**Lab Walkthrough: Exploiting Path-Based Web Cache Poisoning**

**1. Identify a Target Endpoint**

* Launched Burp’s embedded browser.
* Navigated to the lab-provided URL. **A screenshot of a computer

  AI-generated content may be incorrect.**
* Logged in using the credentials:  
  **Username:** wiener

**Password:** peter

* Observed the response after login; notice that it included the API key for user wiener.

A screenshot of a account

AI-generated content may be incorrect.

**2. Find Path Mapping Discrepancy**

* Went to **Proxy > HTTP history**.
* Located the GET /my-account request.
* Right clicked the request and selected **Send to Repeater**.

**Test #1: Arbitrary Path Segment**

* In Repeater, changed the path to /my-account/abc.
* Sent the request.
* Noticed that the response still contained the API key — showing that the server treated /my-account/abc the same as /my-account.

**Test #2: Static File Extension**

* Modified the path to /my-account/abc.js.

A screenshot of a computer

AI-generated content may be incorrect.

* Sent the request.
* Noticed response headers:
  + X-Cache: miss
  + Cache-Control: max-age=30
* Sent the same request again within 30 seconds.
* Observed X-Cache: hit — confirmed that response was now served from the cache.

**3. Craft and Deliver Exploit**

* Opened **Go to exploit server** in Burp’s browser.

A screenshot of a computer

AI-generated content may be incorrect.

* In the exploit body, inserted the following JavaScript payload to redirect the victim:

<script>document.location="https://YOUR-LAB-ID.web-security-academy.net/my-account/wcd.js"</script>

* Replaced YOUR-LAB-ID with the lab’s actual ID.
* Clicked **Deliver exploit to victim**.

**4. Retrieve API Key**

* Visited:  
  https://YOUR-LAB-ID.web-security-academy.net/my-account/wcd.js
* Saw that the response included **carlos’ API key**.

A screenshot of a computer

AI-generated content may be incorrect.

* Copied the key.

**5. Submit Solution**

* Clicked **Submit solution**.
* Pasted **Carlos' API key**.
* Lab completed successfully.

A screenshot of a computer

AI-generated content may be incorrect.