



3/25/2023 2:18:05 PM (UTC+07:00)

Detailed Scan Report

<https://online.hcmue.edu.vn/>

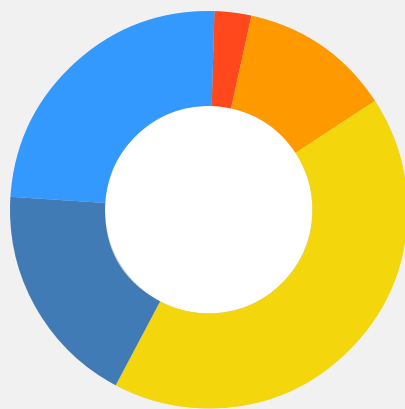
Scan Time	: 3/25/2023 2:02:30 PM (UTC+07:00)
Scan Duration	: 00:00:10:03
Total Requests	: 9,093
Average Speed	: 15.1r/s

Risk Level:
HIGH
















Your website is insecure!
















Some very serious vulnerabilities were identified on your website. You should address them as soon as possible.




Vulnerabilities



Critical	0
High	1
Medium	4
Low	14
Best Practice	6
Information	8
TOTAL	33

Vulnerability	Suggested Action
 Session Cookie Not Marked as Secure	Fix immediately: An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
 HTTP Strict Transport Security (HSTS) Policy Not Enabled	Fix soon: You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Out-of-date Version (IIS)	Fix soon: You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Out-of-date Version (jQuery)	Fix soon: You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Weak Ciphers Enabled	Fix soon: You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 [Possible] Cross-site Request Forgery	Consider fixing after confirmed: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 [Possible] Phishing by Navigating Browser Tabs	Consider fixing after confirmed: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Cookie Not Marked as HttpOnly	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Cookie Not Marked as Secure	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Information Disclosure (Microsoft Office)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Insecure Transportation Security Protocol Supported (TLS 1.0)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Internal Server Error	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Missing X-Frame-Options Header	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Passive Mixed Content over HTTPS	Consider fixing after confirmed: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Programming Error Message	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.

Vulnerability	Suggested Action
 Stack Trace Disclosure (ASP.NET)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (ASP.NET)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 ViewState is not Encrypted	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Windows Short Filename	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Content Security Policy (CSP) Not Implemented	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Expect-CT Not Enabled	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Insecure Transportation Security Protocol Supported (TLS 1.1)	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Missing X-XSS-Protection Header	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Referrer-Policy Not Implemented	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 SameSite Cookie Not Implemented	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 [Possible] Internal Path Disclosure (*nix)	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 [Possible] Internal Path Disclosure (Windows)	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 ASP.NET Identified	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Email Address Disclosure	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Forbidden Resource	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.

Vulnerability	Suggested Action
 Generic Email Address Disclosure	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 OPTIONS Method Enabled	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Version Disclosure (IIS)	No action required: These items are just for your information. You don't need to take any action on them but they might be useful to know.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	12
OWASP 2013	20
OWASP 2017	22
HIPAA	14
ISO27001	33

PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

This report created with 5.8.1.28119-master-bca4e4e
<https://www.netsparker.com>