

# Django web application security

Created by 이윤준 ([yoonyoon.lee@gmail.com](mailto:yoonyoon.lee@gmail.com))

June, 2019

Protecting user data is an essential part of any website design. We previously explained some of the more common security threats in the article [Web security](#) — these slides provides a practical demonstration of how Django's in-built protections handle such threats.

# Overview

The Website security topic provides an overview of what website security means for server-side design, and some of the more common threats that we may need to protect against.

One of the key messages is that almost all attacks are successful when the web application trusts data from the browser.

The good news for Django users is that many of the more common threats are handled by the framework.

The [Security in Django](#) (Django docs) article explains Django's security features and how to secure a Django-powered website.

# Common threats/protections

We'll demonstrate just a few of the security features in the context of our Django *LocalLibrary* tutorial.

## Cross site scripting (XSS)

XSS is a term used to describe a class of attacks that allow an attacker to inject client-side scripts through the website into the browsers of other users.

This is usually achieved by storing malicious scripts in the database where they can be retrieved and displayed to other users, or by getting users to click a link that will cause the attacker's JavaScript to be executed by the user's browser.

Django's template system protects us against the majority of XSS attacks by escaping specific characters that are "dangerous" in HTML.

We can demonstrate this by attempting to inject some JavaScript into our LocalLibrary website using the Create-author form we set up in *Django Tutorial Part 9: Working with forms*.

1. Start the website using the development server (`python3 manage.py runserver`).
2. Open the site in our local browser and login to our superuser account.
3. Navigate to the author-creation page (which should be at URL: `http://127.0.0.1:8000/catalog/author/create/`).
4. Enter names and date details for a new user, and then append the following text to the Last Name field:  
`<script>alert('Test alert');</script>`

← → ↻ ⓘ 127.0.0.1:8000/catalog/author/create/

Home  
All books  
All authors  
User: superman  
My Borrowed  
Logout

**First name:** David (Boonie)

**Last name:** Boon<script>alert('Test alert', 1000)</script>

**Date of birth:** 1960-12-29

**Died:**

Submit

5. Press **Submit** to save the record.

6. When you save the author it will be displayed as shown below.

Because of the XSS protections the `alert()` should not be run. Instead the script is displayed as plain text.

Home  
All books  
All authors  
User: superman  
My Borrowed  
Logout

Author: Boon<script>alert('Test alert');</script>, David (Boonie)

Dec. 29, 1960 -

Books



If you view the page HTML source code, you can see that the dangerous characters for the script tags have been turned into their harmless escape code equivalents (e.g. `>` is now `>`).

```
<h1>  
  Author: Boon<script>alert(&#39;Test alert&#39;);</script>,  
  David (Boonie)  
</h1>
```

Using Django templates protects us against the majority of XSS attacks.

However it is possible to turn off this protection, and the protection isn't automatically applied to all tags that wouldn't normally be populated by user input.

It is also possible for XSS attacks to originate from other untrusted source of data, such as cookies, Web services or uploaded files (whenever the data is not sufficiently sanitized before including in a page).

If we're displaying data from these sources, then we may need to add our own sanitisation code.

## Cross site request forgery (CSRF) protection

CSRF attacks allow a malicious user to execute actions using the credentials of another user without that user's knowledge or consent. For example consider the case where we have a hacker who wants to create additional authors for our LocalLibrary.

In order to do this, they might create an HTML file like the one below, which contains an author-creation form (like the one we used in the previous section) that is submitted as soon as the file is loaded.

They would then send the file to all the Librarians and suggest that they open the file (it contains some harmless information, honest!).

If the file is opened by any logged in librarian, then the form would be submitted with their credentials and a new author would be created.

```
<html>
<body onload='document.EvilForm.submit() '>

<form action="http://127.0.0.1:8000/catalog/author/create/" method="post" name='EvilForm'>
  <table>
    <tr><th><label for="id_first_name">First name:</label></th>
    <td><input id="id_first_name" maxlength="100"
      name="first_name" type="text" value="Mad" required /></td></tr>
    <tr><th><label for="id_last_name">Last name:</label></th>
    <td><input id="id_last_name" maxlength="100"
      name="last_name" type="text" value="Man" required /></td></tr>
    <tr><th><label for="id_date_of_birth">Date of birth:</label></th>
    <td><input id="id_date_of_birth"
      name="date_of_birth" type="text" /></td></tr>
    <tr><th><label for="id_date_of_death">Died:</label></th>
    <td><input id="id_date_of_death"
      name="date_of_death" type="text" value="12/10/2016" /></td></tr>
  </table>
  <input type="submit" value="Submit" />
</form>

</body>
</html>
```

Run the development web server, and log in with your superuser account.

Copy the text above into a file and then open it in the browser. You should get a CSRF error, because Django has protection against this kind of thing.

The way the protection is enabled is that we include the `{% csrf_token %}` template tag in our form definition.

This token is then rendered in our HTML, with a value that is specific to the user on the current browser.

```
<input type='hidden' name='csrfmiddlewaretoken'  
       value='0QRWHnYVg776y2l66mcvZqp8a1rv4lb8S8lZ4ZJUWGZFA5VHrVfL2mpH29YZ39PW' />
```

Django generates a user/browser specific key and will reject forms that do not contain the field, or that contain an incorrect field value for the user/browser.

To use this type of attack the hacker now has to discover and include the CSRF key for the specific target user. They also can't use the "scattergun" approach of sending a malicious file to all librarians and hoping that one of them will open it, since the CSRF key is browser specific.

Django's CSRF protection is turned on by default. We should always use the `{% csrf_token %}` template tag in our forms and use `POST` for requests that might change or add data to the database.

## Other protections

Django also provides other forms of protection:

### SQL injection protection

SQL injection vulnerabilities enable malicious users to execute arbitrary SQL code on a database, allowing data to be accessed, modified, or deleted irrespective of the user's permissions. In almost every case you'll be accessing the database using Django's `QuerySets`/models, so the resulting SQL will be properly escaped by the underlying database driver. If we do need to write raw queries or custom SQL then we'll need to explicitly think about preventing SQL injection.



## Clickjacking protection

In this attack a malicious user hijacks clicks meant for a visible top level site and routes them to a hidden page beneath. This technique might be used, for example, to display a legitimate bank site but capture the login credentials in an invisible `<iframe>` controlled by the attacker. Django contains clickjacking protection in the form of the X-Frame-Options middleware which, in a supporting browser, can prevent a site from being rendered inside a frame.

## Enforcing SSL/HTTPS

SSL/HTTPS can be enabled on the web server in order to encrypt all traffic between the site and browser, including authentication credentials that would otherwise be sent in plain text (enabling HTTPS is highly recommended). If HTTPS is enabled then Django provides a number of other protections we can use:

- `SECURE_PROXY_SSL_HEADER` can be used to check whether content is secure, even if it is incoming from a non-HTTP proxy.
- `SECURE_SSL_REDIRECT` is used to redirect all HTTP requests to HTTPS.
- Use `HTTP Strict Transport Security` (HSTS). This is an HTTP header that informs a browser that all future connections to a particular site should always use HTTPS. Combined with redirecting HTTP requests to HTTPS, this setting ensures that HTTPS is always used after a successful connection has occurred. HSTS may either be configured with `SECURE_HSTS_SECONDS` and `SECURE_HSTS_INCLUDE_SUBDOMAINS` or on the Web server.
- Use 'secure' cookies by setting `SESSION_COOKIE_SECURE` and `CSRF_COOKIE_SECURE` to `True`. This will ensure that cookies are only ever sent over HTTPS.

## Host header validation

Use `ALLOWED_HOSTS` to only accept requests from trusted hosts.

There are many other protections, and caveats to the usage of the above mechanisms.

While this has given us an overview of what Django offers, we should still read the Django security documentation.