TAC

令和6年度秋期　情報処理安全確保支援士試験

情報処理安全確保支援士　解答例

【午　後】

問 1（配点 50 点）

設問 1（40 点：(1)3 点，(2)3 点，(3)3 点，(4)3 点，(5)6 点，(6)6 点，(7)6 点，(8)5 点×2）

(1) a ： PC-C

(2) b ： filesv

(3) c ： ad01¥user019

(4) d ： アカウント停止

(5) 全てのドメインユーザーに対して，プロキシサービスの URL フィルタリング機能の管理者拒否リストに https://△△△.com/ を追加する。

(6) プロキシサービスの通信ログで，感染後の PC-A がアクセスした URL に他の L 社内ホストがアクセスしていないか調査する。

(7) L 社内ホスト全てを対象に，install というタスクが登録されていないか調査する。

(8) ① L 社内ホストの VSCAN_SVC が停止されたときは，情シス部にアラートメールを送付する。

② L 社内ホストで install というタスクが登録又は実行されたときは，情シス部にアラートメールを送付する。

設問 2（10 点 ： 5 点×2）

e ： 各ドメインユーザーの仮想 PC 上のローカルアドミニストレータ権限をはく奪し，仮想 PC からの RDP 接続を禁止する設定を行う。

f ： 社外秘情報 L は機密度に応じてラベル化して暗号化し，新たに DLP を導入する。

問 2（配点 50 点）

設問 1（6 点：(1)3 点，(2)3 点）

(1) a ： A 社ドメイン名

(2) b ： 全て

設問 2（2 点）

c ： SMTPS

設問 3（4 点：(1)2 点，(2)2 点）

(1) エ

(2) d ： イ

設問 4（20 点：(1)6 点，(2)6 点×2，(3)2 点）

(1) 工作機械管理用アプリケーションプログラムやソフトウェア修正プログラムにマルウェアを混入させて配布する。

(2)（メール）パスワード変更申請を行うリンクが記載されたメール

（攻撃）変更したパスワードと A 社ドメイン名のメールアドレスを使用して，社外サービスに不正にログインする。

(3) e : ア

設問 5 (18 点:(1)6 点, (2)6 点×2)

(1) T サービス経由のメールでも SPF 認証が成功するように, SPF レコードに T サービスの IP アドレスを追加する。

(2) (SPF) メールが Y サービスのサーバから送信されるが, S サービスに登録された SPF レコードに Y サービスのサーバが含まれていないため, SPF 認証に失敗する。

(DKIM) DKIM-Signature ヘッダーの h タグに設定されている Subject フィールドが, Y サービスがメールの通番情報を付加することによって変更され, DKIM 署名の検証に失敗し, さらに Y サービスは ARC に対応していないため認証結果を引き継げず, DKIM 認証に失敗する。

問 3 (配点 50 点)

設問 1 (20 点:4 点×5)

a : 5

b : クロスサイトスクリプティング

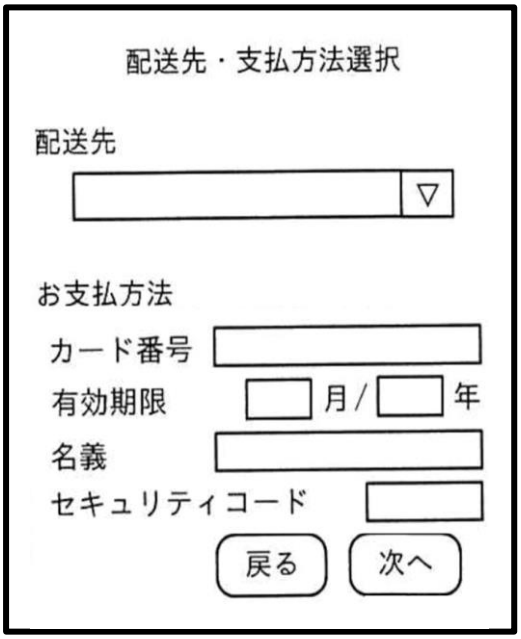
c : 格納

d : 2

e : SQL インジェクション

設問 2 (18 点:(1)6 点, (2)3 点×2, (3)6 点)

(1)



(2) (パラメータ名) order[Payment]

(値) 1

(3) 次へボタンをクリックすると, 入力されたカード番号, 有効期限, 名義, セキュリティコードの情報が URL のクエリパラメータとして, 攻撃者が用意したサーバ https: //i-sha.com/ へ GET リクエストで送信される。

設問 3 (12 点:(1)6 点, (2)6 点)

(1) 攻撃者の Web サーバのアクセスログに記録されたリクエスト URI からクレジットカード情報を取得する。

(2) f : 支払手続画面にアクセスした利用者のアカウント名

問 4（配点 50 点）

設問 1（20 点：(1)2 点，(2)2 点，(3)4 点，(4)4 点，(5)4 点×2）

（1） a ：（イ）

（2） b ： https://test.△△△.jp/

（3） c ： メール受信者の利用者 ID と PW でのログイン認証が成功し，求人企業トップ画面への遷移

（4） d ： 利用者 ID と PW でのログイン認証が成功した後に，セッション ID を再生成し，元のセッション ID を無効化

（5） e ： ブラウザが HTTPS で接続することを強制することで，盗聴や改ざんを防止できる。

f ： ブラウザが Content-Type フィールドで指定されたメディアタイプを強制適用し，不正なスクリプトの実行を防ぐことができる。

設問 2（10 点：5 点×2）

g ： 画面 09 の会社名に攻撃者のメールアドレスを含む文字列を入力して変更ボタンをクリックし，画面 11 で OK ボタンをクリックする。画面 03 でプロパティ変更ボタンをクリックして，再度，画面 09 を表示する。

h ： 画面 04 から，再設定後のパスワードで認証して，APIkey の参照や新たな APIkey の発行を行う。

設問 3（20 点：5 点×4）

i ： 求職者 ID を推測困難な ID にする。

j ： 当該企業以外に問合せや応募をした求職者の求職者属性情報を不正に取得できてしまうから

k ： 求 人企業プロパティ変更時にパスワード入力を求める処理を追加し，メールアドレス以外だけを変更した場合にも変更内容が記載されたメールを送信する。

l ： メールアドレス以外だけを変更した場合にそのまま変更を反映しており，不正に書き換えられる可能性があるから

以上