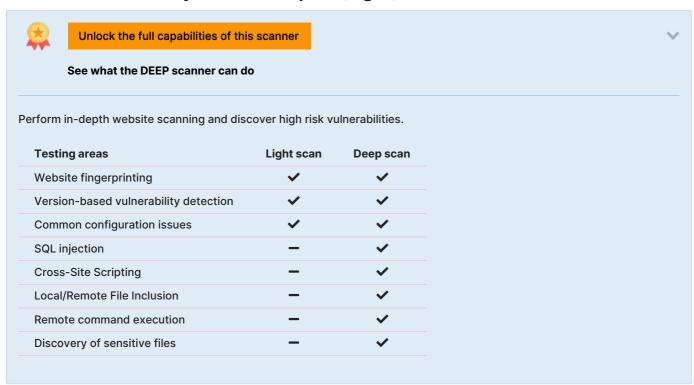


Website Vulnerability Scanner Report (Light)



✓ http://www.itsecgames.com/

•

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





Scan information:

Start time: Sep 05, 2025 / 14:51:49 UTC+03
Finish time: Sep 05, 2025 / 14:52:10 UTC+03

Scan duration: 21 sec
Tests performed: 39/39
Scan status: Finish

Findings



Communication is not secure

port 80/tcp

CONFIRMED

URL	Response URL	Evidence
http://www.itsecgames.com/	http://www.itsecgames.com/	Communication is made over unsecure, unencrypted HTTP.

✓ Details

Risk description:

The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the

Classification:

CWE: CWE-311

OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure OWASP Top 10 - 2021 : A4 - Insecure Design

Missing security header: Content-Security-Policy

CONFIRMED

port 80/tcp

URL	Evidence	
http://www.itsecgames.com/	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 - 2017: A6 - Security Misconfiguration OWASP Top 10 - 2021: A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

CONFIRMED

port 80/tcp

URL	Evidence	
http://www.itsecgames.com/	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 Referer-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 - 2017: A6 - Security Misconfiguration OWASP Top 10 - 2021: A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

port 80/tcp

URL Evidence

✓ 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 - 2017: A6 - Security Misconfiguration OWASP Top 10 - 2021: A5 - Security Misconfiguration

Server software and technology found

port 80/tcp

UNCONFIRMED (1)

Software / Version	Category
Google Font API	Font scripts
Apache HTTP Server	Web servers

▼ 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 - 2017 : A6 - Security Misconfiguration OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

port 80/tcp

CONFIRMED

URL

Missing: http://www.itsecgames.com/.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 - 2017 : A6 - Security Misconfiguration OWASP Top 10 - 2021 : A5 - Security Misconfiguration

HTTP OPTIONS enabled

port 80/tcp



URL	Method	Summary
http://www.itsecgames.com/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: Allow: GET, HEAD, POST, OPTIONS Request / Response

▼ Details

Risk description:

The only risk this might present nowadays is revealing debug HTTP methods that can be used on the server. This can present a danger if any of those methods can lead to sensitive information, like authentication information, secret keys.

Recommendation:

We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your webserver configuration.

References:

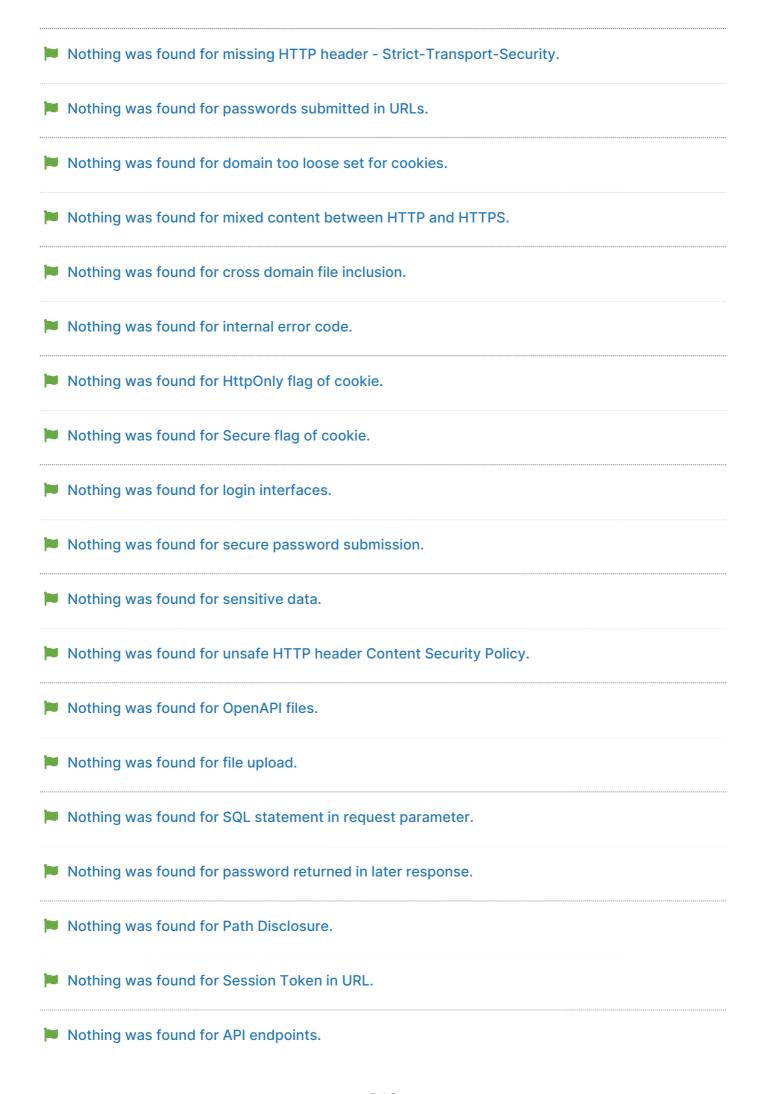
https://techcommunity.microsoft.com/t5/iis-support-blog/http-options-and-default-page-vulnerabilities/ba-p/1504845 https://docs.nginx.com/nginx-management-suite/acm/how-to/policies/allowed-http-methods/

Classification:

CWE: CWE-16

OWASP Top 10 - 2017: A6 - Security Misconfiguration OWASP Top 10 - 2021: A5 - Security Misconfiguration

- Website is accessible.
- Nothing was found for vulnerabilities of server-side software.
- Nothing was found for client access policies.
- Nothing was found for robots.txt file.
- Nothing was found for use of untrusted certificates.
- Nothing was found for enabled HTTP debug methods.
- Nothing was found for directory listing.
- Nothing was found for passwords submitted unencrypted.
- Nothing was found for error messages.
- Nothing was found for debug messages.
- Nothing was found for code comments.



- Nothing was found for emails.
- Nothing was found for missing HTTP header Rate Limit.

Scan coverage information

List of tests performed (39/39)

- ✓ Test initial connection
- ✓ Scanned for missing HTTP header Content Security Policy
- Scanned for missing HTTP header Referrer
- ✓ Scanned for missing HTTP header X-Content-Type-Options
- Scanned for secure communication
- Scanned for website technologies
- Scanned for version-based vulnerabilities of server-side software
- Scanned for client access policies
- Scanned for robots.txt file
- Scanned for absence of the security.txt file
- Scanned for use of untrusted certificates
- ✓ Scanned for enabled HTTP debug methods
- Scanned for enabled HTTP OPTIONS method
- ✓ Scanned for directory listing
- Scanned for passwords submitted unencrypted
- ✓ Scanned for error messages
- Scanned for debug messages
- ✓ Scanned for code comments
- Scanned for missing HTTP header Strict-Transport-Security
- Scanned for passwords submitted in URLs
- Scanned for domain too loose set for cookies
- Scanned for mixed content between HTTP and HTTPS
- Scanned for cross domain file inclusion
- Scanned for internal error code
- Scanned for HttpOnly flag of cookie
- ✓ Scanned for Secure flag of cookie
- Scanned for login interfaces
- Scanned for secure password submission
- Scanned for sensitive data
- Scanned for unsafe HTTP header Content Security Policy
- Scanned for OpenAPI files
- Scanned for file upload
- Scanned for SQL statement in request parameter
- Scanned for password returned in later response
- Scanned for Path Disclosure
- Scanned for Session Token in URL
- Scanned for API endpoints
- Scanned for emails
- Scanned for missing HTTP header Rate Limit

Scan parameters

target: http://www.itsecgames.com/

scan_type: Light authentication: False

Scan stats

Unique Injection Points Detected: 6
URLs spidered: 22
Total number of HTTP requests: 31
Average time until a response was received: 30ms