セキュリティコンテスチャレンジ演習

クラス　　　　　No.　　　氏名

■今回の課題は、今まで学習したセキュリティの知識を使いセキュリティコンテスト(MBSD Cybersecurity Challenges 2016)の環境を使用して脆弱性の発見をします。

■事前準備

1.次のようなサイトにアクセスし、「Sign Up」からユーザを作成しなさい。

　http://IPアドレス　　　＊IPアドレスは先生から聞いてください。

　名前：各自の名前、ログインID：クラス名番号　パスワード：任意　誕生日：任意



2.Sign Upが終了したら、ログインしなさい。

■各ページでサイトの脆弱性と思われることを記述しなさい。

1.Sign Upのページで、脆弱性を確認しなさい。脆弱性と思われることを記述しなさい。＊複数回答可

|  |
| --- |
| パスワードの文字制限がない  同じログインID、名前が同じアカウントを作成することができる |

2.ログインページでログイン成功時と失敗時のステータスコードについて次の問いに答えなさい。

　＊確認はChromeのデベロッパーツール＞ネットワークで確認する。

　①成功時と失敗時のステータスコード（status code）を記述しなさい。

　　成功時：[　　　　　302　　　　　　]　　失敗時：[　　　　　200　　　　　　]

　②①の値を確認し、問題と思われることをインターネットで調べ記述しなさい。

|  |
| --- |
| ステータスコードが異なるため、フィッシングサイトへ悪用される可能性がある |

3.WriteDiaryのページに移動し、脆弱性を調査しなさい。脆弱性と影響されると思われることを記述しなさい。

脆弱性：

|  |
| --- |
| JavaScript（例＜script＞alet=()＜/script＞）を記述し |

影響：

|  |
| --- |
| XSSなどの攻撃を受けてしまう可能性がある |

対策：

|  |
| --- |
| 入力されたタグを無効化する。htmlspecialcharsなどを利用する |

4.serListページに移動し、脆弱性を調査しなさい。脆弱性と影響されると思われることを記述しなさい。

脆弱性：

|  |
| --- |
| ‘or 1=1 --‘ ですべてのユーザーが表示され、SQLインジェクションが発生する可能性がある。  ＝》 name = ‘’ or 1=1 |

影響：

|  |
| --- |
| 不正なSQL文を実行されることで情報漏えい、改ざんが発生する。 |

対策：

|  |
| --- |
| PHP でプレースホルダを利用してコーディングし直す |

5.http://IPアドレス/phpinfo.phpでアクセスしなさい。次のようなページが表示されるが問題と思われることを記述しなさい。

問題点：

|  |
| --- |
| PHP の設定情報が確認できてしまう。Webサーバやデータベースサーバの名前やバージョンがわかってしまうため、  脆弱性を利用される可能性がある |

対策：

|  |
| --- |
| Phpinfo.php ファイルを削除する |

6.chromeの「デベロッパーツール＞ネットワーク」を使用して、レスポンスヘッダを確認しなさい。

　①PHPバージョン：[　　7.0.11 ]

　②PHPのバージョンを確認することができた、そのため発生すると思われる問題を記述しなさい。

|  |
| --- |
| PHPのバージョンの脆弱性を利用され、攻撃される可能性が発生する |

7.上記の脆弱性以外のもがあれば記述しなさい。

|  |
| --- |
| <meta http-equiv=”refresh” content=0;url=http://転送先URL”>などを書き込むことができるため、ユーザを別のサイト転送させることができる。マルウェアダウンロードサイトやフィッシングサイトへ転送されてしまう。  ＊<meta http-equiv=”refresh” content=0;url=http://転送先URL”> ０秒後にリダイレクトされる  ＊＜script＞location.href = <http://転送URL>;</script>でも可能 |