www.pandoralabs.net

PANDORA SECURITY LABS

Expert advice. Experience advantage.

Proactive Security Solutions Through Cutting-Edge Research.

PANDORA SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

Developing Secure Applications

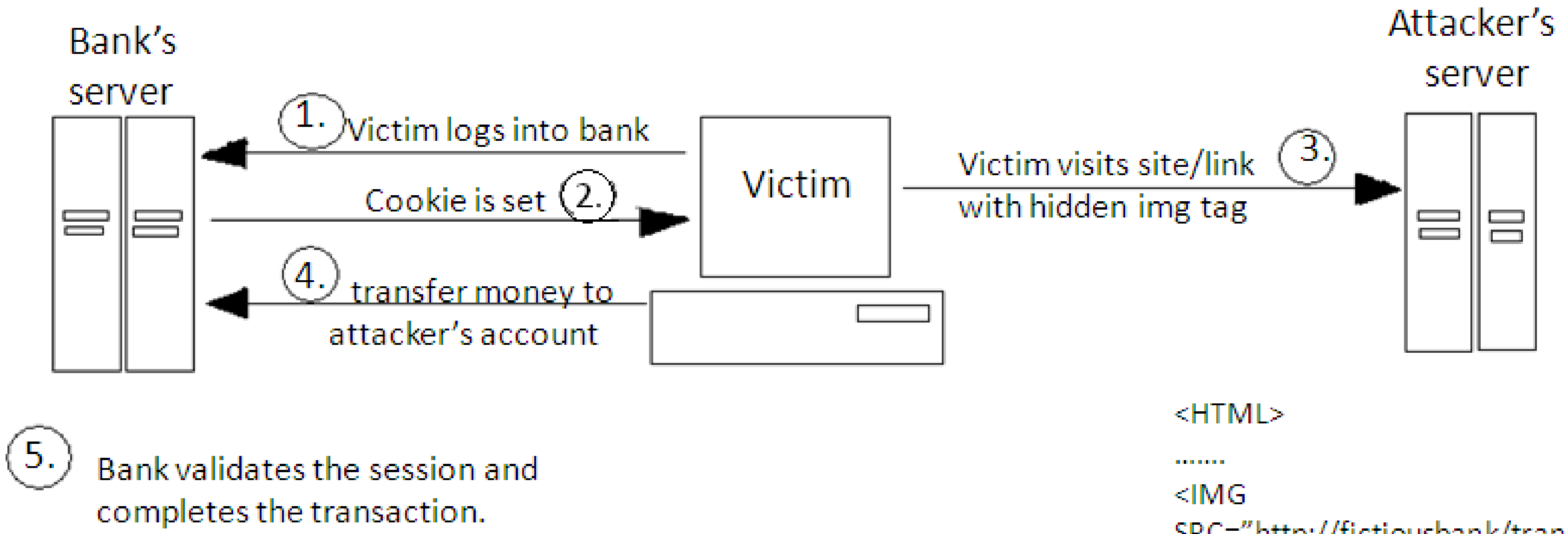
Quick Tips

CSRF Tokens

CSRF!??!

- Pronounced as see-surf
- Cross-Site Request Forgery
- It causes a user to perform an unwanted action on a trusted site

What is CSRF?



Bank's server

Attacker's server

1. Victim logs into bank

2. Cookie is set

Victim

3. Victim visits site/link with hidden img tag

4. transfer money to attacker's account

5. Bank validates the session and completes the transaction.

```
<HTML>
.......
<IMG
SRC="http://fictiousbank/transfer.cgi?from=35367021&to484
12334&amount=5000&date=05072010"  width="0"
height="0">
.......
</HTML>
```

Use anti CSRF Tokens

- Anti-csrf tokens adds a unique token that must be included with the data submission.

```
<% using(Html.Form("UserProfile", "SubmitUpdate")) { %>
     <%= Html.AntiForgeryToken() %>
    <!-- rest of form goes here -->
<% } %>
```

The output will be something like:

```
<form action="/UserProfile/SubmitUpdate" method="post">
    <input name="__RequestVerificationToken" type="hidden"
    value="saTFWpkKN0BYazFtN6c4YbZAmsEwG0srqlUqqloi/fVgeV2ciIFVmelvzwRZpArs" /> <!-- rest of form goes
    here -->
 </form>
```

Use anti CSRF Tokens

```
public class UserProfileController : Controller {
   public ViewResult Edit() { return View();
}
[ValidateAntiForgeryToken]
public ViewResult SubmitUpdate() {
    // Get the user's existing profile data (implementation omitted)
    ProfileData profile = GetLoggedInUserProfile();

      // Update the user object
      profile.EmailAddress = Request.Form["email"];
      profile.FavoriteHobby = Request.Form["hobby"];
      SaveUserProfile(profile);

      ViewData["message"] = "Your profile was updated.";
      return View();
   }
}
```

Use anti CSRF Tokens

- Any state changing operation requires a secure random token (e.g CSRF token) to prevent against CSRF attacks
- Characteristics of a CSRF Token
  - Unique per user & per user session
  - Tied to a single user session
  - Large random value
  - Generated by a cryptographically secure random number generator
- The CSRF token is added as a hidden field for forms or within the URL if the state changing operation occurs via a GET
- The server rejects the requested action if the CSRF token fails validation

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.

Proactive Security Solutions Through Cutting-Edge Research.