Security Assessment Report
2sky NV

TSF | THE SECURITY FACTORY

Table of Contents

Document Properties

Version History

Current version: **1.50**

Version	Date	Status	Author
0.01	13/03/18	Creation	Steven Verscheure
0.02	22/03/18	Update	Steven Verscheure
0.90	30/03/18	Review by QA	Ward Vermeulen
1.00	03/04/18	Final Draft	Steven Verscheure
1.50	03/05/18	Retest	Ward Vermeulen

Target Audience

This document is mainly intended for technical personnel involved in the remediation of the reported vulnerabilities.

Project Details

Scope

The Security Factory was tasked in performing a technical web application penetration test on Vidyano in order to allow 2sky NV to have a clear view on how resilient this application is against an eventual cyber-attack.

The application test occurred against the following URL:

- https://vidyano.azurewebsites.net

The received customer accounts were:

- UserTSF
- AuditorTSF
- AdminTSF

On the 3rd of May 2018 a retest occurred against the same scope, with the same customer accounts.

During this test we also took into consideration which issues are specifically related to the product and which are related to the demo application. This is reflected in our retest reporting.

Not in Scope

The following items were not in scope during this security test:

- Denial of Service or any other destructive techniques
- Functional testing
- Introduction of new vulnerabilities without explicit permission of the customer

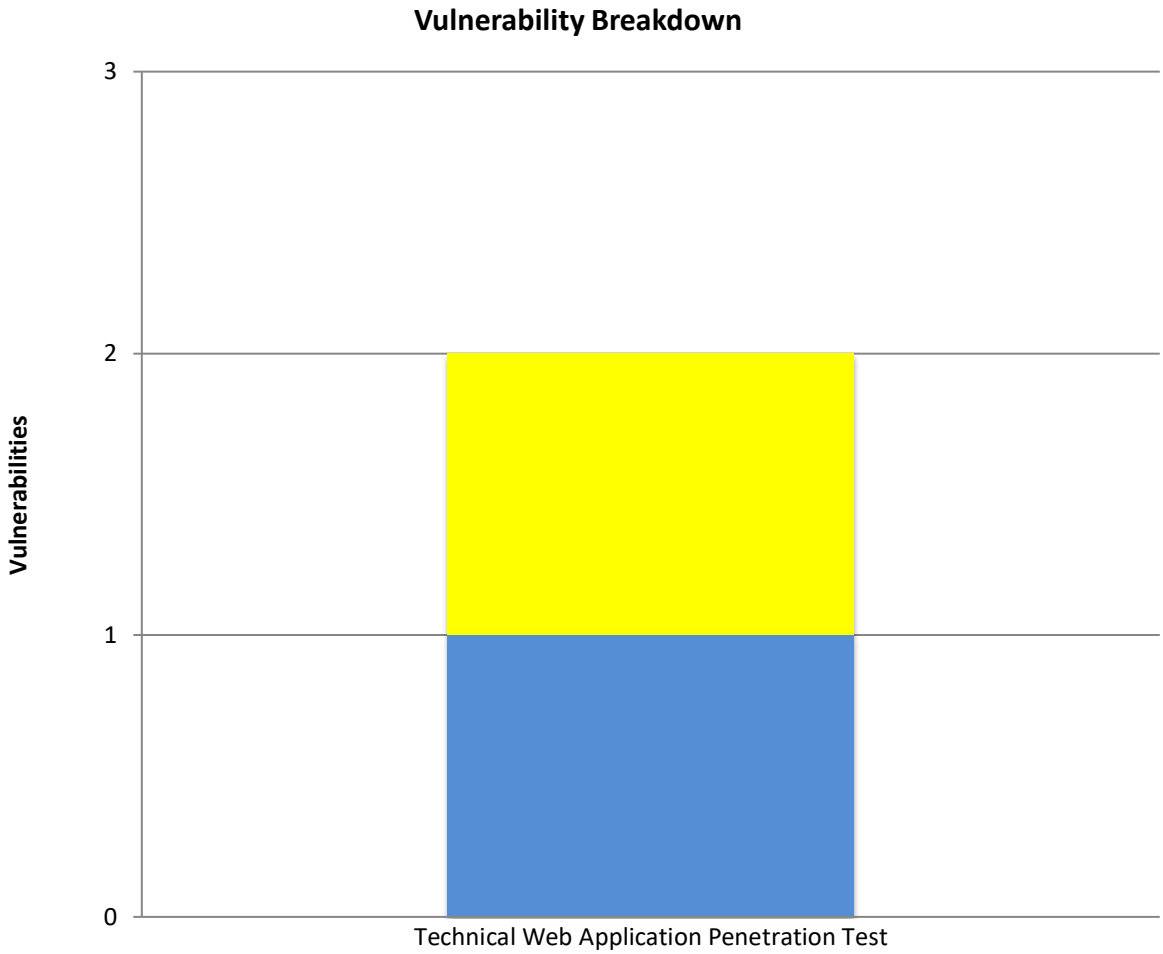
Executive Summary

Background

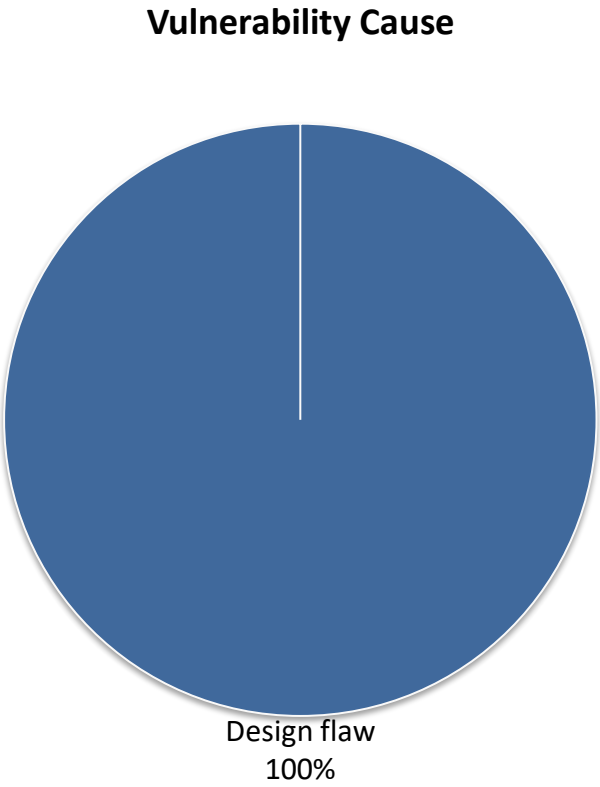
The Security Factory was tasked with performing a number of vulnerability assessments on the environment of 2sky NV. The purpose of this assessment was to verify the effectiveness of the security controls put in place by 2sky NV to secure business-critical information, and the extent to which an attacker can compromise systems and information should these controls fail.

This report represents the findings from the assessment and the associated remediation recommendations to help 2sky NV strengthen its security posture.

General Findings



Critical	0
High	0
Medium	0
Low	1
Note	1



Overall Security Posture

Based on our experience we would rate the security posture of the application in the **higher** regions of good security.

Strategic Overview

Vulnerability Summary

Risk Level	Finding	Category	Retest
Medium	AuthToken can be replayed	Incorrect use	FIXED
Medium	Insufficient brute force detection/protection	Design flaw	FIXED
Medium	Automatic session dropping after acceptable time	Design flaw	CONFIGURABLE
Medium	Old password not required on password change	Design flaw	FIXED
Low	No session drop on password change	Design flaw	FIXED
Low	No out of the box automation protection	Design flaw	BY DESIGN
Low	Stack traces enabled	Misconfiguration	FIXED
Low	TLSv1.0 supported	Misconfiguration	FIXED
Information	API docs are publicly available	Other	BY DESIGN

Remediation Roadmap

1 to 3 months

- ~~Review the Authtoken check on every request~~
- ~~Implement protection against brute-force attacks~~
- ~~Make sure user sessions are dropped after an acceptable amount of time~~
- ~~Fix the flaws in the password change mechanism~~

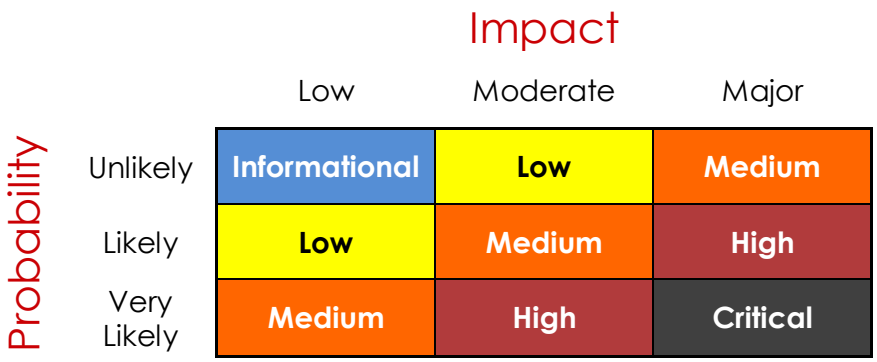
3 to 12 months

- ~~Implement captchas to prevent bots from spamming the application~~
- ~~Make sure no information leaks through error messages~~
- ~~Stop supporting TLSv1.0~~

12+ months

- 3rd Party security re-assessment

Risk Levels Overview



Critical	A critical risk issue is an issue that causes a major impact to the business and is very likely to occur. Examples of issues with major impact include: an permanent downtime of a service, complete destruction of data, disclosure of very sensitive information, severe reputational damage, etc. The probability that this issue will be exploited in the near future is very likely as there are currently multiple reports of this issue being exploited in the wild or if this issue can be exploited without much effort.
High	Issues posing a high risk are either very likely to occur while causing moderate impact or cause a major impact while being likely to occur.
Medium	Medium risk vulnerabilities are either very likely to cause low to moderate impact but unlikely to cause major impact. Examples of moderate impact include a temporary downtime of a service, alteration of data, disclosure of mildly sensitive data, moderate reputational damage, etc. An issue is deemed likely to occur if reports of the issue being exploited in the wild exist or if the exploitation of this issue requires prior knowledge or a moderate investment of time and resources.
Low	Issues posing a low risk are likely to cause low impact or unlikely to cause moderate impact. Examples of low impact include a short interruption of a service, slight corruption of data, disclosure of non-sensitive data, low reputational damage, etc. If an issue is unlikely to occur if there are no reports of this exploit reported in the wild, the exploitation requires extensive prior knowledge or an extensive investment of time and resources.
Informational	Generally, informational issues are issues that are unlikely to cause a low impact. Sometimes issues are discovered that are either out of scope or have no security impact, but which are deemed interesting enough to put in the report. These will be ranked as “informational”

AuthToken can be replayed

Classification

Risk Level	**Medium**
URL(s)	https://vidyano.azurewebsites.net/

Finding

A valid authToken can be replayed in different requests. We confirmed this issue by replaying a seven days old POST request with its token. By design Vidyano issues a new token upon every new request. Hence, the replay of a token should not be possible.

Consequences

Once an attacker gains access to a single valid authToken, he can use it to do multiple requests, and effectively hijack a session.

Remediation Advice

Check if a single authToken is being used for multiple requests and deny access if this is detected.

Screenshots / Evidence

POST request made on 13/03/2018:

```
POST /ExecuteAction HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://vidyano.azurewebsites.net/Home/Note/2
Content-Length: 1545
Content-Type: text/plain;charset=UTF-8
Cookie: __vi=1.16.2; staySignedIn=true
Connection: close


{"clientVersion":"1.16.2-
6406a35","environment":"Web","environmentVersion":"2","userName":"UserTSF","authT
oken":"MTAtMDQtMjAxOCAxMjoyNjoxNC4xNDAxMDk1ICswMDowMDtyaS9JQTlnVU9ZMm5oa3NYVkdhc2
EwRlVRYlcweGdENjhuUzRmZ1BtZVg4PQ==","action":"PersistentObject.Save","parent":{"i
d":"73558aa6-ccaf-3f4d-a18c-
2b6c58a5713e","type":"Note","objectId":"2","securityToken":"$Cs7cdAi1G9wI9xRZzzH0
TNaU9nmmEdLPtQqmvIPbmEbfBOK8g2M=","attributes":[{"id":"d3bf6e99-c302-3a1b-a1da-
924e57352c92","name":"CreatedBy","label":"Gemaakt
door","type":"User","isReadOnly":true,"isRequired":true,"visibility":"Read,
Query","value":"ed65d8e2-d713-488d-be06-
b87d964aa346","options":["UserTSF"]},{"id":"880c4334-4d42-3d5f-9017-
dfa03d3a8d1f","name":"CreatedOn","label":"Gemaakt
op","type":"DateTimeOffset","isReadOnly":true,"isRequired":true,"visibility":"Rea
d, Query","value":"09-03-2018 13:55:58.9311008 +01:00"},{"id":"679cdde5-a2bb-3cfb-
851d-
838470d2b5d3","name":"Description","label":"Beschrijving","type":"MultiLineString
","isRequired":true,"isValueChanged":true,"visibility":"Always","value":"nieuw
testsdfdsfsdfje"},{"id":"58ceb49f-9cb3-3062-be0b-
04fe4c0d2d7b","name":"ModifiedBy","label":"Gewijzigd
door","type":"User","isReadOnly":true,"isRequired":true,"visibility":"Read,
Query","value":"b0e5e9e1-e848-48a4-8e86-
19f41a89e695","options":["AdminTSF"]},{"id":"3cc89a5e-cb08-30db-8526-
3fe367921dec","name":"ModifiedOn","label":"Bewerkt
op","type":"DateTimeOffset","isReadOnly":true,"isRequired":true,"visibility":"Rea
d, Query","value":"09-03-2018 14:03:48.3301901 +01:00"}]}}
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 2125
Content-Type: application/json; charset=utf-8
Expires: -1
Access-Control-Expose-Headers: AuthToken
X-Content-Type-Options: nosniff
Date: Tue, 13 Mar 2018 12:27:37 GMT
Connection: close

{"result":{"type":"Note","objectId":"2","breadcrumb":"nieuw
testsdfdsfsdfje","id":"73558aa6-ccaf-3f4d-a18c-
2b6c58a5713e","newOptions":"","label":"Opmerking","stateBehavior":"None","queryLa
youtMode":"FullPage","tabs":{"":{"id":"ea84d739-3eea-4c21-a2b9-
7c0de6ede35d","name":"Note","columnCount":0}},"attributes":[{"name":"CreatedBy","
type":"User","value":"ed65d8e2-d713-488d-be06-b87d964aa346","id":"d3bf6e99-c302-
3a1b-a1da-
924e57352c92","offset":10,"rules":"Required","isReadOnly":true,"label":"Gemaakt
door","visibility":"Read,
Query","toolTip":"","columnSpan":1,"options":["UserTSF"],"isRequired":true,"group
":"","tab":""},{"name":"CreatedOn","type":"DateTimeOffset","value":"09-03-2018
13:55:58.9311008                          +01:00","id":"880c4334-4d42-3d5f-9017-
dfa03d3a8d1f","offset":20,"rules":"Required","isReadOnly":true,"label":"Gemaakt
op","visibility":"Read,
Query","toolTip":"","columnSpan":1,"isRequired":true,"group":"","tab":""},{"name"
:"Description","type":"MultiLineString","value":"nieuw
testsdfdsfsdfje","id":"679cdde5-a2bb-3cfb-851d-
838470d2b5d3","offset":5,"rules":"NotEmpty;
MaxLength(500)","label":"Beschrijving","visibility":"Always","toolTip":"","column
Span":1,"isRequired":true,"group":"","tab":""},{"name":"ModifiedBy","type":"User"
,"value":"ed65d8e2-d713-488d-be06-b87d964aa346","id":"58ceb49f-9cb3-3062-be0b-
04fe4c0d2d7b","offset":30,"rules":"Required","isReadOnly":true,"label":"Gewijzigd
door","visibility":"Read,
Query","toolTip":"","columnSpan":1,"options":["UserTSF"],"isRequired":true,"group
":"","tab":""},{"name":"ModifiedOn","type":"DateTimeOffset","value":"21-03-2018
10:08:25.975483                           +01:00","id":"3cc89a5e-cb08-30db-8526-
3fe367921dec","offset":40,"rules":"Required","isReadOnly":true,"label":"Bewerkt
op","visibility":"Read,
Query","toolTip":"","columnSpan":1,"isRequired":true,"group":"","tab":""}],"secur
ityToken":"$MmrA9O2HeOzKYrY4mdieWKwv6g2cQ9qLOmdOoAybEIbXT8p+O3E=","fullTypeName":
"MyCRM.Note","notificationType":"Error","ignoreCheckRules":true},"authToken":"MTA
tMDQtMjAxOCAxMjoyNjoxNC4xNDAxMDk1ICswMDowMDtyaS9JQTlnVU9ZMm5oa3NYVkdhc2EwRlVRYlcw
eGdENjhuUzRmZ1BtZVg4PQ==","operations":[{"name":"refreshForUpdate","arguments":[]
,"type":"ExecuteMethod"}]}
```

We carried out the request again a week later and it still appeared to be working.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 2193
Content-Type: application/json; charset=utf-8
Expires: -1
Access-Control-Expose-Headers: AuthToken
X-Content-Type-Options: nosniff
Date: Wed, 21 Mar 2018 08:31:20 GMT
Connection: close

{"result":{"type":"Note","objectId":"2","breadcrumb":"nieuw
testsdfdsfsdfje","id":"73558aa6-ccaf-3f4d-a18c-
2b6c58a5713e","newOptions":"","label":"Opmerking","stateBehavior":"None","queryLa
youtMode":"FullPage","tabs":{"":{"id":"ea84d739-3eea-4c21-a2b9-
7c0de6ede35d","name":"Note","columnCount":0}},"attributes":[{"name":"CreatedBy","
type":"User","value":"ed65d8e2-d713-488d-be06-b87d964aa346","id":"d3bf6e99-c302-
```

```
3a1b-a1da-
924e57352c92","offset":10,"rules":"Required","isReadOnly":true,"label":"Gemaakt
door","visibility":"Read,
Query","toolTip":"","columnSpan":1,"options":["UserTSF"],"isRequired":true,"group
":"","tab":""},{"name":"CreatedOn","type":"DateTimeOffset","value":"09-03-2018
13:55:58.9311008                    +01:00","id":"880c4334-4d42-3d5f-9017-
dfa03d3a8d1f","offset":20,"rules":"Required","isReadOnly":true,"label":"Gemaakt
op","visibility":"Read,
Query","toolTip":"","columnSpan":1,"isRequired":true,"group":"","tab":""},{"name"
:"Description","type":"MultiLineString","value":"nieuwe      test","id":"679cdde5-
a2bb-3cfb-851d-838470d2b5d3","offset":5,"rules":"NotEmpty;
MaxLength(500)","label":"Beschrijving","visibility":"Always","toolTip":"","column
Span":1,"isRequired":true,"group":"","tab":""},{"name":"ModifiedBy","type":"User"
,"value":"ed65d8e2-d713-488d-be06-b87d964aa346","id":"58ceb49f-9cb3-3062-be0b-
04fe4c0d2d7b","offset":30,"rules":"Required","isReadOnly":true,"label":"Gewijzigd
door","visibility":"Read,
Query","toolTip":"","columnSpan":1,"options":["UserTSF"],"isRequired":true,"group
":"","tab":""},{"name":"ModifiedOn","type":"DateTimeOffset","value":"21-03-2018
10:08:25.975483                    +01:00","id":"3cc89a5e-cb08-30db-8526-
3fe367921dec","offset":40,"rules":"Required","isReadOnly":true,"label":"Bewerkt
op","visibility":"Read,
Query","toolTip":"","columnSpan":1,"isRequired":true,"group":"","tab":""}],"secur
ityToken":"$MmrA9O2HeOzKYrY4mdieWKwv6g2cQ9qLOmdOoAybEIbXT8p+O3E=","fullTypeName":
"MyCRM.Note","notificationType":"Error","ignoreCheckRules":true},"authToken":"MTA
tMDQtMjAxOCAxMjoyNjoxNC4xNDAxMDk1ICswMDowMDtyaS9JQTlnVU9ZMm5oa3NYVkdhc2EwRlVRYlcw
eGdENjhuUzRmZ1BtZVg4PQ==","operations":[{"name":"refreshForUpdate","arguments":[]
,"type":"ExecuteMethod"}]}
```


Retest 03/05/2018

This issue has been resolved

Insufficient brute force detection/protection

Classification

Risk Level	**Medium**
URL(s)	https://vidyano.azurewebsites.net/

Finding

We discovered no effective measures in place against brute force login attempts. We were able to keep guessing a password until one matched. Next to the insufficient brute force protection on the login page, there is also no protection on the ‘diagnostics’ page.

Consequences

An attacker could gain access to a user’s account or to authenticated pages by brute forcing the forms.

Remediation Advice

Implement access controls to limit the number of failed requests a single client can issue, for example by blocking access for a certain amount of time or adding a captcha for verification.

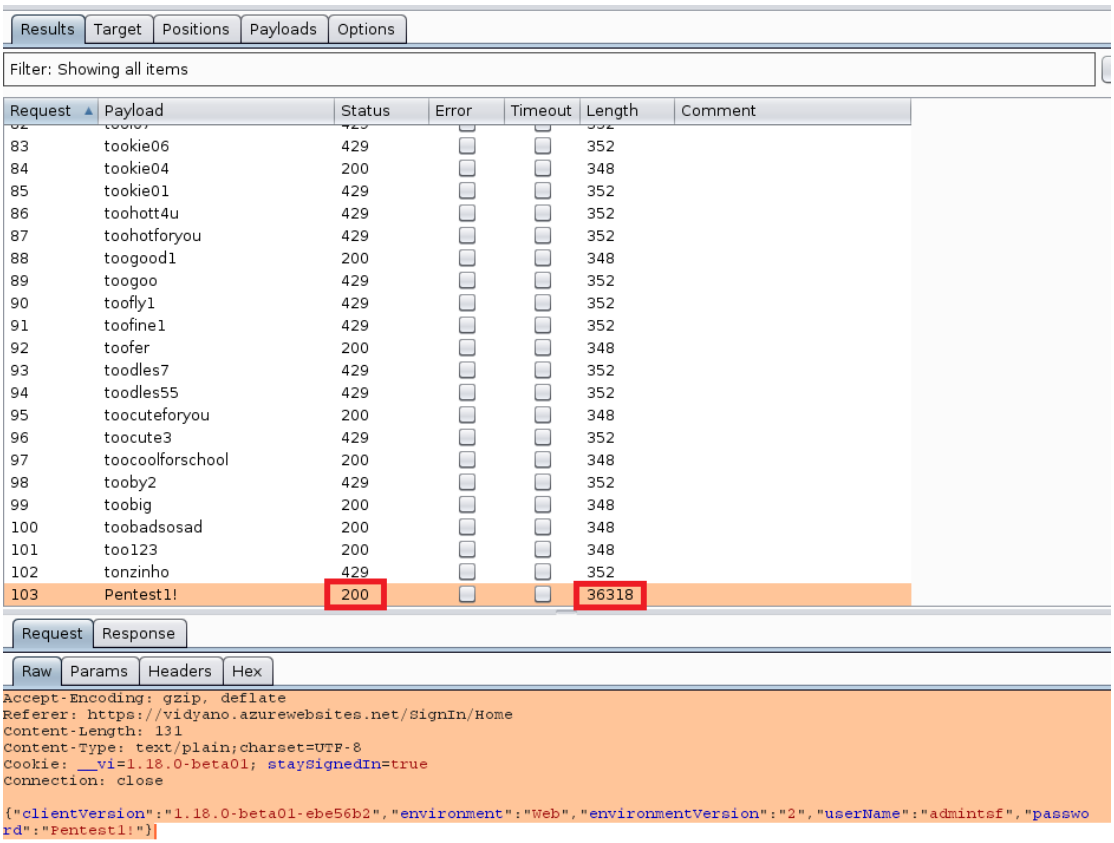
Screenshots / Evidence

The following screenshot shows a successful login after 103 attempts.

```
POST /GetApplication HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://vidyano.azurewebsites.net/SignIn/Home
Content-Length: 131
Content-Type: text/plain;charset=UTF-8
Cookie: __vi=1.18.0-beta01; staySignedIn=true
Connection: close

{"clientVersion":"1.18.0-beta01-ebe56b2","environment":"Web","environmentVersion":"2","userName":"admintsf","password":"$$"}
```

Intruder attack:

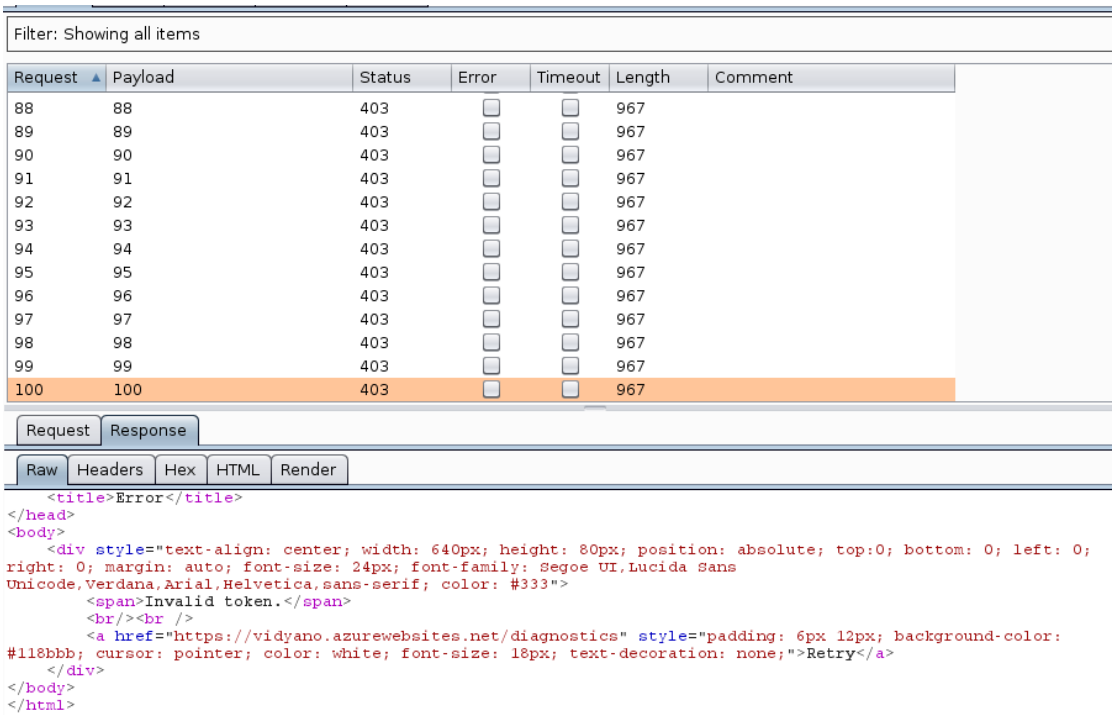


However, some responses do give us a rate limit exceeded exception, the correct password still got accepted after 103 attempts. This indicates that the rate limit exception does not work properly.

Request on diagnostics page:
We were able to keep guessing a token without any limitations

```
POST /diagnostics HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://vidyano.azurewebsites.net/diagnostics
Cookie: __vi=1.18.0-beta01; staySignedIn=true
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

token=RandomToken$$
```



Retest 03/05/2018

This issue has been resolved

Automatic session dropping after acceptable time

Classification

Risk Level	**Medium**
URL(s)	https://vidyano.azurewebsites.net/

Finding

It is possible to have an unused session open for more than one week.

Consequences

The longer a session is open, the bigger the window of opportunity is for an attacker to steal the session.

Remediation Advice

A standard session timeout is 20 minutes. Determine for the application what an acceptable session timeout is.

Screenshots / Evidence

We first logged in on March 13, 2018 and were still logged in on March 21, 2018 without using the session.

Retest 03/05/2018

This can be configured when setting up the product and is thus not an issue of the product in itself but simply for the “demo” application which was tested.

Old password not required on password change

Classification

Risk Level	**Medium**
URL(s)	https://vidyano.azurewebsites.net/

Finding

When changing your password on the website the old password is not required.

Consequences

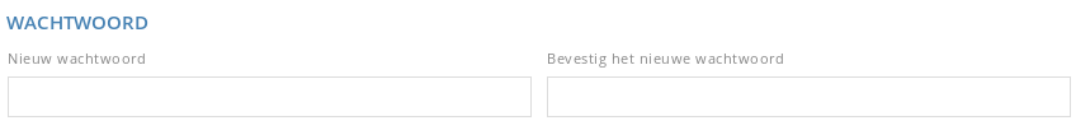
An attacker who somehow gained access to another user’s account/computer, can change this user’s password without knowing his/her original password, essentially locking the original user out.

Remediation Advice

Make sure the original password is a requirement when changing your password.

Screenshots / Evidence

The following request demonstrates the password change functionality:



Retest 03/05/2018

This issue has been resolved

No session drop on password change

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net/

Finding

When a user changes his password, the session is still active.

Consequences

If an attacker is able to compromise the password of a user or receive an authentication token, he can keep working on the active session for a limited time, even when the legit user is changing his password afterwards. This means an attacker has complete access to an account, without having the latest available password.

Remediation Advice

Make sure to invalidate the session that was used to change the password and create a new session for the user.

Screenshots / Evidence

Password change request:

```
POST /ExecuteAction HTTP/1.1

Host: vidyano.azurewebsites.net

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer:    https://vidyano.azurewebsites.net/Home/PersistentObject.b15730ad-9f47-
4775-aacb-0a181e95e53d/ed65d82-d713-488d-be06-b87d964aa346

Content-Length: 2643

Content-Type: text/plain;charset=UTF-8

Cookie: __vi=1.18.0-beta01; staySigneIn=true

Connection: close


{"clientVersion":"1.18.0-beta01-
ebe56b2","environment":"Web","environmentVersion":"2","userName":"USERTSF","authT
oken":"MTktMDQtMjAxOCAxMDozMDoxNS4xNDQ0NzQyICswMDowMDtPczBCL0poN28vTVAxejBjTFpoeW
EyTGFkMTlCUDlUek83bTYwYVVKcjlBPQ==","action":"PersistentObject.Save","parent":{"i
d":"b15730ad-9f47-4775-aacb-
0a181e95e53d","type":"UserSettings","objectId":"ed65d8e2-d713-488d-be06-
b87d964aa346","securityToken":"$PeARa2220nSDSvCUwYnaSqiAtybNXt8CutLpVGyOrabjicdO7
kO=","isSystem":true,"attributes":[{"id":"8f2d1faf-306e-4cac-8ca7-
d24a6831a047","name":"ConfirmPassword","label":"Bevestig        het        nieuwe
wachtwoord","type":"Password","isValueChanged":true,"visibility":"Always","value"
:"Pentest1!"},{"id":"3d6a5fb0-4d7c-407e-a276-
58a25471e9a4","name":"CultureInfo","label":"Datum,            tijd            en
getalnotatie","type":"KeyValueList","isRequired":true,"visibility":"Always","valu
e":"","options":["=Browser","de-DE=Deutsch  (Deutschland)","en-US=English  (United
States)","en-GB=English      (United      Kingdom)","es-ES=espaÃ±ol      (EspaÃ±a,
alfabetizaciÃ³n    internacional)","fr-FR=franÃ§ais    (France)","fr-BE=franÃ§ais
(Belgique)","it-IT=italiano      (Italia)","ja-JP=æ—¥æœ¬èª      (æ—¥æœ¬)","nl-
NL=Nederlands     (Nederland)","nl-BE=Nederlands     (BelgiÃ«)","pt-PT=portuguÃªs
(Portugal)","zh-CHS=ä¸-æ–‡(ç®ä½“)       æ—§ç‰ˆ"]},{"id":"87a34e2d-cb56-4f8a-9d0d-
fad6ce58b44b","name":"Language","label":"Taal","type":"KeyValueList","isRequired"
:true,"visibility":"Always","value":"nl","options":["=Browser","de=Duits        -
Deutsch","en=Engels    -    English","es=Spaans    -    EspaÃ±ol","fr=Frans    -
FranÃ§ais","ja=Japans      -      æ—¥æœ¬èª","nl=Nederlands","pt=Portugees      -
PortuguÃªs"]},{"id":"e96996bb-7415-4883-9dfd-
dd8fdfd2fa05","name":"NewPassword","label":"Nieuw
wachtwoord","type":"Password","isValueChanged":true,"visibility":"Always","value"
:"Pentest1!"},{"id":"9f6d3ecb-29e0-44e6-bd6d-
a373fceafa81","name":"Settings","label":"Settings","type":"String","visibility":"
Never","value":null},{"id":"c6a5333b-b4cc-4de3-9042-
183d94c78f13","name":"TwoFactorCode","label":"Gegenereerde  code  invoeren  van  de
authenticator
app","type":"String","visibility":"Never","value":null},{"id":"f6c9ed4f-32cd-
```

```
4a13-88a1-4595289d428b","name":"TwoFactorEnabled","label":"Gebruik    verificatie
met                                                                  twee
factoren","type":"YesNo","triggersRefresh":true,"visibility":"Always","value":"Fa
lse"},{"id":"db59fff1-707a-4a75-a317-
0906909e4d68","name":"TwoFactorImage","label":"Scan de QR-code in de authenticator
app","type":"Image","isReadOnly":true,"visibility":"Never","value":null},{"id":"4
ae287cf-d71f-4eba-be58-483b9f09f80a","name":"TwoFactorToken","label":"Two  factor
token","type":"String","isReadOnly":true,"visibility":"Never","value":null}]}}
```


Note: after this request, our session is still active.

Retest 03/05/2018

This issue has been resolved

No out of the box automation protection

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net/

Finding

No protections against automation and the use of bots are present. An attacker could submit multiple notes at one time (most likely with different data) in order to spam the database with data.

Consequences

The back-end system could get flooded with an unrealistic number of notes created by one account which might annoy other users and admins that are using the tool.

Remediation Advice

Implement a captcha on the form. This limits the ability of a bot to repeat requests.

Screenshots / Evidence

Flooding example:

%20%3cscript%2fs...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%22%3e%3cimg%...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%253cscript%253e...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#00%3b%3c%...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#0000060	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#000060	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#00060	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#0060	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#060	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#13%3b%3cbli...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#34%3b%26#...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#34%3b%26#...	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#60	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x000003c	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#X000003c	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x000003C	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#X000003C	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x000003c%3b	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#X000003c%3b	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x000003C%3b	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#X000003C%3b	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x00003c	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#X00003c	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM
%26#x00003C	UserTSF	03/13/2018 10:31 AM	UserTSF	03/13/2018 10:31 AM

Retest 03/05/2018

This is by design as it depends on business requirements of the specific setup.

Stack traces enabled

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net/

Finding

Default error messages are still enabled on multiple locations.

Consequences

Stack trace message leak information about the inner working of the application and contain detailed technology version information. One stack trace also contained an internal path. An attacker could use this in a future stage of their attack.

Remediation Advice

Define custom error messages for all error types.

Screenshots / Evidence

Request performed on the API:

```
POST /api/products HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://vidyano.azurewebsites.net/api/index.html
Content-Type: application/json
Origin: https://vidyano.azurewebsites.net
Content-Length: 152
Cookie: __vi=1.18.0-beta01; staySignedIn=true
Connection: close

{
  "ProductID": 3895,
  "Number": "test",
  "Name": "test",
  "Color": "test",
  "Size": "test",
  "Weight": 1,
  "ListPrice": 5,
  "StandardCost": 3
}
```

Response:

```
HTTP/1.1 400 Bad Request
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 3221
Content-Type: application/json; charset=utf-8
Expires: -1
X-Frame-Options: SAMEORIGIN
```

```
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Date: Thu, 22 Mar 2018 09:56:43 GMT
Connection: close

{"Message":"An error has occurred.","ExceptionMessage":"The conversion of a datetime2 data type to a datetime data type resulted in an out-of-range value.\r\nThe statement has been terminated.","ExceptionType":"System.Data.SqlClient.SqlException","StackTrace":"
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)\r\n at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)\r\n at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)\r\n at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady)\r\n at System.Data.SqlClient.SqlDataReader.TryConsumeMetaData()\r\n at System.Data.SqlClient.SqlDataReader.get_MetaData()\r\n at System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption)\r\n at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean describeParameterEncryptionRequest)\r\n at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean inRetry)\r\n at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method)\r\n at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method)\r\n at System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior)\r\n at System.Data.Common.DbCommand.ExecuteReader(CommandBehavior behavior)\r\n at Vidyano.Service.Profiling.VidyanoDbCommand.ExecuteDbDataReader(CommandBehavior behavior)\r\n at System.Data.Common.DbCommand.ExecuteDbDataReaderAsync(CommandBehavior behavior, CancellationToken cancellationToken)\r\n--- End of stack trace from previous location where exception was thrown ---\r\n at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)\r\n at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n at System.Data.Entity.Utilities.TaskExtensions.CultureAwaiter`1.GetResult()\r\n at System.Data.Entity.Core.Mapping.Update.Internal.DynamicUpdateCommand.<ExecuteAsync>d__0.MoveNext()\r\n--- End of stack trace from previous location where exception was thrown ---\r\n at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)\r\n at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n at System.Data.Entity.Core.Mapping.Update.Internal.UpdateTranslator.<UpdateAsync>d__0.MoveNext()"}
```

We were also able to trigger a stack trace/information disclosure alert on the main demo application:

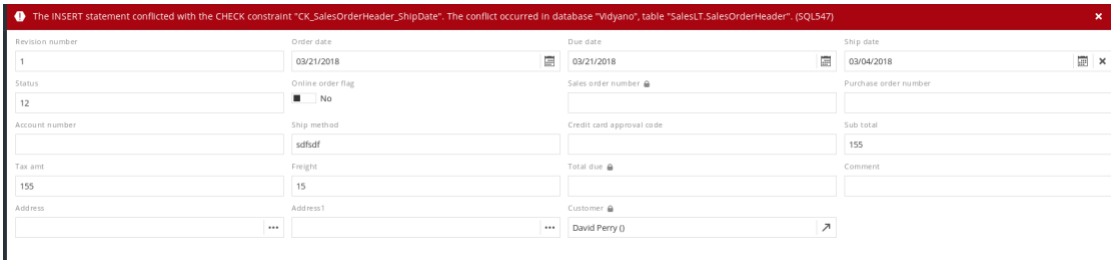
Request:

```
POST /ExecuteAction HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://vidyano.azurewebsites.net/Home/FromAction/b
Content-Length: 5079
Content-Type: text/plain;charset=UTF-8
Cookie: __vi=1.18.0-beta01; staySignedIn=true
Connection: close
```

```
{"clientVersion":"1.18.0-beta01-
ebe56b2","environment":"Web","environmentVersion":"2","userName":"demo","action":
"PersistentObject.Save","parent":{"id":"1cec9c36-a541-4227-8472-
468b0be7d20b","type":"SalesOrderHeader","isNew":true,"securityToken":"$pYm95h4VZb
HhceZi4cfl3X2E3ksoUwlogVCjS3EkXg6yCKO7zfM=","parent":{"id":"0a603854-5426-46d9-
a70f-
061f022ad8e5","type":"Customer","objectId":"20131","securityToken":"$twbzM3Xp24O0
77yq+PhMdLKXpMSEpCrfN69ieRHqATK0TNYCL6U=","attributes":[{"id":"46d0ab32-3315-
4093-9318-2d639f721d41","name":"CompanyName","label":"Company
name","type":"String","visibility":"Always","value":null},{"id":"ff662253-e6b6-
438a-95e7-e30c55a4717a","name":"EmailAddress","label":"Email
address","type":"String","visibility":"Always","value":null},{"id":"c21715f5-
3667-4549-afd4-7ccd934c2495","name":"FirstName","label":"First
name","type":"String","isRequired":true,"visibility":"Always","value":"David"},{"
id":"ea09d114-89e7-42c7-aad7-f92264ce3eed","name":"IsActive","label":"Is
active","type":"Boolean","isRequired":true,"visibility":"Always","value":"True"},
{"id":"3ae6fafa-6e4b-4ec9-9530-4015ff2bd4e7","name":"LastName","label":"Last
name","type":"String","isRequired":true,"visibility":"Always","value":"Perry"},{"
id":"561b43c8-cb7d-4728-b603-7d02a395528f","name":"MiddleName","label":"Middle
name","type":"String","visibility":"Always","value":null},{"id":"49eb3101-ea9d-
4e24-b45e-
b7ae77995fb2","name":"Phone","label":"Phone","type":"String","visibility":"Always
","value":null},{"id":"cd123d3e-3879-4995-9165-
157b8b3bf50a","name":"Suffix","label":"Suffix","type":"String","visibility":"Alwa
ys","value":null}]},"attributes":[{"id":"f3b3fc29-5c2f-44cf-b2ea-
d90d9274c682","name":"AccountNumber","label":"Account
number","type":"String","visibility":"Always","value":null},{"id":"6e8d3c7a-ee81-
482a-8b2c-
b856daff7357","name":"Address","label":"Address","type":"Reference","displayAttri
bute":"AddressLine","visibility":"Always","value":null},{"id":"63d71e3d-a3ef-
45de-965e-
1ab7b303120a","name":"Address1","label":"Address1","type":"Reference","displayAtt
ribute":"AddressLine","visibility":"Always","value":null},{"id":"f9b1f974-7a2b-
4297-b198-
04cfd181b95d","name":"Comment","label":"Comment","type":"String","visibility":"Al
ways","value":null},{"id":"f3e9b114-fd7e-47c3-9ac3-
6c96c90999f7","name":"CreditCardApprovalCode","label":"Credit card approval
code","type":"String","visibility":"Always","value":null},{"id":"5e1cdbd7-66b2-
473a-a9dc-
7cc57ef2f2a5","name":"Customer","label":"Customer","type":"Reference","isReadOnly
":true,"isRequired":true,"isValueChanged":true,"displayAttribute":"FirstName","ob
jectId":"20131","visibility":"Always","value":"David Perry ()"},{"id":"a5ceb537-
8918-4146-a2bf-00b3a640db86","name":"DueDate","label":"Due
date","type":"NullableDate","isRequired":true,"isValueChanged":true,"visibility":
"Always","value":"21-03-2018 00:00:00"},{"id":"d07e8c9c-a9a0-42ee-8658-
d9287e01775d","name":"Freight","label":"Freight","type":"NullableDecimal","isRequ
ired":true,"isValueChanged":true,"visibility":"Always","value":"15"},{"id":"9225e
290-516f-4632-aeb7-3808c7d9061d","name":"OnlineOrderFlag","label":"Online order
flag","type":"Boolean","isRequired":true,"visibility":"Always","value":"False"},{
"id":"ba457f6c-20b0-4802-b4da-e2908eb8b19f","name":"OrderDate","label":"Order
date","type":"NullableDate","isRequired":true,"isValueChanged":true,"visibility":
"Always","value":"21-03-2018 00:00:00"},{"id":"57ad731e-2099-4637-9b99-
e7bf5fa336fe","name":"PurchaseOrderNumber","label":"Purchase order
number","type":"String","visibility":"Always","value":null},{"id":"e59363bf-a43e-
44be-b3d4-f5b322e95936","name":"RevisionNumber","label":"Revision
number","type":"NullableByte","isRequired":true,"isValueChanged":true,"visibility
":"Always","value":"1"},{"id":"ce5a18e4-154d-450b-b708-
c92a6b33a72c","name":"SalesOrderNumber","label":"Sales order
number","type":"String","isReadOnly":true,"isRequired":true,"visibility":"Always"
,"value":null},{"id":"7474bd2c-7021-4411-9b73-
1d6fb0a5ca8f","name":"ShipDate","label":"Ship
date","type":"NullableDate","isValueChanged":true,"visibility":"Always","value":"
04-03-2018 00:00:00"},{"id":"65a573e1-e8dd-41c3-a60f-
e53d0f4c6993","name":"ShipMethod","label":"Ship
method","type":"String","isRequired":true,"isValueChanged":true,"visibility":"Alw
ays","value":"sdfsdf"},{"id":"77a8c2c5-2e56-49d7-be91-
8ad7e758dfe6","name":"Status","label":"Status","type":"NullableByte","isRequired"
:true,"isValueChanged":true,"visibility":"Always","value":"12"},{"id":"6b3cfeff-
627e-4e0e-9d8b-c2e58f31ca96","name":"SubTotal","label":"Sub
total","type":"NullableDecimal","isRequired":true,"isValueChanged":true,"visibili
ty":"Always","value":"155"},{"id":"c7dd3d15-5365-4e44-b3fc-
abe8fed20cd3","name":"TaxAmt","label":"Tax
amt","type":"NullableDecimal","isRequired":true,"isValueChanged":true,"visibility
":"Always","value":"155"},{"id":"815ab8e1-06d5-4511-a53d-
4432181cef8d","name":"TotalDue","label":"Total
due","type":"NullableDecimal","isReadOnly":true,"isRequired":true,"isValueChanged
":true,"visibility":"Always","value":null}]}}
```


Note that the shipping date is earlier than the order date.

Response:



Retest 03/05/2018

This issue has been resolved

TLSv1.0 supported

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net/

Finding

During testing it was discovered that TLSv1.0 was enabled in the SSL/TLS setup of the server. This could potentially allow a sophisticated attacker that is able to perform a Man-In-The-Middle-Attack (MITM) to decrypt the traffic and read all data that is being transferred over the connection.

Consequences

By this outdated standard, an attacker could be able to decrypt the transferred data, downgrade the used encryption, intercept confidential information like usernames and passwords and more.

Remediation Advice

Stop supported TLSv1.0, opting for TLSv1.1 and TLSv1.2 instead.

Screenshots / Evidence

The following shows the output of an sslscan that was performed on the domain, highlighted are the parts of the setup which are considered less secure:

```
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server vidyano.azurewebsites.net on port 443 using SNI name vidyano.azurewebsites.net

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed
```

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.azurewebsites.net
Altnames:   DNS:*.azurewebsites.net,   DNS:*.scm.azurewebsites.net,   DNS:*.azure-
mobile.net, DNS:*.scm.azure-mobile.net, DNS:*.sso.azurewebsites.net
Issuer:   Microsoft IT TLS CA 4

Not valid before: Dec 17 12:40:47 2017 GMT
Not valid after:  Dec 17 12:40:47 2019 GMT
```

Retest 03/05/2018

This issue has been resolved for the demo application.
It should be noted that this specific issue depends on the deployment, and it is therefore not an issue related to the product itself.

API docs are publicly available

Classification

Risk Level	**Informational**
URL(s)	https://vidyano.azurewebsites.net/api/index.html

Finding

We found the API docs from the application to be publicly available. Although this is not a problem in itself, it is still important to decide who can see this documentation.

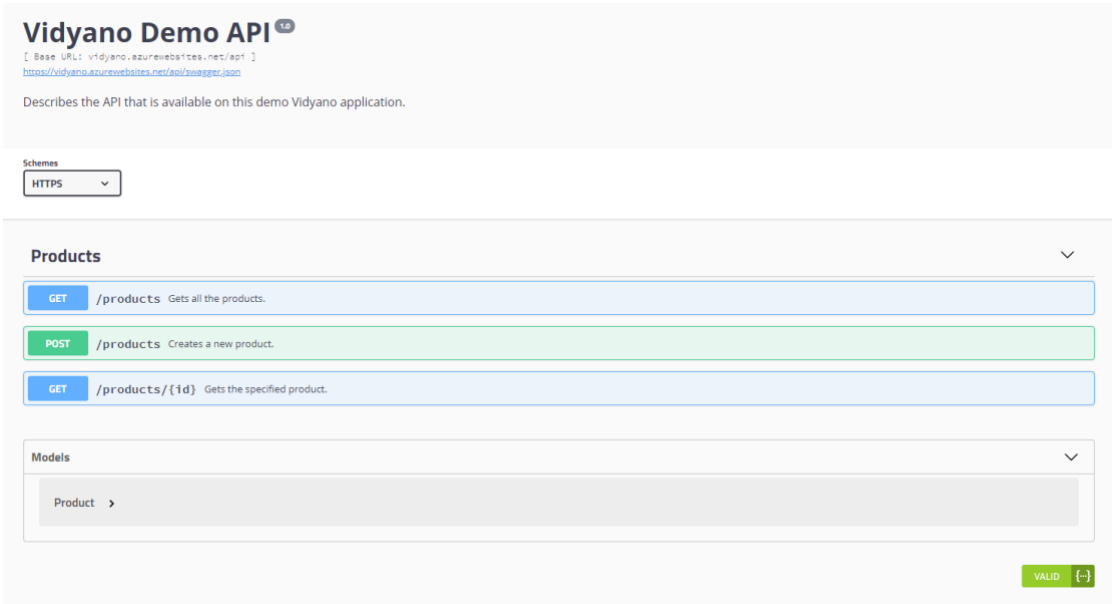
Consequences

An attacker has the ability to create a clear picture of how the application works.

Remediation Advice

Determine if the API documentation should definitely be available publicly to everyone

Screenshots / Evidence



Retest 03/05/2018

This issue is by design, as it makes it easier to work the API and no sensitive information is leaked through this method.