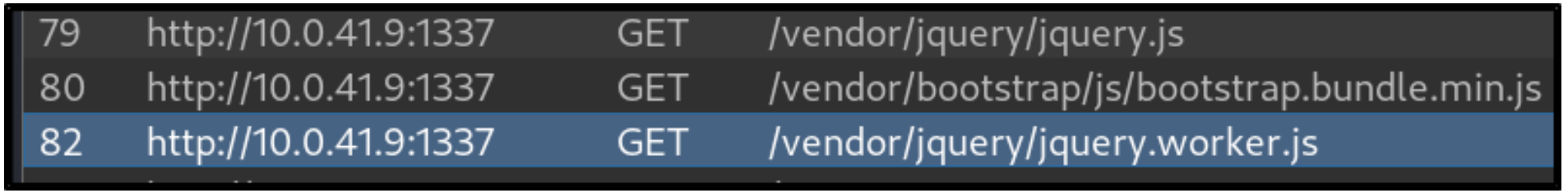
Netz-Arbeiter – HTTP Response Analysis



If you examine the traffic sent between the server and the client, we see that we make a request to the **jquery.worker.js** endpoint

Netz-Arbeiter – HTTP Response Analysis

```
{
  const workerResult =
  'Result: [redacted]';

  //console.log('Worker: Posting message back to main
   script');
  postMessage(workerResult);
}
return  postMessage('Try harder');
```

If we look at the Response from the endpoint, because it is a JavaScript file, we will see the code contained within it

Netz-Arbeiter – HTTP Response Analysis

```
{
  const workerResult =
  'Result: [redacted]';

  //console.log('Worker: Posting message back to main
   script');
  postMessage(workerResult);
}
return  postMessage('Try harder');
```

In a pentest report, this kind of vulnerability would fall under **Client-Side Storage of Sensitive Data** or **Hardcoded Secrets in JavaScript**