Opdracht 6

**1.1: Diagnostic Commands:**

**Traceroute (tracert)**

Met TRACERT kunt u uitzoeken waar een pakket is gestopt in het netwerk.

vb: tracert google.com

**Ipconfig**

Met behulp van ipconfig kan allerlei informatie opgevraagd worden over de netwerkverbindingen, netwerkkaarten, gateway lokale IP-adres en het verloop van de IP-communicatie.

vb: ipconfig /all

**Netstat**

Netstat is een commando dat u kunt gebruiken om de verbindingen van uw computer te tonen op het internet . Het is een nuttig instrument voor het toezicht op de aansluitingen en diagnosticeren van problemen.

vb: netstat -a

**Ping**

Ping is een commando dat wordt gebruikt om de bereikbaarheid, en de vertragingstijd (de latency) te meten van een node.

vb: ping google.com

**PathPing**

PathPing combineert de functionaliteit van ping samen met die van tracert.

vb: pathping google.com

**Nslookup**

Nslookup is een afgeleide van name server lookup. Het wordt gebruikt om DNS-servers te ondervragen voor een domeinnaam, IP-adress of andere DNS gegevens te verkrijgen.

vb: nslookup google.com

**Getmac**

Getmac laat het MAC adress zien van een of meerdere netwerkadapters op een systeem.

**Netsh**

Netsh is een commando waarmee je lokaal of op afstand network devices mee kunt configureren. Afkorting voor Network Shell

vb: Netsh ? (Dit geeft een lijst van mogelijke commando's in de Network Shell)

**route**

route is een commando dat wordt gebruikt om de IP routing table te bekijken en aan te passen.

vb: route -f (Dit cleart de routing table)

**Opdracht 2: Security Tools:**

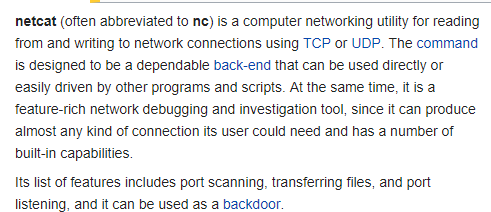
**Metasploit:**



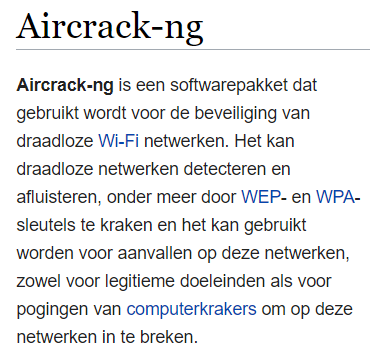
**Burp Suite:**

****

**Netcat:**

****

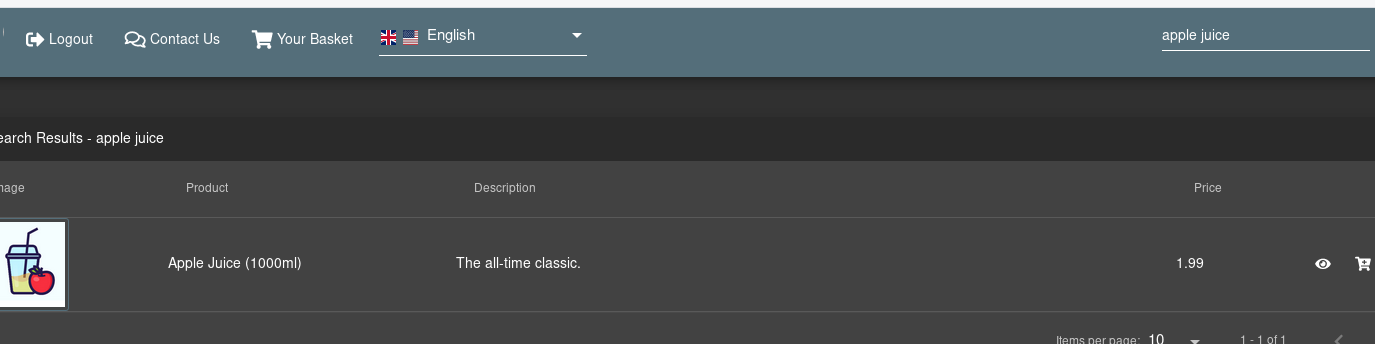
**Aircrack**

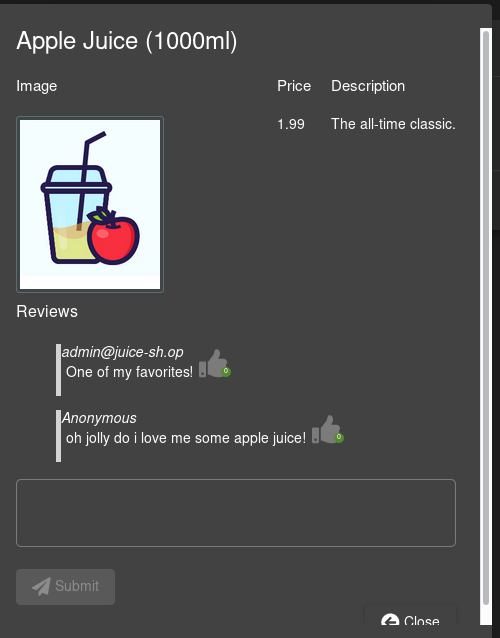
****

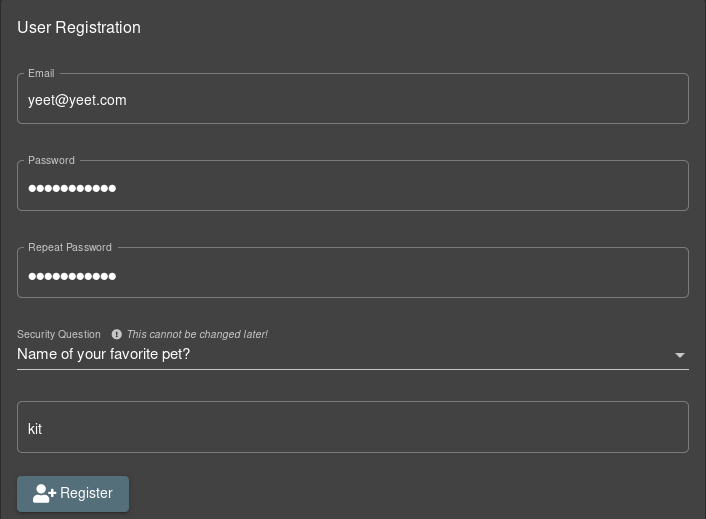
**TCPDump**

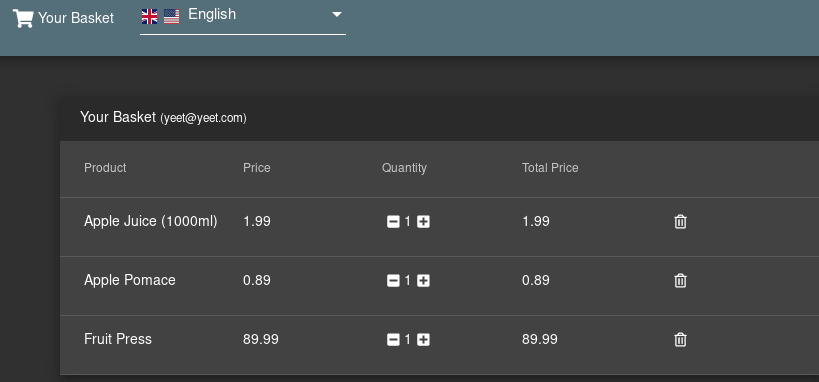
****

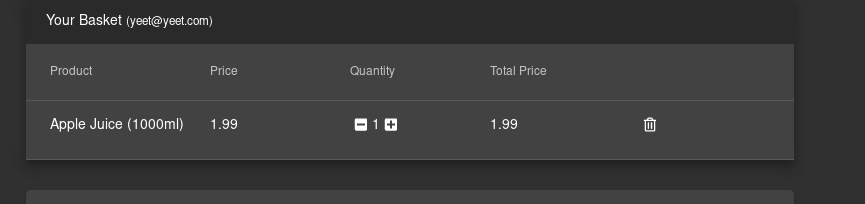
**Opdracht 3: Walk The Happy Path:**

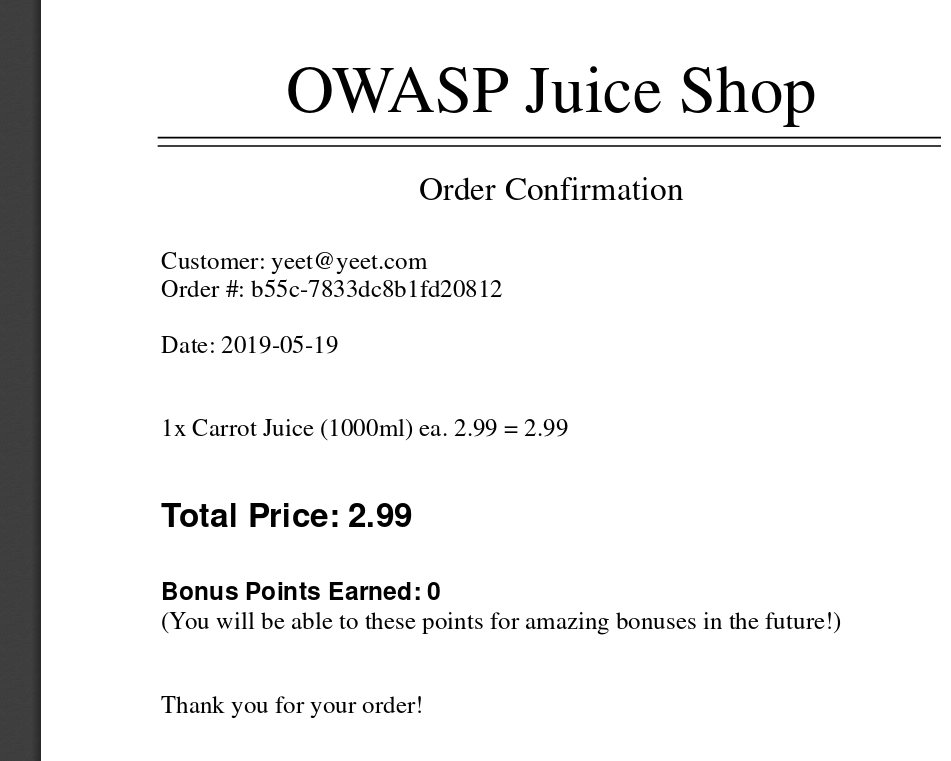
****

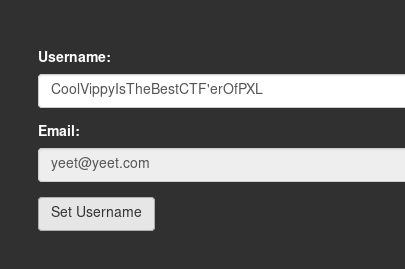
****

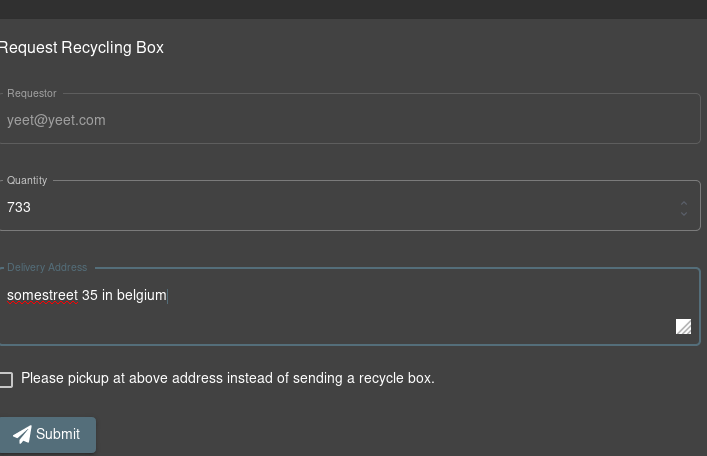
****

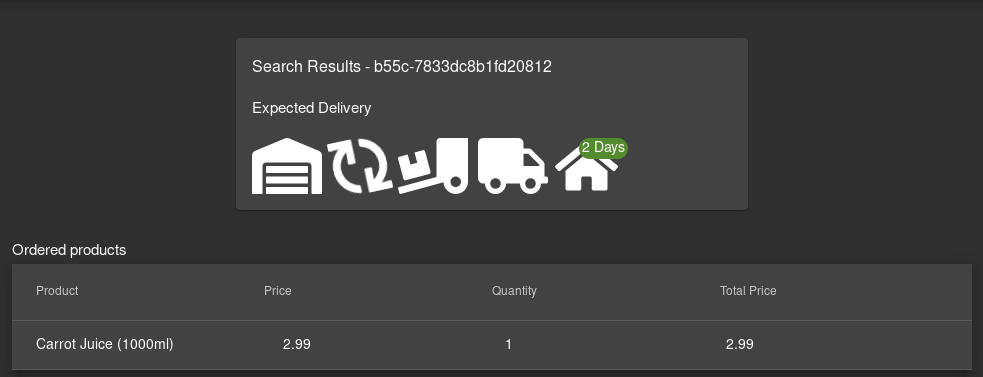
****

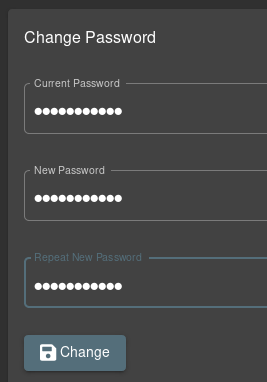
****

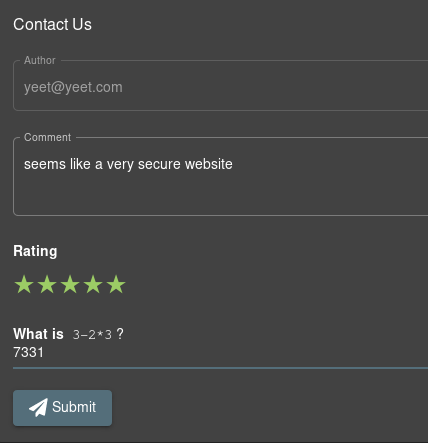
****

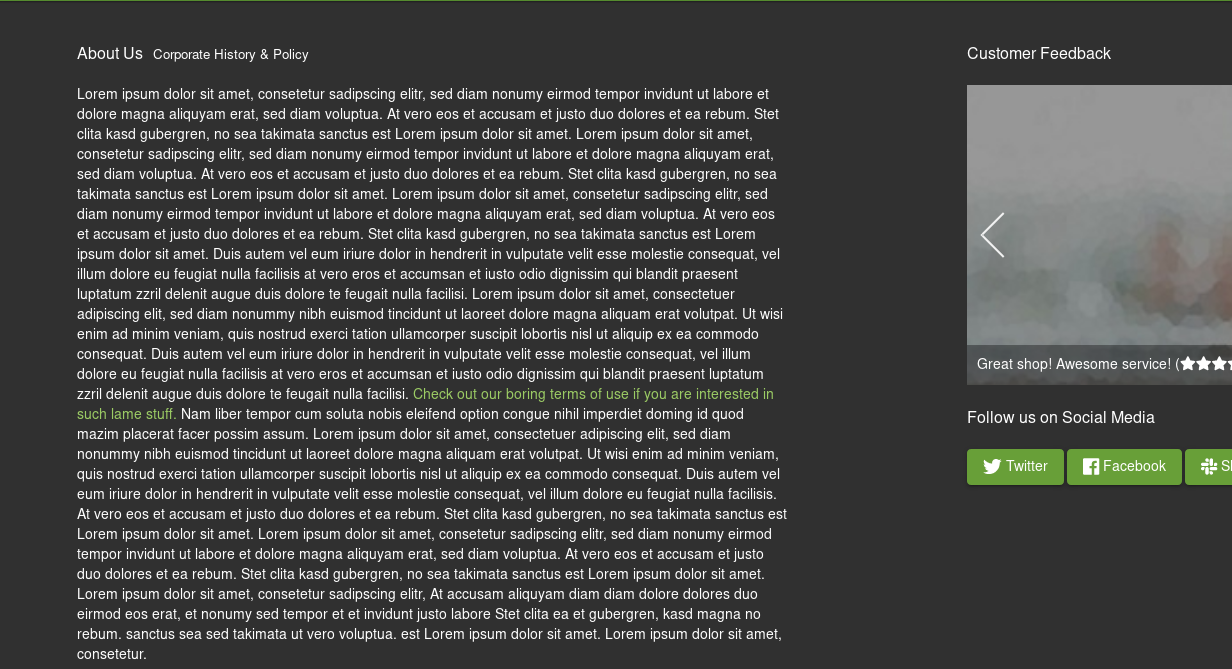
****

****

****

****

****

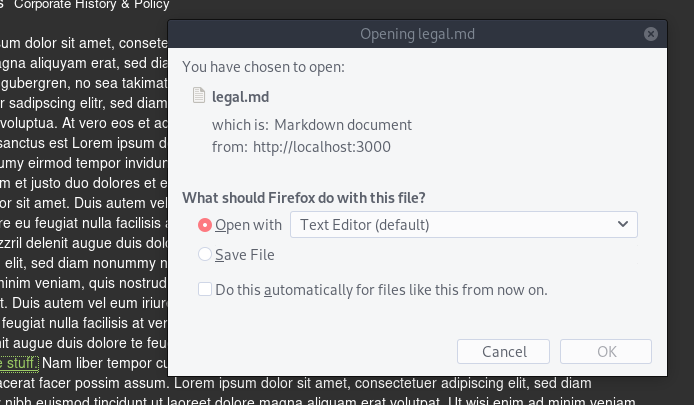
****

**Opdracht 4: Trivial Challenges:**

|  |  |
| --- | --- |
| 2.1: Confidential Document | Bij het openen van de link in een nieuwe tab kunnen we een file downloaden van de ftp server, zonder enige credentials in te geven. dit betekent dus ook dat we door naar de gewone ftp te surfen dus ook toegang hebben tot alle andere files in de server. Beter om SFTP te gebruiken omdat dit beter beveiligd is |
| 2.2: Error Handling | Simpele sql injectie zorgt ervoor dat er een error wordt getoond die geen nuttige info bevat |
| 2.3: Privacy Policy T1 | Hier is geen verdere uitleg aan verbonden |
| 2.4: Redirects T1 | niet gevonden |
| 2.5: Repetitive Registration | Het repeat-password veld checkt maar eenmalig of de passwoorden overeenkomen, als dit de eerste keer klopt, kunnen we in het veld erboven een geheel ander passwoord ingeven zonder foutmelding. Een een oplossing hiervoor kan een constant check zijn die blijft refreshen |
| 2.6: Scoreboard | Door in de url /score-board  te plaatsen komen we op deze pagina terecht. Very obvious pagina- of bestandsnamen kunnen zo aangesproken worden |
| 2.7: XSS T0 | Er wordt geen check gedaan in het invoerveld van het ID, enkel de placeholder geeft iets aan. Er komt ook geen error message wanneer we een kortere string invoeren, vandaar dat een script tag dus waarschijnlijk niet gefilterd wordt |
| 2.8: XSS T1 | Een korte <script> tag met daarin een alert, triggert een popup door het in de zoekbalk in te geven |
| 2.9: Zero Stars | Er wordt geen submit uitgevoerd totdat alle velden correct ingevoerd zijn, maar door deze tag te verwijderen, kunnen we dit bypassen |

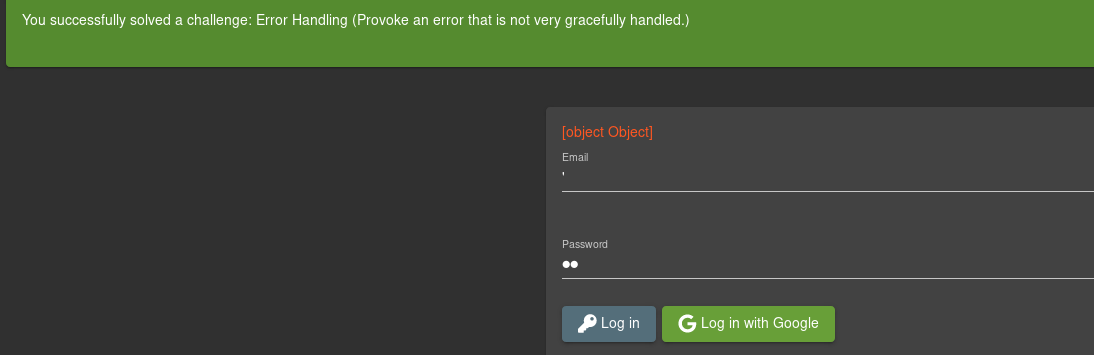
**Printscreens opdracht 4:**

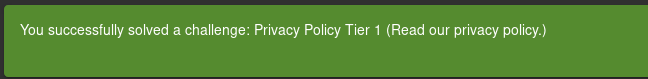
2.1



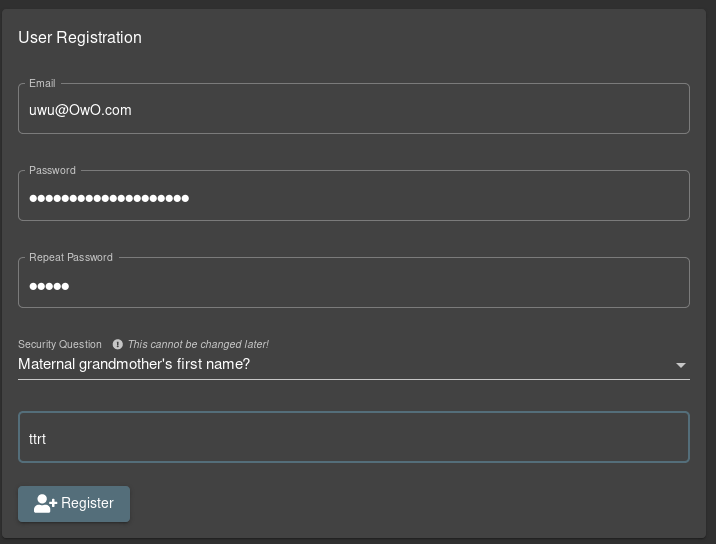


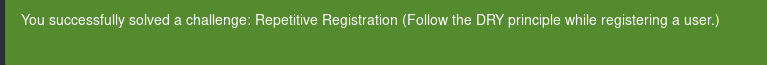
2.2



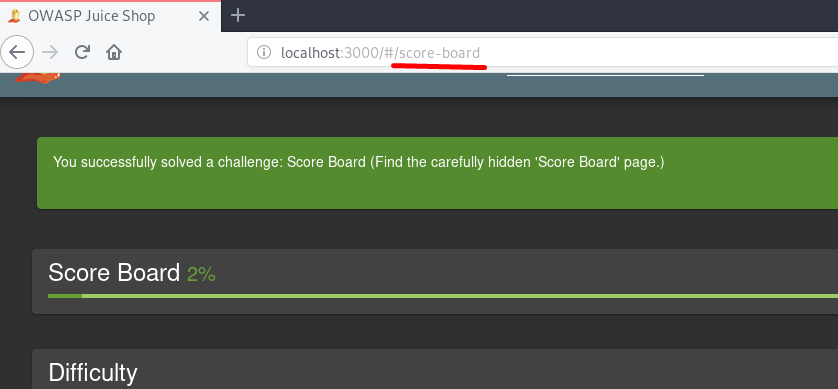
2.3  


2.4

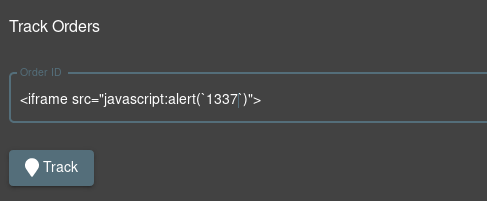
2.5



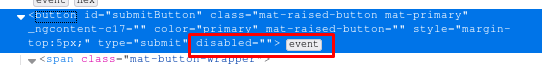
2.6



2.7



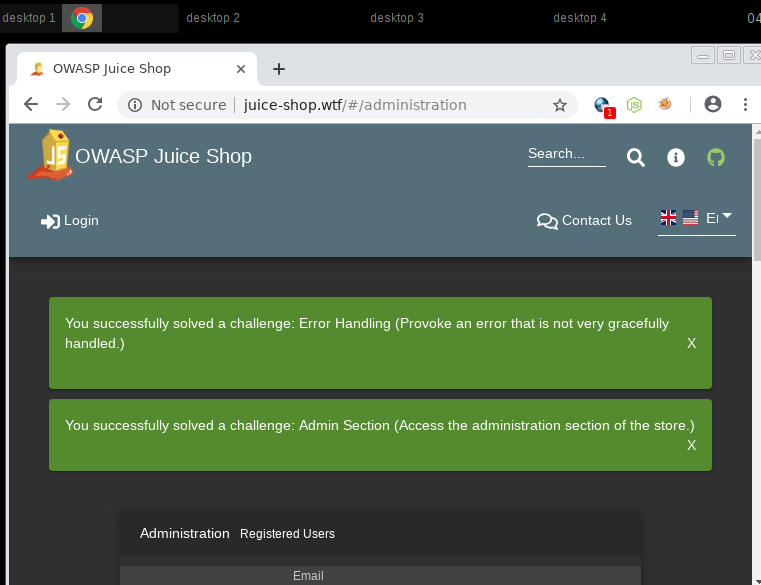
2.8

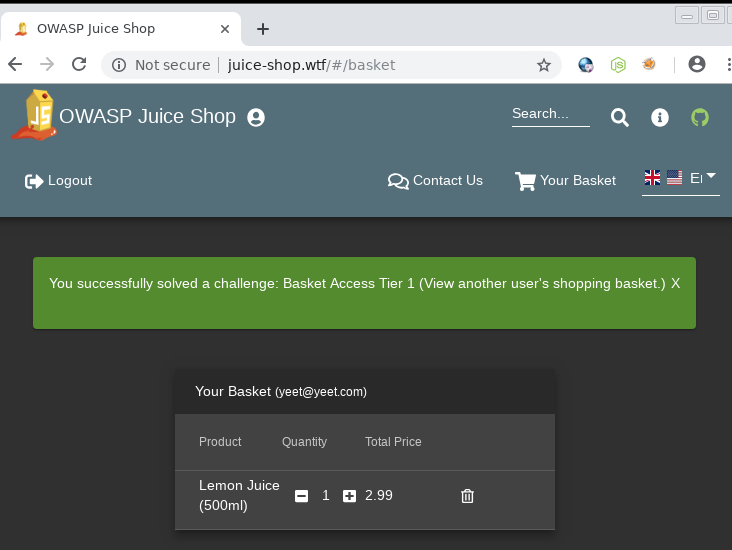
2.9  


**Opdracht 5: Easy Challenges:**

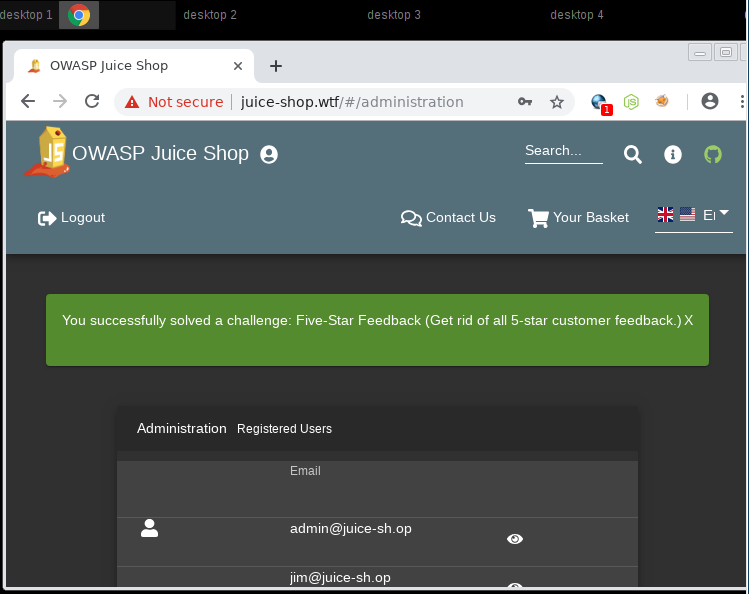
|  |  |
| --- | --- |
| 3.1 Admin Section | doorzoeken van de javascript files |
| 3.2 Basket Access Tier 1 | veranderen van session storage |
| 3.3 Deprecated Interface | xml file uploaden |
| 3.4 Five-Star Feedback | met sql injection inloggen en dan in de administration sectie alle feedback verwijderen |
| 3.5 Login Admin | inloggen via sql ‘ or 1=1 -- |
| 3.6 Login MC SafeSearch | de hints bekijken en logisch redeneren. |
| 3.7 Password Strength | bruteforce met rockyou.txt |
| 3.8 Security Policy | niet gevonden |
| 3.9 Weird Crypto | niet gevonden |
| 3.10 XSS Tier 1.5 | <<a|ascript>alert(`xss`)</script> |

3.1

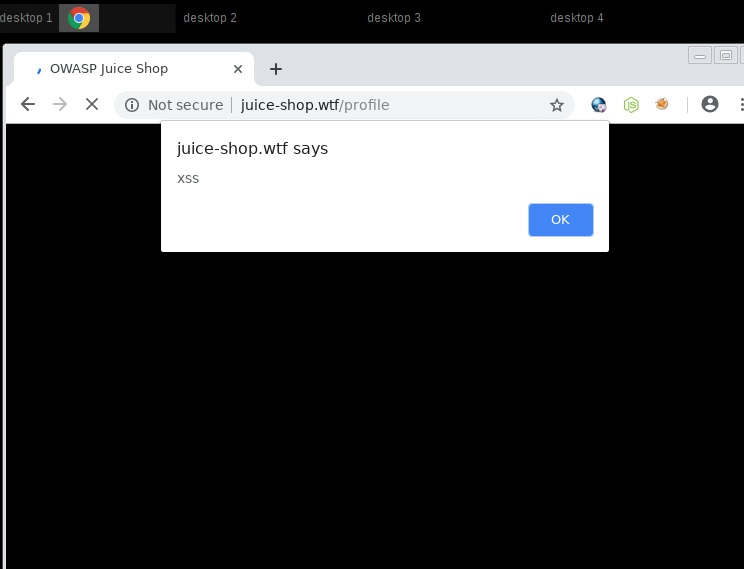


3.2

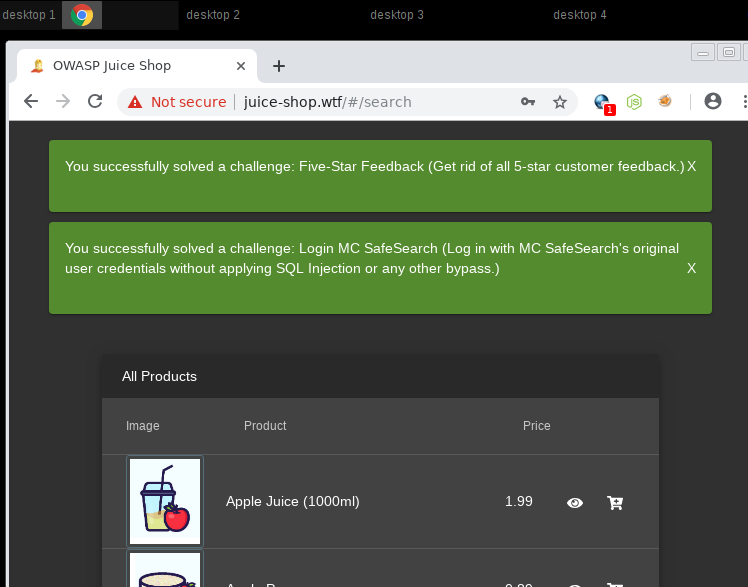
3.4



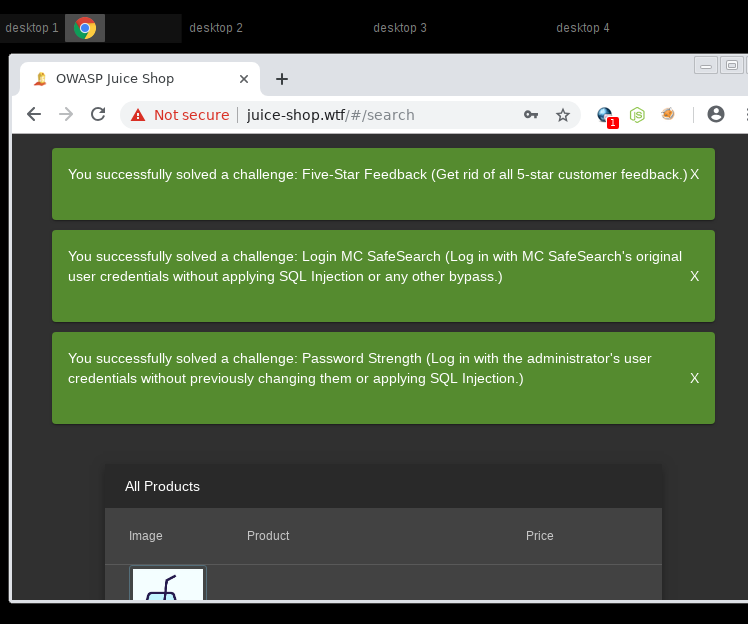
3.10



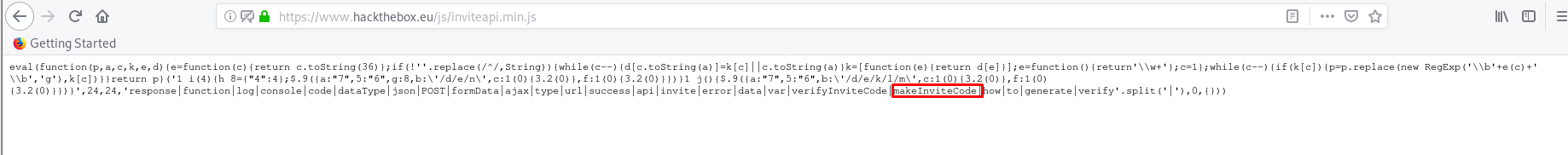
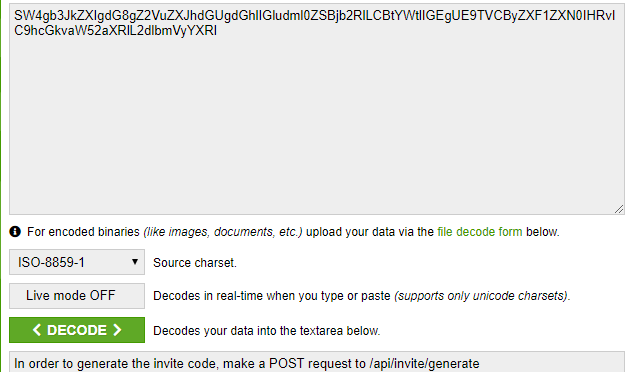
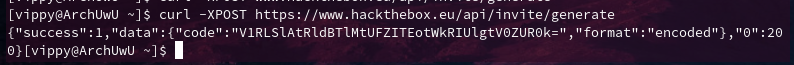
3.6

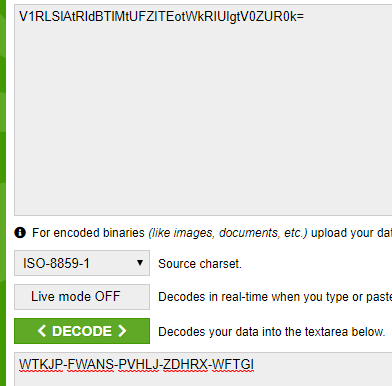


3.7



**Opdracht 7: HackTheBox:**





bij het inspecteren van de pagina staat er bij de vele scriptsources een link naar een inviteapi, als we hiernaar browsen via het filepad in te geven achteraan de URL, zien we onduidelijke code, maar belangrijker, verschillende functies. Door de functie op te roepen in het console venster, wordt deze uitgevoerd en krijgen we een base64 geëncrypteerde string terug (Het is Base64, en dat kon ik meteen herkennen, want het stond eronder :D ). Ik moet dus een post request doen naar de api. Dit doe ik door in de terminal Curl te gebruiken met -XPOST. Ik krijg opnieuw een Base64 string terug, en na dit te decoden zie ik dus mijn invitecode. De invitecode is IP-restricted, dus als ik dit probeer in te geven buiten mijn Arch, krijg ik een foutmelding dat ‘deze invitecode niet geldig is voor dit IP’.

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Opdrachten | Tijd | Totaal |
| Bram | Geen | 0 | 0 |
| Vincent | 6.1 | 45 min | 45 min |
| Vicky | 6.3, 6.4, 6.7, Opmaak document | 10 min, 1.30 uur en 30 min, 30 min | 2.40 uur |
| Igor | 6.2, 6.5 | 60 min | 60 min |