**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 vertelt welke delen van de site ze mogen crawlen of negeren. Het bevat instructies zoals "Disallow: /geheime-map/" (verbiedt toegang tot de map "geheime-map"). Deze instructies helpen zoekmachines bepalen welke inhoud ze moeten indexeren. Het kan aanvallers ook informatie geven voor welke url’s er allemaal beschikbaar zijn.

Voorbeeld: <https://facebook.com/robots.txt>

Vind de geheime locatie

Zijn er geheime locaties of locaties waar het publiek niet direct kan vinden met een google search?

|  |  |
| --- | --- |
| Vind de geheime locatie |  |
| Navigeer naar de geheime locatie |  |
| Noteer de flag |  |

**Afbeeldingen en hun “metadata”**

JPEG-metadata verwijst naar aanvullende informatie die is ingebed in een JPEG-afbeelding. Deze metadata kan details bevatten zoals de camera-instellingen, de datum waarop de foto is genomen, de gebruikte software, en zelfs geografische locatiegegevens (indien beschikbaar). Dit soort gegevens kan je gewoon in een teksteditor of een online metadata viewer website bekijken.

Vind de geboortedatum van Arthur

Tip: open de foto met kladblok (of gebruik een website)

|  |  |
| --- | --- |
| Download de profiel foto van Arthur |  |
| Vind de tips in de metadata |  |
| Vind de geboortedatum van Arthur (dit is de flag) |  |

**OSINT (Open Source Intelligence)**

OSINT verwijst naar het verzamelen en analyseren van informatie die vrij beschikbaar is voor het publiek, zoals online gepubliceerde gegevens, sociale mediaprofielen, nieuwsartikelen en andere openbare bronnen. Het wordt vaak gebruikt door verschillende entiteiten, waaronder beveiligingsprofessionals, onderzoekers en bedrijven, om informatie te verzamelen en inzicht te krijgen in bepaalde individuen, organisaties of gebeurtenissen.

Vind de inloggegevens van Bert

Bert post graag op Facebook, dit kan een risico zijn voor OSINT aanvallen. Daarom is het goed om altijd een sterk wachtwoord te nemen (geen geboortedatums of namen van familieleden/huisdieren) en per account een ander wachtwoord te gebruiken. Maar heeft Bert dit wel gedaan?

|  |  |
| --- | --- |
| Vind het wachtwoord op Bert zijn social media. |  |
| Login als Bert, noteer de flag: |  |

**Ontwikkelaarstools**

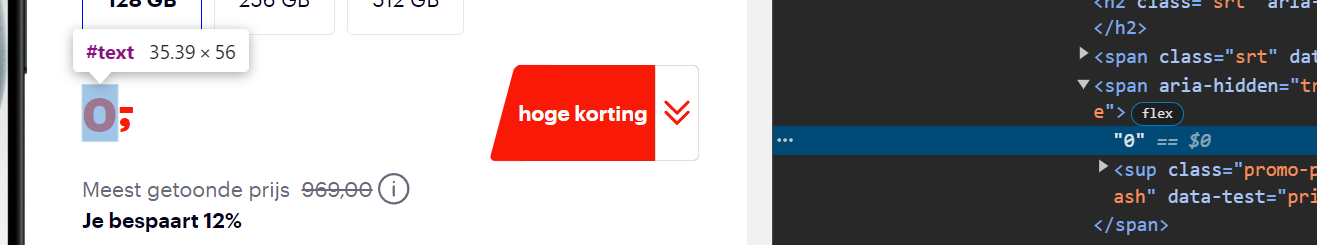
**(dit kan je enkel doen als je ingelogd bent als Bert)**

In de ontwikkelaarstools kun je verschillende gegevens van een website bekijken. Het is ook mogelijk om de inhoud van een website aan te passen. Let op, deze aanpassingen zijn echter alleen zichtbaar voor de gebruiker en hebben geen daadwerkelijke invloed. Zo zal bijvoorbeeld het wijzigen van de prijs van een product op bol.com geen echte korting opleveren.

Afbeelding met tekst, schermopname, Mobiele telefoon, software

Automatisch gegenereerde beschrijving

De ontwikkelaar tools kan je bekijken door op F12 te duwen. En je kan een stukje van de website selecteren door op het icoontje bovenaan te klikken. Daarna kan je alles aanpassen, maar vanaf je de pagina herlaad, is alles terug weg.

****

Dit zal ook **geen** invloed hebben op de effectieve prijs van een product.

Pas het loon aan van een medewerker

De PT bank heeft echter een zeer slechte website, kan jij als hacker het loon aanpassen van een medewerker op dezelfde manier? Probeer het aan te passen naar 10000 euro.

|  |  |
| --- | --- |
| Open de ontwikkelaarstools |  |
| Vind het “max” attribuut van het salaris invoerveld |  |
| Pas het “max” attribuut aan naar een hoger getal |  |
| Vul 10000 in en noteer de flag: |  |

**Netwerkanalyse**

De "netwerk" tab in een browser's ontwikkelaarstools biedt een overzicht van alle netwerkaanvragen bij het laden van een webpagina. Hierin worden statuscodes, laadtijden en gedetailleerde headers weergegeven, ook data van aanvragen kan je hierin zien. De ontwikkelaar tools kan je bekijken door op F12 te duwen. Vinden jullie de geheime flag in 1 van de netwerkaanvragen?

|  |  |
| --- | --- |
| Vind de ontwikkelaarstools en de “netwerk” tab |  |
| Vind de “employees” aanvraag |  |
| Noteer de flag: |  |

Afbeelding met tekst, schermopname, software, Multimediasoftware

Automatisch gegenereerde beschrijving

**Local Storage**

De “local storage” is een soort database per website. Websites maken er gebruik van om gegevens in op te slaan. Kan je de volgende tip vinden?

Local storage kan je bekijken door op F12 te drukken. (bij Application) 

Inloggen als administrator

Met de tip die je kan vinden in de local storage, kan je verder om het wachtwoord van de administrator te vinden. Succes!

**Tip: gebruik** [**https://gchq.github.io/CyberChef/**](https://gchq.github.io/CyberChef/)

|  |  |
| --- | --- |
| 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: |  |