○○専門学校

チーム○○

MBSD Cybersecurity Challenges

調査結果報告書

2016年11月

* 1. 調査手法に関する説明

ツールを使った・作った、チームメンバの役割分担、調査手法など、脆弱性発見を網羅的・効率的に実施するために行った工夫があれば、アピールしてください。

※上記欄に収める必要はありません。複数ページで記載いただいて問題ありません。

7

* 1. 発見した脆弱性詳細

1. フレンド以外にメッセージが送信可能

* 対象

メッセージ送信

http://10.128.0.21/sendmail.php

* 危険度

**Medium**

* 解説

メッセージ送信画面では、フレンドのみセレクトボックスで選択出来るようになっているため、フレンドにしかメッセージが送信出来ない仕様と推測される。

しかし、ブラウザの開発者ツールなどを利用し次のようにパラメータ値を書き換えることにより、フレンドではないユーザにメッセージを送信出来ることが確認出来た。

▼再現方法

正常パラメータ：to\_id=3 (フレンドのユーザID）

操作パラメータ：to\_id=10 (フレンドではないユーザのID）

▼条件

フレンドではないユーザのIDを推測する必要がある。

しかし、ユーザIDは連番のため、他ユーザのIDを推測することは容易である。

▼該当箇所

(1)　メッセージ送信

* 想定される被害・影響

フィッシングやspam送信などに悪用される可能性がある。

* 対策

サーバ側のアプリケーションにおいて、指定された送信先(to\_id)がフレンドかどうか確認し、フレンドの場合のみメッセージを送信する。フレンドのIDではない場合はエラーにする。

* 備考

特になし。

1. SNMPデフォルトコミュニティ名の付与

* 対象

検出したホスト（ポート番号）

10.128.0.21(161/udp)

* 危険度

**Low**

* 解説

SNMPコミュニティ名にpublicが設定されている。

publicやprivate等の名称は、SNMPコミュニティ名のデフォルト値としてよく利用されるため、容易に推測される。

* 想定される被害・影響

SNMP MIB情報を取得される。

* 対策

SNMPコミュニティ名を推測しにくい名称に変更する。

* net-snmpの場合

snmpd.confを以下の通り変更する。

例）コミュニティ名をmbsd0123に変更する場合

変更前:

com2sec notConfigUser default public

変更後:

com2sec notConfigUser default mbsd0123

* Microsoft Windows Server(SNMP Service)の場合

1. サービスからSNMP Serviceのプロパティを選択する。
2. セキュリティタブ内、「受け付けるコミュニティ名」の

「削除」、「追加」にて任意のコミュニティ名に変更する。

* その他の場合

対策方法の詳細はベンダに確認する。

* 備考

特になし。

1. 脆弱性名

* 対象

機能名

http://www.xxxx.jp/

* 危険度

**High**

* 解説

脆弱性についての解説を記載

* 想定される被害・影響

想定される被害や影響について記載

* 対策

どのような修正を施せば良いか、対策について記載

* 備考

その他上記に当てはまらないが報告すべきことがあれば記載

1. 弱いpasswordを設定できる

* 対象

弱いpassword設定

http://192.168.71.128/register.php

* 危険度

**High**

* 解説

弱いpasswordが推測されやすいから、自分の情報を他人にばれやすい

* 想定される被害・影響

自分のアカウントが他人に不当登録される

* 対策

ユーザーsign up時に、設定されたpasswordをチェックする.弱いpasswordなら、warningして、（英数混合8文字以上）のpasswordしか登録できない

* 備考

その他上記に当てはまらないが報告すべきことがあれば記載

2.他のユーザーのdiaryをすべて読める

* 対象

他のユーザーのdiaryを読める

http://192.168.71.128/readdiary.php?id=

* 危険度

**High**

* 解説

Readdirry.phpページに、URLのreaddiary.php?id=の所に数字を入力して、他のユーザーのdiaryを読める

* 想定される被害・影響

他のユーザーのdiaryはすべて読まれて、個人情報が漏れる

* 対策

Readdiary.phpページの$\_GET[“id”]をチェックする。$\_GET[“id”]が空の場合は何をやらずにindex.phpに戻る.

Readdiary.phpページの$diaryのwriter\_user\_idをチェックする。writer\_user\_idが自分のidじゃない場合は何をやらずにindex.phpに戻る.

変更前：

$diary = Diary::getDiary ( $\_GET ["id"] );

$writer = $diary->write\_user ();

if ($diary) {

$title = $diary->title == "" ? "(無題)" : $diary->title;

printHeader ();

変更後：

$diary = Diary::getDiary ( $\_GET ["id"] ? $\_GET ["id"] : -1);

If($diary){

$writer = $diary->write\_user ();

If($user->id != $write){

header ( "Location: ./index.php" );

exit ();

}

$title = $diary->title == "" ? "(無題)" : $diary->title;

printHeader ();

}

* 備考

その他上記に当てはまらないが報告すべきことがあれば記載

3.他のユーザーのdiaryをすべて編集できる

* 対象

他のユーザーのdiaryを編集できる

Readdiary.phpの編集ボタン

* 危険度

**High**

* 解説
* 想定される被害・影響
* 対策
* 備考

その他上記に当てはまらないが報告すべきことがあれば記載