

Netz-Arbeiter – HTTP Response Analysis

79	http://10.0.41.9:1337	GET	/vendor/jquery/jquery.js
80	http://10.0.41.9:1337	GET	/vendor/bootstrap/js/bootstrap.bundle.min.js
82	http://10.0.41.9:1337	GET	/vendor/jquery/jquery.worker.js

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: HTTP_200 OK (text/html); charset=UTF-8';  
  
  //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**