Frog and Toad
Learn Django Security

@phildini
#djangotoad

@phildini
#djangotoad

Bezos Books

- A site for selling books
- Authors have a form where they can put in book information
- That book information gets rendered to a book page
- There is a form on the book page for buying the book

Django!

@phildini
#djangotoad

XSS

Cross-Site Scripting

@phildini
#djangotoad

```
<script>alert(‘hello’)</script>
```

```
&lt;script&gt;alert(&#39;hello&#39;)&lt;/script&gt;
```

```
return mark_safe(
    force_text(text)
    .replace('&', '&amp;')
    .replace('<', '&lt;')
    .replace('>', '&gt;')
    .replace('"', '&quot;')
    .replace("'", '&#39;')
)
```

@phildini
#djangotoad

django.utils.html

https://github.com/django/django/blob/master/django/utils/html.py#L47

@phildini
#djangotoad

Context ->
VariableNode ->
conditional_escape ->
escape

https://github.com/django/django/blob/master/django/template/base.py mark_safe(), | n, | safe

CSRF

Cross-Site Request Forgery

@phildini
#djangotoad

CsrfViewMiddleware

https://github.com/django/django/blob/master/django/middleware/csrf.py

```
if request is a POST:
    get csrf_token from cookie
    get csrfmiddlewaretoken from request.POST
    if both match:
        accept
    else:
        reject
```

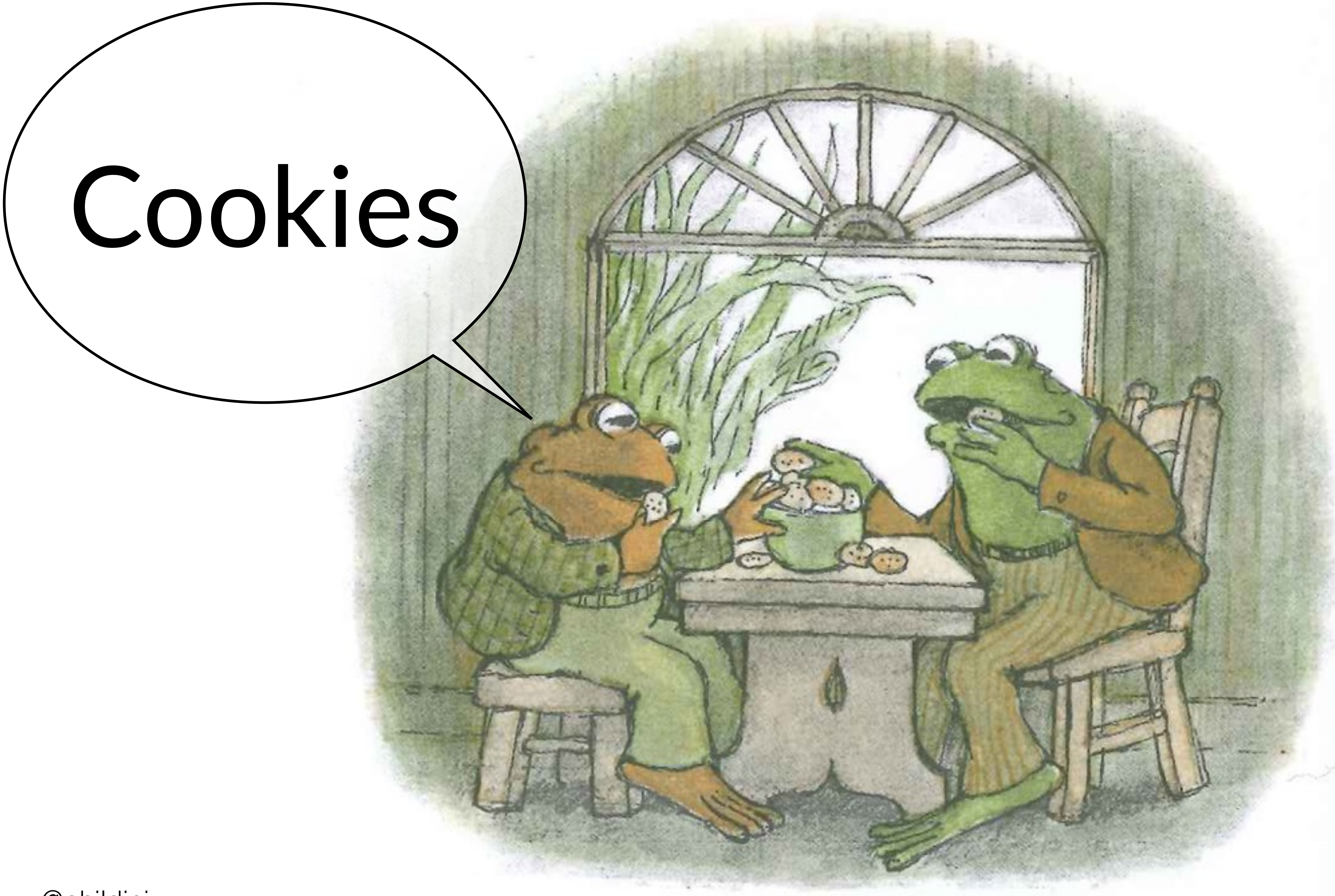
```
def csrf_exempt(view_func):
    def wrapped_view(*args, **kwargs):
        return view_func(*args, **kwargs)
    wrapped_view.csrf_exempt = True
    return wraps(
            view_func, assigned=available_attrs(view_func)
    )(wrapped_view)
```

django.views.decorators.csrf.csrf_exempt

```
@csrf_exempt
def my_view(request):
    ...

@method_decorator(csrf_exempt, dispatch)
class MyCBV(View):
    ....
```

```
if request is a POST and not view.csrf_exempt:
    get csrf_token from cookie
    get csrfmiddlewaretoken from request.POST
    if both match:
        accept
    else:
        reject
```



@phildini
#djangotoad

SQLi

SQL Injection

[This Slide Intentionally Left Blank]

.extra(), RawSQL(), .raw()

@phildini
#djangotoad

XFrameOptionsMiddleware

https://github.com/django/django/blob/master/django/middleware/clickjacking.py

```
@xframe_options_exempt
def my_view(request):
    ...
```

```
@method_decorator(xframe_options_exempt, dispatch)
class MyCBV(View):
    ....
```

Internet Explorer 8+
Firefox 3.6.9+
Opera 10.5+
Safari 4+
Chrome 4.1+

@phildini
#djangotoad

get_host()

https://github.com/django/django/blob/master/django/http/request.py#L95

@phildini
#djangotoad

```
if domain and in ALLOWED_HOSTS:
    proceed
else:
    raise error
```

@phildini
#djangotoad

django.contrib.auth.hashers.check_password

https://github.com/django/django/blob/master/django/contrib/auth/hashers.py

@phildini
#djangotoad

@phildini
#djangotoad

Constant Vigilance!

HTTPS

CSP Reporting

Content Security Policy

django_encrypted_fields

https://github.com/defrex/django-encrypted-fields

django-secure

http://django-secure.readthedocs.org/en/v0.1.2/

Pony Checkup

https://www.ponycheckup.com/

Making Django Ridiculously Secure

http://nerd.kelseyinnis.com/blog/2015/09/08/making-django-really-really-ridiculously-secure/

@phildini
#djangotoad

The End.

Philip James
@phildini
http://bit.ly/djangotoad