Website Vulnerability Scanner Report

✔ **https://code.ptit.edu.vn/login**

Target added due to a redirect from https://code.ptit.edu.vn/

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	4
Low:	6
Info:	8

Scan information:

Start time:	Apr 29, 2024 / 08:02:26
Finish time:	Apr 29, 2024 / 08:02:52
Scan duration:	26 sec
Tests performed:	18/18
Scan status:	Finished

Findings

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://code.ptit.edu.vn/login	XSRF-TOKEN	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: XSRF-TOKEN=eyJpdiI6IjVMQ3dhKzdXeEx6RWt5cWdlRHVIK1E9PSIsInZhbHVlIjoiOFc4L1ErY0diU0xkTTNuVE1MdUpOdy9IYUNQRVVlb1F1TWNWcU4wUVBJOFJkczNadi9QTm94WHBjanhZTUUybEdHQmNLWUtFLys5Umh1YmFUQ0pQUDUxdGQrRnlkdmFBMTV5REc3cWRKOVk5YVhlSHBZZXJFdnYyL3BpcmtTVGsiLCJtYWMiOiJkZDMwZjQ1YWI2MmNjNDkzMjg2NmE5OWQwNTJiOTBiNzJhMmM2YjgxMTkyYzdhMzk4OWE4YzM4MzRlMDgyYjY5IiwidGFnIjoiIn0%3D Request / Response

Details

Risk description:

The risk is that an attacker who injects malicious JavaScript code on the page (e.g. by using an XSS attack) can access the cookie and can send it to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:

Ensure that the HttpOnly flag is set for all cookies.

References:

https://owasp.org/www-community/HttpOnly

Classification:

CWE : CWE-1004
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Insecure cookie setting: domain too loose

CONFIRMED

URL	Cookie Name	Evidence

https://code.ptit.edu.vn/login	XSRF-TOKEN	Set-Cookie: .code.ptit.edu.vn Request / Response

Details

Risk description:
The risk is that a cookie set for example.com may be sent along with the requests sent to dev.example.com, calendar.example.com, hostedsite.example.com. Potentially risky websites under your main domain may access those cookies and use the victim session from the main site.

Recommendation:
The `Domain` attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to `Domain=app.mysite.com`

Classification:
CWE : CWE-614
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence
https://code.ptit.edu.vn/login	XSRF-TOKEN	Set-Cookie: XSRF-TOKEN=eyJpdiI6IjVMQ3dhKzdXeEx6RWt5cWdlRHVIK1E9PSIsInZhbHVlIjoiOFc4L1ErY0diU0xkTTNuVE1MdUpOdy9IYUNQRVVlb1F1TWNWcU4wUVBJOFJkczNadi9QTm94WHBjanhZTUUybEdHQmNLWUtFLys5Umh1YmFUQ0pQUDUxdGQrRnlkdmFBMTV5REc3cWRKOVk5YVhlSHBZZXJFdnYyL3BpcmtTVGsiLCJtYWMiOiJkZDMwZjQ1YWI2MmNjNDkzMjg2NmE5OWQwNTJiOTBiNzJhMmM2YjgxMTkyYzdhMzk4OWE4YzM4MzRlMDgyYjY5liwidGFnIjoiIn0%3D; expires=Mon, 29-Apr-2024 11:02:29 GMT; Max-Age=21600; path=/; domain=code.ptit.edu.vn; samesite=lax, ptit_code_session=eyJpdiI6Inp2S3BMZDlRYzBXRndDMWJibmJROGc9PSIsInZhbHVlIjoiSWlMSXZ1NGQ4UUw1MkhkTmU3eE1HY1BZTnltVEo2b3BGbStrVE9vQWhvaGtXbldkUUxXclI4OHBqakwvTklmcEZUbkhRK2dMdlBybHdNRUFQOVBNYkVlZXdhQmx5clVSblBLbjVCQjVKNXpROE45UXdwT0VWQm9ZTmN3a0Z1bEgiLCJtYWMiOiJlNWIyMDM1Njg3YWQwN2U3Mzg1ZTBjMjQxOGQ0ZGMwMTE2YTFkYTE1Y2NkODM2MzgyZTk5YjEyOWY3NGZiYzJjliwidGFnIjoiIn0%3D; expires=Mon, 29-Apr-2024 11:02:29 GMT; Max-Age=21600; path=/; domain=code.ptit.edu.vn; httponly; samesite=lax Request / Response

Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:
CWE : CWE-614
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software
	6.5	CVE-2021-23337	Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.	lodash 4.17.19

	5.8	CVE-2020-8203	Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.	lodash 4.17.19
	5	CVE-2020-28500	Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.	lodash 4.17.19

Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://code.ptit.edu.vn/login	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://code.ptit.edu.vn/login	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

Details

Risk description:
The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

Classification:
CWE : CWE-693

OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://code.ptit.edu.vn/login	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://code.ptit.edu.vn/login	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Robots.txt file found

CONFIRMED

URL
https://code.ptit.edu.vn/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website

(ex. administration panels, configuration files, etc).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

Software / Version	Category
jQuery UI 1.12.1	JavaScript libraries
Lodash 4.17.19	JavaScript libraries
Bootstrap 4.5.0	UI frameworks
Axios	JavaScript libraries
jQuery 3.5.1	JavaScript libraries
Popper	Miscellaneous
reCAPTCHA	Security

Details

Risk description:
The risk is that 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 permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

URL
Missing: https://code.ptit.edu.vn/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Website is accessible.

Nothing was found for client access policies.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for unsafe HTTP header Content Security Policy.

Scan coverage information

List of tests performed (18/18)

- Starting the scan...
- Checking for HttpOnly flag of cookie...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - Referrer...
- Checking for domain too loose set for cookies...
- Checking for Secure flag of cookie...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for absence of the security.txt file...
- Checking for use of untrusted certificates...
- Checking for enabled HTTP debug methods...
- Checking for secure communication...
- Checking for directory listing...
- Checking for unsafe HTTP header Content Security Policy...

Scan parameters

Target:	https://code.ptit.edu.vn/login
Scan type:	Light
Authentication:	NULL

Scan stats

Unique Injection Points Detected:	2
URLs spidered:	2
Total number of HTTP requests:	10
Average time until a response was received:	554ms