平成 25 年度 秋期 情報セキュリティスペシャリスト

＜午後 I　解答･解説＞

＜問1＞ Web システムのクロスサイトスクリプティング対策

■設問 1

〔試験センターによる解答例〕

(1)

パターン 1 : ②

パターン 2 : ②

パターン 3 : ②

パターン 4 : ③

(2) a : 4

(3) b : 18

(4) "http://"又は"https://"で始まる URL だけを許可する。(36 字)

(1)

表 2 の検出パターン 1,2 については,「脆弱性ありと判定する基準」に「……検査文字列がエスケープ処理などを行われずに出力される場合,脆弱性ありと判定」とあることから,表 1 の②の不備を検出できるものであることがわかる。また,検出パターン 3 についても同様に「……検査文字列をエンコードせずに挿入したときエスケープされずに出力される場合,脆弱性ありと判定」とあることから,②の不備を検出できるものであることがわかる。

外部からの入力データやデータベースから読み込んだデータ,演算によって生成した文字列等から HTML を生成する Web アプリケーションにおいて,処理の対象となる文字列中に "<", ">", "&" などのメタキャラクタが存在した場合,HTML 出力時にそれらに対するエスケープ処理を確実に行うとともに,HTML タグの属性値についてはダブルクォート（二重引用符）で囲む必要がある。

検出パターン 4 については,「脆弱性ありと判定する基準」に「……特定の URI 属性（src, action, background, href, content）に検査文字列が出力される場合,脆弱性ありと判定」とあることから,表 1 の③の不備を検出できるものであることがわかる。

URL には "http://" や "https://" 以外に,"javascript:" などの形式で始まるものもある。外部からの入力データ等から「<a href="リンク先の URL">」のような形式で HTML を出力する Web アプリケーションの場合,リンク先の URL として "javascript:" 等の文字列が入力されると,不正なスクリプトを埋め込まれてしまう可能性がある。"href", "src"等の URL を出力する場合には,"http://" 又は "https://" で始まるものだけを許可するようにする必要がある。

(2) 図 1 のプログラムでは,7～9 行目で "name"（物件名称）, "loc"（地区名）, "url"（URL 情報）の三つのパラメタを取得し,各々 "rqName", "rqLoc", "rqUrl" に格納している。格納したパラメタは 18～20 行目で HTML として出力しているが,その際に "escapeHTML"メソッドで HTML の特殊文字をエスケープ処理しているため,検出パターン 1～3 は該当しない。しかし,18 行目で "rqUrl" から"href"属性を出力する際に,出力する URL 文字列のチェックを行っていないため,検出パターン 4 の検査では脆弱性ありと判定されることになる。

(3) 上記(2)で解説した通り, b に該当するのは 18 行目である。

(4) 上記(1)で解説した通り,URL を出力する場合には,**"http://" 又は "https://" で始まるものだけを許可する**ようにする必要がある。

■設問２

〔試験センターによる解答例〕

(1)

c：17

d：24

※c と d は順不同。

(2) e：②

(3) f：GET パラメタ及び POST パラメタ（17 字）

(4) g：escapeHTML

(5) h：26

(6) i：④

(7) j：out.print("document.form1.loc.value");

(1) 設問 1 の(1)で解説したように,XSS 対策においては,外部からの入力データやデータベースから読み込んだデータ,演算によって生成した文字列等から HTML を生成する際に,HTML 出力時にそれらに対するエスケープ処理を確実に行う必要がある。図 3 のプログラムにおいては,データベースから取得して HTML として出力する文字列である,"rsKey","rsLoc" がその対象となる。"rsKey" については 17 行目,"rsLoc "については 24 行目で各々エスケープ処理することなく HTML として出力しており,対策が不十分である。

(2) 上記(1)で解説した通り,**エスケープ処理の不備**であるから,表 1 の実施項目②に該当する。

(3) 上記(1)で解説した通り,図3のプログラムではデータベースから取得して HTML として出力する文字列において XSS 対策の不備があったが,社内検査ではこの脆弱性を検出できなかった。これは,表 2 の「検査文字列を入力する場所」にあるように,検査対象を**「GET パラメタ及び POST パラメタ」**に限定しているからである。

(4) 図 1 の注記にあるように,**"escapeHTML"**が HTML の特殊文字 5 文字のエスケープ処理を行うメソッドとして定義されており,これを適用すべきである。

(5) 図 4 のプログラムでは,14 行目から 30 行目で HTML 中にスクリプトを出力している。図 2 の④で F 社より「スクリプト要素の内容を動的に生成している。命令として解釈される可能性がある」と指摘を受けていることから,これに該当する箇所を探すと,26 行目であることがわかる。

(6) 上記(5)で解説した通り,**スクリプト要素の動的生成**であるから,表 1 の実施項目④に該当する。

(7) 図 4 の 22 行目と 23 行目の間にあるコメントを参考にプログラムを読んでいくと,26 行目では,"【"と"】"の間に表示する地区名を出力していることがわかる。図 4 の 47 行目,48 行目にあるように,変数"rqLoc"はフォーム"form1"の hidden フィールド"loc"の"value"にセットされている。したがって,26 行目でスクリプトを動的生成しないように修正するには,変数"rqLoc"ではなく,フォーム"form1"の hidden フィールド"loc"の値("value")を用いて,**「out.print("document.form1.loc.value");」**とすればよい。記述においては,18 行目,20 行目等が参考になるだろう。

＜問2＞ スマートフォンアプリケーション

■設問 1

〔試験センターによる解答例〕

(1) 秘密情報ではないという特性（13 字）

(2) イ

(3) スマホアプリをリバースエンジニアリングする。(22 字)

(1) 利用者認証には,生体情報による認証,IC カード等の所有物による認証,パスワード,暗証番号等の秘密情報による認証等,様々な方式がある。いずれの方式においても,セキュリティを確保するためには,当該利用者のみが知り得る秘密情報であること,もしくは当該利用者のみが利用できることが求められる。

IMEI は,あくまでも端末をユニークに識別するための番号であるため,通常端末本体に記載されているほか,端末の設定メニューや,電話番号「*#06#」をコールすることによって確認できる機種も多い。したがって,IMEI は秘密情報とはいえず,利用者を認証するための情報として使用するのは不適切である。

(2) 鍵付きハッシュ関数に該当するのは,**HMAC**（Keyed-Hashing for Message Authentication Code）である。HMAC は,ハッシュ値の計算時に秘密鍵の値を加えることで,固有のハッシュ値を求められるようにする。

(3) スマホアプリ内に格納された鍵を取り出す手法としては,**リバースエンジニアリング**が有効である。リバースエンジニアリングとは,ソフトウェアやハードウェアなどを分解したり,動作を解析することで,その構造や仕様,ソースコードなどを明らかにすることである。サーバ側にプログラムが存在する WebAP などと異なり,スマホアプリはその仕組み上,プログラムが端末上に存在するため,リバースエンジニアリングがしやすいという特徴がある。加えて,多くのスマホアプリが,動作環境に依存しない Java や.NET の中間コードとなっていることも,リバースエンジニアリングを容易にしている。

専用のツール等を用いてアプリケーションを難読化することで,リバーエンジニアリングへの一定の対抗策となるが,あくまでも解析を難しくするものであり,完全な対策とはならない。したがって,暗号化やハッシュ化で用いる鍵などの重要な情報はアプリ内には格納せず,リバースエンジニアリングが行われたとしてもセキュリティ上の問題が発生しないようにしておく必要がある。

■設問 2

〔試験センターによる解答例〕

スマホアプリでメールアドレスを選択して,それを WebAP に送信する。(34 字)

〔予約案内サービスの問題〕の冒頭にあるように,予約案内サービスは,利用者がスマートフォンのアドレス帳から選択したパーティの参加予定者に対し,予約した日時,店舗の情報をメールで通知するというものである。そのためにアドレス帳の全件データを WebAP に送信するという仕様は,説明責任の点だけでなく,情報漏えいのリスクを高め,無用な通信データを増やすことにもなり,多くの問題がある。これを改善し,アドレス帳の全件データ送信を行わずに済むようにするには,**スマートフォンのアドレス帳からメールアドレスを選択する部分をスマホアプリ側で行うようにし,選択済みのメールアドレスのみを WebAP に送信する**ようにすることである。

■設問３

〔試験センターによる解答例〕

(1)

① パラメタ：YoyakuCode

内容：利用者 W の YoyakuCode

② パラメタ：DateTime

内容：送信時とのずれが 5 分未満の時刻

※①と②は順不同。

(2) YoyakuCode の値が AuthKey に対応する予約明細コードでないときはアプリケーションエラーを返す。(53 字)

(1) まず,表 2 で「WebAP から受信した内容」がエラーとなっていないものに着目すると,次の三つの操作内容であることがわかる。

① AuthKey パラメタの値を別利用者の値に変更

→YoyakuCode が 201310000034 の予約情報の表示

② YoyakuCode パラメタの値を 201310000071 に変更

→YoyakuCode が 201310000071 の予約情報の表示

③ DateTime パラメタの値を現在から 4 分前の時刻に変更

→YoyakuCode の値に該当する予約情報の表示

図 4, 図 5 より,利用者 V, 利用者 W が予約情報を表示した際のリクエストにおける YoyakuCode は,それぞれ"201310000034", "201310000071"であることから,利用者 V が利用者 W の予約情報を取得できるのは,YoyakuCode,DateTime の二つのパラメタを変更した場合であることがわかる。

図 3 の(d)にあるように,YoyakuCode パラメタについては,値が DB サーバに保持されていれば該当する予約情報を返す仕様になっているため,同パラメタの値を「利用者 W の YoyakuCode」に変更すればよい。

また,DateTime パラメタについては,図 3 の(e)にあるように,サーバ側の時刻とのずれが 5 分未満であれば該当する予約情報を返す仕様になっているため,同パラメタの値を「送信時とのずれが 5 分未満の時刻」などとすればよい。

(2) 他人の予約情報を取得できてしまう主な原因は,誰からのリクエストであろうと関係なく,YoyakuCode の値が DB サーバに保持されてさえいれば該当する予約情報を返してしまうことにある。これを改善するには,利用者情報と予約情報の整合性をチェックし,一致する場合のみ予約情報を返すようにする必要がある。具体的には,リクエストされた YoyakuCode の値が,AuthKey に対応する予約明細コードでない場合には,アプリケーションエラーを返す仕様を追加することが考えられる。

＜問3＞ パブリッククラウドサービスの安全な利用

■設問 1

〔試験センターによる解答例〕

方法：第三者自身の携帯電話メールアドレスを指定して申請（24 字）

対策：管理責任者が申請者に直接申請の事実を確認する。(23 字)

図 2 の「C サービスの利用者 ID 登録手順案」では,利用者が指定した携帯電話メールアドレスに対し,管理責任者は本人確認や内容の適切性確認等を行うことなく仮パスワードを送信している。そのため,第三者が利用者になりすまし,第**三者自身の携帯電話メールアドレスを指定して申請**することで,容易に仮パスワードを入手することが可能である。

本人確認については,申請メールを受け取った時点で,**管理責任者が申請された利用者 ID**(会社が付与したメールアドレス）**宛てにメールを送り,申請の事実を確認する**とよい。

■設問 2

〔試験センターによる解答例〕

理由：クッキーが有効である間，不正使用が可能だから（22 字）

対策：C サービスの認証に使用している携帯電話は，紛失や盗難時の届出を義務化し，届出を受けたら直ちに C サービスのパスワードを変更する。（63 字）

図 3 の(6)にあるように，ログインに成功した利用者 ID には，有効期間が 90 日のクッキーが発行され，ブラウザに保存される仕組みとなっている。そして，それ以降は利用者 ID とパスワードでログインし，有効期間内のクッキーを提示すれば C サービスを利用することができる。そのため，個人の携帯電話が盗まれ，かつ，利用者 ID とパスワードが推測されてしまった場合には，**クッキーが有効である間，C サービスを不正に使用することが可能**となる。

〔C サービスの認証の強化〕にあるように，P 社貸与の携帯電話は，盗難，紛失があった場合には必ず総務部に連絡することになっており，盗難届，紛失届を受けると，総務部は速やかに対応している。一方，個人所有の携帯電話については，このような手続きが義務化されていないため，盗難，紛失の事実を P 社が認識することができず，被害が拡大するおそれがある。P 社貸与，個人所有にかかわらず，C サービスの認証に使用している携帯電話は，**紛失や盗難時の P 社総務部への届出を義務化し，届出を受けたら直ちに C サービスのパスワードを変更する**ことで，C サービス不正使用のリスクを最小化することができる。

■設問３

〔試験センターによる解答例〕

a：プロジェクト資料を定期的にファイルサーバへバックアップ（27 字）

b：バックアップしたプロジェクト資料を共有（19 字）

c：データの移行方法（8 字）

a：C サービスのサーバが被災し，2 週間にわたって停止するような事態が生じた場合に，C サービスが停止してから 24 時間後にプロジェクト資料を使う業務を再開するために事前準備として実施しておくことが問われている。表 2 の「想定シナリオが現実化してから実施すること」に「ファイルサーバを用いて，……」とあることからもわかるように，このような事態が生じた場合には，P 社のファイルサーバを活用すればよい。そのためには，事前準備として，**プロジェクト資料を定期的にファイルサーバへバックアップしておく**必要がある。

b:プロジェクト資料を使う業務を再開するためにファイルサーバを用いて行うことであるから，［b］には，事前準備として**バックアップしておいたプロジェクト資料を関係者に共有する**ことが該当する。

c ：C サービスが 1 か月後にサービス終了となる場合に事前準備として実施することが問われている。表 2 の「想定シナリオが現実化してから実施すること」に，「C サービスのデータを代替サービスに移行する」とあることから推測されるように，［ c ］には**「データの移行方法」**が該当する。