https://www.paypal.com/

Scan Time 10/20/2020 6:08:13 PM (UTC+05:30)

Scan Duration 03:20:46:44

Total Requests: 644,179
Average Speed: 1.9r/s

Risk Level:
MEDIUM

Your website is fairly insecure!

There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.

What's the Worst that could Happen?

An attacker could access and control logged in user or admin accounts if attack succeeds

An attacker can abuse a vulnerability on the website to attack individual users of the website. If this attack succeeds, the attacker can hijack their session. This would enable them to take any action that those users can take and to steal their information. For example, an admin might have complete access to the database and the ability to change the website.

Vulnerabilities

Critical	0
High	0
Medium	56
Low	7
Best Practice	5
Information	14
TOTAL	**82**

Vulnerability	Suggested Action
[Possible] BREACH Attack Detected	**Confirmed soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
[Possible] Cross-site Scripting	**Confirmed 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] Internal IP Address Disclosure	**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.
Internal Server Error	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Misconfigured Access-Control-Allow-Origin Header	**Consider fixing after confirmed:** 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.
User Controllable Cookie	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
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.
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.
Subresource Integrity (SRI) 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 (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.
[Possible] UNC Server and Share 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.
An Unsafe Content Security Policy (CSP) Directive in Use	**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.
Crossdomain.xml Detected	**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.
data: Used in a Content Security Policy (CSP) Directive	**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.
ExpressJS 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.
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.
Nonce Usage Detected in Content Security Policy (CSP) Directive	**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.
Robots.txt Detected	**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.
Weak Nonce Detected in Content Security Policy (CSP) Declaration	**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.
Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	**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.
Wildcard Detected in Port Portion of Content Security Policy (CSP) Directive	**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.

Impacts

Severity	Impact
Critical	**An attacker could access and control logged in user or admin accounts if attack succeeds** An attacker can abuse a vulnerability on the website to attack individual users of the website. If this attack succeeds, the attacker can hijack their session. This would enable them to take any action that those users can take and to steal their information. For example, an admin might have complete access to the database and the ability to change the website.
High	**An attacker could access user information sent over the internet or public Wi-Fi or a similar environment** This might include passwords, usernames, and the content of web pages viewed.
Medium	**An attacker could use your website to trick your users into providing them with sensitive information** This could include usernames, passwords and credit card details. This could be done by redirecting users from your site to separate web pages that look like your site.
Low	**An attacker could view information about your system that helps them find or exploit vulnerabilities** This may enable them to take control of your website and access sensitive user and admin information. These issues mostly indicates the lack of the security best practice implementation.
Low	**An attacker could access information that helps them to exploit other vulnerabilities** This information gives them a better understanding of your system.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	55
OWASP 2013	65
OWASP 2017	65
WASC	71
HIPAA	56
ISO27001	81

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.