Web Penetration Test
Phase II

coinspect

MINDS

Minds Web Penetration Test Phase II

Prepared for Minds • September 2019

MINDSv2019

1. Executive Summary

In September 2019, Minds engaged Coinspect to perform a source code review of their web application.

The objective of the audit was to evaluate the security of the Minds social network web application. During the assessment, Coinspect identified the following issues:

High Risk	Medium Risk	Low Risk	Zero Risk
0	4	5	0

The present report contains the issues identified in the second phase of the audit.

2. Introduction and Scope

Minds is a social network. A white-box security audit was conducted on the Minds web application (engine and core APIs) in order to detect security, privacy, and availability related problems. The present report was completed on September 25th.

The objective of the second phase of the audit requested was to test the Minds web application. The analysis included but was not limited to the following checks:

- Input validation
- Session Management
- Brute-force protection
- Cryptographic weaknesses
- Authentication and Authorization
- Denial of service prevention
- Command Injection
- Web attacks: CSRF, XSS, Clickjacking

3. Summary Of Findings

ID	Description	Risk
MND-001	Outdated Software Libraries	Medium
MND-002	Improper Restriction of Excessive Authentication Attempts	Medium
MND-003	Password Not Required to Change Email	Medium
MND-004	Password Sent as URL Parameter	Medium
MND-005	Two-Factor Authentication via SMS	Low
MND-006	Missing Account Activity Alerts	Low
MND-007	CORS: Arbitrary Origin Trusted	Low
MND-008	Multiple Sessions Allowed	Low
MND-009	Sessions Not Terminated On Password Change	Low
MND-010	Missing Content Security Policy	Zero
MND-011	Server Version Disclosure via HTTP Headers	Zero

4. Findings

MND-001 Outdated Software Libraries

Total Risk
Medium

Impact
High

Likelihood
Low

Location
./engine/composer.lock

Category
Configuration Management

Description

Coinspect identified outdated software libraries locked on the dependencies manager configuration file of the Minds Engine project. The libraries listed below are outdated, newer versions including security patches for critical and high risk vulnerabilities are available.

Outdated software dependencies included on the Minds project:

- symfony/dependency-injection (v2.8.45)
  [CVE-2019-10910]: Check service IDs are valid (Severity: Critical)

- erusev/parsedown (1.7.1)
  [CVE-2019-10905]: Class-Name Injection (Severity: High)

- phpmailer/phpmailer (v5.2.26)
  [CVE-2018-19296]: Object injection (Severity: High)

Recommendation

Upgrade vulnerable software libraries. Consider checking the security of dependencies in a systematic way by implementing a process that will create an inventory of software dependencies and monitor for security patches using public databases and security advisories.

MND-002 Improper Restriction of Excessive Authentication Attempts

Total Risk
Medium

Impact
Medium

Likelihood
High

Location
https://www.minds.com/api/v2/oauth/token

Category
Authentication

Description

The current account lockout mechanism detects and restricts login attempts on the main login of the web application. However authentication attempts are not restricted on the mobile counterpart. Coinspect identified this issue by a successful authentication of a test account after 30 consecutive invalid login attempts with a wrong password. This issue affects the authentication endpoint for the mobile application (OAuth).

The image below shows how the API endpoint successfully authenticated a user account, after 29 login attempts with a wrong password:

Request	Payload	Status	Error	Timeout	Length	Comment
15	Invalid15	200	☐	☐	415	
16	Invalid16	200	☐	☐	415	
17	Invalid17	200	☐	☐	415	
18	Invalid18	200	☐	☐	415	
19	Invalid19	200	☐	☐	415	
20	Invalid20	200	☐	☐	415	
21	Invalid21	200	☐	☐	415	
22	Invalid22	200	☐	☐	415	
23	Invalid23	200	☐	☐	415	
24	Invalid24	200	☐	☐	415	
25	Invalid25	200	☐	☐	415	
26	Invalid26	200	☐	☐	415	
27	Invalid27	200	☐	☐	415	
28	Invalid28	200	☐	☐	415	
29	Invalid29	200	☐	☐	415	
30	Password1!	200	☐	☐	1914	Contains a JWT

Request | Response

Raw | Headers | Hex | JSON Beautifier | JSON Web Tokens

```
HTTP/1.1 200 OK
Date: Wed, 18 Sep 2019 22:42:58 GMT
Content-Type: application/json
Connection: close
Server: nginx/1.13.12
X-Powered-By: PHP/7.1.17
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
No-Cache: 1
X-No-Cache: 1
Content-Length: 1612

{"token_type":"Bearer","expires_in":259200,"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiI
jJiMGVhZGQyIn0.eyJhdWQiOiJtb2JpbGUiLCJqdGkiOiI1ZTIwOTVlYzNkMWYyZjM3NWRkYWMzY2Y4ZGU0ODkxMDQ4ZjY
CJleHAiOjE1NjkxMDU3NzgsInN1YiI6IjEwMjA5MDYyODE4NzcxMTg5OTQiLCJzY29wZXMiOltdfQ.gKM8s3lXoNAT2O6k
Ajup-XGtkaoTpQrgcaWV_MvodZIEc1UoUnMaaQmJ38m6RfdTNg9XUy2m0CUkpoZG7m3QbsgICNub1OzJ8NbiQZZoz2_qKk
Es5PBvyVwytia8C5LQgw","refresh_token":"def502005fdce291976b9921caf0fc1a51cb39f985b44e4d6b68b21
9de70b4c005d75ef7473444cb5825f1d256375309fc9f3af495a00fbd5646f7ce6c9758926cb1325f5b54c47711db1
3fd17810c1def492a7544a3ec407564bf6db5874bfed0040e20cf2c01f818869cf397e3d70b5b695c8b8f75437c27e
6b553d543cfec0d1ce69cc1645f72b0a41bdc82f0b7e6374cdc10cdc76a221829cf3104ab3216f21e74c0a6a2b1e7b
":"success"}
```

Recommendation

Implement a CAPTCHA to prevent automated password guessing attacks. Require users to solve a CAPTCHA challenge after 5 invalid login attempts. The current lockout mechanism could be abused by attackers to deny access to legitimate users. For further recommendations, refer to the following guide: OWASP - Blocking Brute Force Attacks

MND-003 Password Not Required to Change Email

Total Risk
Medium

Impact
Medium

Likelihood
High

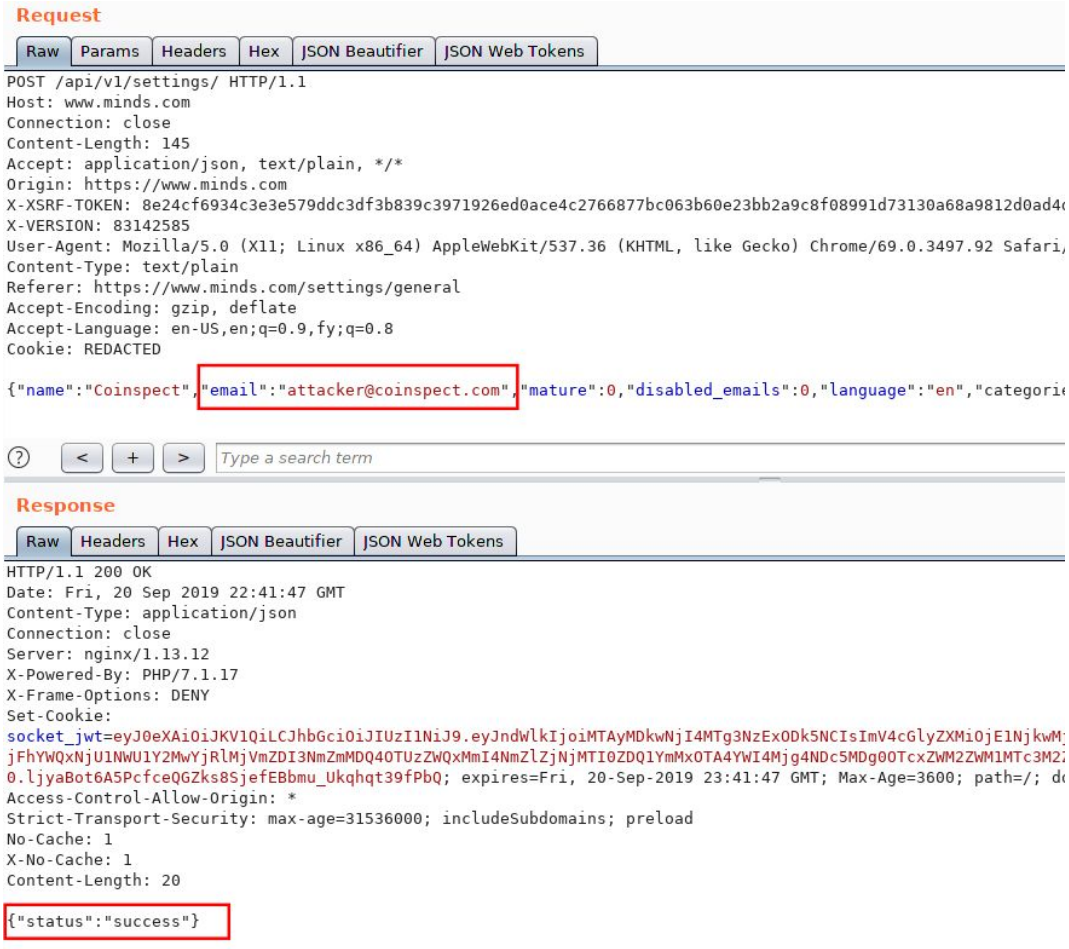
Location
https://www.minds.com/api/v1/settings
https://www.minds.com/api/v2/settings/emails

Category
Authentication

Description

The application allows users to change the email address without requiring the current password. This allows attackers with access to an open session (via XSS or other vulnerability) to gain permanent access to the account by changing the current email to an attacker's controlled address and then requesting a password reset.

Both applications (web and mobile) did prompt for current password when attempting to change the email on the profile settings. However, the verification was implemented on the user-interface and did not prevent an attacker from sending a direct request (with valid credentials) to the /settings API endpoint.



Recommendation

Enforce the verification of the current password on the '/settings' endpoint. Always require the current password to change the email address associated with the account.

MND-004 Password Sent as URL Parameter

Total Risk
Medium

Impact
Medium

Likelihood
Medium

Location
https://www.minds.com/api/v2/messenger/keys?password=

Category
Communications Security

Description

When sensitive data is passed in parameters of a URL, attackers might be able to obtain the data from several locations such as: web server's access logs, client's browser cache, and downloads folder metadata.
In this case, the "password" parameter used to unlock the private key and access chat content was sent as a parameter in the URL.

```
GET /api/v2/messenger/keys?password=Password1!&cb=1568831479544 HTTP/1.1
cache-control: no-cache, no-store, must-revalidate
pragma: no-cache
app-version: 3.9.1
authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImJkNzRhNDE1NzkxNGIxMWU2MTI3Y2I4Z
n0.eyJhdWQiOiJtb2JpbGUiLCJqdGkiOiJiZDc0YTQxNTc5MTRiMTFlNjEyN2NiOGQ5YmYzYThiNj
U2ODg0MjI4OCwibmJmIjoxNTY4ODQyMjg4LCJleHAiOjE1NjkxMDE0ODgsInN1YiI6IjEwMjA5MDY
K2L_msfBnBzL6TF6fcw059qh1KXWVsUVfoz9Np7Pk_pWvo1NMQ8H0Io9hixMc8E5RF4BTL2xS5m7V
oGnuUbnpt_iX3THv_MbeY8rYUbVXn0LW89hMnFjinbAAGmJ4uPJs7pWcnbepMuic7yXq682j_g_58
Host: www.minds.com
Connection: close
Accept-Encoding: gzip, deflate
Cookie: XSRF-TOKEN=3f8cf3b8212e02a33f15ba2640f22110c8ecf9b6608612531bcf4f3d99
messenger-secret=spLsOTMsSKn0W1UYV4CYsc1rkEi7VDXjb0HEae9Gk3GWO3%2FuXQUTNBwKT4
j8myn4jrnUwBW7onP%2F0W6Kr4UO9fzs7b%2BR97smY%3D
User-Agent: okhttp/3.12.1
```

Recommendation

Use POST method to send sensitive parameters.

MND-005 Two-Factor Authentication via SMS

Total Risk	Impact	Location
Low	Low	https://www.minds.com
	Likelihood	Category
	Low	Authentication

Description

Two factor authentication based on SMS is insecure against carrier network vulnerabilities, mobile number porting, and SIM swapping attacks. These attacks have taken place recently against cryptocurrency users.
Additionally, the National Institute of Standards and Technology (NIST) no longer recommends two-factor authentication systems that use SMS in its Digital Identity Guidelines.

NIST 800-63B: Authentication using the Public Switched Telephone Network:
"Verifiers SHOULD consider risk indicators such as device swap, SIM change, number porting, or other abnormal behavior before using the PSTN (Public Switched Telephone Network) to deliver an out-of-band authentication secret."

Recommendation

Consider to implement additional stronger two-factor authentication mechanisms such as a TOTP and FIDO U2F.

MND-006 Missing Account Activity Alerts

Total Risk	Impact	Location
Low	Low	https://www.minds.com
	Likelihood	Category
	Low	Session Handling

Description

The application does not inform the user of activities related to the security of the account, such as: password changes and logins from new devices or different locations. This could allow an attacker to compromise an account without alerting the user, and therefore use the site as the compromised user on a regular basis.

Recommendation

Implement notifications via email to alert the user when account's information such as: password and email address are updated. Additionally, notify the user when there is a login from a new device or different location.

MND-007 CORS: Arbitrary Origin Trusted

Total Risk	Impact	Location
Low	Low	engine/Core/Router.php:74
	Likelihood	Category
	Low	Access Control

Description

The CORS configuration of the application allows requests from any domain. Specifically, this setting allows third-party sites to send requests on behalf of the authenticated user and read the content of the response from the Minds APIs. In this case, the impact of the issue is reduced because the application also validates the XSRF header, which is not allowed in CORS requests.

engine/Core/Router.php:74

```
        if ($request->getMethod() === 'OPTIONS') {
            header("Access-Control-Allow-Origin:
{$_SERVER['HTTP_ORIGIN']}");
            header('Access-Control-Allow-Credentials: true');
            header('Access-Control-Max-Age: 86400');
            header('Access-Control-Allow-Methods: GET, POST, PUT,
DELETE, OPTIONS');
            header('Access-Control-Allow-Headers:
Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Ke
ep-Alive,Origin,User-Agent,X-Mx-ReqToken,X-Requested-With,X-No-Cache');
            return null;
        }
```

Recommendation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

MND-008 Multiple Sessions Allowed

Total Risk
Low

Impact
Low

Likelihood
Low

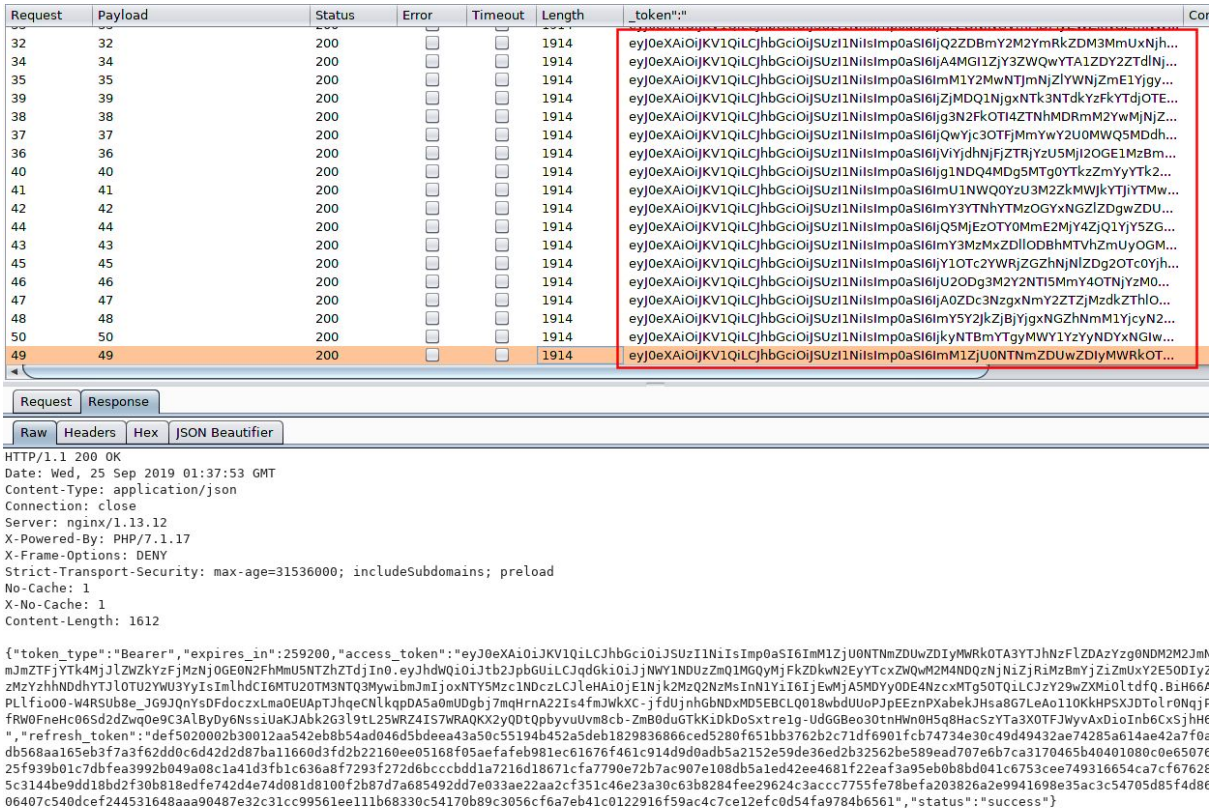
Location
https://www.minds.com/api/v2/oauth/token

Category
Session Handling

Description

The application does not limit the number of active sessions for a single user. The longer a session remains active, the higher the possibility a session has of becoming compromised. Allowing a user to have multiple valid sessions at once increases a user's susceptibility to token compromise, as the user might lose track of all active sessions.

The application allowed more than 50th active sessions for a single user:



Request	Payload	Status	Error	Timeout	Length	_token":"	Cor
32	32	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjQ2ZDBmY2M2YmRkZDM3MmUxNjh...	
34	34	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjA4MGI1ZjY3ZWQwYTA1ZDY2ZTdlNj...	
35	35	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImM1Y2MwNTJmNjZlYWNjZmE1Yjgy...	
39	39	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjZjMDQ1NjgxNTk3NTdkYzFkYTdjOTE...	
38	38	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6Ijg3N2FkOTI4ZTNhMDRmM2YwMjNjZ...	
37	37	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjQwYjc3OTFjMmYwY2U0MWQ5MDdh...	
36	36	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjViYjdhNjFjZTRjYzU5MjI2OGE1MzBm...	
40	40	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6Ijg1NDQ4MDg5MTg0YTkzZmYyYTk2...	
41	41	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImU1NWQ0YzU3M2ZkMWJkYTJiYTMw...	
42	42	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImY3YTNhYTMzOGYxNGZlZDgwZDU...	
44	44	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjQ5MjEzOTY0MmE2MjY4ZjQ1YjY5ZG...	
43	43	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImY3MzMxZDllODBhMTVhZmUyOGM...	
45	45	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjY1OTc2YWRjZGZhNjNlZDg2OTc0Yjh...	
46	46	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjU2ODg3M2Y2NTI5MmY4OTNjYzM0...	
47	47	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjA0ZDc3NzgxNmY2ZTZjMzdkZThlO...	
48	48	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImY5Y2JkZjBjYjgxNGZhNmM1YjcyN2...	
50	50	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjkyNTBmYTgyMWY1YzYyNDYxNGIw...	
49	49	200			1914	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImM1ZjU0NTNmZDUwZDIyMWRkOT...	

Request | Response

Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Wed, 25 Sep 2019 01:37:53 GMT
Content-Type: application/json
Connection: close
Server: nginx/1.13.12
X-Powered-By: PHP/7.1.17
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
No-Cache: 1
X-No-Cache: 1
Content-Length: 1612

{"token_type":"Bearer","expires_in":259200,"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6ImM1ZjU0NTNmZDUwZDIyMWRkOTA3YTJhNzFlZDAzYzg0NDM2M2JmM
mJmZTFjYTk4MjJlZWZkYzFjMzNjOGE0N2FhMmU5NTZhZTdjIn0.eyJhdWQiOiJtb2JpbGUiLCJqdGkiOiJjNWY1NDUzZmQ1MGQyMjFkZDkwN2EyYTcxZWQwM2M4NDQzNjNiZjRiMzBmYjZiZmUxY2E5ODIy
zMzYzhhNDdhYTJlOTU2YWU3YyIsImlhdCI6MTU2OTM3NTQ3MywibmJmIjoxNTY5MzclNDczLCJleHAiOjE1Njk2MzQ2NzMsInN1YiI6IjEwMjA5MDYyODE4NzcxMTg5OTQiLCJzY29wZXMiOltdfQ.BiH66A
PLlfioO0-W4RSUb8e_JG9JQnYsDFdoczxLmaOEUApTJhqeCNlkqpDA5a0mUDgbj7mqHrnA22Is4fmJWkXC-jfdUjnhGbNDxMD5EBCLQ018wbdUUoPJpEEznPXabekJHsa8G7LeAo11OKkHPSXJDTolr0NqjF
fRW0FneHc06Sd2dZwqOe9C3AlByDy6NssiUaKJAbk2G3l9tL25WRZ4IS7WRAQKX2yQDtQpbyvuUvm8cb-ZmB0duGTkKiDkDoSxtre1g-UdGGBeo3OtnHWn0H5q8HacSzYTa3X0TFJWyvAxDioInb6CxSjhH6
","refresh_token":"def5020002b30012aa542eb8b54ad046d5bdeea43a50c55194b452a5deb1829836866ced5280f651bb3762b2c71df6901fcb74734e30c49d49432ae74285a614ae42a7f0a
db568aa165eb3f7a3f62dd0c6d42d2d87ba11660d3fd2b22160ee05168f05aefafeb981ec61676f461c914d9d0adb5a2152e59de36ed2b32562be589ead707e6b7ca3170465b40401080c0e65076
25f939b01c7dbfea3992b049a08c1a41d3fb1c636a8f7293f272d6bcccbdd1a7216d18671cfa7790e72b7ac907e108db5a1ed42ee4681f22eaf3a95eb0b8bd041c6753cee749316654ca7cf67628
5c3144be9dd18bd2f30b818edfe742d4e74d081d8100f2b87d7a685492dd7e033ae22aa2cf351c46e23a30c63b8284fee29624c3accc7755fe78befa203826a2e9941698e35ac3c54705d85f4d86
06407c540dcef244531648aaa90487e32c31cc99561ee111b68330c54170b89c3056cf6a7eb41c0122916f59ac4c7ce12efc0d54fa9784b6561","status":"success"}
```

Recommendation

Limit the number of active tokens for a single user. Additionally, consider providing a feature that allows a user to view all active tokens and invalidate them.

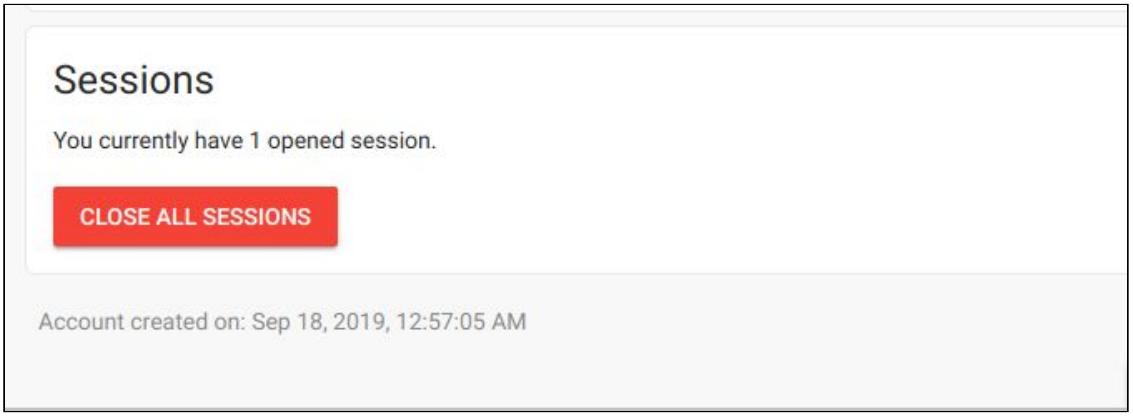
MND-009 Sessions Not Terminated On Password Change

Total Risk	Impact	Location
Low	Low	https://www.minds.com
	Likelihood	Category
	Low	Session Handling

Description

The application does not terminate the active sessions after a user forces a password change. If an account is compromised, the legit owner does not have an option to terminate the session controlled by the attacker.
The web application does include an option to allow the user to close all the sessions. However, this option does not terminate the sessions on the mobile application.

The option below does not terminate the sessions on the mobile application:



Recommendation

Terminate all the user sessions (web and mobile) on the server side after a password change.

MND-010 Missing Content Security Policy

Total Risk	Impact	Location
Zero	Zero	https://www.minds.com
	Likelihood	Category
	Zero	Access Control

Description

Content Security Policy (CSP) is an additional layer of defense that helps to detect and mitigate certain types of attacks, including data injection and Cross-Site-Scripting (XSS). This security mechanism enforces the loading of resources (scripts, images, etc.) from restricted locations that are trusted by the application.

The application did not include the Content-Security-Policy header:

```
HTTP/1.1 200 OK
Date: Tue, 24 Sep 2019 18:52:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Server: nginx/1.13.12
X-Powered-By: PHP/7.1.17
X-Frame-Options: DENY
Set-Cookie:
socket_jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJndWlkIjoiMTAyMzAzOTI3MzMzNjU3ODA2NSIsImV4cG
VlNzJlYjcxNTczMGMxZmY3M2E4ZWJiNDY5NzA5YTI4YWRmZWNjM2I0NTJmMmUyM2Y3ZWQxNzczIn0.VO7iwKzLrs-90vMu
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Cache: BYPASS
No-Cache: 1
X-No-Cache: 1
Content-Length: 24902
```

Recommendation

Follow the Mozilla guide for implementing CSP:
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP#Using_CSP

MND-011 Server Version Disclosure via HTTP Headers

Total Risk	Impact	Location
Zero	Zero	https://www.minds.com
	Likelihood	Category
	Zero	Configuration Management

Description

The web server disclosed software name and version information in the HTTP headers. The information revealed could help attackers to plan and launch further attacks against the application. The following header was included in the HTTP responses:

```
Server: nginx/1.13.12
X-Powered-By: PHP/7.1.17
```

Recommendation

Remove version information from HTTP headers and error pages by following the guides below:

- PHP Remove 'X-Powered-By' Header
- Nginx Remove Version Info from HTTP Headers and Error Pages

5. Disclaimer

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. This report should not be considered a perfect representation of the risks threatening the analysed system, networks and applications.