平成 27 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 サイトの脆弱性と対策

■設問 1

〔試験センターによる解答例〕

(1) 画面 B

(2) 暗号化されない HTTP 通信において，セッション ID が送信されるから（33 字）

secure 属性を設定すると，HTTPS（SSL/TLS）で通信している場合のみ Cookie を送出する。逆に secure 属性を設定していないと，暗号化されていない HTTP 通信においても Cookie が送信されるため，第三者にセッション ID を盗聴されるリスクがある。図 1 を見ると，試験用サイトの画面において HTTP で通信しているのは**画面 B** である。そのため，画面 B に遷移するときにセッション ID を盗聴されるリスクがある。

■設問 2

〔試験センターによる解答例〕

(1) a：%0d%0a%0d%0a

(2) b：ウ

(3) c：・出力文字列に改行コードがあるとエラー画面を出力（23 字）

・出力文字列の改行コード以降の文字列を削除（20 字）

(1) HTTP のメッセージヘッダとメッセージボディの境界は空行（二つの連続した改行コード）で識別する仕様となっている。HTTP ヘッダインジェクションとは，ユーザの入力データをもとに HTTP メッセージのレスポンスを生成する Web アプリケーションに対し，任意の場所に空行を挿入して不正なスクリプトを実行させたり，任意のヘッダフィールドを追加したりする攻撃手法である。

図 8 の ASCII 文字一覧より，図 7 では，

"<html><body><script>alert("1")</script></body><html>"

というスクリプトであることが分かる。HTTP ヘッダインジェクションの脆弱性を突いてこれを実行させるには，上記文字列の前に空行を挿入すればよい。空行は二つの連続した改行コード（CRLFCRLF）であるため，これを図 8 に従って URL エンコードすると**"%0d%0a%0d%0a"**となる。

(2) 攻撃者が指定した任意のスクリプトをクライアント側で実行する攻撃は，**クロスサイトスクリプティング**である。

(3) HTTP ヘッダインジェクションへの対策としては，問題文に示されているもののほか，HTTP レスポンスヘッダを生成する**出力文字列に改行コードが含まれていた場合にエラーメッセージを出力**したり，**改行コード以降の文字列を削除**したりするなどの処理を実装する方法がある。

■設問３

〔試験センターによる解答例〕

(1) d：09 又は 17

e：27

※d，e は順不同

(2) f：01234

(3) 攻撃者 J が取得したセッション ID で利用者 K にログインさせているから（33 字）

(4) g：新しいセッション ID によるセッションを開始する（23 字）

(1) セッションフィクセーションとは，Web アプリケーションにおけるセッションハイジャックの手法の一つであり，「セッション ID の固定化攻撃」とも呼ばれる。セッションフィクセーションは，既に確立されているセッションをハイジャックするわけではなく，ターゲットユーザに対して攻撃者が生成したセッション ID を含む不正な URL を送りつけることで意図的にセッションを確立させ，そのセッションをハイジャックするというものである。
会員制のサイトなどで，ログイン画面を表示した時点でセッション ID が発行され，ログイン後も同じセッション ID を使用する仕様になっているような場合には，攻撃者がセッション ID を容易に入手可能であるため，この攻撃が成立する可能性がある。
図 6 の HTTP ヘッダを見ると，行番号 09, 17, 27 の 3 か所にセッション ID があるが，いずれも同じ値になっている。注記にあるように，これらのセッション ID は下記で使用されていることが分かる。

①リクエスト X とレスポンス X は最初に画面を表示した際の HTTP ヘッダ
②リクエスト Y とレスポンス Y は画面 A から画面 B に遷移した際の HTTP ヘッダ
③リクエスト Z とレスポンス Z は画面 C から画面 D に遷移した際の HTTP ヘッダ

これらのうち，①と②が同じセッション ID であることは問題ないが，③はログイン後の商品取引画面であるため，このままではセッションフィクセーションが成立する可能性がある。したがって，[d]，[e] には，"**09** 又は **17**", "**27**"（順不同）が入る。

(2) Cookie の属性の一つに"domain"があり，その Cookie が有効となるドメイン名を「.」から始まる形式（例：.shoeisha.co.jp）で指定する。指定があった場合は，そのドメイン名が含まれていることが Cookie を送出する条件となり，サブドメイン名やホスト名が異なる場合であっても Cookie の共有が可能となるが，セキュリティ確保のため，「.co.jp」「.com」「.net」などの指定は無効となる。
Cookie Monster Bug とは，一部のブラウザでこの"domain"の指定が正しく機能しないというバグであり，これにより，セッションフィクセーションやクロスサイトリクエストフォージェリ（CSRF）といった攻撃を成立させやすくしてしまう可能性がある。
前述のように，セッションフィクセーションでは，攻撃者は自分が取得したセッション ID を含む不正な URL を利用者に送りつけることで意図的にセッションを確立させ，そのセッションをハイジャックするというものである。したがって，[f] には"**01234**"が入る。

(3) 攻撃者 J は，**自分が取得したセッション ID"01234"で利用者 K にログインさせている**ため，後から同じセッション ID を用いることで，利用者 K になりすまし，本来はアクセス権限がない画面にアクセスできるようになる。

(4) ログインの前後で同じセッション ID を使い続けていると，セッションフィクセーションが成立する可能性が高まる。そのため，ユーザがログインに成功した後に**新たなセッション ID を発行し，それを用いてセッションを開始する**ようにすることが有効な対策となる。

＜問2＞ 情報漏えいインシデントの調査

■設問 1

〔試験センターによる解答例〕

(1) FW のログで当該通信の記録を確認する。

(2) a：FW

b：プロキシサーバ

c：MAC アドレス

(1) 問題文の FW に関する説明において，「許可した通信，拒否した通信ともにログを取得するように設定し，取得したログは全てログ管理サーバに送信している」とあることから，**FW のログで当該通信の記録を確認**すればよいことが分かる。

(2)

a：問題文の FW に関する説明に「NAPT 機能を使用している」とある。NAPT（Network Address and Port Translation）とは，パケットの中継時に IP アドレスとポート番号の両方を変換する方式である。NAPT を使用すると，FW を通過してインターネットに出ていくパケットの送信元 IP アドレスは，すべて **FW** の IP アドレスに変換される。

b：図 3 の項番 3 に，「当該 C&C サーバに [b] 経由で HTTP 接続を行っていた」とある。表 2 の FW のフィルタリングルールより，インターネット上のサーバと HTTP 通信が許可されているのは**プロキシサーバ**のみであることが分かる。

c：DHCP（Dynamic Host Configuration Protocol）では IP アドレスが動的に割り当てられるため，IP アドレスのみで機器を特定することはできない。表 1 にあるように，PC の MAC（Media Access Control）アドレスや管理者従業員番号などの情報が IT 資産管理サーバに保管されており，通常 DHCP サーバでは IP アドレスを割り当てた MAC アドレスの情報を記録していることから，[c] には **MAC アドレス**が入る。

■設問 2

〔試験センターによる解答例〕

(1) DNS による名前解決ができず，TCP/IP 接続要求が出ないから（31 字）

(2) プロキシサーバで C&C サーバへの通信の URL をブラックリストに設定する。（36 字）

(1) PC 内のマルウェアがプロキシサーバを利用せずに C&C サーバへの接続を試みる場合，まず DNS サーバに C&C サーバの FQDN（Fully Qualified Domain Name）の名前解決要求を行う。図 2 にあるように，PC には名前解決先として内部 DNS サーバが設定されているが，表 1 にあるように，内部 DNS サーバは L 社ネットワーク上にある機器の名前解決しかできないため，マルウェアの**名前解決要求は失敗する**。そのため，インターネット上の C&C サーバに対する **TCP/IP 接続要求ができず**，FW のログには記録されない。

(2) 攻撃者は，C&C サーバの IP アドレスを短時間で変更してしまうことが多いため，IP アドレスをもとにした FW では C&C サーバへの通信を遮断できない可能性がある。図 4 より，マルウェアは下線②の試みに失敗すると，それ以降はプロキシサーバを利用した接続の試みを繰り返すことが分かる。また，表 1 を見ると，プロキシサーバにはブラックリスト型の URL フィルタリング機能があることが分かる。したがって，**C&C サーバへの通信の URL をプロキシサーバのブラックリストに設定**し，当該通信を遮断するのが有効である。

■設問 3

〔試験センターによる解答例〕

(1) ファイル配信サーバからマルウェアを拡散する攻撃（23 字）

(2) V さんの利用者 ID の無効化（13 字）

(3) ログ管理サーバに保存されているログとの比較（21 字）

(1) 表 1 より，ファイル配信サーバは，パッチの自動配信やパッチの強制適用に利用されていることが分かる。配信する先は L 社の PC やサーバ等であるため，最初のマルウェア感染後にファイル配信サーバから配信されたファイルを調査するのは，当該サーバを悪用した**マルウェアの拡散攻撃**を想定してのことである。

(2) 図 3 の項番 8 に，V さんはサーバにアクセスするための利用者 ID とパスワードを PC に保管していなかったとあるが，図 4 のマルウェアの種別に「キーロガー」とあることから，当該サーバを V さんの利用者 ID でアクセス可能な状態にしておくと，マルウェアに V さんの利用者 ID とパスワードが盗まれ，不正な操作が行われる可能性がある。そのため，当該サーバのサービス停止を行わずとも実行可能で効果の見込まれる対策としては，**V さんの利用者 ID を無効化する**ことである。

(3) 問題文の冒頭にあるように，各サーバは，アクセスログ，操作ログ，ミドルウェアのログ及びアプリケーションプログラムのログをログ管理サーバに送信するとともに，各サーバ上でも直近 3 か月分のログを保存している。したがって，3 台のサーバ上のログの

改ざんの痕跡を確認するには，**ログ管理サーバに保存されているログとの比較**を行えばよい。

＜問3＞ パスワードへの攻撃

■設問 1

〔試験センターによる解答例〕

多くの文字列のハッシュ値を計算したものと，漏えいしたファイル中のハッシュ値を突合し，パスワードを推測する攻撃（54 字）

ファイルに保存されたハッシュ値からパスワードを推測する攻撃手法であり，ソルトを用いることによって防ぐことができる攻撃手法が問われている。

ソルトが用いられていない場合は，パスワード文字列をそのままハッシュ関数で計算した値（ハッシュ値）がパスワードファイルに保存されている。これを推測するためには，あらかじめ**多くの文字列のハッシュ値を計算した結果のリストを用意しておき，そのリストと漏えいしたパスワードファイルの中のハッシュ値を突合する**方法がある。

これに対し，ソルトを用いた場合は下線①にあるように，ソルトとパスワードを結合したものをハッシュ関数でハッシュ化して保存する。このように，ソルトとは，パスワードからハッシュ値を求める際に，パスワードに付加する文字列のことである。ソルトには，ユーザごとにランダムな文字列であることと，ある程度の長さ（少なくとも 20 文字程度）であることが求められる。これらの要件を満たしたソルトを使用することにより，同じパスワードであっても出力されるハッシュ値が変わり，ハッシュ値から元のパスワードを特定することが困難になる。

■設問 2

〔試験センターによる解答例〕

(1) a：32

(2) b：単位時間当たりの同一 IP アドレスからのログイン試行数（26 字）

(3) c：多数の IP アドレス（9 字）

(1) SHA-256 では 256 ビットのハッシュ値が出力されるため，これをバイトに換算すると**32 バイト**である。

(2) C 氏が「方法（イ）では，今回の攻撃のように，同一 IP アドレスからのリバースブルートフォース攻撃を検知します」と説明していることから，同一 IP アドレスからのログ

イン試行数がしきい値であることが分かる。したがって,解答としては,図 3 の方法(ア)や(ウ)と同様に,「**単位時間当たりの同一 IP アドレスからのログイン試行数**」となる。なお,リバースブルートフォース攻撃とは,パスワードを固定して何通りものユーザ ID の組合せを試行する手法である。

(3) 図 3 にあるように,方法(ウ)は方法(ア)でも方法(イ)でも検知されない場合に対処するための検知方法であり,単位時間当たりのログイン失敗数のしきい値を設定している。C 氏の方法(イ)に関する説明「同一 IP アドレスからのリバースブルートフォース攻撃を検知します」と対比されるように「方法(ウ)では, c から行われるパスワード攻撃を検知します」とあることから, c には同一 IP アドレスとは逆の「**多数の IP アドレス**」「異なる複数の IP アドレス」などが入る。

■設問 3

〔試験センターによる解答例〕

d：**10^6**

e：200

f：**80^8**

d：パスワードが数字 1 桁の場合は 10 通り,数字 2 桁の場合は 10 × 10 ＝ 10^2で 100 通りの組合せとなる。したがって,パスワードが数字 6 桁の場合は**10^6 ＝ 1,000,000 通り**である。

e：図 4 の【前提条件】(iv)にあるように,パスワード攻撃の試行回数の上限は 1 日当たり 5,000 件である。その前提で数字 6 桁のパスワードの全組合せを試行すると,1,000,000 件÷5,000 件／日＝200 日である。したがって,少なくとも **200 日**掛かる計算になる。

f：文字種が 10 種で 6 桁のパスワードの全組合せが 10^6通りであるように,文字種が 80 種で 8 桁のパスワードの全組合せは**80^8通り**である。

■設問 4

〔試験センターによる解答例〕

他のサイトから流出した利用者 ID とパスワードの組合せによるパスワード攻撃（36 字)

多くの利用者が複数のサイトで同一の利用者 ID とパスワードを使い回している状況に目

をつけ，他のサイトから流出した利用者 ID とパスワードの組合せを不正に入手し，それらを自動的に連続入力するプログラムなどを用いて会員向けサイトへのログインを試行する「パスワードリスト攻撃」による被害が近年多発している。下線②はこのような攻撃による被害を避けるための注意喚起である。