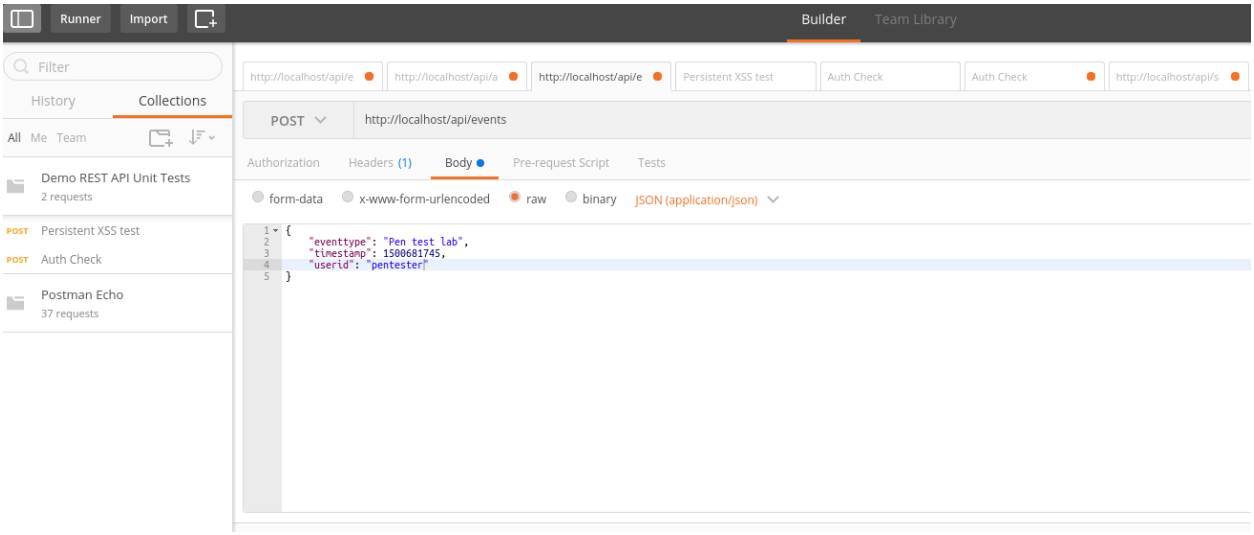
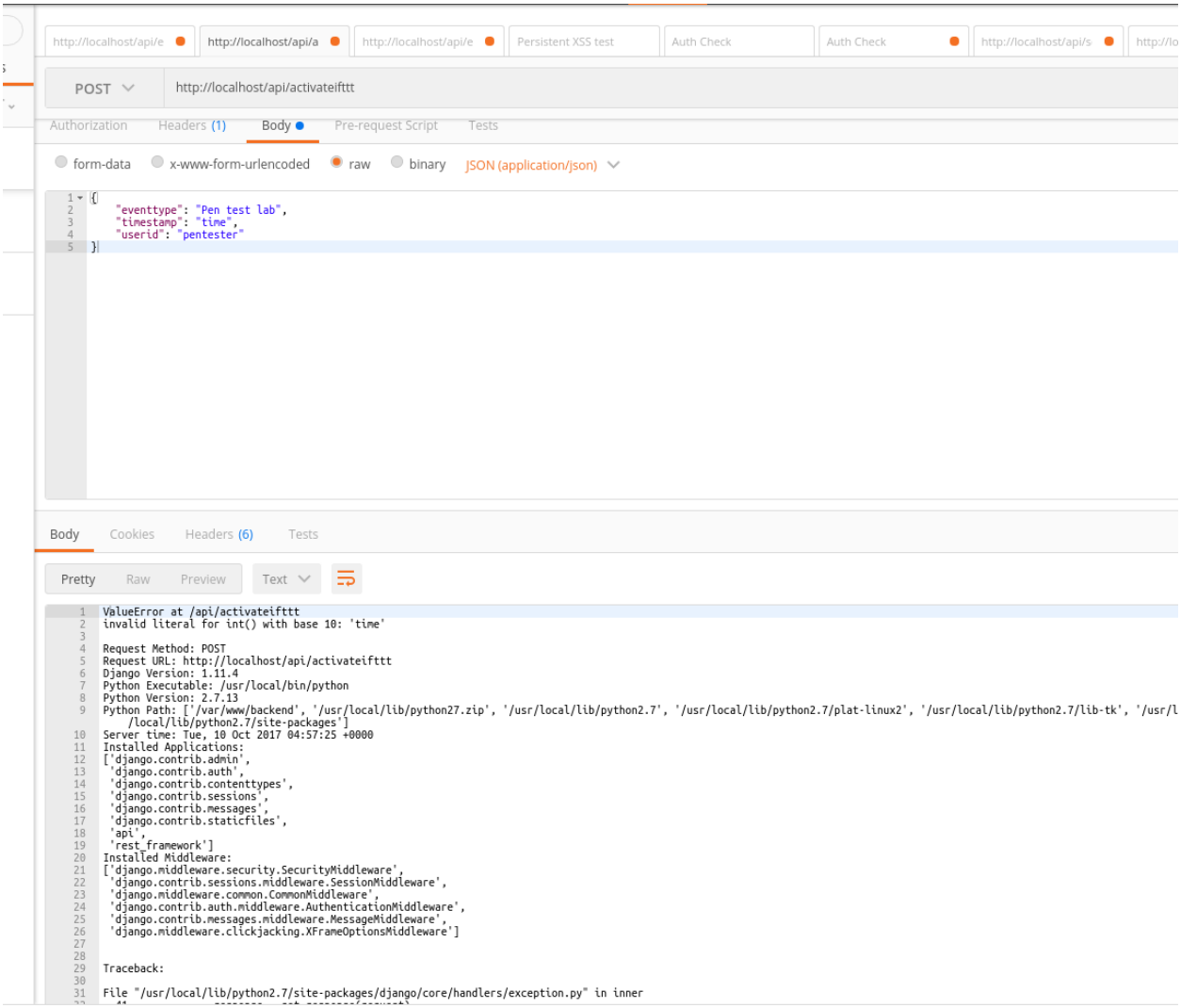
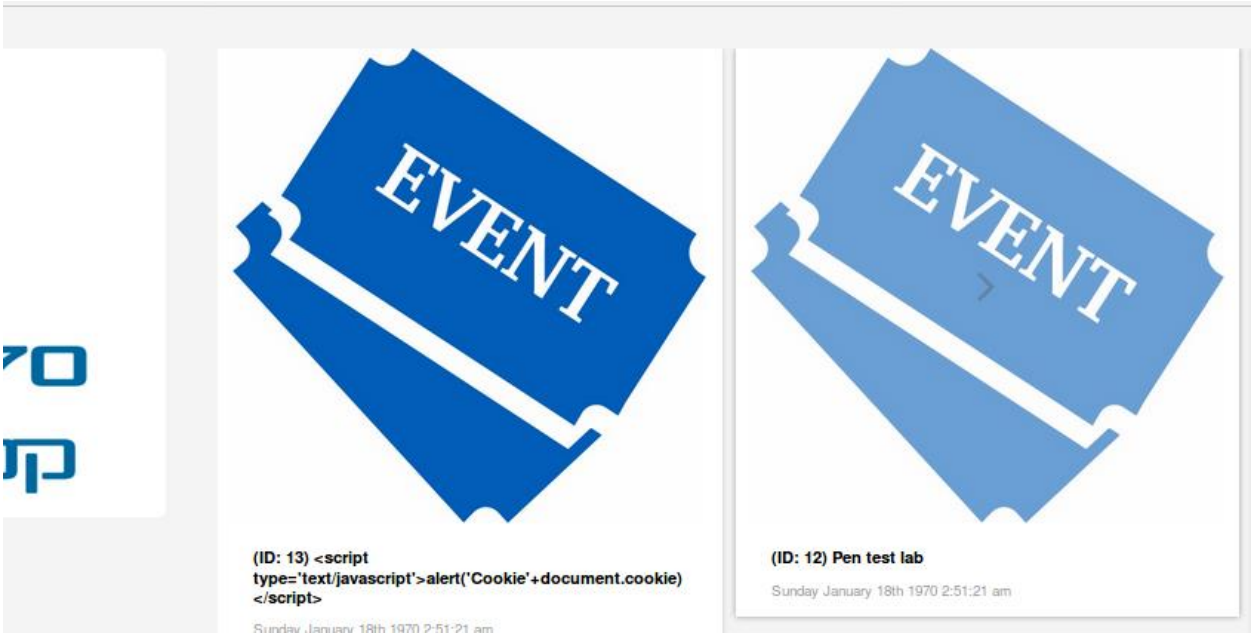
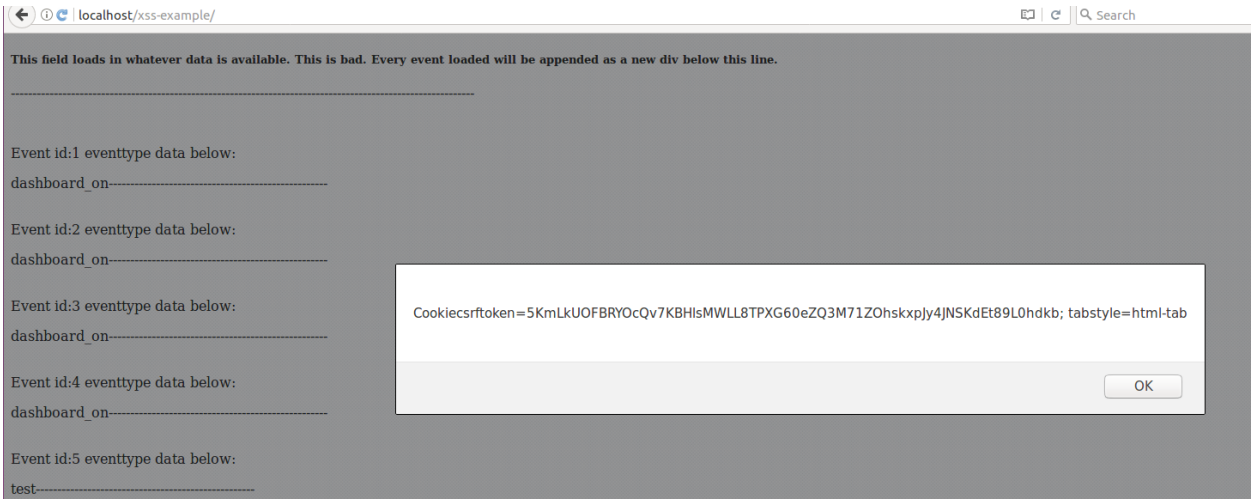
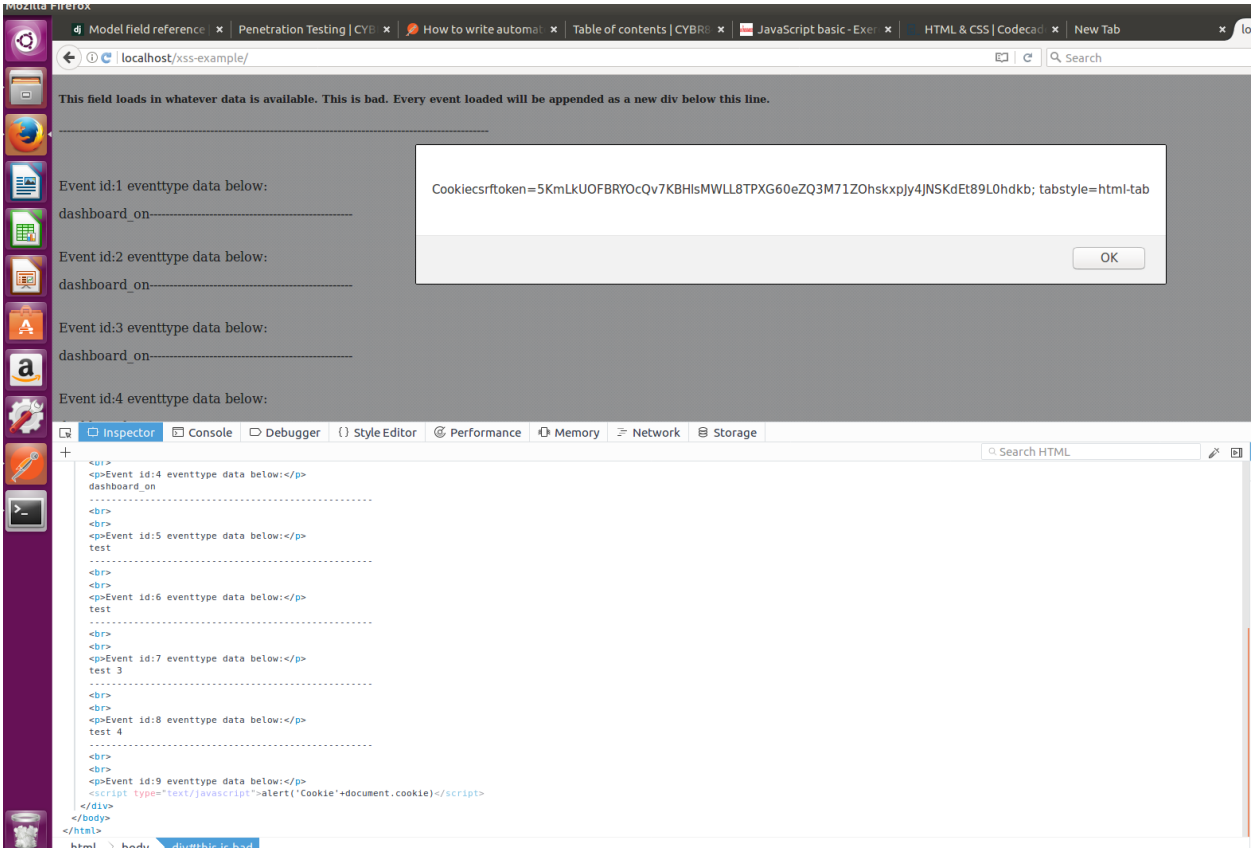

Runner
Import
Builder
Team Library
Filter
History
Collections
All Me Team
Demo REST API Unit Tests
2 requests
POST Persistent XSS test
POST Auth Check
Postman Echo
37 requests
http://localhost/api/e
http://localhost/api/a
http://localhost/api/e
Persistent XSS test
Auth Check
Auth Check
http://localhost/api/s
POST
http://localhost/api/events
Authorization
Headers (1)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{
"eventtype": "Pen test lab",
"timestamp": 1500681745,
"userid": "pentester"
}

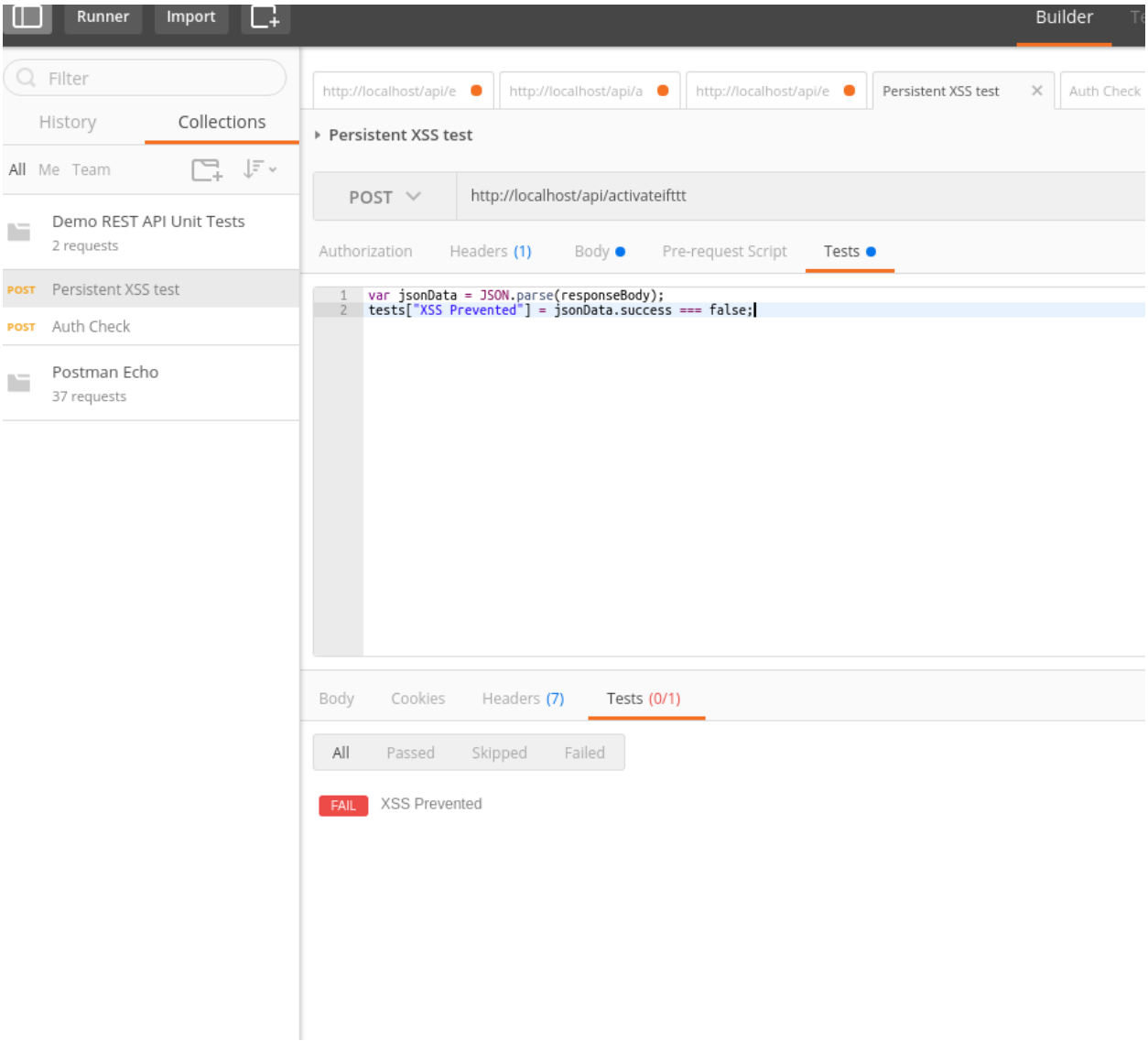

http://localhost/api/e
http://localhost/api/a
http://localhost/api/e
Persistent XSS test
Auth Check
Auth Check
http://localhost/api/s
POST
http://localhost/api/activateifttt
Authorization
Headers (1)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{
"eventtype": "Pen test lab",
"timestamp": "time",
"userid": "pentester"
}
Body
Cookies
Headers (6)
Tests
Pretty
Raw
Preview
Text
ValueError at /api/activateifttt
invalid literal for int() with base 10: 'time'
Request Method: POST
Request URL: http://localhost/api/activateifttt
Django Version: 1.11.4
Python Executable: /usr/local/bin/python
Python Version: 2.7.13
Python Path: ['/var/www/backend', '/usr/local/lib/python27.zip', '/usr/local/lib/python2.7', '/usr/local/lib/python2.7/plat-linux2', '/usr/local/lib/python2.7/lib-tk', '/usr/l
/local/lib/python2.7/site-packages']
Server time: Tue, 10 Oct 2017 04:57:25 +0000
Installed Applications:
['django.contrib.admin',
'django.contrib.auth',
'django.contrib.contenttypes',
'django.contrib.sessions',
'django.contrib.messages',
'django.contrib.staticfiles',
'api',
'rest_framework']
Installed Middleware:
['django.middleware.security.SecurityMiddleware',
'django.contrib.sessions.middleware.SessionMiddleware',
'django.middleware.common.CommonMiddleware',
'django.contrib.auth.middleware.AuthenticationMiddleware',
'django.contrib.messages.middleware.MessageMiddleware',
'django.middleware.clickjacking.XFrameOptionsMiddleware']
Traceback:
File "/usr/local/lib/python2.7/site-packages/django/core/handlers/exception.py" in inner

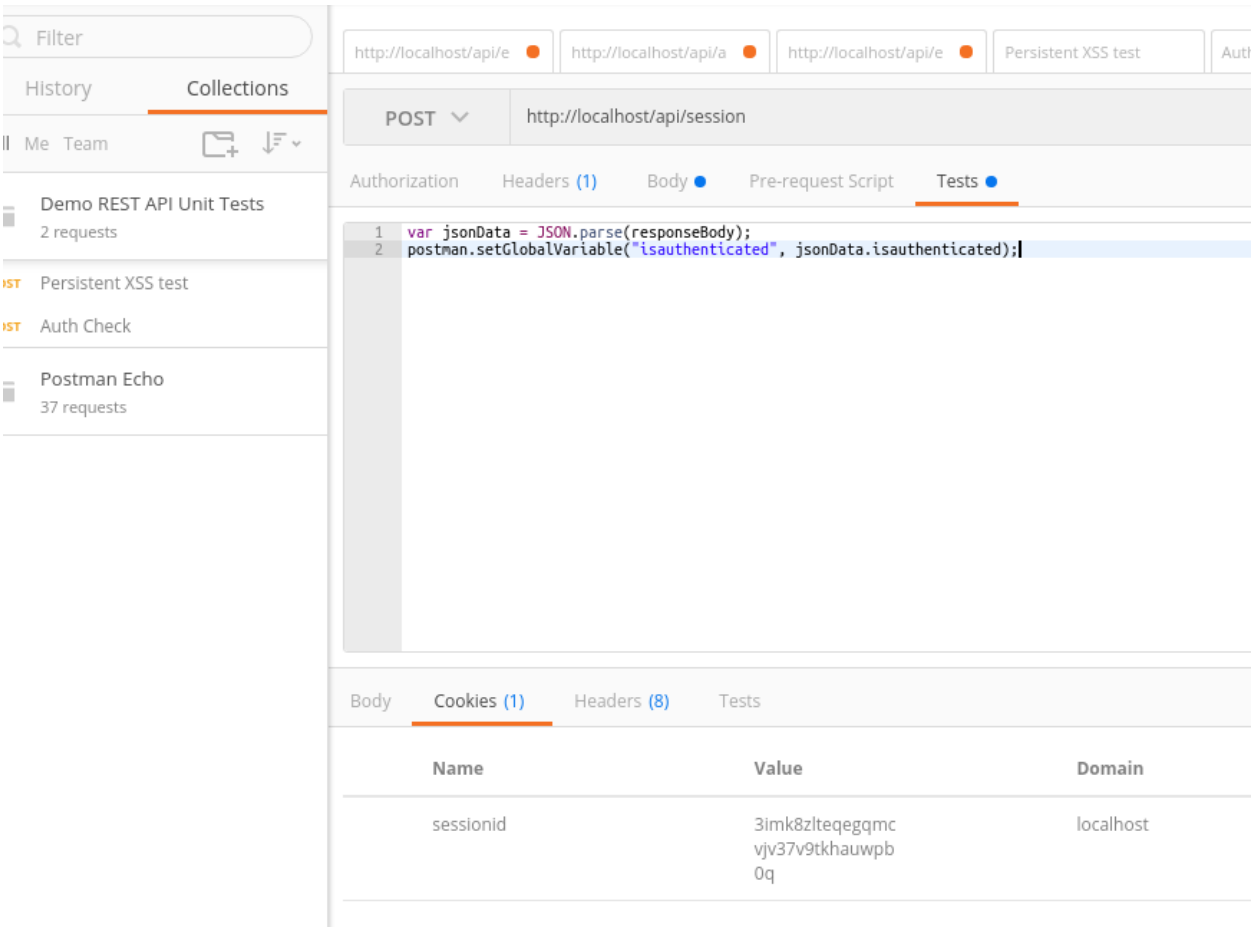

EVENT
(ID: 13) <script type='text/javascript'>alert('Cookie'+document.cookie)</script>
EVENT
(ID: 12) Pen test lab
Sunday January 18th 1970 2:51:21 am

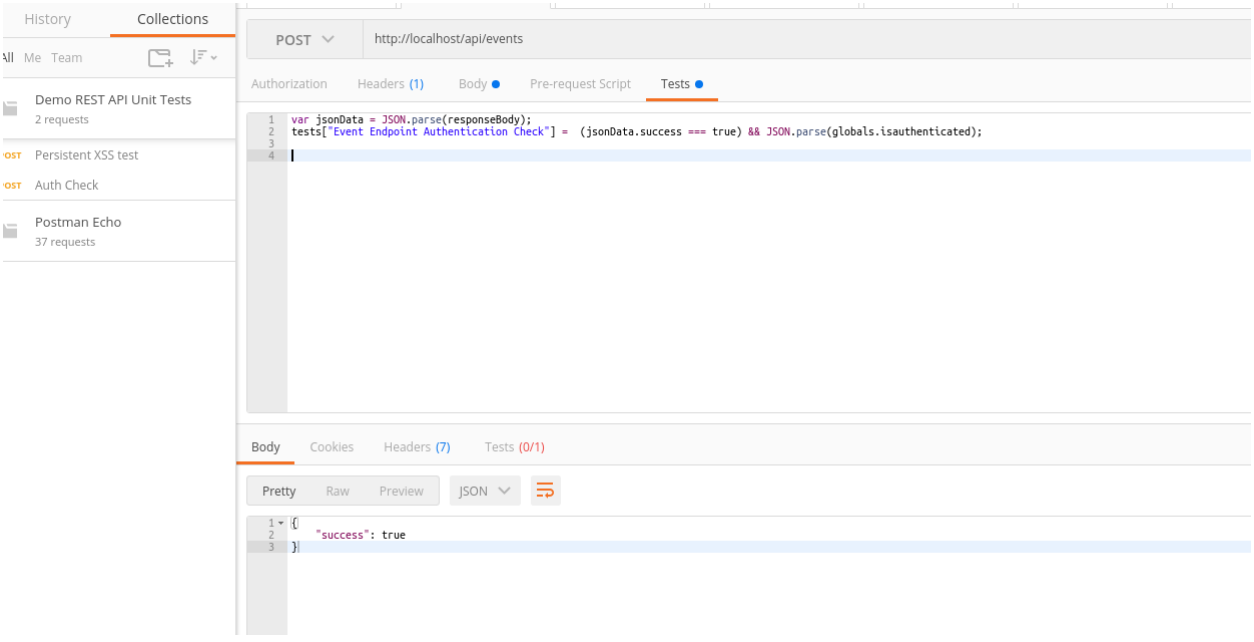

localhost/xss-example/
Search
This field loads in whatever data is available. This is bad. Every event loaded will be appended as a new div below this line.
Event id:1 eventtype data below:
dashboard_on
Event id:2 eventtype data below:
dashboard_on
Event id:3 eventtype data below:
dashboard_on
Event id:4 eventtype data below:
dashboard_on
Event id:5 eventtype data below:
test
Cookiecsrftoken=5KmLkUOFBRYOcQv7KBHlsMWLL8TPXG60eZQ3M71ZOhskxpJy4JNSKdEt89L0hdkb; tabstyle=html-tab
OK

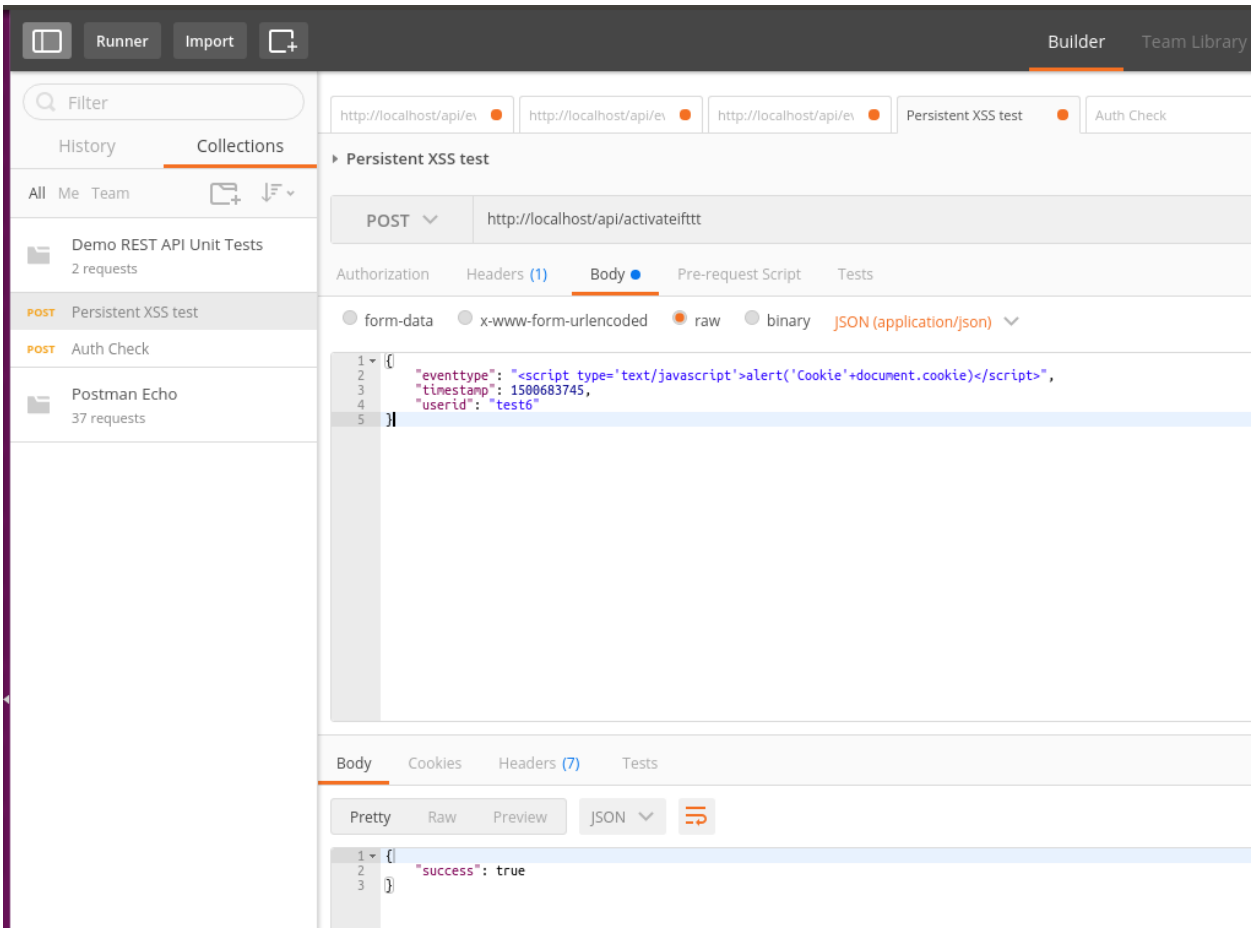

Model field reference
Penetration Testing | CYB
How to write automat
Table of contents | CYBR
JavaScript basic - Exer
HTML & CSS | Codecad
New Tab
localhost/xss-example/
Search
This field loads in whatever data is available. This is bad. Every event loaded will be appended as a new div below this line.
Event id:1 eventtype data below:
dashboard_on
Event id:2 eventtype data below:
dashboard_on
Event id:3 eventtype data below:
dashboard_on
Event id:4 eventtype data below:
Cookiecsrftoken=5KmLkUOFBRYOcQv7KBHlsMWLL8TPXG60eZQ3M71ZOhskxpJy4JNSKdEt89L0hdkb; tabstyle=html-tab
OK
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Search HTML
Event id:4 eventtype data below:
dashboard_on
Event id:5 eventtype data below:
test
Event id:6 eventtype data below:
test
Event id:7 eventtype data below:
test 3
Event id:8 eventtype data below:
test 4
Event id:9 eventtype data below:
<script type="text/javascript">alert('Cookie'+document.cookie)</script>

</body>
</html>


Runner
Import
Builder
Filter
History
Collections
All Me Team
Demo REST API Unit Tests
2 requests
POST Persistent XSS test
POST Auth Check
Postman Echo
37 requests
http://localhost/api/e
http://localhost/api/a
http://localhost/api/e
Persistent XSS test
Auth Check
Persistent XSS test
POST
http://localhost/api/activateifttt
Authorization
Headers (1)
Body
Pre-request Script
Tests
1 var jsonData = JSON.parse(responseBody);
2 tests["XSS Prevented"] = jsonData.success === false;
Body
Cookies
Headers (7)
Tests (0/1)
All
Passed
Skipped
Failed
FAIL
XSS Prevented

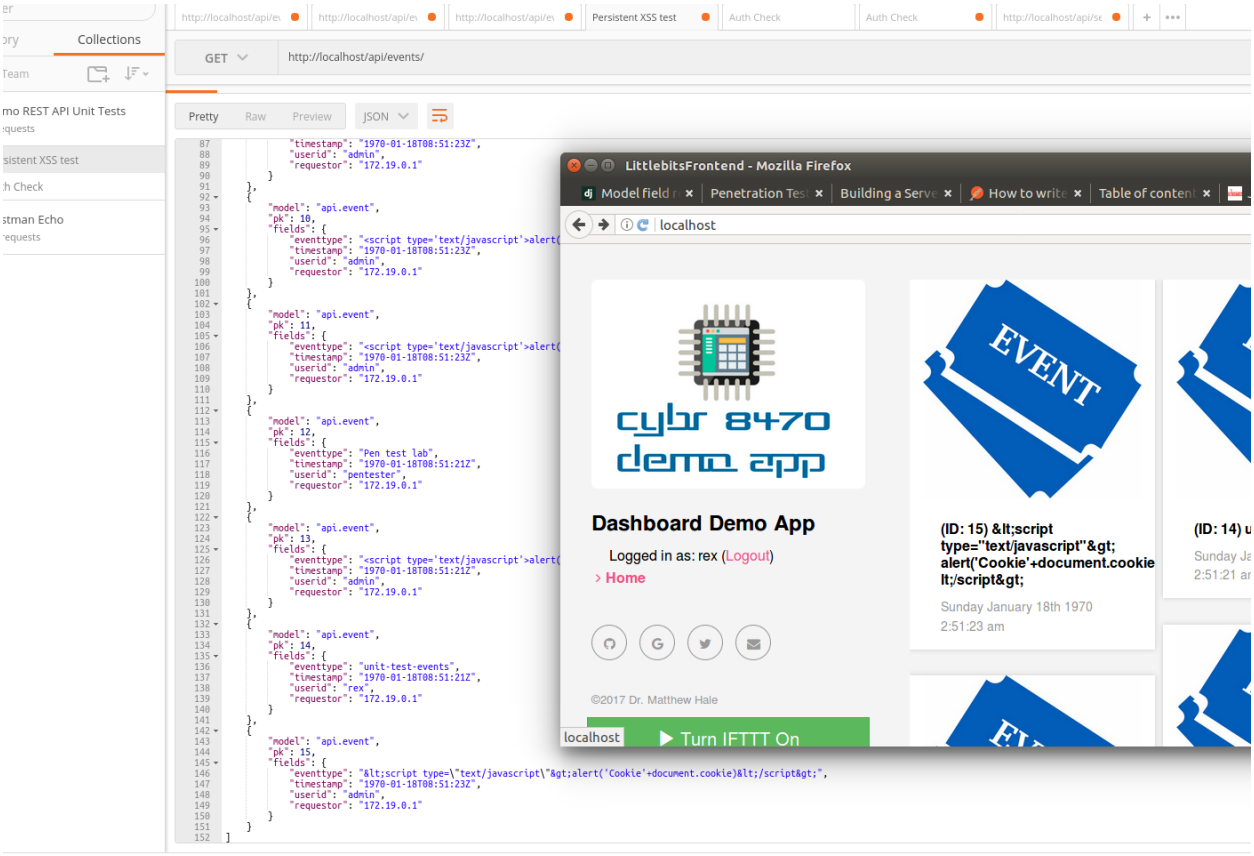

Filter
History
Collections
Me Team
Demo REST API Unit Tests
2 requests
Persistent XSS test
Auth Check
Postman Echo
37 requests
http://localhost/api/e
http://localhost/api/a
http://localhost/api/e
Persistent XSS test
POST
http://localhost/api/session
Authorization
Headers (1)
Body
Pre-request Script
Tests
var jsonData = JSON.parse(responseBody);
postman.setGlobalVariable("isauthenticated", jsonData.isauthenticated);
Body
Cookies (1)
Headers (8)
Tests
Name
Value
Domain
sessionid
3imk8zlteqegqmc vjv37v9tkhauwpb 0q
localhost

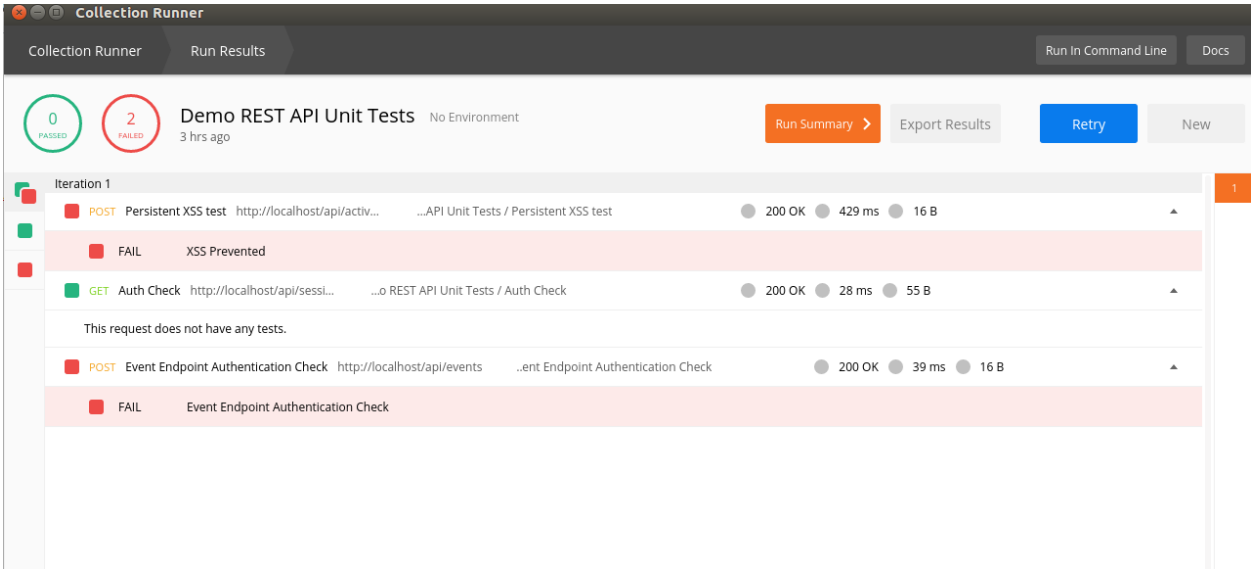

History
Collections
Demo REST API Unit Tests
2 requests
Persistent XSS test
Auth Check
Postman Echo
37 requests
POST
http://localhost/api/events
Authorization
Headers (1)
Body
Pre-request Script
Tests
var jsonData = JSON.parse(responseBody);
tests["Event Endpoint Authentication Check"] = (jsonData.success === true) && JSON.parse(globals.isauthenticated);
Body
Cookies
Headers (7)
Tests (0/1)
Pretty
Raw
Preview
JSON
{
"success": true
}


Runner
Import
Builder
Team Library
Filter
History
Collections
All Me Team
Demo REST API Unit Tests
2 requests
POST Persistent XSS test
POST Auth Check
Postman Echo
37 requests
Persistent XSS test
Auth Check
Persistent XSS test
POST
http://localhost/api/activateifttt
Authorization
Headers (1)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{
"eventtype": "<script type='text/javascript'>alert('Cookie'+document.cookie)</script>",
"timestamp": 1500683745,
"userid": "test6"
}
Body
Cookies
Headers (7)
Tests
Pretty
Raw
Preview
JSON
{
"success": true
}

pentest.md models.py

```python
from __future__ import unicode_literals

from django.db import models
from django.core.validators import *

from django.contrib.auth.models import User, Group

from django.contrib import admin
import base64
from django_bleach.models import BleachField

class Event(models.Model):
    #eventtype = models.CharField(max_length=1000, blank=False)
    eventtype = BleachField()
    timestamp = models.DateTimeField()
    userid = models.CharField(max_length=1000, blank=True)
    requestor = models.GenericIPAddressField(blank=False)

    def __str__(self):
        return str(self.eventtype)

class EventAdmin(admin.ModelAdmin):
```





Code changes for Django bleach can be found at - https://github.com/akhampariya/CYBR8470-building-a-webservice-lab/tree/my-work