Penetration Testing Report

Executive Summary

A series of penetration tests were performed on the HackThisSite.org platform from levels 1-11 to identify security vulnerabilities, determine the impact, document all findings in a clear manner and provide remediation recommendations.

Scope

The scope of this penetration test includes missions from the ‘basic’ category on the HackThisSite.org platform from levels 1-11

Findings

Basic Level 1:

- **Vulnerability Identified**: HTML Source code analysis
- **Key Findings**: The password for this level was hidden within a comment tag within the source code of the site.
- **Recommendations**: Users should be educated on the importance of protecting all sensitive information and preventing putting them in the source code.

Basic Level 2:

- **Vulnerability Identified**: Password Bypass
- **Key Findings**: An empty string password is accepted in order to gain access to the password protected page
- **Recommendations:** Stronger authentication techniques need to be put in place to ensure only those with the authorised access can view the protected content.

Basic Level 3:

- **Vulnerability Identified**: Exposed sensitive file
- **Key Findings**: A sensitive file containing the password is stored within the HTML source code. The PHP file is also named “password.php” which makes it easier for cybercriminals

to find.
- **Recommendations:** Password managers should be used to save passwords

Basic Level 4:

- **Vulnerability Identified**: Personal Details exposed within HTML source code
- **Key Findings**: A script was created to send the password to the email of the user of the account. The email address of the user is stored in plain text within the HTML source mode. This vulnerability can be exploited by changing the username to one that can gain access to in order to retrieve the password.
- **Recommendations:** Similar to Basic level 3, password managers should be utilised to prevent unauthorised access to user accounts. Sensitive information such as email addresses and names also shouldn't be stored in plain text within the HTML source code.

Basic Level 5

- **Vulnerability Identified**: Personal details exposed within HTML source code
- **Key Findings**: Similar to level 4, the email address of the owner of the account is visible within the HTML source code. This means anyone can exploit this vulnerability using JavaScript to alter the email in order to retrieve the password.
- **Recommendations:** Password managers should be used to keep password safe

Basic Level 6

- **Vulnerability Identified**: Weak Encryption Pattern
- **Key Findings**: The encryption pattern for the password is easy for any cybercriminal to crack.
- **Recommendations:** Stronger encryption patterns need to be utilised to prevent unauthorised access

Basic Level 7

- **Vulnerability Identified**: Exposed files containing sensitive information on the server
- **Key Findings**: Basic Linux commands can be used to inject a command to reveal all files on the server.
- **Recommendations:** File permissions need to be set in place with restricted access to ensure sensitive files are not compromised.

Basic Level 8

- **Vulnerability Identified**: Exposed files containing sensible information on the server.
- **Key Findings**: Similar to level 7, basic Linux commands can be injected to reveal sensitive files on the server
- **Recommendations:** File permissions need to be set in place with restricted access to ensure sensitive files are not compromised.

Basic Level 9

- **Vulnerability Identified**: Exposed files containing sensible information on the server.
- **Key Findings**: Similar to level 7 and 8, basic Linux commands can be injected to reveal sensitive files on the server
- **Recommendations:** File permissions need to be set in place with restricted access to ensure sensitive files are not compromised.

Basic Level 10

- **Vulnerability Identified**: Cookie Manipulation
- **Key Findings**: The authentication process can be bypassed by manual altering the value of the cookies within the browser. Once the authorisation value is changed from “no” to “yes”, access is gained
- **Recommendations:** Secure cookie handling methods need to be put in place to prevent unauthorised access

Basic Level 11

- **Vulnerability Identified**: Cyrptographic Weakness
- **Key Findings**: An obvious Elton puzzle is put in place which reveals the password for the account. This puzzle can easily be exploited to gain unauthorised access.
- **Recommendations:** Stronger encryption methods that aren’t easy to guess need to be implemented to protect sensitive information.