Web Security
SQL Injection, CSRF, XSS

EECS 388
Feb 11, 2015

Web Review | HTTP

GET / HTTP/1.1
Host: gmail.com

HTTP/1.1 200 OK
…
<html>
<head>
<script>alert('Hi!')</script>
</head>

gmail.com

http://gmail.com/ says:

Hi!

GET /img.png HTTP/1.1
Host: gmail.com

HTTP/1.1 200 OK
…
<89>PNG^M ...

Web Review | AJAX (jQuery style)

GET / HTTP/1.1
Host: gmail.com

HTTP/1.1 200 OK
…
<script>
$.get('http://gmail.com/msgs.json',
function (data) { alert(data) });
</script>

gmail.com

http://gmail.com/ says:

{ new_msgs: 3}

GET /msgs.json HTTP/1.1
Host: gmail.com

HTTP/1.1 200 OK
…
{ new_msgs: 3 }

Web Review | Same-Origin Policy (SOP)

(evil!)
facebook.com

GET / HTTP/1.1
Host: facebook.com

HTTP/1.1 200 OK
…
<script>
$.get('http://gmail.com/msgs.json',
function (data) { alert(data); }
</script>

$.get('http://gmail.com/msgs.json',
function (data) { alert(data); }

GET /msgs.json HTTP/1.1
Host: gmail.com

gmail.com

HTTP/1.1 200 OK
…
{ new_msgs: 3 }

Web Review | Same-Origin Policy (SOP)

GET / HTTP/1.1
Host: facebook.com

facebook.com

HTTP/1.1 200 OK
…

?

gmail.com

Web Review | Same-Origin Policy (SOP)

GET / HTTP/1.1
Host: facebook.com

facebook.com

HTTP/1.1 200 OK
…

GET /img.png HTTP/1.1
Host: gmail.com

gmail.com

HTTP/1.1 200 OK
…
<89>PNG^M ...

Web Review | Same-Origin Policy (SOP)

GET / HTTP/1.1
Host: facebook.com

facebook.com

HTTP/1.1 200 OK
…
<script src="http://gmail.com/chat.js"/>

?

gmail.com

Web Review | Same-Origin Policy (SOP)

GET / HTTP/1.1
Host: facebook.com

facebook.com

HTTP/1.1 200 OK
…
<script src="http://gmail.com/chat.js"/>

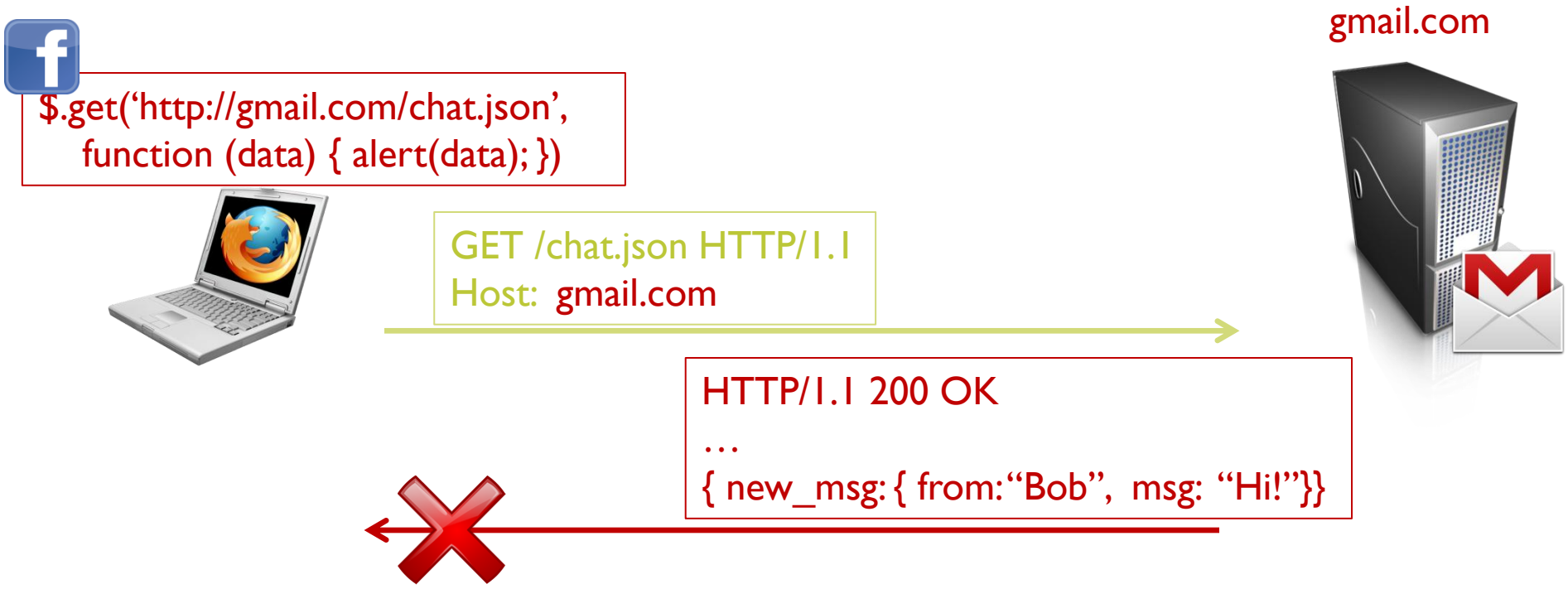
$.get('http://gmail.com/chat.json',
function (data) { alert(data); })

GET /chat.js HTTP/1.1
Host: gmail.com

gmail.com

HTTP/1.1 200 OK
…
$.get('http://gmail.com/chat.json',
function (data) { alert(data); })

Web Review | Same-Origin Policy (SOP)



Web Review | Same-Origin Policy (SOP)

GET / HTTP/1.1
Host: facebook.com

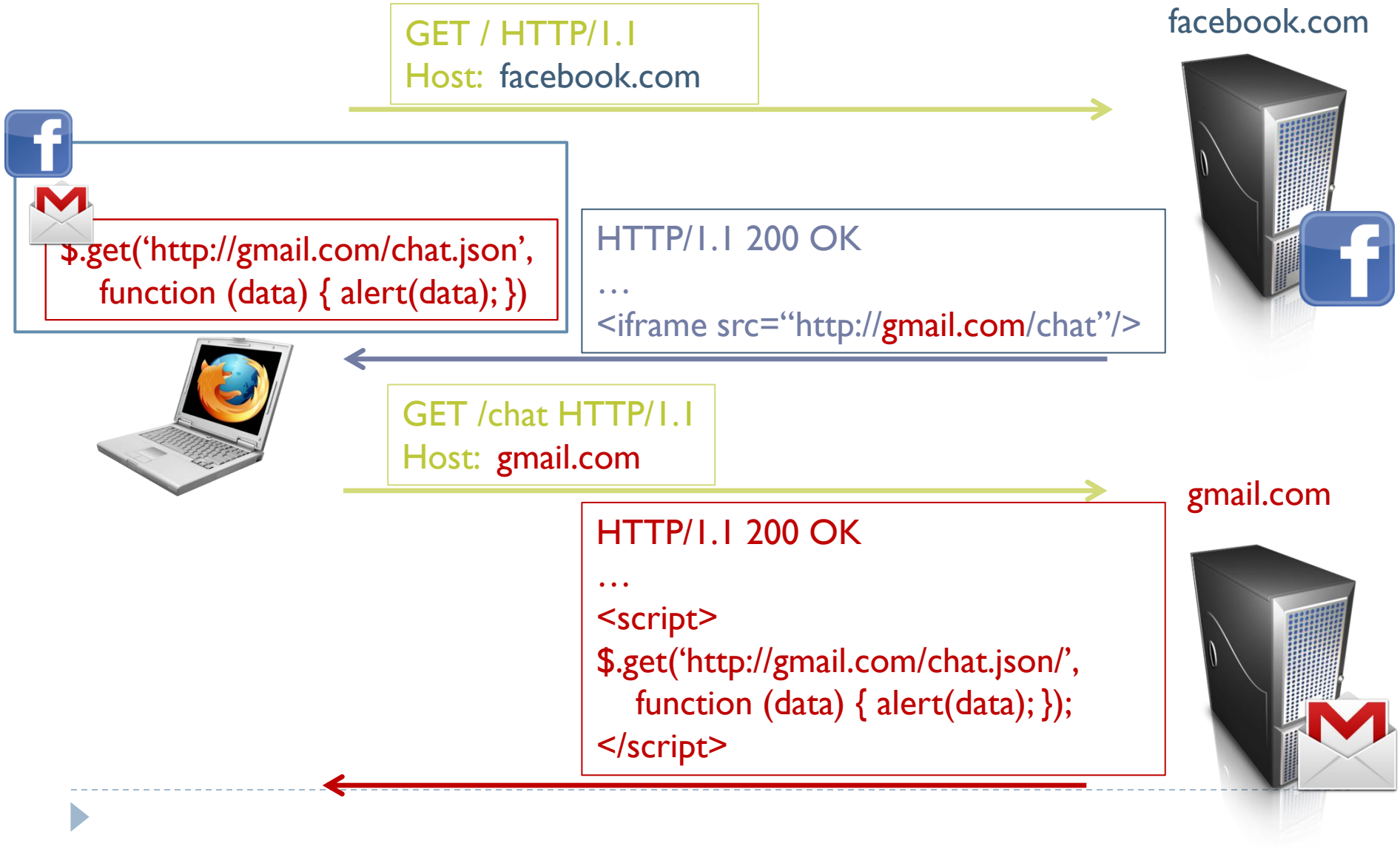
facebook.com

HTTP/1.1 200 OK
…
<iframe src="http://gmail.com/chat"/>

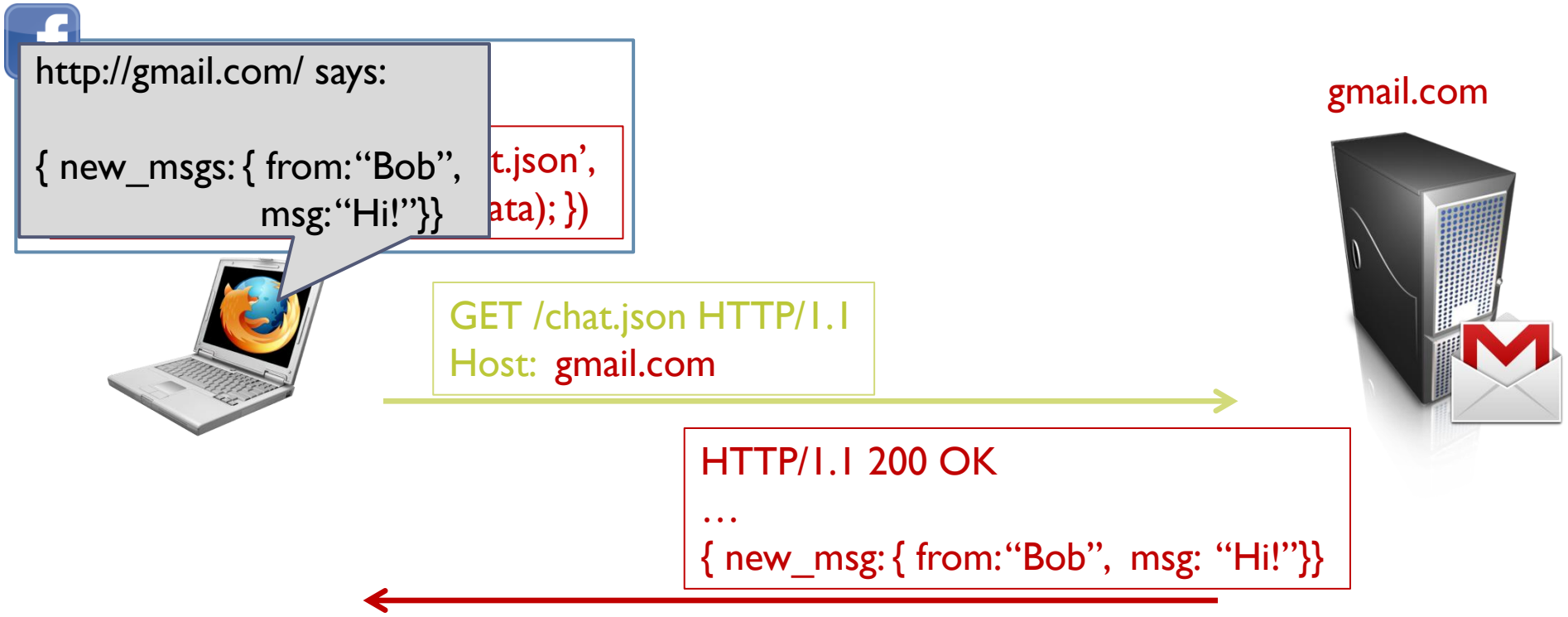
?

gmail.com

Web Review | Same-Origin Policy (SOP)



Web Review | Same-Origin Policy (SOP)



Code Injection

```
<?php

echo system("ls " . $_GET["path"]);
```

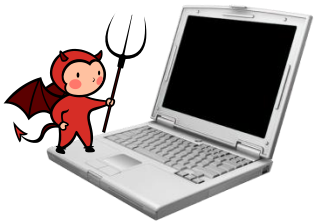
GET /?path=/home/user/ HTTP/1.1

HTTP/1.1 200 OK
…
Desktop
Documents
Music
Pictures

Code Injection

```
<?php

echo system("ls " . $_GET["path"]);
```

GET /?path=$(rm –rf /) HTTP/1.1




```
<?php

echo system("ls $(rm -rf /)");
```

Code Injection

- Confusing **Data** and **Code**
  - Programmer thought user would supply data,
    but instead got (and unintentionally executed) code

```
<?php

echo system("ls $(rm -rf /)");
```

- Common and dangerous class of vulnerabilities
  - Shell Injection
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Control-flow Hijacking (Buffer overflows)

SQL

- Structured **Query** Language
  - Language to ask ("query") databases questions:
    - How many users live in Ann Arbor?

```
"SELECT COUNT(*) FROM `users` WHERE location = 'Ann Arbor'"
```

    - Is there a user with username "bob" and password "abc123"?

```
"SELECT * FROM `users` WHERE username='bob' and
   password='abc123'"
```

    - Burn it down!

```
"DROP TABLE `users`"
```

SQL Injection

- Consider an SQL query where the attacker chooses $city:

```
SELECT * FROM `users` WHERE location='$city'
```

- What can an attacker do?

SQL Injection

- Consider an SQL query where the attacker chooses $city:

```
SELECT * FROM `users` WHERE location='$city'
```

- What can an attacker do?

$city = "Ann Arbor'; DELETE FROM `users` WHERE 1='1"

```
SELECT * FROM `users` WHERE location='Ann Arbor';
DELETE FROM `users` WHERE 1='1'
```

SQL Injection Defense

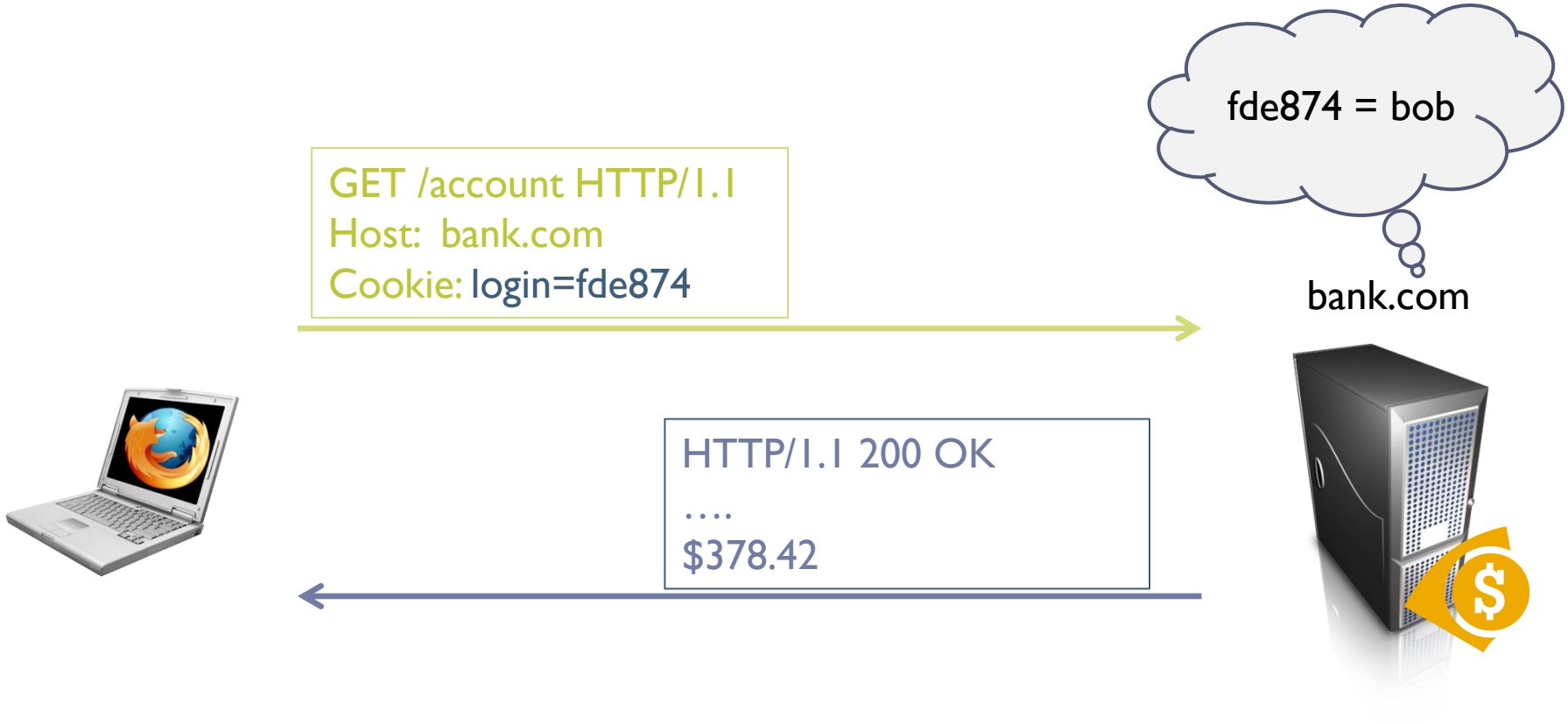
- Make sure **data** gets interpreted as **data**!
  - Basic approach: escape control characters (single quotes, escaping characters, comment characters)
  - Better approach: Prepared statements – declare what is data!

```
$pstmt = $db->prepare(
    "SELECT * FROM `users` WHERE location=?");
$pstmt->execute(array($city));   // Data
```

Cross-site Request Forgery (CSRF)

- Suppose you log in to bank.com

Cross-site Request Forgery (CSRF)

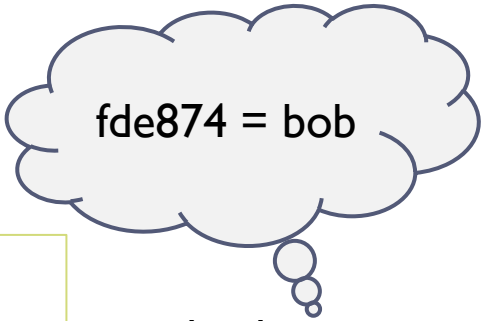


CSRF Defenses

- Need to "authenticate" each user action originates from our site
- One way: each "action" gets a token associated with it
  - On a new action (page), verify the token is present and correct
  - Attacker can't find token for another user, and thus can't make actions on the user's behalf

Cross-site Request Forgery (CSRF)

Click me!!!
http://bank.com/transfer?to=badguy&amt=100



bank.com

GET /transfer?to=badguy&amt=100 HTTP/1.1
Host: bank.com
Cookie: login=fde874

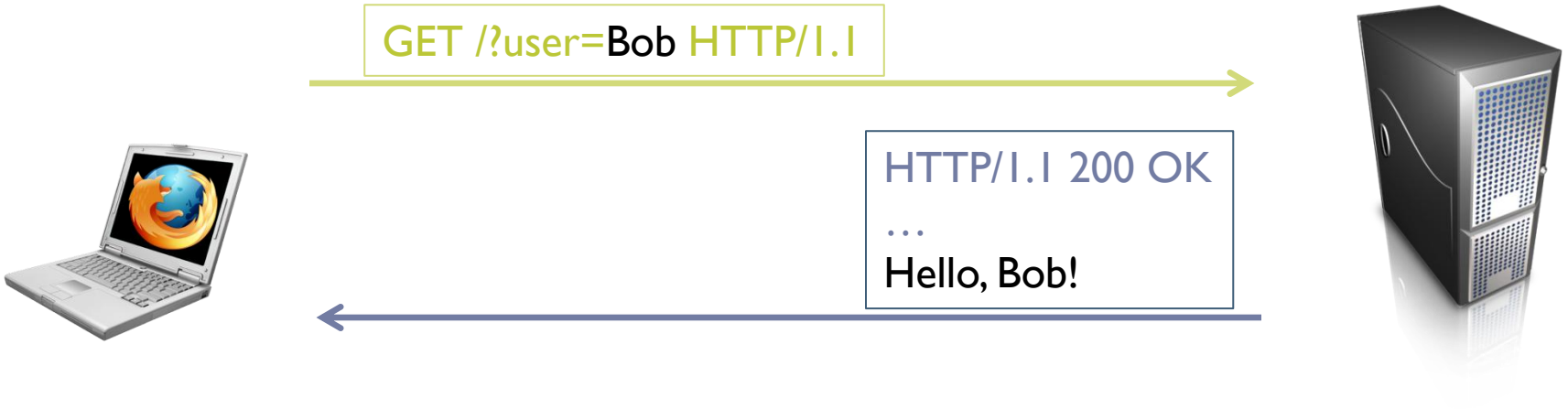
HTTP/1.1 200 OK
….
Transfer complete: -$100.00

CSRF Defenses

Pay $25 to Joe:
http://bank.com/transfer?to=joe&amt=25&token=8d64

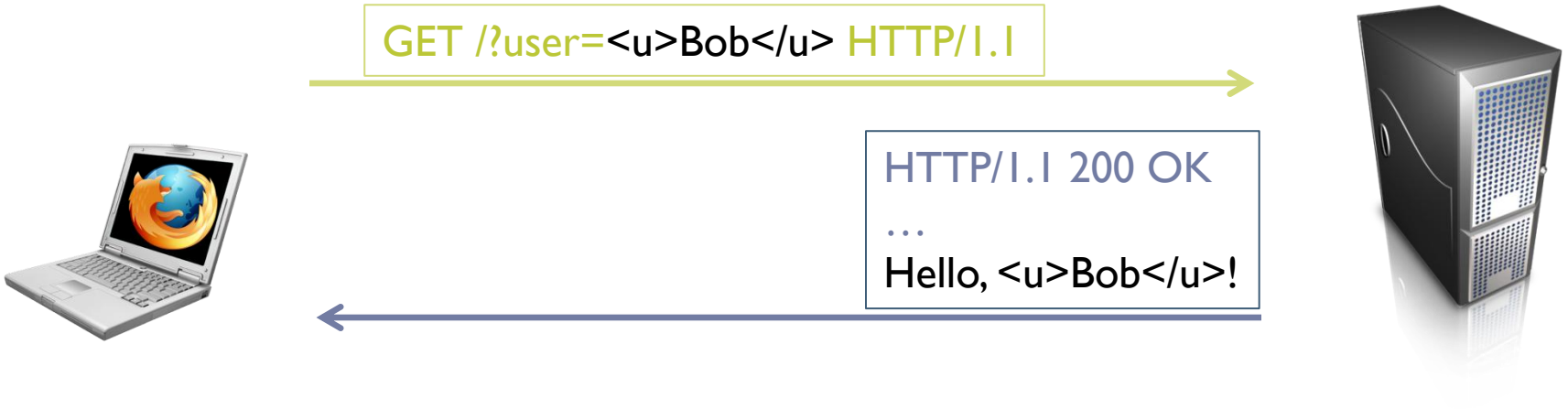
Cross-Site Scripting (XSS)

```
<?php

echo “Hello, ” . $_GET[“user”] . “!”;
```



Cross-Site Scripting (XSS)

```
<?php

echo “Hello, ” . $_GET[“user”] . “!”;
```



Cross-Site Scripting (XSS)

```
<?php

echo “Hello, ” . $_GET[“user”] . “!”;
```

http://vuln.com/ says:

XSS

GET /?user=<script>alert(‘XSS’)</script> HTTP/1.1

HTTP/1.1 200 OK

…

Hello, <script>alert(‘XSS’)</script>!

Click me!!!

http://vuln.com/?user=<script>alert(‘XSS’)</script>

Web Review | Same-Origin Policy (SOP)

(evil!)
facebook.com

GET / HTTP/1.1
Host: facebook.com

HTTP/1.1 200 OK
…
<script>
$.get('http://gmail.com/msgs.json',
function (data) { alert(data); }
</script>

GET /msgs.json HTTP/1.1
Host: gmail.com

gmail.com

HTTP/1.1 200 OK
…
{ new_msgs: 3 }

Cross-Site Scripting (XSS) Attack

GET / HTTP/1.1
Host: facebook.com

(evil!)
facebook.com

HTTP/1.1 200 OK
…
<iframe src="http://gmail.com/?user=<script>
$.get('http://gmail.com/msgs.json',
function (data) { alert(data); })
</script>"></iframe>

$.get('http://gmail.com/
msgs.json', function (data)
{ alert(data); })

GET /?user=<script>$.get(' … </script> HTTP/1.1
Host: gmail.com

gmail.com

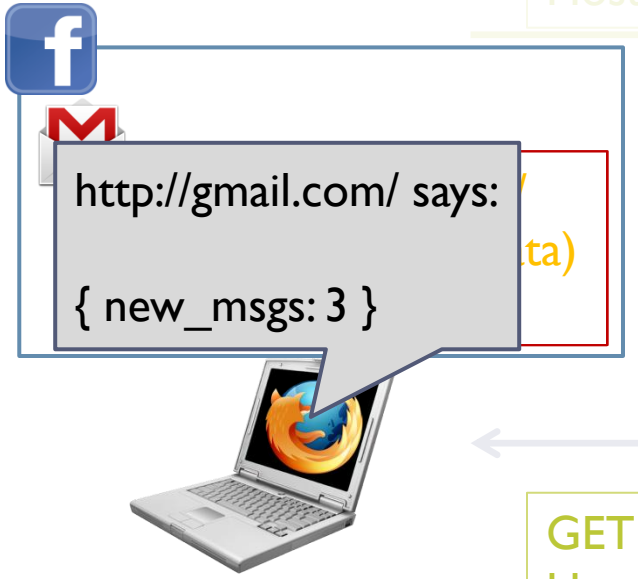
HTTP/1.1 200 OK
…
Hello,
<script>$.get('http://gmail.com/msgs.json',
function (data) { alert(data); }) </script>

Cross-Site Scripting (XSS) Attack

GET / HTTP/1.1
Host: facebook.com

(evil!)
facebook.com

HTTP/1.1 200 OK
…
<iframe src="http://gmail.com/?user=<script>
$.get('http://gmail.com/msgs.json',
function (data) { alert(data); })
</script>"></iframe>



GET /msgs.json HTTP/1.1
Host: gmail.com

gmail.com

HTTP/1.1 200 OK
…
{ new_msgs: 3 }

XSS Defenses

- Make sure **data** gets shown as **data**, not executed as code!
  - Escape special characters
    - Which ones? Depends what context your $data is presented
      - Inside an HTML document? $data
      - Inside a tag? <a href="http://site.com/$data">
      - Inside Javascript code? var x = "$data";
    - Make sure to escape every last instance!
  - Frameworks can let you declare what's user-controlled data and automatically escape it