Attps://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



## Your website is fairly insecure!

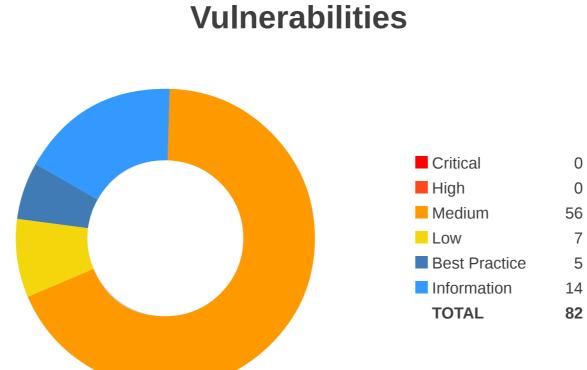
There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.

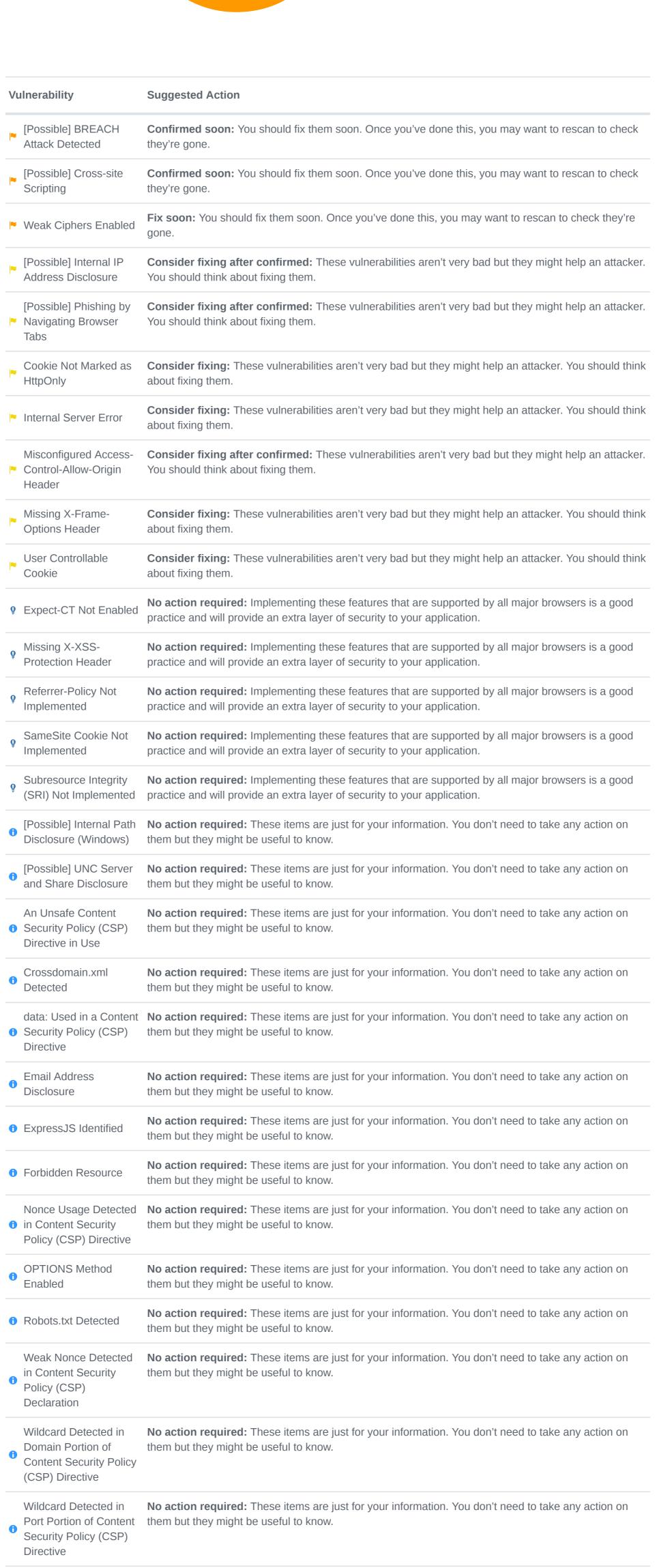
## What's the Worst that could Happen?

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.





## Severity

**Impact** 

**Impacts** 

<b>9</b> 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.	
<b>≈</b> 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.	
<b>≈</b> 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**

56

HIPAA

vendor.

Compliance	Vulnerabilities	
PCI DSS v3.2	55	
OWASP 2013	65	
OWASP 2017	65	
WASC	71	

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