CySec – les 4

Database security, Database injections
en JWT

Nova College

Programma

- Terugblik vorige les
- Leerdoelen
- Database secruity
- Database injections
- JWT
- Volgende week

Actualiteit

Actualiteit - Odido

- 3 aanvallen
  - Phishing
  - Autoritair
  - Hacking
- 2 (vermeende) verdedigingen
  - Logging
  - Download blokkade

Wat weten we nog van vorige les?

Nova College

Leerdoelen

- Aan het einde van de les:
  - Weet je de kernprincipes van databases beveiligen
  - Weet je hoe rollen data kan beschermen.
  - Weet je wat een database injection is.
  - Kan je een database injection uitvoeren in een gecontroleerde omgeving.
  - Weet je hoe je database injections kan weren.
  - Weet je wat een JWT is.
  - Weet je hoe je een JWT toepast.

Inlog gegevens voor deze les zijn

Gebruikersnaam: Student

Wachtwoord: P1zzaParty!

Nova College

Graag even inloggen

Nova College

Database security – werkvorm – 5 minuten

- Iedereen heeft een kaartje met een D, K of H erop.
- Sommige zijn klanten (K) en sommige hackers (H)
- Developers (D) hebben het wachtwoord
- Klanten en hackers willen het wachtwoord om data te krijgen van de database (Docent)
- Hackers moeten zich voordoen als Klanten, wordt je ontmaskert ben je uit.
- Hackers en Klanten doel: verkrijg Data
- Developers doel: geef klanten toegang maar niet de Hackers

Graag even inloggen

Nova College

Database security opties

- Wachtwoord beveiliging
- Toegang tot specifieke datasets
- Rollen en rechten
- CRUD beveiliging
- Download blokkades
- Monitoring

Graag even inloggen

Nova College

Database security

Wachtwoord beveiliging

- Het minste dat erin moet zitten is een wachtwoord dat niet “root” of “password” of 1234 is
- Sterke wachtwoorden beschermen al een klein deel van je data.

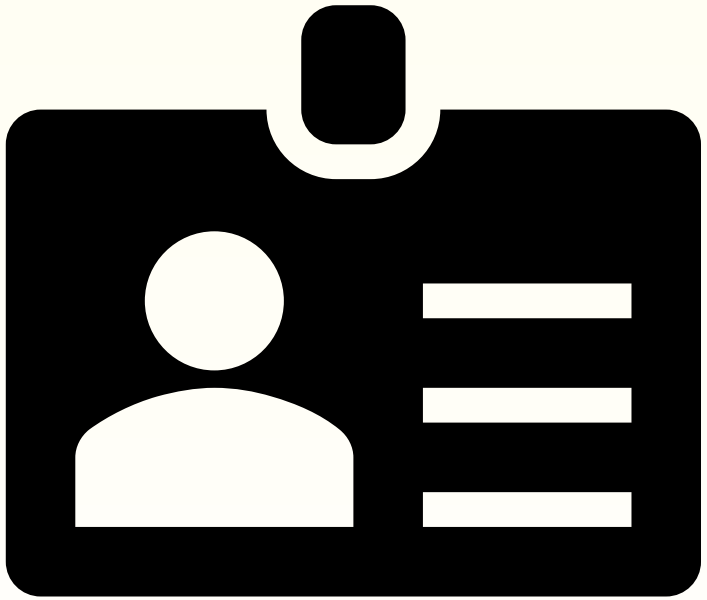
Toegang tot specifieke datasets

- Verleen alleen toegang tot data die absoluut nodig is.
- Als de klanten de film namen nodig heeft, geef ze dan niet ook toegang tot klantrekeningnummers
- Map uit wie wat nodig heeft.

Graag even inloggen

Nova College

Rollen en rechten



- Je kan rollen/Gebruikerprofielen maken voor een database.
- Deze rollen bevatten bepaalde rechten zoals:
  - Of dit type gebruiker mag toevoegen, verwijderen of wijzigen.
  - Welke tabellen dit type gebruiker mag inzien.
  - Of de gebruiker op grote schaal aanpassingen mag maken.

Graag even inloggen

Nova College

CRUD beveiliging

- **Create** – Mag een type gebruiker data aanmaken
- **Read** – Mag een type gebruiker data inzien
- **Update** – Mag een type gebruiker data wijzigen
- **Delete** – Mag een type gebruiker data verwijderen

- Dit kan op tabel, lijst, datapunt en kolom niveau bepaald worden

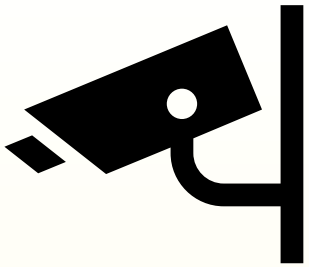
Customers

CustomerId	FirstName	LastName	DateCreated
1	Homer	Simpson	13/06/2014 3:33:37 PM
2	Peter	Griffin	13/06/2014 9:09:56 PM
3	Stewie	Griffin	13/06/2014 9:16:07 PM
4	Brian	Griffin	13/06/2014 9:16:36 PM
5	Cosmo	Kramer	13/06/2014 9:16:41 PM
6	Philip	Fry	13/06/2014 9:17:02 PM
7	Amy	Wong	13/06/2014 9:22:05 PM
8	Hubert J.	Farnsworth	13/06/2014 9:22:19 PM
9	Marge	Simpson	13/06/2014 9:22:37 PM
10	Bender	Rodríguez	13/06/2014 9:22:52 PM
11	Turanga	Leela	13/06/2014 9:23:37 PM
(New)			15/06/2014 9:00:01 PM

Graag even inloggen

Nova College

Database security



Download blokkades

- Speciale software regels die downloaden van data (bijna) onmogelijk maken.
- Vereist vaak de goedkeuring van meerdere hoge managers.
- Voorkomt massa dataleks.
- Wordt niet vaak genoeg gebruikt.
- Zo sterk/zwak als de rest van de beveiliging.

Monitoring

- Databases worden gemonitord door mens en machine.
- Machines geven signalen af als er verdachte activiteit is.
- Mensen nemen actie om data veilig te stellen.
- 24/7 monitoring voor grote data bedrijven.

Graag even inloggen

Nova College

Database injections

Graag even inloggen

Nova College

Database injections

- Database injections zijn een invoer in een veld waarbij data gemanipuleerd wordt op wijzes waarvoor die niet bedoeld zijn.
- Dit kan onschuldig zijn maar is dat vaak niet.
- Meeste systemen zijn hier tegen beschermd. De weinige die dat niet zijn geven informatie vrij.

Graag even inloggen

Nova College

Database injections - **ILLEGAAL**

- Database injections op een systeem waar je geen toestemming van hebt is **ILLEGAAL**
- Lichte straffen voor data opvragen, tot zware straffen van data verspreiden en/of verwijderen
- Zeer makkelijk te traceren
- Juridisch kan hier een straf op zitten van:
  - Een ban van de website/service
  - 20.000 euro
  - Tot 20 jaar de cel in

Graag even inloggen

Nova College

Database injections – Hoe werkt het

- Grofweg:
  - Je doelwit programma heeft een invoer veld.
  - Met dit invoer veld kan je zoeken naar een item.
  - In plaats van een normaal zoek resultaat geef je een afsluiting van SQL mee en daar achter een SQL command van wat je wilt bereiken.

- Veel SQL applicaties hebben al enkele beveiliging hiervoor maar niet geheel!

Graag even inloggen

Nova College

Database injections - bescherming

- 2 bekende manieren
- 1. je zoekt naar symbolen die niet thuishoren in een normaal verwacht invoerveld en keurt daarop een input goed of fout
- 2. Je laat een package controleren of de input correct is of niet

- 1 is meer werk maar zelf inzicht, 2 kan betrouwbaar en snel zijn maar kan iets over het hoofd zien.

Graag even inloggen

Nova College

Opdracht op github

- Een van de 5 verplichte opdrachten

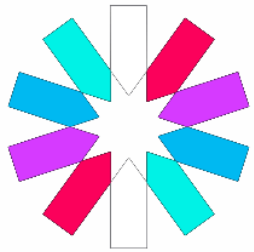
Graag even inloggen

Nova College

Zijn jullie het al zat om in te loggen?

Graag even inloggen

Nova College



JWT

- JSON Web tokens, zijn tokens die bewaard worden op een lokale browser.
- Deze tokens voorkomen dat inloggen niet consistent nodig is voor iedere actie.
- Vooral bedoeld voor web development maar kan ook gebruikt worden voor reguliere applicaties
- Wordt universeel gebruikt en is makkelijk terug te zoeken in een browser, het is een type Cookie

JWT - gebruik

- De gebruiker logt in.
- De gegevens worden gecontroleerd
- De server maakt een token aan die gekoppeld is aan een gebruiker en tijdsframe. (Soms ook IP bij hoge beveiliging)
- De gebruiker kan nu doen wat hij/zij wilt tot de gebruiker uitlogt of tot de tijd op is.

JWT – gebruik in code

- (Bijna) iedere taal heeft een package waarmee je JWT kan genereren, vereist vaak een install.
- Je maakt een private key van random letters en cijfers.
- Laat JWT het generen
- Stuurt het op naar de gebruiker, deze slaat het op in de browser
- De gebruiker stuurt met iedere actie de JWT mee.
- JWT controleert zichzelf of de actie nog kan en of de juiste persoon acties uitvoert.

Opdrachten: Database injections & JWT

- Twee opdrachten deze week:
  - Database injection oefening met de mogelijkheid om een database te manipuleren op wijze die niet bedoeld zijn.
  - JWT oefening waarmee je een tijdelijke token kan maken en gebruik ervan maken.

Volgende week

- Netwerken
  - Afluisteren
  - Beschermen
  - VPN
- Man in de middle
- Wireshark