Computer Security (COM-301)
Adversarial Thinking

Which of these are true?

Which of the following approaches does NOT help to ensure that you do not run adversarial code in the Trusted Computing Base?

(a) Make sure code updates are signed.

(b) Sanitize the compiler code before compiling updates.

(c) Only accept updates encrypted with your public key.

(d) Check for new updates using an antivirus

XS…?

While you are logged into your bank's website (https://creditbank.com) in your browser, you receive an email with the following subject: "Job opportunity at Appgle! Apply now", and fully load the email in the same browser. In the email, there is an image attachment with the following HTML image tag:

<img src="https://creditbank.com/enabletransaction?account=ATTACKERACCOUNT&amount=10000">

As soon as you are done reading the email, you find that your bank account is missing 10'000 CHF. Which of the following CWE was exploited here?

a) Cross-site request forgery, because the code that loads the image takes advantage of an existing creditbank.com session cookie to execute the request on your behalf.
b) Cross-site scripting, because the arguments to the URL to access the bank's website are not properly sanitized.
c) Cross-site request forgery, because the arguments to the URL to access the bank's website are not properly sanitized.
d) Cross-site scripting, because the code that loads the image takes advantage of an existing creditbank.com session cookie to execute the request on your behalf.

Which of these are true?

Which of the following countermeasures are a **good choice** to avoid Cross Site Request Forgery attacks:

(a) Only authorize actions after the authentication step

(b) Sanitize the cookies before they are processed

(c) Not execute anything received from the user

(d) Verify the origin of the information

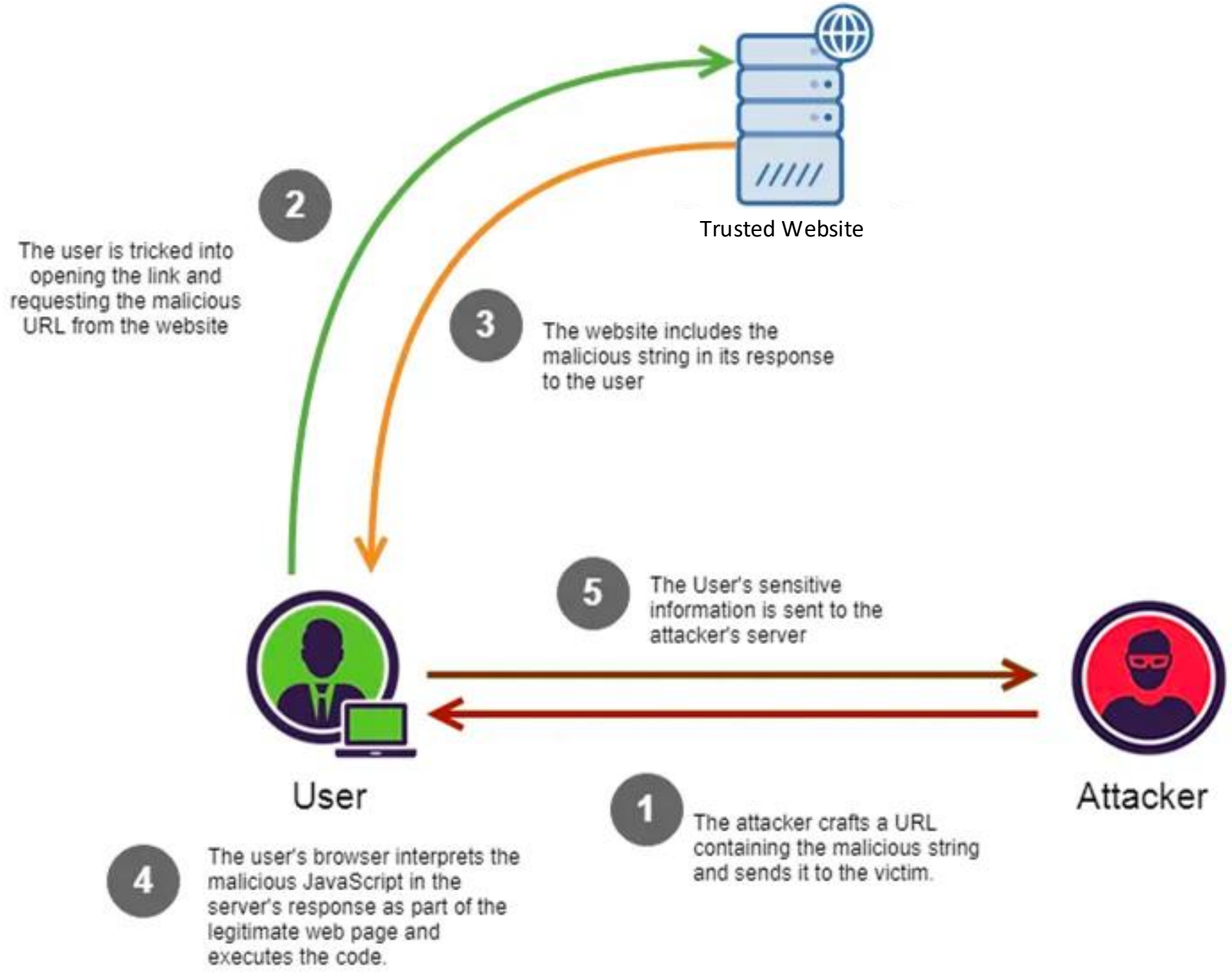
AwesomeWebsite.com/hello.php has the following PHP code

```
$userid = $_GET['userID'];
echo '<div class="header">Hello, '.$userid.'</div>';
```

1. Write a URL to inform a third party, http://iamcharlie.com, of the cookie of the user visiting the page.

2. What instructions would you give to the programmer to fix this?

XSS through the looking glass mirror



1. As an attacker, how would you perform step 1 (and 2) to exploit step 4?

1. What can the different entities do against this attack?