TIC4301

PROJECT

MAYNARD WONG

A0194157X

WEDDING WEB

Guests to Login

Details for Wedding

Leaving Comments

1

PenTest

Discussed Scope of PenTest

2

Login Page

Evaluate vulnerabilities for logging in

1. User
2. Admin

3

Form Page

Evaluate vulnerabilities in the form page

1. Submission
2. Displaying

LOGIN PAGE

SQL Injection

Allows for injection of code into user inputs

Issue 1

Can bypass login as a normal user

Issue 2

Can bypass login as an admin with admin privileges

Post Exploit

With admin privileges, can do malicious things within the site.

FORM PAGE

XSS

Scripts can be injected into the comments form

Issue 1

Reflected XSS can be performed

Issue 2

Stored XSS can be performed

Post Exploit

Can do more malicious things with scripts such as CSRF

Login – SQLi
7.1 (High)

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Form – XSS
5.8 (Med)

CVSS:3.0/AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N

Recommendations

For SQL Injection

1

Sanitise SQL

Use prepared statements to avoid user input SQL from execution

2

Salt & Hash Passwords

Protect passwords from being exploited via SQL injection

Recommendations

For SQL Injection

3

Timeout

Have a time out after a certain number of entries

4

More authentication

Using OTPs or Captcha for entries would prevent constant SQL injection / brute force

Recommendations

For XSS

1

Sanitise User Input

Use htmlspecialchars() to escape scripting language and special characters

Thank You

QUESTIONS?

MAYNARD WONG

A0194157X