# Bevindingen

**Kwetsbaarheidstitel: zero stars (laag risico)**

**Beschrijving:**

De naam geeft het al weg, maar in bij deze kwetsbaarheid geven een rating van 0 ipv de keuze

1 t/m 5 die ze geven.

**Stappen om de kwetsbaarheid te reproduceren**:

1. Natuurlijk ben ik eerst in een veilige omgeving gaan hacken door middel van een docker.
2. Vervolgens ben ik random gaan exploiten en kwam ik erbij dat je geen 0 kon geven als rating bij de beoordeling.
3. Toen ben ik naar Burp Suite gegaan (een web hacking tool)
4. Zij hebben een eigen browser waarin je verkeer kan sturen en kan aanpassen, daarin heb ik de customer feedback gestuurd met rating 1.
5. Vervolgens zag ik hem in mijn burp suite
6. Daar heb ik de 1 verandert in een 0
7. Vervolgens heb ik op “forward” geklikt en toen kreeg ik de melding dat het was gelukt.

**Impact:**

De impact van zo een kwetsbaarheid is in dit geval wel minder dan andere, maar er kan wel worden gespeeld met het review systeem. Mensen kunnen zo spelen met de punten en die aanpassen hoe ze willen. Stel voor dat een hacker admin privileges zou hebben, dan zou hij alle ratingsystemen kunnen aantasten.

<https://nvd.nist.gov/vuln/detail/CVE-2022-40310>

**Aanbevolen oplossing:**

Zorg ervoor dat alleen beoordelingen van 1 tot 5 worden geaccepteerd door de invoer te controleren. Implementeer ook maatregelen om ervoor te zorgen dat alleen geautoriseerde en ingelogde gebruikers toegang hebben tot het beoordelingssysteem, en dat ze de beoordelingen niet kunnen wijzigen.

**Bijlagen:**

A computer screen shot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Password strenght (hoog risico)**

**Beschrijving:**

In deze kwetsbaarheid probeer ik toegang te krijgen tot het admin paneel, zodra je toegang hebt tot het admin paneel kan je heel doen.

**Stappen om de kwetsbaarheid te reproduceren:**

1. Eerst zoeken naar de admin email, die kan je vinden door op een product te klikken en vervolgens die recensies en daar staat de email: [admin@juice-sh.op](mailto:admin@juice-sh.op)
2. Vervolgens ga je proberen in te loggen met een willekeurige wachtwoord
3. Je zult zien dat dat niet werkt en dus heb ik mijn verzoek gestuurd naar de burp suite om te kijken wat hij laat zien
4. Vervolgens heb ik geprobeerd het wachtwoord te brute force (heel veel wachtwoorden proberen door middel van een tool) met de wordlist: /usr/share/wordlists/wifi-fer/common.txt
5. Daar kwam het wachtwoord: admin123 uit

**Impact:**

Deze kwetsbaarheid is belangrijk omdat toegang tot het admin-paneel aanzienlijke controle biedt, wat ernstige gevolgen kan hebben voor een bedrijf.

<https://nvd.nist.gov/vuln/detail/CVE-2022-3874>

**Aanbevolen oplossing:**

Implementeer sterkere wachtwoordbeveiliging, waardoor het moeilijker wordt om wachtwoorden te raden. Moedig gebruikers aan om unieke en complexe wachtwoorden te gebruiken en implementeer automatische vergrendeling na een aantal mislukte inlogpogingen om brute force-aanvallen te voorkomen.

**Bijlagen:**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Admin Sectie (hoog risico)**

**Beschrijving:**

Proberen toegang te krijgen tot het admin gedeelte van de Juice Shop, waar je systeemaanpassingen kunt maken.

**Stappen om de kwetsbaarheid te reproduceren:**

1. Controleer eerst of er een administratiesectie in de URL aanwezig is.
2. Als deze sectie bestaat, probeer dan in te loggen op het admin-account (zie vorige kwetsbaarheid).
3. Log in op het admin-paneel met de volgende gegevens: E-mail: [admin@juice-sh.op](mailto:admin@juice-sh.op) Wachtwoord: admin123.
4. Voer opnieuw "administration" in de URL in.
5. Eenmaal daar, heb je toegang tot het administratiepaneel.

**Impact:**

De impact kan groot zijn als iemand die niet geautoriseerd is toegang krijgt tot deze sectie. Je kan namelijk allerlei aanpassingen maken, bijvoorbeeld het verwijderen van gebruikers.

**Aanbevolen oplossing:**

Om dit probleem op te lossen, moet de toegang tot het admin-paneel beter worden beveiligd. Dit kan worden bereikt door sterke wachtwoordbeveiliging te implementeren, beperkte toegangscontrole in te stellen en ervoor te zorgen dat alleen geautoriseerde personen toegang hebben tot het admin-gedeelte.

**Bijlagen:**

**A screenshot of a computer

Description automatically generated**

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Confidential Document (mid risico)**

**Beschrijving:**

Het verkrijgen van toegang tot een vertrouwelijk document binnen de Juice Shop.

**Stappen om de kwetsbaarheid te reproduceren**

1. Ga naar de "Over ons" pagina en merk op dat er een FTP-directory wordt vermeld.
2. Voeg "/ftp" toe aan het einde van de URL om toegang te krijgen tot die directory.
3. In de directory zie je verschillende documenten die kunnen worden bekeken.
4. Klik op een document naar keuze om toegang te krijgen tot vertrouwelijke informatie.

**Impact:**

De impact van een dergelijke directory kan aanzienlijk zijn, vooral als bedrijven belangrijke documenten op een FTP-server opslaan en iedereen er zonder beperkingen bij kan. Dit kan leiden tot ongewenste toegang tot gevoelige bedrijfsinformatie.

<https://nvd.nist.gov/vuln/detail/CVE-2023-33956>

**Aanbevolen oplossing:**

Om deze kwetsbaarheid te verhelpen, is het essentieel om de toegangscontrole op de FTP-directory te verbeteren. Dit kan worden bereikt door striktere beperkingen en authenticatiemaatregelen in te voeren om te voorkomen dat ongeautoriseerde personen toegang krijgen tot gevoelige documenten. Het is belangrijk om de beveiliging van opgeslagen documenten te versterken en te zorgen voor gepaste autorisatie voor gebruikers die toegang nodig hebben.

**Bijlagen:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Security Policy (mid risico)**

**Beschrijving:**

Je moet je gedragen zoals elke white-hat hacker (goede intentie hacker) zou gedragen. Elk bedrijf zou een security policy moeten hebben en daarbij ook een security.txt file moeten hebben, deze gaan we proberen te vinden in de juice-shop.

**Stappen om de kwetsbaarheid te reproduceren:**

1. Zoek op het internet waar de security.txt file normaal gesproken moet staan.
2. Hij zou moeten staan in de: /.well-know/security.txt directory.
3. Deze zoek je dan op in de URL.
4. En dan zit je in de security.txt directory van de site

**Impact:**

Het identificeren van de security.txt-directory kan wellicht gevolgen hebben, maar het hangt af van de inhoud van dit bestand. Als de security.txt informatie bevat over beveiligingsmaatregelen en contactgegevens voor een bekendmaking van kwetsbaarheden, kan het helpen bij de beveiligingsrapportage Maar als dit bestand niet goed is opgesteld of verkeerd is ingesteld, kan dit de beveiliging van de website in gevaar brengen.

<https://nvd.nist.gov/vuln/detail/CVE-2023-2639>

**Aanbevolen oplossing:**

Om dit probleem op te lossen, is het een goed idee voor bedrijven om een speciaal bestand genaamd "security.txt" te maken. In dit bestand moeten ze juiste contactgegevens opnemen, zodat mensen beveiligingsproblemen kunnen melden. Ook moeten ze belangrijke beveiligingsinformatie in dit bestand zetten. Het is belangrijk om duidelijke regels te hebben over hoe ze met beveiligingszaken omgaan en hoe mensen problemen kunnen melden. Het gebruik van de "/.well-known/security.txt"-map kan helpen bij het verbeteren van de communicatie over beveiliging en samenwerking met goede hackers.

**Bijlagen:**

A screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Missing Encoding (hoog risico)**

**Beschrijving:**

Als je naar de foto´s gaat dan zie je dat er geen foto is te zien, maar een url met een error. Bij deze kwetsbaarheid ga ik deze foto proberen terug te halen.

**Stappen om de kwetsbaarheid te reproduceren:**

1. Eerst kijken we naar de foto wall die staat in de juice-shop.
2. Rechtermuisklik op de foto die niet te zien is.
3. Dan klik je op inspect
4. Dan ga je naar de source foto (jpg). Zie bijlage
5. Daar verander je de # naar %23, want de html code pakt geen # en in plaats daarvan moet je dus %23 want dan kan hij de foto wel lezen.
6. Dan druk je op enter en kan je de foto zien

**Impact:**

Deze kwetsbaarheid zorgt ervoor dat foto's op de website niet goed worden weergegeven. In plaats van de foto te zien, krijg je een foutmelding. Dit is vervelend voor mensen die de website bezoeken omdat ze de informatie of afbeeldingen niet kunnen zien zoals bedoeld.

<https://nvd.nist.gov/vuln/detail/CVE-2021-33672>

**Aanbevolen oplossing:**

Om dit probleem op te lossen, moeten we ervoor zorgen dat de website de foto's op de juiste manier laat zien, zonder dat bezoekers de URL handmatig moeten aanpassen. Hier is wat we kunnen doen:

1. **Reparatie van de links:** Zorg ervoor dat de links naar de foto's correct zijn. Dit betekent dat de tekens in de link, zoals "#" en andere speciale tekens, goed worden weergegeven zonder rare foutmeldingen.
2. **Controle van de invoer:** Zorg ervoor dat als mensen iets op de website invoeren, zoals een zoekopdracht of een opmerking, dit geen rare effecten heeft op de links. Dit helpt om te voorkomen dat de website kapot gaat door verkeerde input van de gebruiker.

**Bijlagen:**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door: Erdem**

**Kwetsbaarheidstitel: Forgotten Developer Backup**

**Beschrijving:**

Toegang krijgen tot een developer backup die hij vergeten is te verbergen.

**Stappen om de kwetsbaarheid te reproduceren:**

1. Ga naar de FTP server (kijk voor meer informatie bij de voorgaande kwetsbaarheid met de FTP server)
2. Daar moet je weer de FTP directory openen en naar package.json.bak gaan.
3. Daar zie je dat hij hem niet wil openen en dus moet je om de server te omzeilen #2500.md achter het verzoek zetten.
4. Dan download hij gelijk wat er in de desbetreffende bestand staat.
5. Zo kan je dan kijken naar de backup code die de programmeur heeft gemaakt.

**Impact:**

De "Forgotten Developer Backup" kwetsbaarheid kan tot gevolg hebben dat onbevoegde personen toegang krijgen tot belangrijke ontwikkelingsbestanden. Dit kan leiden tot het lekken van geheime informatie en de veiligheid van gegevens in gevaar brengen.

**Aanbevolen Oplossing:**

Om dit probleem op te lossen, is het belangrijk om strenge regels en beveiliging toe te passen op de manier waarop bestanden worden bewaard. Ontwikkelaars moeten regelmatig controleren welke bestanden ze bewaren en onnodige bestanden verwijderen. Ze moeten ook leren hoe ze bestanden veilig kunnen opslaan en delen om de risico's te verminderen. Het is belangrijk om ervoor te zorgen dat de geheimhouding en bescherming van deze bestanden.

**Bijlagen:**

A screenshot of a computer

Description automatically generated

**Kwetsbaarheid gevonden door Erdem**