherche steht fest, diese sind mit T85 codiert worden; CyberChef hilft beim Decodieren:

Hier sieht man nun, dass alle Coupons nach demselben Prinzip aufgebaut sind: Monat-Jahr-Prozente.
So können wir uns einfach selbst einen Coupon mit CyberChef und dem aktuellen Monat erstellen: Oct-25-81 wird zu: pEw8ph7Z^x



Wenn wir nun Produkte in den Warenkorb legen, können wir beim Checkout den Coupon einlösen und tatsächlich funktioniert es! Schlanke 81% gespart und die Challenge gelöst.



5.8.2 Auswirkungen

Durch eine einfache Verschlüsselung und nicht-existenten Zugriffsrechten kann einfach selbst ein Coupon erstellt werden.

6 Attack Narrative

6.1 Mögliche Angreifer

Angreifer können aus verschiedenen Bereichen kommen: Beispielsweise können das Konkurrenten sein, Script Kiddies, oder auch Angreifer, die aus wirtschaftlichen Gründen den Angriff starten. Auch ehemalige Mitarbeiter kommen in Betracht.

6.2 Ziel der Angreifer

Ziele könnten sein:
- Erpressung
- Datenexfiltration
- Zufügen wirtschaftlichen Schadens

6.3 Vorgehensweise der Angreifer

Die Vorgehensweise ist die Ausnutzung der Schwachstellen der WebApp.

6.4 Angriffsverlauf

Der Verlauf möglicher Angriffe ist im Kapitel 5 im Detail beschrieben.

6.5 Auswirkungen eines Angriffs

Die Auswirkungen eines Angriffs können sein:
- Datenverlust
- Schaden am Ruf des Unternehmens
- Betriebsunterbrechung
- Finanzieller Schaden

7 Recommendations / Remediation

7.1 Empty User Registration

Die auf der Webseite eingegebenen Daten müssen vor der Übergabe an die Datenbank nochmals auf Gültigkeit geprüft werden.

7.2 Deluxe Fraud

Die von der Webseite übermittelten Zahlungsdaten müssen vor Abschluss der Zahlung auf Plausibilität geprüft werden. Ein Zahlungsmittel „none“ darf nicht akzeptiert werden.

7.3 Login Admin: Log in with the administrator's user account.

Verhindern lässt sich „Log in with the administrator's user account“ am effektivsten durch die Kombination aus verpflichtendem Admin-MFA, serverseitiger Rollenprüfung (RBAC), Brute-Force-Protection (Rate-Limiting & Account-Lockout) und einem separaten/geschützten Admin-Interface.

7.4 Zero Stars

Die Bewertung muss bei der Übergabe an den Server auf gültige Werte (1-5) geprüft werden, um ungültige Einträge zu verhindern.

7.5 Weird Crypto

Die verwendeten kryptografischen Algorithmen müssen auf Sicherheit überprüft und veraltete/unsichere Algorithmen ersetzt werden.

7.6 View Basket View another user's shopping basket.

Das „View Basket“-Szenario kann durch eine serverseitige Autorisierungsprüfung verhindert werden, die sicherstellt, dass nur der Eigentümer eines Warenkorbs Zugriff darauf hat.

7.7 Forgotton Sales Backup / Poison Null Byte

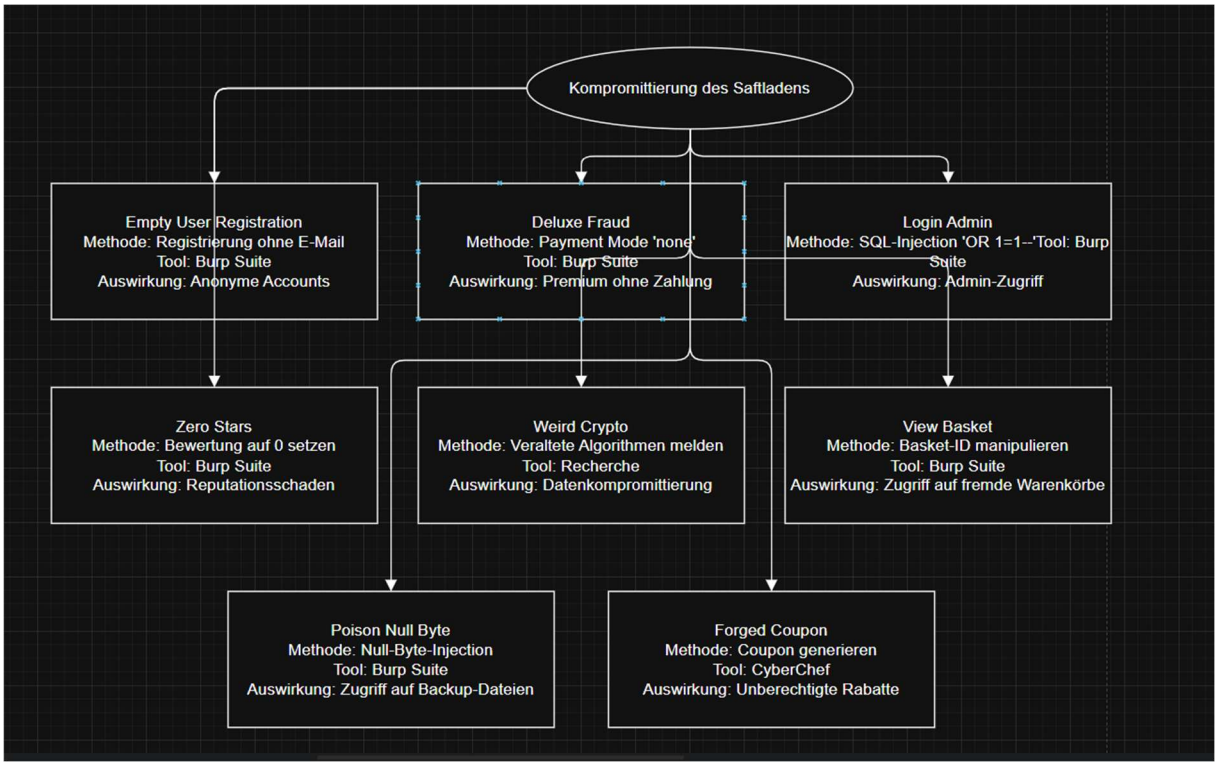
Alte bzw. ungenutzte Ordner sollten gelöscht werden. Alternativ sollte der Zugriff für authorisierte Nutzer beschränkt werden, z.B. durch IP-Whitelisting. Auch eine Verweigerung auf die Pfade von Seiten des Webservers ist einstellbar.
Eingaben von \x00 müssen explizit abgelehnt werden, z.B. durch Blacklists. Außerdem könnten die Pfade mit fuzzing unkenntlich gemacht werden.

7.8 Forged Coupon

Eine Erstellung von random Token mit 128 oder 256bit Verschlüsselung, die auf einer internen Datenbank mit Metadaten (Erstellungsdatum, Ablaufdatum, Discount, erlaubte Nutzer) gespeichert werden. Bei Nutzung wird ein Token abgerufen, Metadaten gecheckt und sofort als genutzt markiert.

8 Anhang

8.1 Attack Tree



8.2 Assessment Scope

Es wurden keine Änderungen am Scope vorgenommen.

8.3 Assessment Artefacts (Artefakte zur Bewertung)

Es sind keine Artefakte durch die Prüfung entstanden.

8.4 Tools Used

Folgende Befehle und Tools kamen zum Einsatz:

- Burp Suite
- Cyber Chef

Demoort, 15.10.2025

[redacted]

Erich Geldreich, [redacted]