**Prosperity Trust Bank**

**Kan jij onze website hacken?**

Link = <https://react-vti-cyber.web.app/>

**Robots.txt**

robots.txt is een tekstbestand op websites dat webrobots specifieke instructies geeft over welke delen van de site ze mogen doorzoeken of dienen te negeren. Deze instructies zijn bedoeld om zoekmachines te helpen bepalen welke inhoud ze moeten indexeren. Echter, het kan ook kwaadwillende actoren informatie verschaffen over beschikbare URL's.

Een voorbeeld hiervan is te vinden op <https://facebook.com/robots.txt>. Het is mogelijk om geheime locaties of plekken die niet direct door het publiek te vinden zijn via een Google-zoekopdracht, te ontdekken. De uitdaging is om de verborgen URL en de bijbehorende flag te vinden.

Vind de geheime URL

|  |  |
| --- | --- |
| Noteer de flag |  |

**Afbeeldingen en hun “metadata”**

JPEG-metadata verwijst naar aanvullende informatie die is ingebed in een JPEG-afbeelding. Deze metadata kan gedetailleerde informatie bevatten, zoals camera-instellingen, de opnamedatum, gebruikte software en zelfs geografische locatiegegevens (indien beschikbaar). Je kunt dit soort gegevens eenvoudig bekijken met een teksteditor of via een online metadata-viewerwebsite.

Vind de geboortedatum van Arthur

|  |  |
| --- | --- |
| Vind de geboortedatum van Arthur (dit is de flag) |  |

**OSINT (Open Source Intelligence)**

OSINT verwijst naar het verzamelen en analyseren van informatie die publiekelijk beschikbaar is, zoals gegevens online, sociale mediaprofielen en nieuwsartikelen.

Bert is actief op sociale media, wat een potentieel risico kan inhouden voor OSINT-aanvallen. Het benadrukken van het belang van sterke wachtwoorden (zonder gebruik van bv. familieleden of andere huisgenoten) en het gebruik van unieke wachtwoorden per account is cruciaal.

Is Bert zich bewust van deze beveiligingspraktijken?

|  |  |
| --- | --- |
| Login als Bert met het gevonden wachtoord, noteer de flag: |  |

**Ontwikkelaarstools**

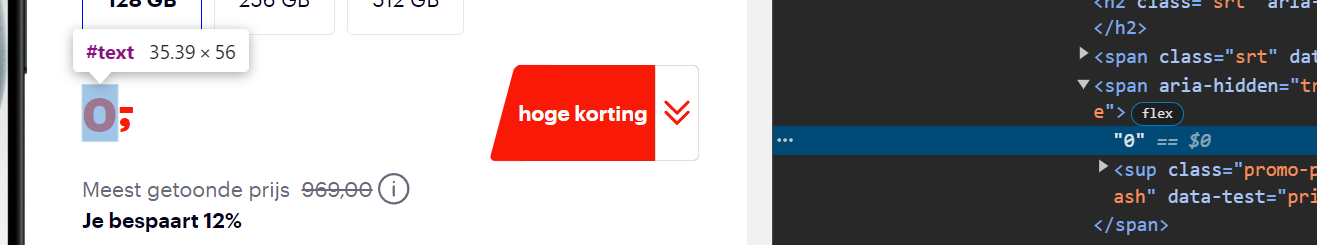
**(dit kan je enkel doen als je ingelogd bent als Bert)**

In de ontwikkelaarstools kun je diverse gegevens van een website bekijken en zelfs de inhoud ervan aanpassen.

Je kunt de ontwikkelaarstools openen door op F12 te drukken. Vervolgens kun je een deel van de website selecteren door te klikken op het icoontje bovenaan. Aanpassingen blijven deze alleen zichtbaar totdat de pagina opnieuw wordt geladen.

Het is cruciaal om te begrijpen dat, hoewel je bijvoorbeeld de prijs van een product lokaal kunt aanpassen via ontwikkelaarstools, deze wijziging geen effect heeft op de daadwerkelijke prijs, tenzij de server-side beveiliging zeer zwak is.  
  
Afbeelding met tekst, schermopname, Mobiele telefoon, software

Automatisch gegenereerde beschrijving

****

Pas het loon aan van een medewerker

De PT bank heeft toevallig een zeer slechte beveiliging, kan jij als hacker het loon aanpassen van een medewerker op dezelfde manier? Probeer het aan te passen naar 10.000 euro.

|  |  |
| --- | --- |
| Verander het loon naar 10.000 in en noteer de flag: |  |

**Netwerkanalyse**

De "netwerk" tab in de ontwikkelaarstools van een browser geeft een overzicht van alle netwerkaanvragen tijdens het laden van een webpagina. Hierin worden statuscodes, laadtijden en gedetailleerde headers weergegeven, inclusief de gegevens van de aanvragen. Om toegang te krijgen tot de ontwikkelaarstools, druk op F12. Kunnen jullie de geheime flag vinden binnen een van de netwerkaanvragen?

Hint: Begin je zoektocht op de homepagina.

|  |  |
| --- | --- |
| Vind de flag tussen de netwerk aanvragen |  |

Afbeelding met tekst, schermopname, software, Multimediasoftware

Automatisch gegenereerde beschrijving

**Finale opdracht: Local Storage + Hashing**

De "local storage" is een specifieke database per website waarin gegevens kunnen worden opgeslagen. Websites maken hier vaak gebruik van om informatie te bewaren. Kun je de volgende aanwijzing vinden?

Je kunt de local storage bekijken door op F12 te drukken en naar het gedeelte 'Application' te gaan. Eenmaal daar kun je mogelijk een hint ontdekken die je helpt bij het inloggen als admin. Met deze hint kun je vervolgens het wachtwoord van de admin achterhalen. Succes!

Hint: Gebruik [https://gchq.github.io/CyberChef/](https://gchq.github.io/CyberChef/%20) om verder te gaan.   
Probeer ook <https://hashes.com/en/tools/hash_identifier> om het type hash te bepalen.

|  |  |
| --- | --- |
| Vind de tip in local storage |  |
| Navigeer naar de juiste locatie |  |
| Ontrafel de sleutel |  |
| Gebruik de ontwikkelaarstools om de login te raden. |  |
| Noteer de flag: |  |