令和６年度　春期　情報処理安全確保支援士試験　解答例

午後試験

問１

出題趣旨
多くのシステムにおいて，スマートフォンのアプリケーションプログラムを利用した API 連携が行われる中，API の脆弱性を作り込むケースが増えている。 本問では，API セキュリティを題材として，指摘された脆弱性に対して対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１		a	ステートレス	
設問２	(1)	b	500	
	(2)	データ	JWT ヘッダ内の alg に指定された値	
		内容	NONE でないことを検証する。	
	(3)	JWT に含まれる利用者 ID が mid の値と一致するかどうかを検証する処理		
	(4)	c	共通モジュール P	
	(5)	d	連続失敗回数がしきい値を超えたらアカウントをロックする処理	
設問３	(1)	テストサーバの index.html へのアクセスを記録し，確認する仕組み		
	(2)	e	Header	
		f	Header	
	(3)	・¥W[jJ][nN][dD][iI]¥W ・¥W(j|J)(n|N)(d|D)(i|I)¥W		
	(4)	利点	誤検知による遮断を防ぐことができる。	
		内容	アラートを受信したら攻撃かどうかを精査する。	

問２

出題趣旨
リモートワークが普及した状況下で，VPN を狙った攻撃が増加している。また，企業を狙った DDoS 攻撃も後を絶たない。 本問では，サイバー攻撃への対策を題材として，与えられた環境下で，リモートワークのセキュリティ対策，及び DDoS 攻撃に対するセキュリティ対策を設計，構築する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	公開 Web サーバ，取引先向け Web サーバを攻撃対象に，HTTP GET リクエストを繰返し送る。	
	(2)	正常な通信を異常として検知してしまう。		
	(3)	b	DNS-K	
		c	DNS-F	
設問２	(1)	d	攻撃者が，正規の VPN ダイアログに利用者 ID とパスワードを入力すると，正規利用者のスマートフォンにセキュリティコードが送信される。	
		e	正規利用者が受信したセキュリティコードを，罠の Web サイトに入力すると，攻撃者がそれを読み取り，正規のセキュリティコード入力画面に入力することで認証される。	
	(2)	認証情報の入力は，受信したメール内の URL リンクをクリックして起動した画面には行わず，VPN ダイアログにだけ行う。		
設問３	(1)	盗聴したパケットと同じ順番に通信要求を送信する。		
	(2)	SPA パケットはユニークであり，同じパケットを再利用すると破棄されるから		
設問４	(1)	・DDoS 対策機能を有する CDN サービス ・クラウド型ファイアウォールサービス ・ISP が提供する DDoS 防御サービス		
	(2)	・取引専用 PC 以外からの通信は取引先向け Web サーバに到達しないから ・UTM の設定変更によって，ボットネットからの通信が遮断されるから ・UTM の設定変更に伴って，外部からの接続対象サーバではなくなったから		

問３

出題趣旨
Web サイトの脆弱性については，多くの Web サイトで対策が進んできたものの，一部の Web サイトは開発者の理解が不十分で，IPA“安全なウェブサイトの作り方”で取り上げられている脆弱性においても対策に不備が生じている場合がある。 本問では，Web サイトの脆弱性を題材として，脆弱性診断及び対策の知識と，その脆弱性に起因してどのような攻撃が行われるかを分析する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	9		
	(2)	攻撃者がわなリンクを用意し，管理者にそのリンクを踏ませることで管理者権限の cookie を攻撃者の Web サイトに送信させ，その値を読み取って利用することで管理者としてサイト X にアクセスし，利用者情報を取得する。		
設問２	(1)	攻撃者が自らのアカウントで取得した csrf_token と一緒に利用者情報をサイト X に送るように構成したわなフォームに，詐欺メールなどで利用者を誘導し，利用者情報を変更させる。		
	(2)	a	×	
		b	×	
		c	○	
		d	×	
設問３	(1)	order-code の下 6 桁を総当たりで試行する。		
	(2)	cookie の値で利用者アカウントを特定し，order-code の値から特定したものと違っていれば，エラーにする。		
設問４	(1)	変更後の URL に POST データは送ることができないから		
	(2)	パラメータ page の値を IMDS のクレデンシャル情報を返す URL に変更する。		
	(3)	トークンを発行する URL に PUT メソッドでアクセスしてトークンを入手し，そのトークンをリクエストヘッダに含めて，IMDS のクレデンシャル情報を返す URL にアクセスする。		
	(4)	パラメータ page の値がサイト P 以外の URL ならエラーにする。		

問４

出題趣旨
Java と RDBMS で実装された Web アプリケーションプログラムの開発において，有識者によるセキュリティレビューを実施することによって，セキュリティの不備が発見される場合がある。 本問では，Java と RDBMS で実装された Web アプリケーションプログラムを題材として，セキュアプログラミングに関する能力を問う。

<table>
<tr><th colspan="2">設問</th><th colspan="4">解答例・解答の要点</th><th>備考</th></tr>
<tr><td rowspan="3">設問１</td><td>(1)</td><td>a</td><td colspan="3">ア</td><td></td></tr>
<tr><td>(2)</td><td>b</td><td colspan="3">personal</td><td></td></tr>
<tr><td>(3)</td><td>c</td><td colspan="3">4</td><td></td></tr>
<tr><td rowspan="6">設問２</td><td>(1)</td><td>d</td><td colspan="3">5</td><td></td></tr>
<tr><td>(2)</td><td>e</td><td colspan="3">例外</td><td></td></tr>
<tr><td rowspan="3">(3)</td><td rowspan="2">システム運用担当者</td><td>アクセスできてしまう情報</td><td rowspan="2">不備により設問が成立しない。</td><td rowspan="2"></td></tr>
<tr><td>出力される場所</td></tr>
<tr><td rowspan="2">システム開発者</td><td>アクセスできてしまう情報</td><td>パスワード，氏名，住所，電話番号，メールアドレス</td><td></td></tr>
<tr><td>出力される場所</td><td>オ</td><td></td></tr>
<tr><td>(4)</td><td>f</td><td colspan="3">・SHA-256
・SHA-384
・SHA-512</td><td></td></tr>
<tr><td>(5)</td><td>g</td><td colspan="3">・throw new RuntimeException(e)
・ランタイムエラーを例外として throw する。</td><td></td></tr>
<tr><td>(6)</td><td>h</td><td colspan="3">finally</td><td></td></tr>
<tr><td>(7)</td><td colspan="4">ア</td><td></td></tr>
</table>