平成 28 年度 春期 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 システムの開発

■設問 1

〔試験センターによる解答例〕

(1) a：wama.example.jp

(2) kensho.m-sha.co.jp

(3) b：エ

(4) c：https://kensho.m-sha.co.jp/Gamen2_2

　　d：keyword

(5) 懸賞メンバとしてログインしている状態（18 字）

(1)改変された画面 2-2 のスクリプトである図 6 を確認する。画面上のログインボタンが押されると，form タグの action 属性で指定した URL（“https://wana.example.jp/login”）に入力値が送信される。解答するのはホスト名の FQDN（Fully Qualified Domain Name）であるから，“**wana.example.jp**”である。

(2)問題文に「図 1 中の画面の URL のホスト部は，全て kensho.m-sha.co.jp であり，…」「例えば，攻撃者は，URL パラメタである keyword に攻撃用の文字列として（中略）を組み込んだ https://kensho.m-sha.co.jp/Gamen2_2 へのリンクを含む電子メールを作成し，被害者に送付します」とあることからわかるように，Web ブラウザのアドレスバーに表示される URL のホスト部の FQDN は，“**kensho.m-sha.co.jp**”である。

(3)攻撃者の Web サーバ上のコンテンツ内のスクリプトで懸賞システムのコンテンツを参照することができない，ということから，該当するのは“**Same Origin Policy**”である。

“Same Origin Policy”とは，悪意のあるサイトに対し，不用意に Cookie や個人情報等を送ってしまわないようにするなど，セキュリティを確保するための仕組みであり，ドメインの異なるサイトにリクエストを送信できないように制限されている。

©2016 Takayuki Uehara

(4)N さんの説明に，「攻撃者は，URL パラメタである keyword に攻撃用の文字列として（中略）を組み込んだ https://kensho.m-sha.co.jp/Gamen2_2 へのリンクを含む電子メールを作成し，…」とあるように，図 7 の攻撃用 HTML ソースコードでは，4 行目で URL”https://kensho.m-sha.co.jp/Gamen2_2" の ”keyword" パラメタに “https://wama.example.jp/getFrame.js” というスクリプトをセットしている。したがって，［ c ］には “**https://kensho.m-sha.co.jp/Gamen2_2**”，［ d ］には “**keyword**” が入る。

(5)図 1 の注記 2 に「ログインしていない状態で画面 3-3～画面 3-9 の URL を指定した場合は，画面 1-1 へリダイレクトされる」とあることから，ログインしていない状態では下線①の窃取は成功しないことがわかる。したがって，下線①の窃取が成功するには，被害者が**懸賞メンバとしてログインしている状態**でなければならない。

■設問２

〔試験センターによる解答例〕

(1) e：ランダムな値（6 字）

f：hidden（6 字）

(2) ウ

(1) CSRF の主な対策は次の通りである。

・POST メソッドを使用し，hidden フィールドにランダムな値をセットする

画面を遷移する前に，擬似乱数等によって生成したランダムな値を hidden フィールドにセットする。画面遷移時に受信したデータが，前画面でセットしたランダムな値と一致した場合にのみ処理を実行する。これにより，正規の画面を経ていないリクエストを排除することが可能となる。なお，Referer 情報からランダムな値が漏えいしないように，この一連の処理には POST メソッドを使用する必要がある。

したがって，［ e ］には「**ランダムな値**」，［ f ］には「**hidden**」が入る。

上記のほか，次のような対策もある。

・重要な処理の直前でパスワードを入力させる

重要な処理の前にパスワードの入力を求め，入力されたパスワードが正しい場合のみ処理を実行するようにする。これにより，パスワード入力のないリクエストを排除することが

©2016 Takayuki Uehara

可能となる。

・Referer 情報を用いてリンク元の正当性を確認する
　Referer 情報を確認することで，不正なサイトから送られてきたリクエストを排除することが可能となる。ただし，クライアントの設定などで Referer 情報を送付しないようにしている場合には，正当なリクエストであっても排除されてしまうことになる。

・重要な操作を行った後で，その内容を登録アドレスにメール送信する
　CSRF の被害を防ぐことにはならないが，攻撃があった事実を利用者に気付かせることができる。ただし，メールの本文に重要な情報を入れないようにする等の注意が必要である。

(2) CSRF は，ユーザ認証やセッション管理の不備を突いて，サイトの利用者に，不正な処理要求を行わせる手法である。したがって，前の画面で入力されたデータ等をパラメタとして引き渡し，データの更新を伴うようなアプリケーションを実行させる画面遷移において対策が必要である。前の画面で入力されたデータをそのまま表示したり，処理実行後に元の画面に復帰したりするような画面遷移では対策は不要である。
　図 1 で g か h に入る記号は，(い)，(く)，(さ)，(し)，(す)，(せ)である。図 1，表 1 にあるように，これらの中で，(さ)と(せ)については画面遷移時に受け渡すパラメタはなく，次の画面表示や元の画面に復帰するのみであるため，対策は不要である。また，(い)については前画面で入力された「キーワード」をパラメタで受け渡して検索処理を実行するが，データの更新はなく，検索結果を表示するのみであるため，対策の必要性は低いといえる。一方，入力データで修正を実行する(す)では対策が必要である。この結果から，適切な組合せは**ウ**である。

■設問３

〔試験センターによる解答例〕

(1) 攻撃者は，画面 2-1 を経由させずに直接画面 2-2 へアクセスさせるから（34 字）

(2) i：サーバサイド（6 字）

(3) j：URL（3 字）

(1)〔XSS 脆弱性の説明と修正〕にあるように，**攻撃者は，画面 2-1 を経由させずに**，攻撃用の文字列を“keyword”パラメタに組み込み，**直接画面 2-2 にアクセスさせる**ことにより，

©2016 Takayuki Uehara

任意のスクリプトを実行させる。そのため，画面 2-1 で入力値を検査しても XSS 攻撃を防ぐことはできない。

(2)下線②のように，Web ブラウザ側のスクリプトなど，クライアントサイドで稼働するプログラムで入力値を検査しても，攻撃者に回避されてしまう可能性がある。これを防ぐためには，**サーバサイド**で稼働するプログラムで入力値が正当かどうかを検査する必要がある。

(3)HTML の a タグの href 属性，img タグの src 属性等，**URL** を出力する箇所に“javascript:xxxx”のようにスクリプトがセットされると，そのまま実行されてしまう可能性がある。そのため，そうした箇所では“javascript”などの文字列を排除する必要がある。

＜問 2＞ DMZ 上の機器の情報セキュリティ対策

■設問 1

〔試験センターによる解答例〕

a：オープンリレー（7 字）

b：送信ドメイン（6 字）

a：メールサーバがエンベロープの宛先メールアドレスのドメイン名が U 社ドメイン以外のメールであっても転送する設定になっていると，迷惑メールの送信に悪用されてしまう可能性がある。このような設定や状態を「**オープンリレー**」もしくは「第三者中継」と呼ぶ。また，オープンリレー状態となっているメールサーバは「オープンリレーサーバ」と呼ばれる。

b：迷惑メール対策として普及している SPF，DKIM（DomainKeys Identified Mail）等の技術は，「**送信ドメイン認証**」と呼ばれる。

■設問 2

〔試験センターによる解答例〕

c：リフレクション（7 字）

オープンリゾルバとは，問合せ元のアドレスや問合せ対象ドメインの制限なく，名前解決要求に応じる DNS キャッシュサーバのことである。オープンリゾルバ防止機能が適切に設

©2016 Takayuki Uehara

定されていないと，DNS リフレクション攻撃や DNS キャッシュポイズニング攻撃の被害を受けやすくなる。DNS リフレクション（反射）攻撃（「DNS リフレクター攻撃」とも呼ばれる）は，他のサイトを攻撃するために，DNS キャッシュサーバを攻撃パケットの踏み台として悪用する手法である。この攻撃により，踏み台となった DNS サーバ自体の負荷が高まり，サービス不能状態となる場合もある。応答メッセージを増幅させて負荷を高めることから「DNS amp」とも呼ばれる。

■設問３

〔試験センターによる解答例〕

(1) d：送信元ポート番号（8 字）

(2) e：外部メールサーバ（8 字）

影響：取引先宛てのメールを，攻撃者が用意したメールサーバに転送してしまう。（34 字）

(3) パス名を送信しないという仕様（14 字）

(1)DNS キャッシュポイズニング攻撃とは，ターゲットとなる DNS キャッシュサーバからの名前解決要求に対し，悪意ある DNS キャッシュサーバが，正当な DNS キャッシュサーバからの応答が返る前に，正常な応答に加えて悪意あるサイトに誘導するための不正な名前解決情報も付加して返すことで，DNS のキャッシュに登録させる攻撃である。そのようにしてキャッシュが汚染された DNS キャッシュサーバを利用すると，意図せず悪意あるサイトに誘導されてしまう可能性がある。

DNS キャッシュポイズニング攻撃を成功させるためには，攻撃者は，送信元ポート番号（名前解決要求の送信元ポート番号であり，応答時の宛て先ポート番号となる），トランザクション ID を本来の応答レコードと合致させる必要がある。そのため，UDP ヘッダの**送信元ポート番号**のランダム化設定を行うことが有効な対策となる。しかし，こうした対策が行われておらず，送信元ポート番号，宛て先ポート番号ともに 53 番に固定する設定となっていることも多く，DNS キャッシュポイズニング攻撃を容易にさせている。

(2)図 4 の攻撃の結果，プロキシサーバの DNS キャッシュに保存された不正な MX レコードを参照し，メール配送に影響を生じさせる機器は，「**外部メールサーバ**」である。図 4 にあるように，攻撃者は取引先ドメイン名の不正な MX レコードをプロキシサーバの DNS キャッシュに保存している。その結果，外部メールサーバが取引先宛てのメールを転送する際に不正な MX レコードを参照し，本来の転送先ではなく，**攻撃者が用意したメールサーバ**

©2016 Takayuki Uehara

にメールを転送してしまうことになる。

(3) CONNECT メソッドの仕様上，パス名を含めた URL 全体は送信されず，ホスト名部分（FQDN）だけが送信される。そのため，プロキシサーバを経由する HTTP over TLS 通信では，URL フィルタリングがホスト単位となる。

■設問 4

〔試験センターによる解答例〕

変更箇所：ブラックリスト 3（8 字）

変更内容：scanner@u-sha.co.jp を登録する。（25 字）

表 2 の「複合機」にある通り，複合機は送信メールアドレスとして複合機用メールアドレス（scanner@u-sha.co.jp）を用い，スキャンしたイメージを添付したメールを，イメージを作成した本人又は同じ部署の従業員のメールアドレスに送信する。複合機が当該メールを送信するのは U 社の本社 LAN からである。複合機用メールアドレスを詐称したインターネットからのメールを防ぐには，外部メールサーバのフィルタリング機能を活用すればよい。攻撃者はメール受信者を騙すために複合機用メールアドレスを詐称するので，当該アドレスをセットするのはエンベロープの送信者アドレスではなく，受信者の目に触れるメールヘッダの送信者メールアドレスである。したがって，外部メールサーバの**ブラックリスト 3** に**“scanner@u-sha.co.jp”を登録**すればよい。

＜問 3＞ スマートフォンアプリケーションの試験

■設問 1

〔試験センターによる解答例〕

(1) a：S サーバ

(2) b：試験用 Web サーバ

(3) c：試験の実施よりも前の日時（12 字）

(4) d：S アプリがサーバ認証エラー画面を表示する。（21 字）

(1)，(2)図 2 に，「S アプリ内に，S サーバの FQDN が組み込まれている」とあり，図 3 の

©2016 Takayuki Uehara

サーバ証明書の検証試験環境では，S サーバに代わって試験用 Web サーバが接続先となることから，［ a ］には「**S サーバ**」，［ b ］には「**試験用 Web サーバ**」が入る。

(3)表 2 の項番 2 では，サーバ証明書が有効期間内でないことの検出を行う。したがって，サーバ証明書の「有効期間の終了」には，**試験の実施よりも前の日時**を設定する必要がある。

(4)表 2 の各試験において期待される結果は，「S アプリがサーバ証明書を認証できない」である。図 2 にあるように，S アプリが S サーバを認証できなかった場合は，サーバ認証エラー画面を表示する仕様になっている。したがって，［ d ］には「**S アプリがサーバ認証エラー画面を表示する。**」が入る。

■設問２

〔試験センターによる解答例〕

(1) e : 1，2，3，4

f : 3

g : 1

(2) SSID，暗号化方式と事前共有鍵に，公衆無線 LAN で使用されているものを設定する。（41 字）

(1)

e : 発行者の検証不備があると，表 3 で発行者が「攻撃者が準備するプライベート認証局」であっても認証が成立する。さらにサブジェクトのコモンネームの検証不備があると，表 3 でサブジェクトのコモンネームが「攻撃者が所有しているドメインを使用した FQDN」や「上記二つ以外の FQDN」であっても認証が成立する。したがって，表 4 の項番 1 では，表 3 の **1，2，3，4** の全ての証明書で中間者攻撃が成功する。

f : 発行者の検証不備があると，表 3 で発行者が「攻撃者が準備するプライベート認証局」であっても認証が成立するが，サブジェクトのコモンネームの検証不備がなければ，サブジェクトのコモンネームが「S サーバの FQDN」の場合のみ認証が成立する。したがって，表 4 の項番 2 では，表 3 の **3** の証明書のみ中間者攻撃が成功する。

g : サブジェクトのコモンネームの検証不備があると，表 3 でサブジェクトのコモンネームが「攻撃者が所有しているドメインを使用した FQDN」や「上記二つ以外の FQDN」であ

©2016 Takayuki Uehara

っても認証が成立するが，発行者の検証不備がなければ，発行者が「スマートフォンに対応している商用認証局」の場合のみ認証が成立する。したがって，表 4 の項番 3 では，表 3 の **1** の証明書のみ中間者攻撃が成功する。

(2)無線 LAN に自動的に接続するためには，アクセスポイントの SSID を認識しており，かつ，使用している暗号化方式（WEP，WPA，WPA2 など），そして各々の暗号化方式で使用する事前共有鍵を設定しておく必要がある。したがって，W-AP の **SSID，暗号化方式，事前共有鍵に，公衆無線 LAN で使用されているものを設定**すれば，公衆無線 LAN の利用者のスマートフォンを自動的に W-AP に接続させることができてしまう。

©2016 Takayuki Uehara