QUALYS® FREESCAN

Vulnerability Scan

06 July 2015 at 13:00

URL : https://fdago.conceptplusllc.net

OWASP Summary : 9 vulnerabilities found

Pages impacted : 7

Vulnerabilities Detected : 9

Risk percentage by scanned pages

0 Pages Scanned

Impacted Pages: 7 (0%)

Impacted Pages by Category

Injection

0 Impacted Pages

Description

OWASP: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No Injection vulnerabilities were identified with QualysGuard Freescan.

Broken Authentication and Session Management

2 Impacted Pages

QID: 150122 🟥

Cookie Does Not Contain The "secure" Attribute

https://fdago.conceptplusllc.net/

QID: 150123 🟥

Cookie Does Not Contain The "HTTPOnly" Attribute

https://fdago.conceptplusllc.net/

Description

OWASP: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users identities. Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted. Such flaws may allow some or even all accounts to be attacked. Privileged accounts are frequently targeted. To prevent Broken Authentication and Session Management develop and use a single set of strong authentication and session manage controls.

Cross-Site Scripting (XSS)

Not Checked

Description

OWASP: XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc. To prevent XSS the preferred option is to properly escape all untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) that the data will be placed into.

No XSS vulnerabilities were identified with QualysGuard Freescan.

Insecure Direct Object References

2 Impacted Pages (Partially verified)

QID: 150023
Directory Listing

https://fdago.conceptplusllc.net/views/.

https://fdago.conceptplusllc.net/images/.

Description

OWASP: A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. Such flaws can compromise all the data that can be referenced by the parameter. Unless the name space is sparse, it's easy for an attacker to access all available data of that type. To prevent Insecure Direct Object References use per user or session indirect object references. This prevents attackers from directly targeting unauthorized resources. Alternatively include an access control check to ensure the user is authorized for the requested object.

Security Misconfiguration

4 Impacted Pages (Partially verified)

QID: 150023
Directory Listing

https://fdago.conceptplusllc.net/views/.

https://fdago.conceptplusllc.net/images/.

QID: 150079
Slow HTTP headers vulnerability

https://fdago.conceptplusllc.net/

QID: 150086

Server accepts unnecessarily large POST request body

https://fdago.conceptplusllc.net

Description

OWASP: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application. Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise. To prevent Security Misconfiguration use repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down, ensure you are applying software patches and upgrades, ensure a strong architecture and good separation and security between components and consider running scans and doing audits periodically.

Sensitive Data Exposure

1 Impacted Pages (Partially verified)

QID: 150122
Cookie Does Not Contain The "secure" Attribute

https://fdago.conceptplusllc.net/

Description

OWASP: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Missing Function Level Access Control

Not Checked

Description

OWASP: Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

No Missing Function Level Access Control vulnerabilities were identified with QualysGuard Freescan.

Cross-Site Request Forgery (CSRF)

Not Checked

Description

OWASP: OWASP notes: a CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. Attackers can cause victims to change any data the victim is allowed to change or perform any function the victim is authorized to use. To prevent CSRF the preferred option is to include the unique token in a hidden field.

No CSRF vulnerabilities were identified with QualysGuard Freescan.

Using Components with Known Vulnerabilities

Not Checked

Description

OWASP: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

No Using Components with Known Vulnerabilities vulnerabilities were identified with QualysGuard Freescan.

Unvalidated Redirects and Forwards

Not Checked

Description

OWASP: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

No Unvalidated Redirects and Forwards vulnerabilities were identified with QualysGuard Freescan.