Security Assessment Report

2Sky - Webapp Vidyano

TSF | THE SECURITY FACTORY

Table of Contents

Project Details

Scope

The Security Factory was tasked to perform a technical web application penetration test to provide 2Sky with a clear view of how resilient 2Sky is against a cyber-attack.

Start Date: 27/09/2023
End Date: 29/09/2023
Pentester(s): Tess Deboel, Stijn Follet
Reviewer: Steven Verscheure
Performed from: 81.82.219.230 (the Security Factory HQ)
Accounts:

- NoteUser1
- NoteUser2
- NoteAdmin
- NoteAuditor

Scope:

Asset	Type
https://demo.vidyano.com/	Web Application

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 the explicit permission of the customer

Executive Summary

Background

The Security Factory was tasked with performing a number of web application vulnerability assessments on the environment of 2Sky. The purpose of this assessment was to verify the effectiveness of the security controls put in place by ClientName 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 strengthen its security posture.

General Findings

The testers of the Security Factory validated the application, where applicable, against an extensive list of more than 200 vulnerabilities. This list covers the and many more vulnerabilities categorized within weak passwords, missing OS patches, outdated software, human errors, misconfiguration, incorrect use, vulnerable software, malware, excessive permissions, design flaws, legacy, and many more.

Observations

This section documents our positive and negative observations made during the application testing phase. This section serves as a keystone for defining the final security posture of the application.

Under "Positive observations" we highlight aspects that performed significantly better or were exceptionally good compared to other applications typically tested by our team. On the other hand, "Negative observations" indicate areas where there is room for improvement, indicating the most significant risks currently present within your application.

Positive Observations

- Following a password change, the authentication tokens are rendered invalid.
- Robust safeguards are in place to thwart any attempts at user enumeration.
- The employment of hash functions serves as a defense mechanism to prevent any unauthorized modifications to the immutable note fields.

Significant Issues

- We only identified low vulnerabilities, indicating that there are no major ongoing issues.

Overall Security Posture

Comparing the security posture of the application tested at 2Sky with our experience in the market, we rate this application as currently having a **high-security** posture.

Strategic Overview

Vulnerability Summary

Vulnerability	Severity
No brute force protection on login	Low
No out of the box automation protection	Low
Concurrent sessions	Low
Server response headers information leakage	Low

Risk Levels Overview

Severity	Description
Critical	A critical risk issue is an issue that causes a major impact on the business and is very likely to occur. Examples of issues with major impact include a permanent downtime of service, destruction of data, disclosure of very sensitive information, severe reputational damage, etc. The probability that this issue will be exploited shortly 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 very likely to have a minor to moderate impact, but probably not a 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 a minor impact include brief interruptions of a service, minor data damage, disclosure of non-sensitive data, minor 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.
Info	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".

Technical Web Application Test

Findings

No brute force protection on login

Classification

Severity:	Low
Assets:	• https://demo.vidyano.com/

Finding

The web application is vulnerable to brute force attacks. This type of attack involves repeatedly attempting to guess an account's password by trying various character combinations. Attackers can use their own created passwords or utilize commonly used passwords and even those obtained from past data breaches found on the internet.

Consequences

Brute force attacks can have several negative consequences, including:

- Security breaches: If a brute force attack is successful, the attacker can gain access to sensitive information, such as personal data, financial information, and other confidential material.
- Damage to reputation: If an attacker gains access to sensitive information, it can damage the reputation of the organization or individual that was targeted.
- Loss of revenue: A security breach can result in loss of revenue, as customers may choose to take their business elsewhere.
- Legal issues: If personal information is stolen during a security breach, the organization or individual that was targeted may be subject to legal action.Increased IT costs:
- Brute force attacks can consume a lot of server resources and cause performance issues, which can lead to increased IT costs.Disruption of service: Brute force attacks can cause a disruption of service, which can be frustrating for users and can lead to loss of productivity.
- Risk of future attacks: Once an attacker has gained access to a system, they may be able to use that access to launch additional attacks or to leave backdoors for later use. Therefore, it is crucial to take steps to prevent brute force attacks and to have a plan in place to respond quickly if an attack does occur.

Remediation Advice

There are several ways to remediate brute force attacks on login forms, including:

- Implementing a lockout policy: This involves temporarily disabling a user's account or IP address after a certain number of unsuccessful login attempts.
- Using CAPTCHAs: This helps to ensure that the user attempting to log in is a human, rather than an automated script.
- Implementing rate limiting: This involves limiting the number of login attempts that can be made within a certain time period.
- Using Two-Factor Authentication: This adds an extra layer of security by requiring users to provide a one-time code in addition to their password to gain access.
- Monitoring and logging: Keep track of failed login attempts and IP addresses, and alert administrators if there is an unusual number of failed attempts.

- Use a password manager: Encourage users to use a password manager to store their unique, complex passwords, so that they don't have to remember them.
- Use encryption: encrypt any sensitive information that is transmitted between client and server to protect against eavesdropping.

It is important to note that no single solution can completely prevent brute force attacks, so a combination of these measures will provide the best security.

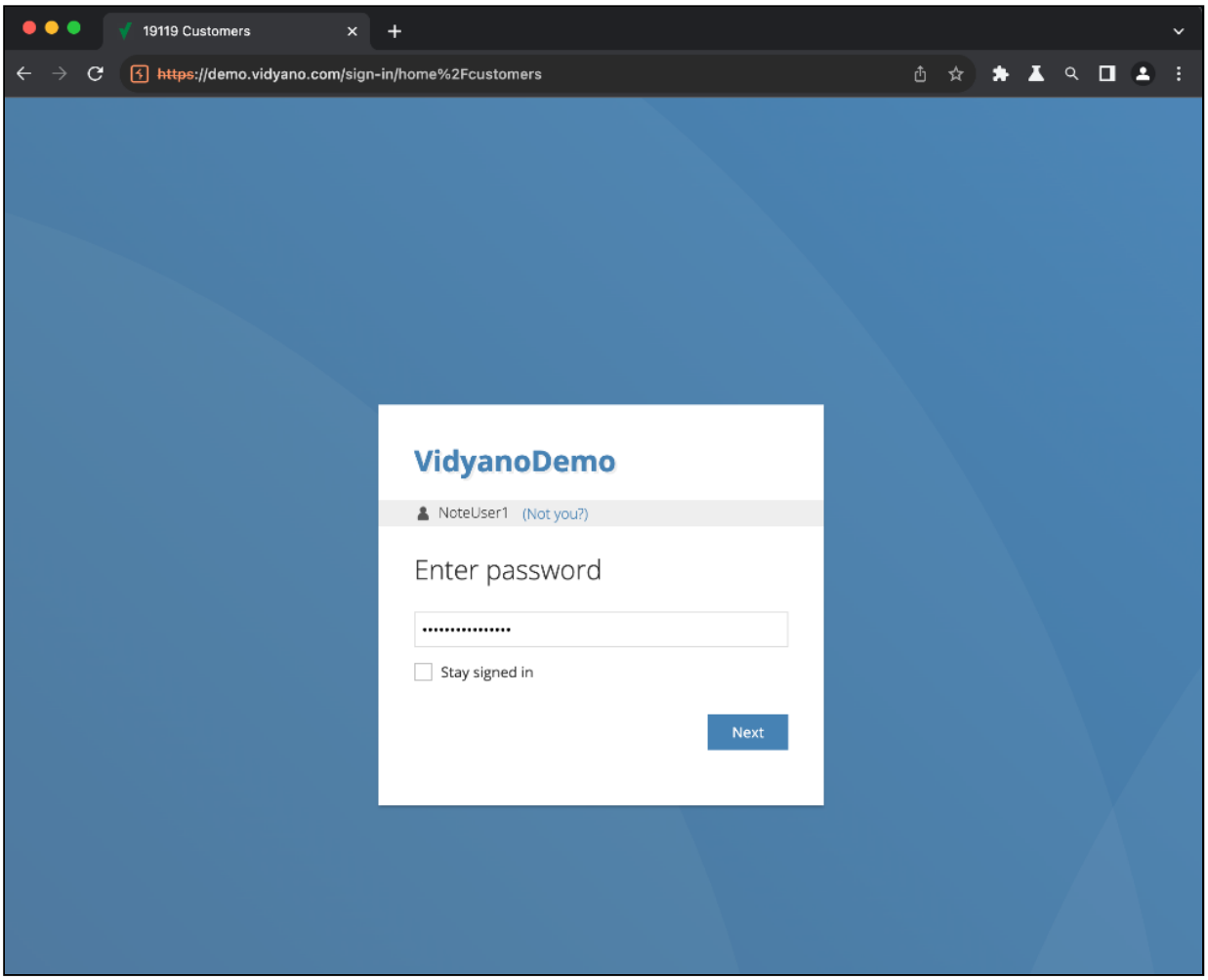
Evidence

Brute Force

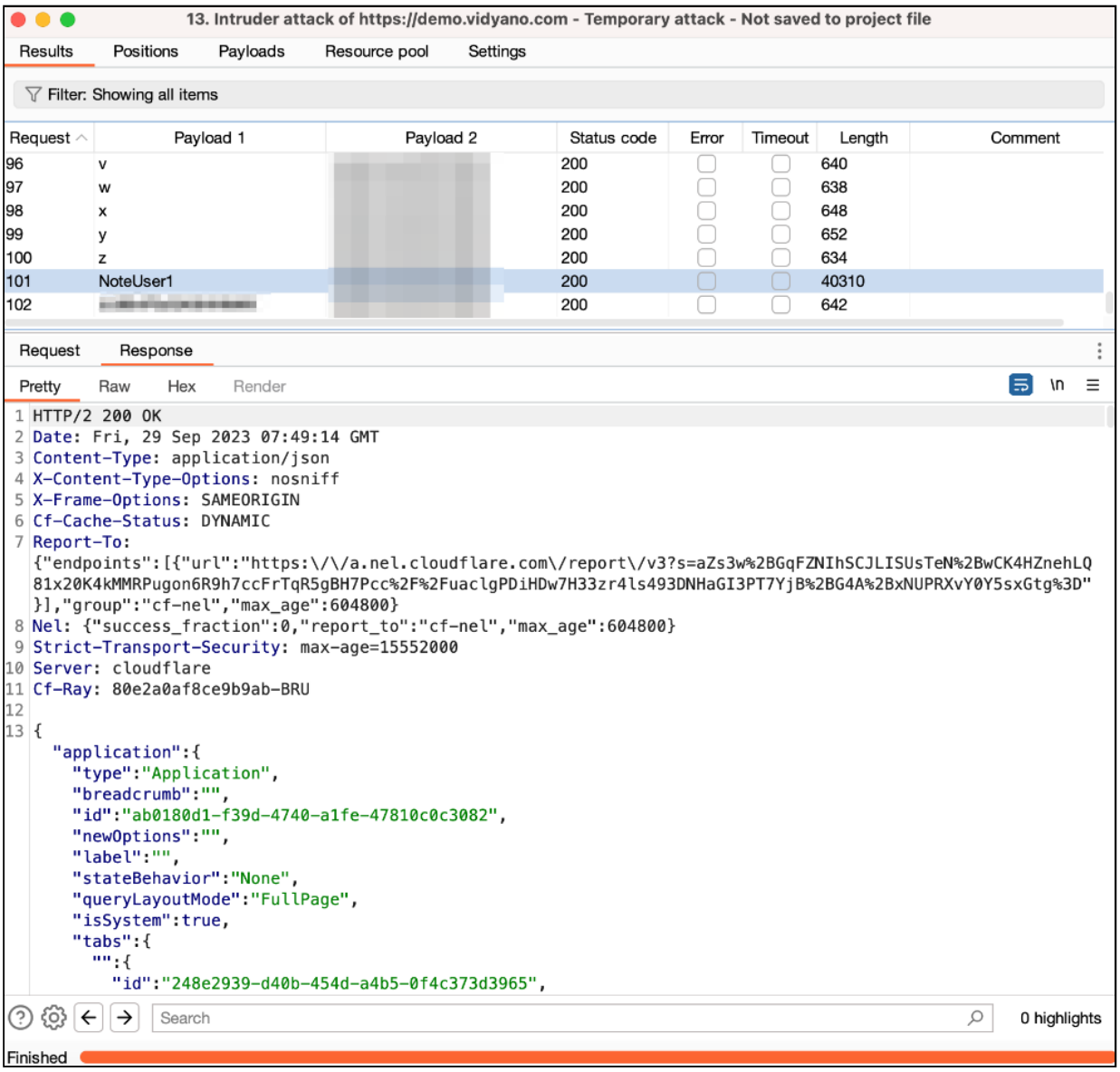
Location: demo.vidyano.com

Issue details

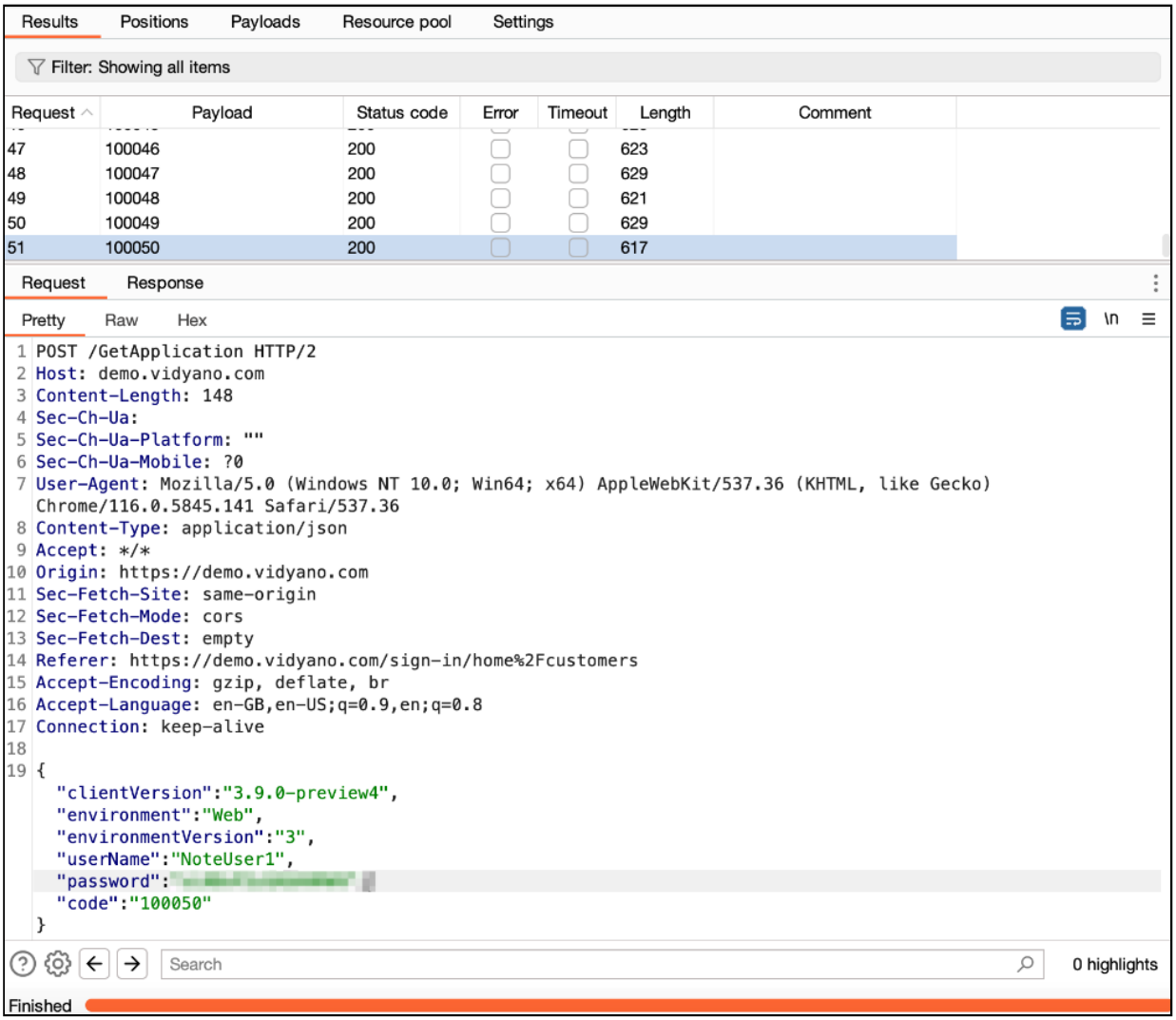
During the login process, it is possible to perform a brute-force attack. This brute-force attack is not only executable on the password, but can also be performed on the 2FA code if it is enabled. We are aware that the number of attempts on the 2FA code is limited because the lifetime of a 2FA code is not unlimited.



As seen below, it is possible to send at least 100 interrupted requests in an attempt to gain access.



Below you can see, for example, that we were also able to brute force the 2FA code


Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Request
Payload
Status code
Error
Timeout
Length
Comment
47 100046 200 623
48 100047 200 629
49 100048 200 621
50 100049 200 629
51 100050 200 617
Request
Response
Pretty
Raw
Hex
\n
1 POST /GetApplication HTTP/2
2 Host: demo.vidyano.com
3 Content-Length: 148
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Platform: ""
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
8 Content-Type: application/json
9 Accept: */*
10 Origin: https://demo.vidyano.com
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://demo.vidyano.com/sign-in/home%2Fcustomers
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: keep-alive
18
19 {
"clientVersion":"3.9.0-preview4",
"environment":"Web",
"environmentVersion":"3",
"userName":"NoteUser1",
"password":
"code":"100050"
}
Search
0 highlights
Finished

No out of the box automation protection

Classification

Severity: Low

Assets:

- https://demo.vidyano.com/

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.

In a previous test, we reported this issue as well, and we were informed that it was intentionally designed this way. Unfortunately, the existing business environment we received for our test is not equipped with a spam protection, which is why we are required to report it.

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.

Evidence

Flooding

Issue details

Flooding example:

nafterscriptexecute%3dalert(1)%3e%3cscript%3e1%3c%2fscript%3e	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
@keyframes%20x%7bfrom%20%7bleft%3a0%3b%7dto%20%7bleft%3a%201000px%3b%7d%7d%3atarget%20%7b...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
@keyframes%20x%7b%7d%3c%2fstyle%3e%3cpre%20style%3d%22animation-name%3ax%22%20onanimation...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
@keyframes%20slidein%20%7b%7d%3c%2fstyle%3e%3cpre%20style%3d%22animation-duration%3a1s%3b...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
@keyframes%20x%7b%7d%3c%2fstyle%3e%3cpre%20style%3d%22animation-name%3ax%22%20onanimation...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
%3atarget%20%7bcolor%3a%20red%3b%7d%3c%2fstyle%3e%3cpre%20id%3dx%20style%3d%22transition%...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
%3atarget%20%7bcolor%3ared%3b%7d%3c%2fstyle%3e%3cpre%20id%3dx%20style%3d%22transition%3ac...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
ncut%3dalert(1)%20value%3d%22XSS%22%20autofocus%20tabindex%3d1%20style%3ddisplay%3ablock%3...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
nmousedown%3d%22alert(1)%22%20style%3ddisplay%3ablock%3etest%3c%2fpre%3e	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
:0name%3d%22alert(1)%22%20src%3d%22https%3a%2f%2fportswigger-labs%2enet%2fxss%2fxss%2ephp%...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
3cscript%3e%26%23x5c%3b%26%23x75%3b%26%23x30%3b%26%23x30%3b%26%23x36%3b%26%23x31%3b%26%23x...	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55
rc%3dx%20onerror%3dlocation%3datob%60amF2YXNjcmlwdDphbGVydChkb2N1bWVudC5kb21haW4p%60%3e	NoteUser2	27/09/2023 11:55	NoteUser2	27/09/2023 11:55

Concurrent sessions

Classification

Severity:	Low
Assets:	• https://demo.vidyano.com/

Finding

It has been identified that multiple concurrent sessions can be opened for the same user without requiring a logout.

Consequences

This vulnerability allows an attacker to exploit a user's session without the user's knowledge, as multiple active sessions are permitted.

Remediation Advice

Immediately acting upon each new authentication event is generally recommended. Any new authentication events should implicitly terminate previously active sessions associated with the user's account.

It is advisable to display a warning message informing the user that a new session has been created, which may indicate a compromise of their account. This way, users are promptly notified of any unauthorized activity.

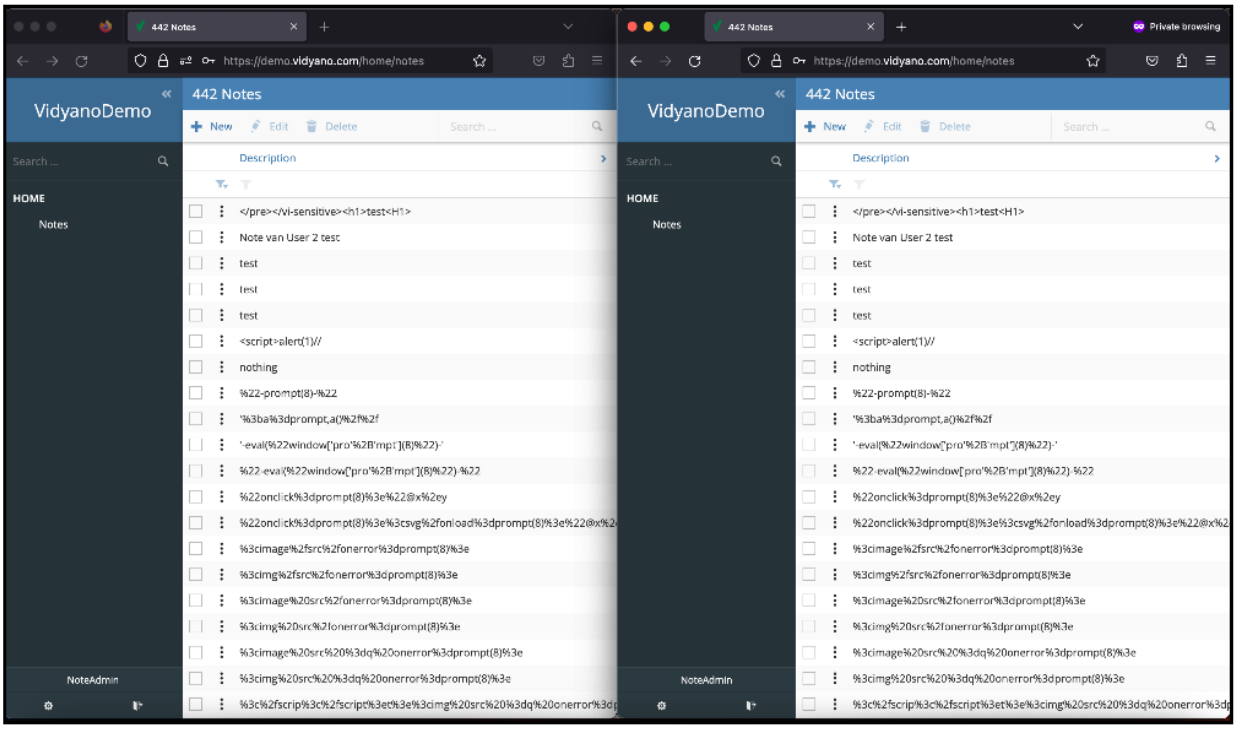
Evidence

Concurrent sessions

Location: https://demo.vidyano.com

Issue details

As you can see on the image below we can open 2 sessions at the same time and the user is not notified.


442 Notes
https://demo.vidyano.com/home/notes
VidyanoDemo
442 Notes
New
Edit
Delete
Search ...
Description
HOME
Notes
NoteAdmin
</pre></vi-sensitive><h1>test<H1>
Note van User 2 test
test
test
test
<script>alert(1)//
nothing
%22-prompt(8)-%22
'%3ba%3dprompt,a()%2f%2f
'-eval(%22window['pro'%2B'mpt'](8)%22)-'
%22-eval(%22window['pro'%2B'mpt'](8)%22)-%22
%22onclick%3dprompt(8)%3e%22@x%2ey
%3cimage%2fsrc%2fonerror%3dprompt(8)%3e
%3cimg%2fsrc%2fonerror%3dprompt(8)%3e
%3cimage%20src%2fonerror%3dprompt(8)%3e
%3cimg%20src%2fonerror%3dprompt(8)%3e
%3cimage%20src%20%3dq%20onerror%3dprompt(8)%3e
%3cimg%20src%20%3dq%20onerror%3dprompt(8)%3e
Private browsing

Server response headers information leakage

Classification

Severity: Low

Assets:
- https://demo.vidyano.com/

Finding

The web server has a signature present that leaks information about the technologies and their version.

Consequences

With the used technologies and their versions disclosed, an attacker can look for specific vulnerabilities against those versions. An attacker also gains knowledge about systems used in a future attack.

Remediation Advice

Disable the affected headers as indicated in the evidence section below.

Evidence

Server response information leakage

Issue details

The application responses shows us that use Cloudflare.

```
HTTP/2 200 OK
Date: Wed, 27 Sep 2023 08:07:18 GMT
Content-Type: application/json
X-Content-Type-Options: nosniff
Cf-Cache-Status: DYNAMIC
Report-To:  {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=rolTtWfi9TCbG4Z2Oi1Q%2BNXYF
EYZndwqobeow9yqdfOZNEb8j7YOicA%2BPa%2B6lTEmEhdRo8XNZFBX0S2k4yUe9jd0iENpRel1cC5fNmHpDgR%2FLtG2IoJeFhfgog3d
uMFlKuU%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Strict-Transport-Security: max-age=15552000
Server: cloudflare
Cf-Ray: 80d240969bcc2e5c-BRU
[SNIP]
```

Endpoint in response

Location: *

Issue details

As you can see in the response below the application returns information about the endpoint.

```
HTTP/2 200 OK
Date: Wed, 27 Sep 2023 09:57:21 GMT
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Cf-Cache-Status: DYNAMIC
Report-To:  {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gin8mm3RlpIfkTWCV9Rhegsam9i
W9LWh8HjEnMcX2OrnsaFJnACMew7%2BYvbV1ZRR7uzZ1J4FCjqg6qxrHgEOPQp1RGUj35F0KoeZoGwCQg31%2B5hbXZWY%2BqUAUJskt5
qBaik%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Strict-Transport-Security: max-age=15552000
Server: cloudflare
Cf-Ray: 80d2e1c74e9083db-BRU
```

```
[SNIP]
```