Datalek cijfers UvA

Tiko Huizinga David Garay

Juni 2019

Abstract

Begin mei hebben wij een datalek in het Studenten Informatie Systeem van de UvA gevonden. Via dit datalek was het mogelijk om als ingelogde student alle cijfers van alle medestudenten in te zien. Dit was mogelijk door het veranderen van een studentnummer en vaknummer in de URL en het uitschakelen van javascript. Wij hebben dit met toestemming van de betrokken medestudenten getest. Nadat we dit lek gemeld hadden bij de universiteit, was het binnen een dag gedicht.

1 Student Informatie Systeem (SIS)

Het Student Informatie Systeem (SIS) is een systeem waarin vakinschrijvingen, studievoortgang, cijfers, betalingsstatussen en andere belangrijke zaken van studenten geregeld worden. Het wordt via een samenwerkingsverband gebruikt door de Universiteit van Amsterdam (UvA), Hogeschool van Amsterdam (HvA) en de Universiteit Leiden. Deze samenwerking gebeurt via het bedrijf SaNS in Utrecht[1].

Het systeem is gebaseerd op Oracle PeopleSoft Campus Solutions. Dit systeem wordt wereldwijd door ruim 750 academische onderwijsinstellingen gebruikt.

Volgens Folia zijn de kosten van dit systeem van 2004 tot 2012 opgelopen tot 25 miljoen euro voor de UvA en 14,6 miljoen euro voor de HvA[2].

[1] `https://sans-ec.nl/`
[2] `https://www.folia.nl/actueel/32040/sis-duur-laat-en-matig`

2 Het lek

Het lek zit in de URL van de volgende pagina[3]:

`www.sis.uva.nl:8011/psc/S3PRD/EMPLOYEE/SA/c/SNS_CUSTOMIZATIONS_NLD.SNS_CRSE_ENRL_DTL.NLD?Page=SNS_CRSE_ENRL_DTL&Action=U&CRSE_ID=111111&CRSE_OFFER_NBR=1&EMPLID=88888888`
In het specifiek deze twee velden:

- `CRSE_ID` geeft aan voor welk vak je het cijfer wil bekijken
- `EMPLID` geeft aan van welke student je het cijfer wil bekijken.

Verander het `EMPLID` naar het studentnummer van een andere student en je ziet zijn naam, de naam van dat vak en zijn cijfer voor hetzelfde vak. Verander vervolgens het `CRSE_ID` naar dat van een ander vak en je ziet het cijfer van deze student voor dat andere vak. Op basis van experimenten met test data, hebben we het volgende geconstateerd:

- Deze pagina blijft ongeveer een halve seconde zichtbaar waarna je wordt doorverwezen naar een pagina die aangeeft dat je niet geautoriseerd bent om deze inhoud te bekijken.
- Het feit dat deze doorverwijzing gebeurt nadat de student al het cijfer heeft kunnen zien geeft aan dat de data al binnen is en de autorisatie daarna client side gebeurt.
- In dit geval gebeurde dit via javascript. Het uitschakelen van javascript in de browser was genoeg om het cijfer te kunnen blijven zien.
- Als je het studentnummer leeg laat, krijg je een overzicht te zien van alle studentnummers op de UvA.
- Als je de vakcode leeg laat, krijg je een overzicht met alle vakcodes op de UvA.

Dit lek is een typisch voorbeeld van waarom client side autorisatie slecht is. Wat hier gebeurt is dat een gebruiker een resource van de server opvraagt. De server checkt of het inderdaad door een ingelogde gebruiker wordt opgevraagd. Als dat het geval is, stuurt de server de resource (in dit geval de naam, het vak en het cijfer) naar de gebruiker. De pagina wordt geladen en dan wordt in de browser via javascript een check gedaan of deze gegevens inderdaad van deze user zijn. Als dat niet zo is wordt de gebruiker doorgestuurd naar een pagina met een foutmelding. Een developer moet er altijd vanuit gaan dat code die op de machine van de gebruiker draait onbetrouwbaar is omdat een gebruiker die kan aanpassen. In dit geval was dit de javascript code en kon de gebruiker javascript uitzetten. Hierdoor gebeurde de doorverwijzing niet.

[3]Log als student in op het Student Informatie Systeem van de UvA - https://sis.uva.nl, dan Ga naar "Mijn academic plan" en klik op een cijfer

De OWASP top 10 is een overzicht met de 10 meest gemaakte beveiligingsfouten. Ze zeggen het volgende over access control: *Access control is only effective if enforced in trusted server-side code or server-less API, where the attacker cannot modify the access control check or metadata.* [4]

3 Impact

Door dit lek was het voor alle studenten van de UvA mogelijk om (eventueel geautomatiseerd met behulp van een script) alle namen, studentnummers en cijfers van alle andere 34000 studenten te bekijken. Om dit van een specifieke student te bekijken was het alleen nodig om het studentnummer en vakcode te vervangen in de URL. Het was mogelijk om met een eenvoudig script alle cijfers van alle studenten op deze manier te downloaden. SIS is het Student Informatie Systeem ontwikkeld door SaNS. Het systeem wordt ook gebruikt door onder andere de Universiteit Leiden en de Hogeschool van Amsterdam. Over de universiteit Leiden hebben we gehoord dat ze wisten van het kwetsbare onderdeel van het systeem en dit al eerder hadden uitgeschakeld.

4 Responsible disclosure timeline

Maandag 6 mei

Op maandag 6 mei 2019 vinden we bij toeval deze kwetsbaarheid in SIS. We testen de kwetsbaarheid met de studentnummers van een klein aantal medestudenten met hun toestemming en waar ze bij zijn.

Dinsdag 7 mei

Om 19:01 sturen we een mail aan het Computer Emergency Response Team (CERT) van de UvA met onze bevindingen. Om 21:37 krijgen we een mail waarin we hartelijk worden bedankt voor onze inspanning en de manier van melden.

Woensdag 8 mei

Om 09:14 krijgen we een follow-up dat de melding bij de SIS systeemeigenaar van de UvA ligt en dat die er voor zullen zorgen dat het lek zo spoedig mogelijk zal worden gedicht. Om 09:51 een terugkoppeling van de systeemeigenaar: De melding is gereproduceerd en terwijl het lek wordt gefixt, worden de rechten

[4] `https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control`

van studenten op deze pagina ingetrokken. Er bestaat een pagina op SIS waar dit lek niet bestaat waar studenten nog wel hun eigen cijfers kunnen bekijken.

Donderdag 8 mei

We krijgen een telefoontje van het hoofd van de afdeling SIS van de UvA waarin we nogmaals hartelijk bedankt worden voor onze inspanningen en als we nog ooit iets dergelijks vinden, het zeer gewaardeerd wordt als we het op dezelfde manier melden.

Vrijdag 10 mei

Om 13:01 vragen we via CERT of we, nu het lek gedicht is, dit verhaal ook mogen publiceren. 13:24 krijgen we een reactie dat ze daar binnenkort op terug zouden komen.

Maandag 13 mei

De UvA reageert op onze publicatievraag. Wat betreft het CERT is er voldaan aan de responsible disclosure procedure en maken ze geen bezwaar tegen publicatie.

Woensdag 12 juni

We informeren de UvA dat we van plan zijn deze week te publiceren. Hierbij sturen we de op dat moment meest recente versie van dit artikel. Op het zelfde moment benaderen we Folia, de onafhankelijke krant van de UvA met onze bevindingen en ook dit artikel er bij. We spreken af dat ze wachten met publiceren totdat de UvA kans heeft gehad om hierop te reageren.

We worden dezelfde dag gebeld door het hoofd van SIS van de UvA. Hij geeft aan dat het lek direct gemeld was bij de functionaris gegevensbescherming van de UvA. Die heeft het ook gemeld bij het bestuur van de UvA. In overleg met het bestuur van de UvA is ingeschat dat het risico van dit lek voor de studenten laag is, gegeven dat uit hun onderzoek bleek dat er geen scripts zijn gedraaid. Echter, merken ze nu op dat studentnummers persoonsgegevens zijn en het feit dat een lijst van alle studentnummers op te vragen was, gemeld moet worden bij de Autoriteit Persoonsgegevens (AP). Dit hadden ze eerder nog niet gedaan omdat ze toen gefocust hebben op de cijfers.

Donderdag 13 juni

We krijgen een mail van het hoofd SIS van de UvA. Hij geeft aan dat een (voorlopige) melding is gedaan bij het AP over de mogelijkheid om een lijst van studentnummers op te vragen.

Wij geven aan dat we de volgende dag (vrijdag 14 juni) ons artikel gaan publiceren.

5 Conclusie en discussie

Volgens de Algemene Verordening Persoonsgegevens moeten datalekken die een risico vormen voor de rechten en vrijheden van betrokkenen gemeld worden bij de autoriteit persoonsgegevens. Verder moeten lekken gemeld worden aan betrokkenen (studenten in dit geval) als het lek "een *hoog* risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. [...] Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade."[5]

De UvA heeft ons verteld dat ze het lek direct na onze melding hebben gemeld bij hun functionaris gegevensbescherming. Daarna hebben ze onderzoek gedaan of dit lek op grote schaal misbruikt is. Uit hun onderzoek is geconcludeerd dat er niet op grote schaal misbruik van gemaakt is. Op basis daarvan, is een risicoanalyse gemaakt waarna ze hebben besloten dat het niet nodig was dit te melden bij het AP.

Dit is niet de eerste keer dat systemen van de UvA betrokken zijn bij datalekken: twee jaar geleden is Blackboard, het toenmalige studenten administratie systeem, in het nieuws gekomen na een hack[6]. In 2016 ontdekte HvA-student Nelson Berg een datalek waardoor hij foto's, namen en studentnummers van 130.000 studenten en medewerkers kon downloaden. Hij kwam hier achter bij het inschrijven voor een vak waarna hij zijn studentnummer verving met dat van iemand anders. [7].

Wij vonden de volledige responsible disclosure procedure prettig verlopen. Er werd altijd snel, serieus en kundig gereageerd op onze mails. Desondanks merken we op dat er meerdere beveiligingsincidenten geweest zijn met dit systeem. Dit lek zijn wij toevallig tegen gekomen, wellicht dat een groter beveiligingsonderzoek nog meer problemen in kaart brengt.

[5] `https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf`

[6] `https://www.folia.nl/actueel/110890/studenten-ontdekken-ernstig-datalek-in-blackboard`

[7] `https://www.folia.nl/actueel/101874/hva-student-ontdekt-groot-datalek-in-sis`