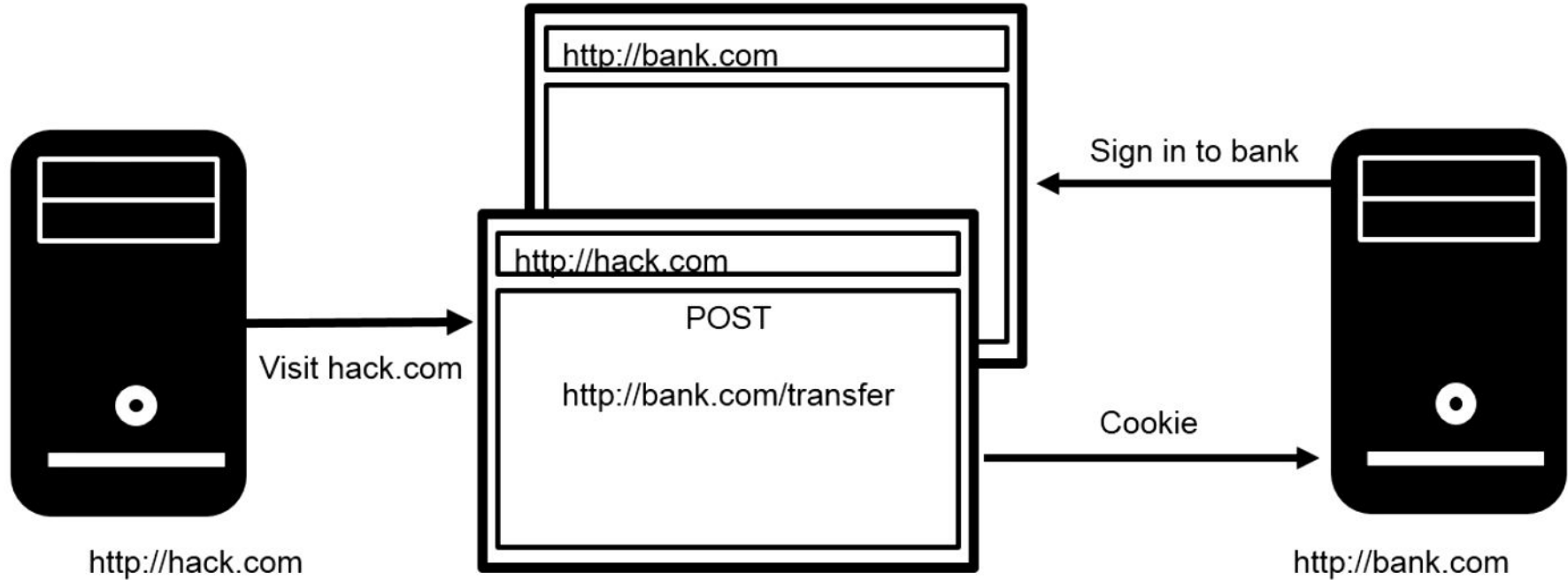


CSRF

Cross Site Request Forgery



Form

```
<spring:url value="/players/save" var="saveUrl"/>

<form:form action="${saveUrl}" method="post" modelAttribute="player">
  <div class="form-group">
    <label for="player-name"><spring:message code="label.User.firstname"/></label>

    <form:input path="firstName" cssClass="form-control" id="player-name" />

  </div>
  <div class="form-group">
    <label for="player-lastname"><spring:message code="label.User.lastname"/></label>

    <form:input path="lastName" cssClass="form-control" id="player-lastname" />

  </div>
  <button type="submit" class="btn btn-default"><spring:message code="button.submit"/></button>
</form:form>
```

Controller

- `@ModelAttribute` - binds a method parameter or method return value to a named model attribute, exposed to a web view

```
@RequestMapping(value = "/save", method = RequestMethod.POST)
public String delete(@ModelAttribute Player player, Model model) {
    Player saved = playerService.save(player);
    return "players/form";
}
```

- `@SessionAttribute` - list the names of model attributes which should be transparently stored in the session or some conversational storage, serving as form-backing beans

```
@Controller
@RequestMapping("/players")
@SessionAttributes("player")
public class PlayerController {
}
```