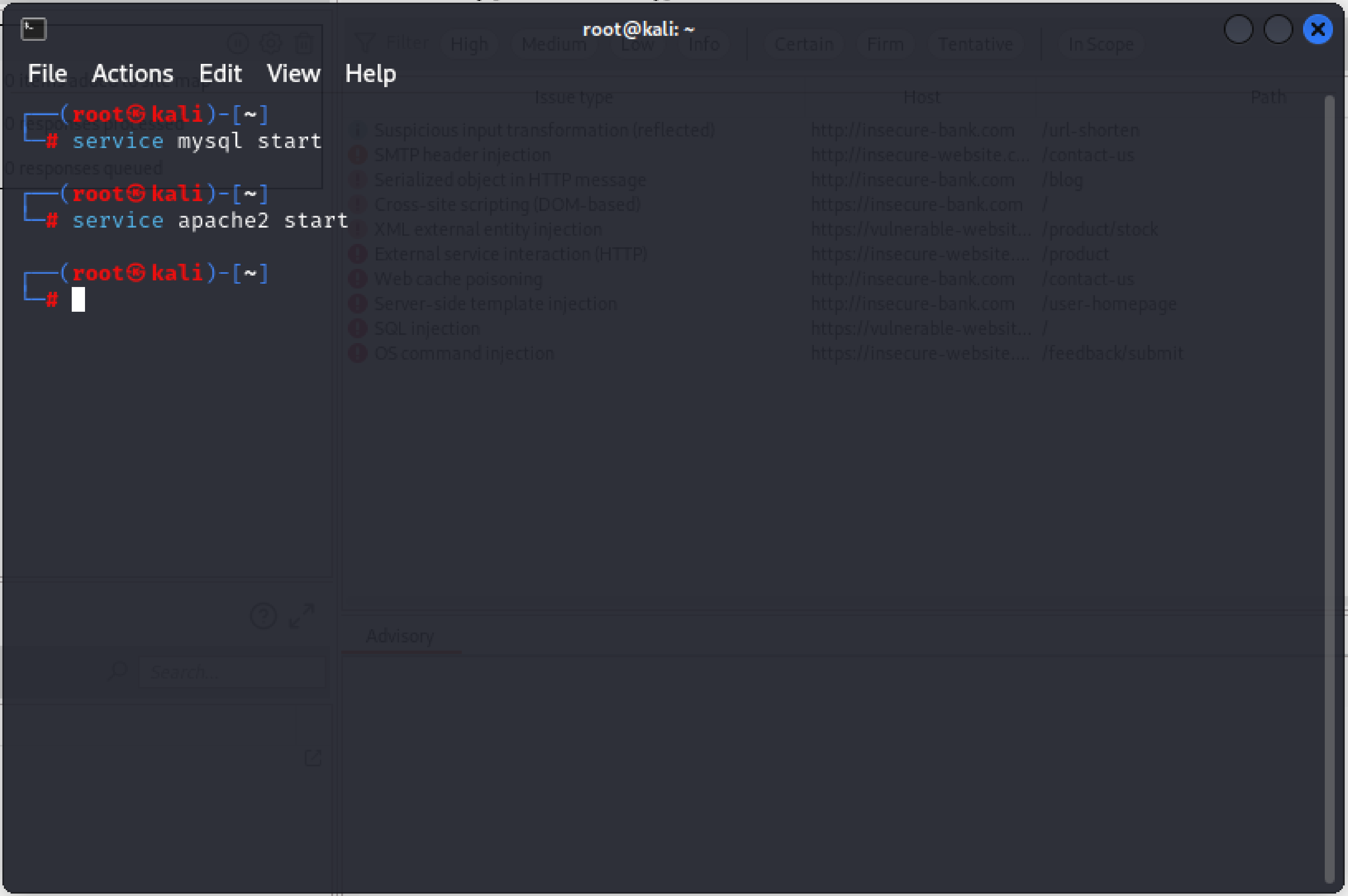


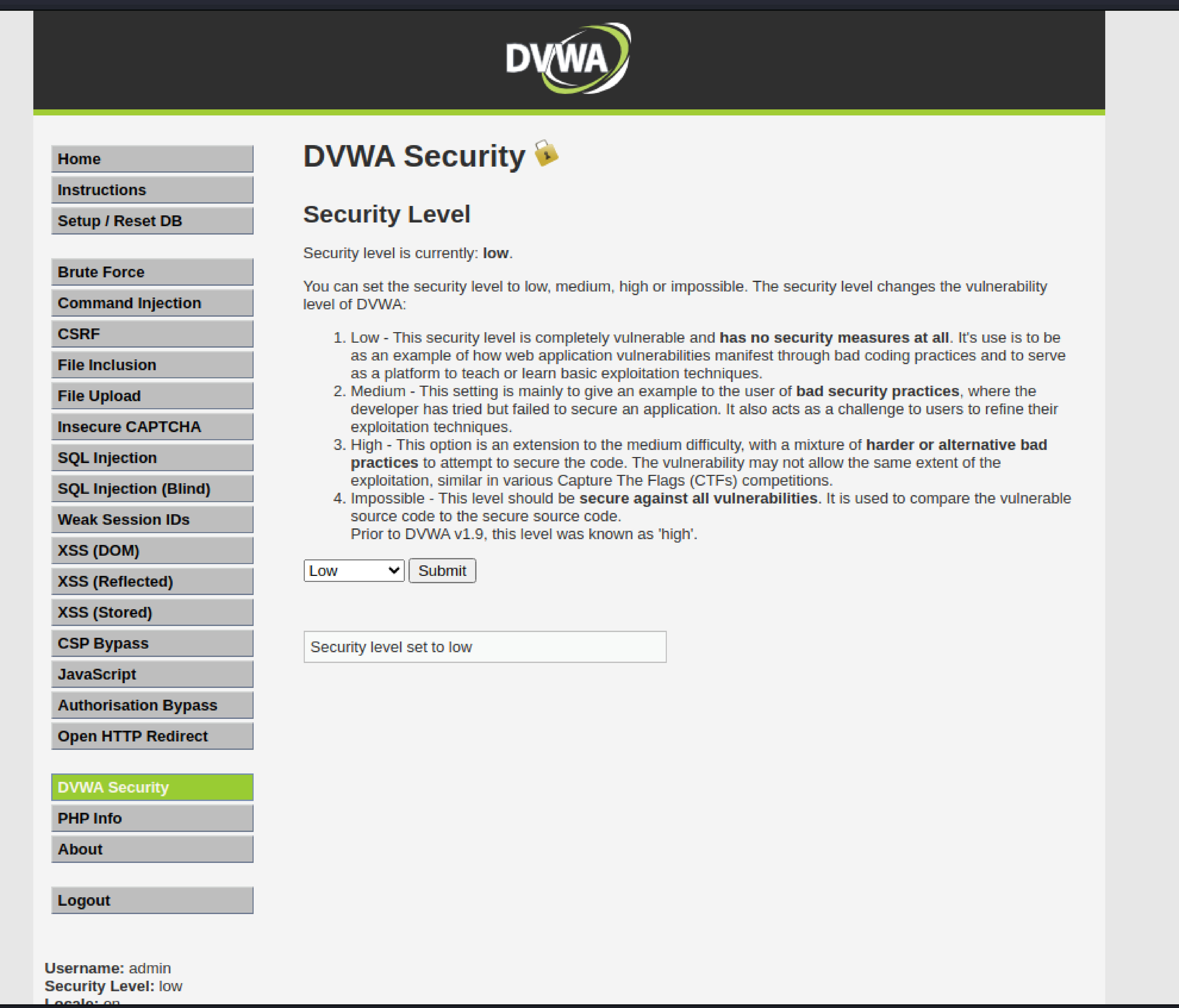
```
┌──(root㉿kali)-[~]
└─# service mysql start

┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# 
```

0 items added to site map
0 responses processed
0 responses queued

| Issue type | Host | Path |
|---|---|---|
| Suspicious input transformation (reflected) | http://insecure-bank.com | /url-shorten |
| SMTP header injection | http://insecure-website.c... | /contact-us |
| Serialized object in HTTP message | http://insecure-bank.com | /blog |
| Cross-site scripting (DOM-based) | https://insecure-bank.com | / |
| XML external entity injection | https://vulnerable-websit... | /product/stock |
| External service interaction (HTTP) | https://insecure-website.... | /product |
| Web cache poisoning | http://insecure-bank.com | /contact-us |
| Server-side template injection | http://insecure-bank.com | /user-homepage |
| SQL injection | https://vulnerable-websit... | / |
| OS command injection | https://insecure-website.... | /feedback/submit |



# DVWA Security

## Security Level

Security level is currently: **low**.

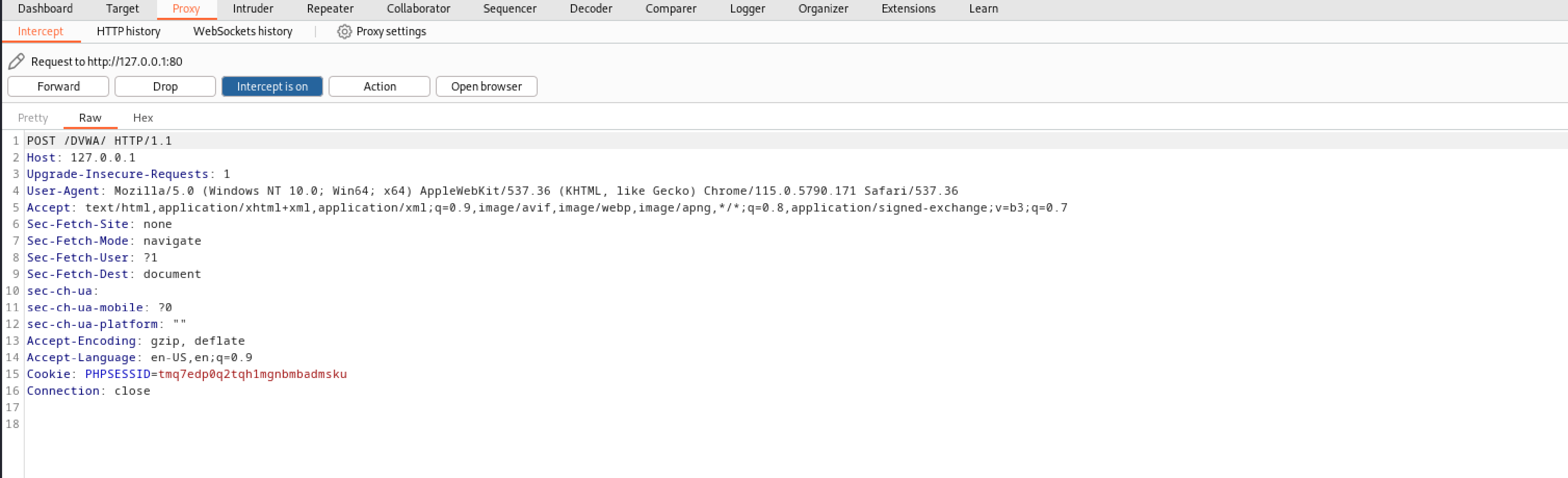
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low ▾ Submit

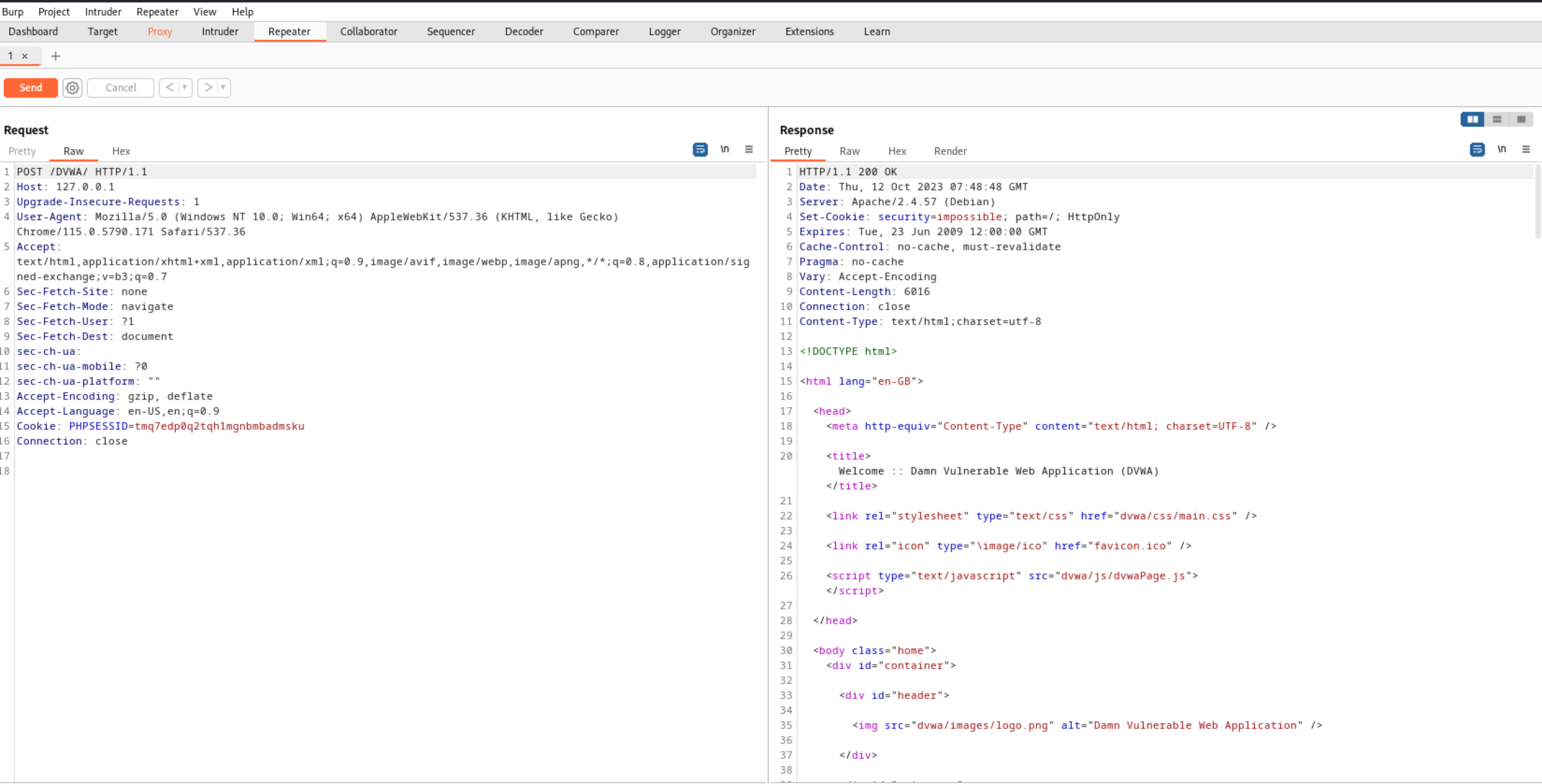
Security level set to low

**Username:** admin
**Security Level:** low
**Locale:** en



```
POST /DVWA/ HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=tmq7edp0q2tqh1mgnbmbadmsku
Connection: close


```



Request

```
POST /DVWA/ HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=tmq7edp0q2tqh1mgnbmbadmsku
Connection: close


```

Response

```
HTTP/1.1 200 OK
Date: Thu, 12 Oct 2023 07:48:48 GMT
Server: Apache/2.4.57 (Debian)
Set-Cookie: security=impossible; path=/; HttpOnly
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6016
Connection: close
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Welcome :: Damn Vulnerable Web Application (DVWA)
    </title>

    <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

    <link rel="icon" type="\image/ico" href="favicon.ico" />

    <script type="text/javascript" src="dvwa/js/dvwaPage.js">
    </script>

  </head>

  <body class="home">
    <div id="container">

      <div id="header">

        <img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

      </div>

```