Pentest-Tools.com

Website Vulnerability Scanner Report (Light)

See what the FULL scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Full scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	✗	✓
Cross-Site Scripting	✗	✓
Local/Remote File Inclusion	✗	✓
Remote command execution	✗	✓
Discovery of sensitive files	✗	✓

Get a PRO Account to unlock the full capabilities of this scanner!

✓ http://tk-naidu.github.io/

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	4
Info:	6

Scan information:

Start time:	2019-10-06 23:02:12 UTC+03
Finish time:	2019-10-06 23:02:19 UTC+03
Scan duration:	7 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Server software and technology found

Software / Version	Category
Twitter Bootstrap	Web Frameworks
Firebase	Databases
Varnish	Cache Tools
Font Awesome	Font Scripts
Moment.js	JavaScript Frameworks
Select2	JavaScript Frameworks
jQuery 3.2.1	JavaScript Frameworks

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002).

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

Details

Risk description:
Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://www.owasp.org/index.php/Clickjacking

The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP X-Content-Type-Options header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend you to add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks.
More information about this issue:
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

We recommend setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

We recommend setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Redirect from HTTP to HTTPS

http://tk-naidu.github.io/ redirects to:
https://tk-naidu.github.io/

Details

Risk description:
The application redirects the HTTP requests to HTTPS. While this is an accepted practice, an attacker playing man-in-the-middle could intercept the first HTTP response (clear-text) and modify it in order to inject malicious JavaScript code or just to disable the HTTPS redirection. This type of attack is called "SSL stripping" and it is described in detail here:
http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf
https://moxie.org/software/sslstrip/

Recommendation:
We recommend you to enable HTTP Strict Transport Security (HSTS) which forces the web browser to initiate only HTTPS connections to the protected websites.

More information about this issue:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Password auto-complete is enabled

```
<input class="input100" id="pw" name="pass" type="password"/>
```

Details

Risk description:

When password auto-complete is enabled, the browser will remember the password entered into the login form, such that it will automatically fill it next time the user tries to login.

However, if an attacker gains physical access to the victim's computer, he can retrieve the saved password from the browser's memory and use it to gain access to the victim's account in the application.

Furthermore, if the application is also vulnerable to Cross-Site Scripting, the attacker could steal the saved password remotely.

Recommendation:

We recommend you to disable the password auto-complete feature on the login forms by setting the attribute `autocomplete="off"` on all password fields.

More information about this issue:

https://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_(OTG-AUTHN-005).

No vulnerabilities found for server-side software

No security issue found regarding HTTP cookies

Robots.txt file not found

No security issue found regarding client access policies

Directory listing not found (quick scan)

Passwords are submitted over an encrypted channel

Scan coverage information

List of tests performed (10/10)

- ✓ Fingerprinting the server software and technology...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Analyzing the security of HTTP cookies...
- ✓ Analyzing HTTP security headers...
- ✓ Checking for secure communication...
- ✓ Checking robots.txt file...
- ✓ Checking client access policies...
- ✓ Checking for directory listing (quick scan)...
- ✓ Checking for password auto-complete (quick scan)...
- ✓ Checking for clear-text submission of passwords (quick scan)...

Scan parameters

Website URL:	http://tk-naidu.github.io/
Scan type:	Light
Authentication:	False