SecurePurple®

Be Internet Secure

CYBER HEALTH CHECK REPORT

E-GATEWAY PEC REPORT

Table of Content

Executive Summary:

Presented here is the comprehensive cyber health check report for the https://egateway.pec.org.pk/ website, as per your request. The primary aim of this assessment is to uncover and address any existing security vulnerabilities and weaknesses, providing you with valuable insights into the robustness of your infrastructure. Through a simulated hacker attack from the internet, the exercise was conducted to evaluate the target system within the defined scope. It's essential to note that the outcomes of this assessment serve to furnish you with a holistic overview and assessment of the health of the specified scope, empowering you to make informed decisions and take proactive measures to fortify your cybersecurity posture.

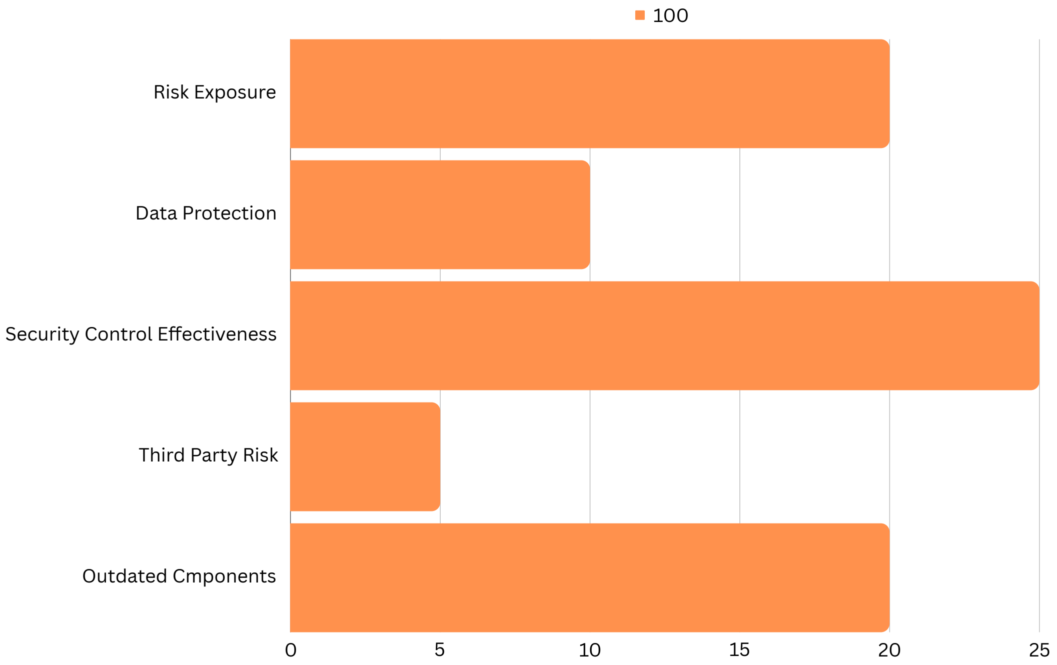
Engagement Scope:

The target in scope for this activity was:

S/No	Asset in Scope	Testing Method
1	https://egateway.pec.org.pk/	Black Box

Summarised Analysis:

Here is a summarised analysis of the cyber health-check report in terms of resilience:



Recommended Summary:

Upon conducting a comprehensive evaluation of your website, we've identified several vulnerabilities that require immediate attention and improvement. These vulnerabilities span various aspects of your website's security, ranging from Critical to Low severity. Addressing these issues is paramount to safeguarding your online presence and protecting your digital assets from potential exploitation.

For further insights into the security posture of your infrastructure, we welcome you to contact us at ask@securepurple.com. Our team is dedicated to assisting you in strengthening your website's defenses and safeguarding it against evolving security risks.

Health-Check Overview

Here are the findings regarding the security posture of the target within the defined scope.

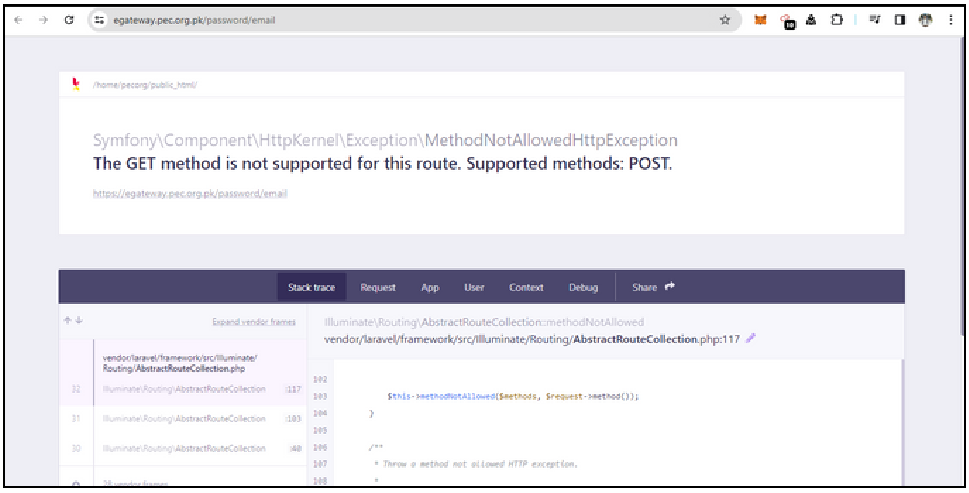
Laravel debug mode enabled:

Vulnerable Urls:

- https://egateway.pec.org.pk/clients
- https://egateway.pec.org.pk/password/email

Status: Open

When Laravel debug mode is enabled, it allows detailed error messages to be displayed, potentially exposing sensitive information about the application's configuration, database structure, or even user data. This vulnerability could lead to security breaches, as attackers can exploit the disclosed information to identify and exploit weaknesses in the application. To mitigate this vulnerability, ensure that debug mode is disabled in production environments by setting the APP_DEBUG variable to false. Additionally, implement proper error handling mechanisms to gracefully handle errors without revealing sensitive information to users. Regularly review and update your Laravel application and dependencies to patch any known security vulnerabilities.



Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException

The GET method is not supported for this route. Supported methods: POST.

https://egateway.pec.org.pk/password/email

vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php

32 Illuminate\Routing\AbstractRouteCollection :117

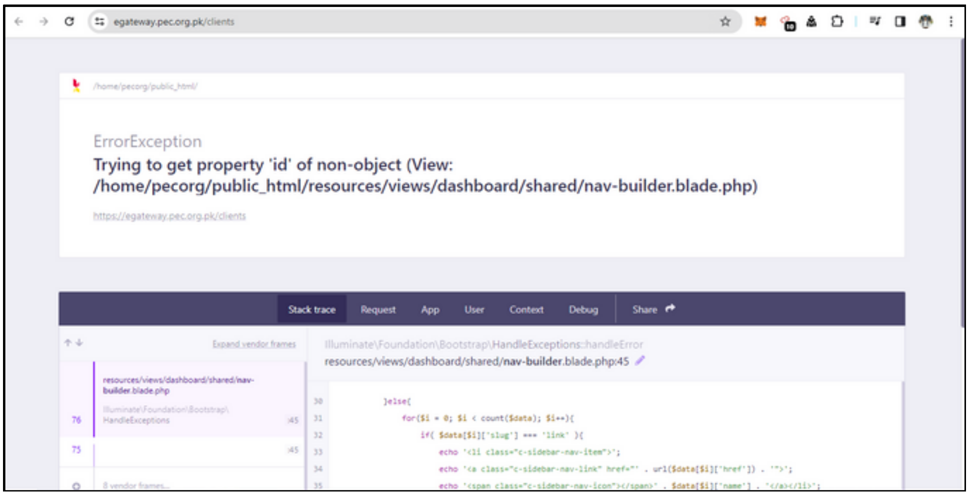
31 Illuminate\Routing\AbstractRouteCollection :103

30 Illuminate\Routing\AbstractRouteCollection :40

Illuminate\Routing\AbstractRouteCollection::methodNotAllowed

vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php:117

```

            $this->methodNotAllowed($methods, $request->method());
        }

        /**
         * Throw a method not allowed HTTP exception.
         *
```



ErrorException

Trying to get property 'id' of non-object (View: /home/pecorg/public_html/resources/views/dashboard/shared/nav-builder.blade.php)

https://egateway.pec.org.pk/clients

resources/views/dashboard/shared/nav-builder.blade.php

76 Illuminate\Foundation\Bootstrap\HandleExceptions :45

75 :45

Illuminate\Foundation\Bootstrap\HandleExceptions::handleError

resources/views/dashboard/shared/nav-builder.blade.php:45

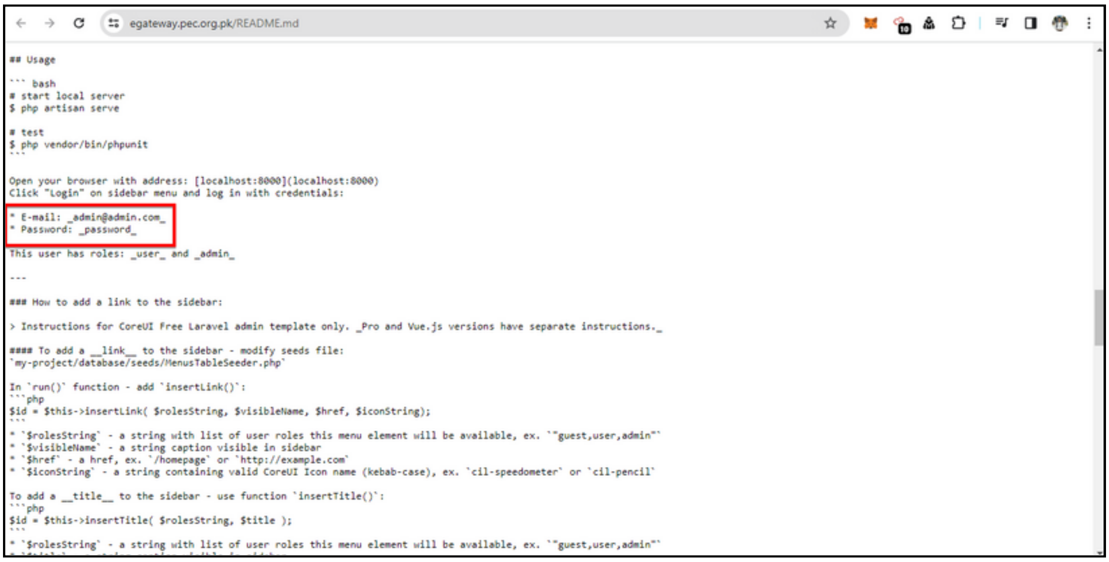
```
        }else{
            for($i = 0; $i < count($data); $i++){
                if( $data[$i]['slug'] === 'link' ){
                    echo '<li class="c-sidebar-nav-item">';
                    echo '<a class="c-sidebar-nav-link" href="' . url($data[$i]['href']) . '">';
                    echo '<span class="c-sidebar-nav-icon"></span>' . $data[$i]['name'] . '</a></li>';
```

Documentation files:

Vulnerable Url: http://egateway.pec.org.pk/README.md

Status: Open

When documentation files such as readme.txt or changelog.txt are present in a web application's production environment, they can potentially reveal information about the application's technology stack, version, and sometimes even sensitive configuration details. This information could aid attackers in targeting vulnerabilities specific to the application version or technology. To mitigate this risk, it's advisable to remove these documentation files from production systems altogether. Alternatively, if the files are necessary for reference, ensure they don't disclose sensitive information and restrict access to them through proper permissions or by placing them outside the web root directory where they can't be accessed via HTTP. Regularly review and update these files to remove any inadvertent disclosures of sensitive information.



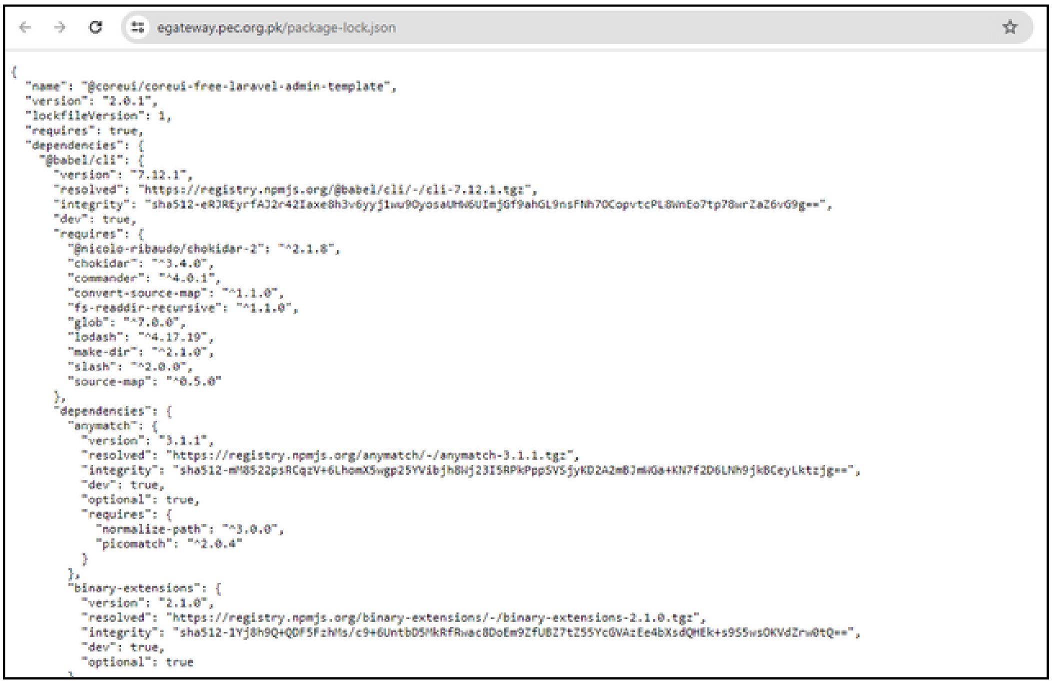
~~~
## Usage

``` bash
# start local server
$ php artisan serve

# test
$ php vendor/bin/phpunit
```

Open your browser with address: [localhost:8000](localhost:8000)
Click "Login" on sidebar menu and log in with credentials:

* E-mail: _admin@admin.com_
* Password: _password_

This user has roles: _user_ and _admin_

---

### How to add a link to the sidebar:

> Instructions for CoreUI Free Laravel admin template only. _Pro and Vue.js versions have separate instructions._

#### To add a __link__ to the sidebar - modify seeds file:
`my-project/database/seeds/MenusTableSeeder.php`

In `run()` function - add `insertLink()`:
```php
$id = $this->insertLink( $rolesString, $visibleName, $href, $iconString);
```
* `$rolesString` - a string with list of user roles this menu element will be available, ex. `"guest,user,admin"`
* `$visibleName` - a string caption visible in sidebar
* `$href` - a href, ex. `/homepage` or `http://example.com`
* `$iconString` - a string containing valid CoreUI Icon name (kebab-case), ex. `cil-speedometer` or `cil-pencil`

To add a __title__ to the sidebar - use function `insertTitle()`:
```php
$id = $this->insertTitle( $rolesString, $title );
```
* `$rolesString` - a string with list of user roles this menu element will be available, ex. `"guest,user,admin"`
~~~

Unauthorized Exposure of package-lock.json:

Vulnerable Url: https://egateway.pec.org.pk/package-lock.json

Status: Open

This file is associated with npm (Node Package Manager) and maintains a record of the precise versions of every package installed. Unauthorized access to this file could potentially reveal information about the versions of packages used in the system, which might aid attackers in exploiting known vulnerabilities. We recommend restricting access to this file to only authorized personnel and implementing proper access controls.



```
{
  "name": "@coreui/coreui-free-laravel-admin-template",
  "version": "2.0.1",
  "lockfileVersion": 1,
  "requires": true,
  "dependencies": {
    "@babel/cli": {
      "version": "7.12.1",
      "resolved": "https://registry.npmjs.org/@babel/cli/-/cli-7.12.1.tgz",
      "integrity": "sha512-eRJREyrfAJ2r42Iaxe8h3v6yyj1wu9OyosaUHW6UImjGf9ahGL9nsFNh7OCopvtcPL8WnEo7tp78wrZaZ6vG9g==",
      "dev": true,
      "requires": {
        "@nicolo-ribaudo/chokidar-2": "^2.1.8",
        "chokidar": "^3.4.0",
        "commander": "^4.0.1",
        "convert-source-map": "^1.1.0",
        "fs-readdir-recursive": "^1.1.0",
        "glob": "^7.0.0",
        "lodash": "^4.17.19",
        "make-dir": "^2.1.0",
        "slash": "^2.0.0",
        "source-map": "^0.5.0"
      },
      "dependencies": {
        "anymatch": {
          "version": "3.1.1",
          "resolved": "https://registry.npmjs.org/anymatch/-/anymatch-3.1.1.tgz",
          "integrity": "sha512-mM8522psRCqzV+6LhomX5wgp25YVibjh8Wj23I5RPkPppSVSjyKD2A2mBJmWGa+KN7f2D6LNh9jkBCeyLktzjg==",
          "dev": true,
          "optional": true,
          "requires": {
            "normalize-path": "^3.0.0",
            "picomatch": "^2.0.4"
          }
        },
        "binary-extensions": {
          "version": "2.1.0",
          "resolved": "https://registry.npmjs.org/binary-extensions/-/binary-extensions-2.1.0.tgz",
          "integrity": "sha512-1Yj8h9Q+QDF5FzhMs/c9+6UntbD5MkRfRwac8DoEm9ZfUBZ7tZ55YcGVAzEe4bXsdQHEk+s9S5wsOKVdZrw0tQ==",
          "dev": true,
          "optional": true
```

Email Enumeration at password reset and client creation:

Vulnerable Urls:

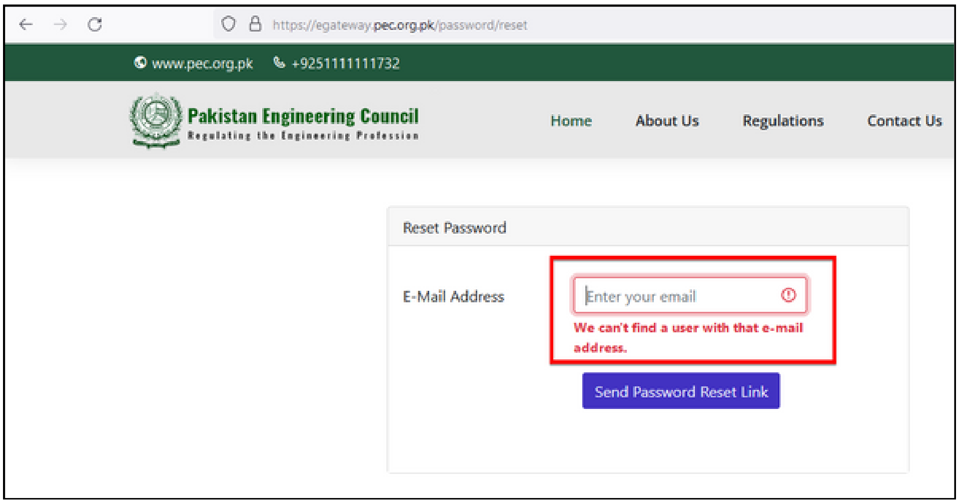
- https://egateway.pec.org.pk/password/reset
- https://egateway.pec.org.pk/clients/create

Status: Open

Email enumeration refers to the process of determining valid user email addresses by exploiting responses from the system during specific interactions, such as password reset requests or client creation attempts. This vulnerability can pose a significant security risk, allowing malicious actors to identify valid user accounts and potentially exploit them for malicious purposes.

The system provides different responses for valid and invalid email addresses during the password reset process. When a valid email address is provided, the system responds with a message indicating that an email has been sent with instructions for password reset. However, when an invalid email address is provided, the system responds with an error message indicating that "We can't find a user with that e-mail address". This differential response allows an attacker to determine whether an email address is valid or not, facilitating email enumeration.

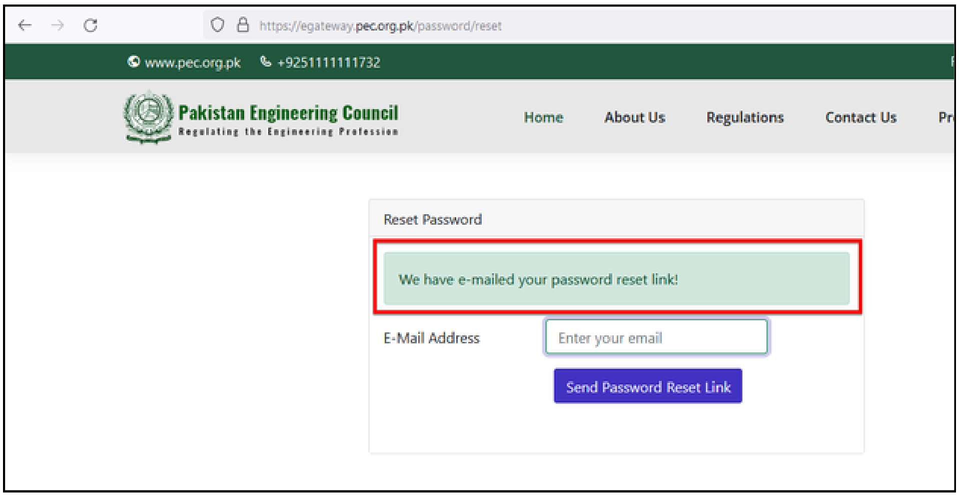
Similar to the password reset endpoint, the client creation endpoint also exhibits differential responses for valid and invalid email addresses. When attempting to create a new client account with a valid email address, the system responds with a message indicating that the account creation was successful. Conversely, when an invalid email address is provided, the system responds with an error message stating that "The email has already been taken". This behavior allows attackers to enumerate valid email addresses by observing the system's response to client creation attempts.


https://egateway.pec.org.pk/password/reset
www.pec.org.pk
+9251111111732
Pakistan Engineering Council
Regulating the Engineering Profession
Home
About Us
Regulations
Contact Us
Send Password Reset Link

Reset Password

E-Mail Address: Enter your email

We can't find a user with that e-mail address.


https://egateway.pec.org.pk/password/reset
www.pec.org.pk
+9251111111732
Pakistan Engineering Council
Regulating the Engineering Profession
Home
About Us
Regulations
Contact Us
Pr
Send Password Reset Link

Reset Password

We have e-mailed your password reset link!

E-Mail Address: Enter your email

Cache-control misconfiguration:

Vulnerable Urls:

- https://egateway.pec.org.pk/client_dashboard
- https://egateway.pec.org.pk/client/post_project
- https://egateway.pec.org.pk/client/projects
- https://egateway.pec.org.pk/client/publicproject
- https://egateway.pec.org.pk/messages
- https://egateway.pec.org.pk/client/consultants
- https://egateway.pec.org.pk/client/profile
- https://egateway.pec.org.pk/hash_password

Status: Open

This vulnerability arises from misconfigurations in cache control headers, allowing sensitive information to be cached by the browser even after the user has logged out. After logging out from a sensitive information page, pressing the back button may lead the user back to the cached page, thereby exposing sensitive data.

This poses a significant risk to the confidentiality of sensitive information as it allows unauthorized users who gain access to the same device or browser session to view previously accessed sensitive data even after the user has logged out. It undermines the intended security measures of the application and compromises user privacy.

Fails to Invalidate Session after password change:

Vulnerable Url: https://egateway.pec.org.pk/password/reset

Status: Open

This vulnerability occurs when a user changes their password but remains logged in on other active sessions, such as in different browsers or devices. Despite changing the password, the old session remains active, allowing potential unauthorized access. This poses a significant security risk as it allows unauthorized users to maintain access to the account even after the password has been changed. It compromises the confidentiality and integrity of the user's data and exposes them to potentially malicious activities. To prevent this issue, implement session invalidation mechanisms that force logout from all active sessions upon password change.

Conclusion

In conclusion, this assessment has provided a detailed overview, flagging identified vulnerabilities, potential risks, and best practices based on the latest information available. It is strongly advised to promptly address the issues highlighted in this report to bolster the overall security posture of your IT infrastructure. However, it's important to recognize that the threat landscape is continually evolving, necessitating ongoing vigilance and adaptation to emerging risks.

For further guidance on enhancing the security of your digital assets and staying ahead of cyber threats, we encourage you to reach out to us at ask@securepurple.com. We remain dedicated to supporting you in safeguarding your organization's digital assets and maintaining a resilient security posture.

THANK YOU

Thank you for choosing us in your journey towards a safer and more secure digital world. For more details about this proposal please contact:

Address

Plot 24-B, Street 6, H9/1, Islamabad

Email

ask@securepurple.com

Website

www.securepurple.com