

Lab: Information disclosure on debug page

1. With Burp running, browse to the home page.
2. Go to the "Target" > "Site Map" tab. Right-click on the top-level entry for the lab and select "Engagement tools" > "Find comments". Notice that the home page contains an HTML comment that contains a link called "Debug". This points to `/cgi-bin/phpinfo.php`.

```
Request
Pretty Raw Hex
1 GET /cgi-bin/phpinfo.php HTTP/1.1
2 Host: 0a2d001a049abe27c0c67bb2006f00a2.web-security-academy.net
3 Cookie: session=kSxUU7mRoTIkyI3oeku1ji6zmtKuokFC
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/201001
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
6 Accept-Language: en-GB,en;q=0.5
```

5. In the site map, right-click on the entry for `/cgi-bin/phpinfo.php` and select "Send to Repeater".
6. In Burp Repeater, send the request to retrieve the file. Notice that it reveals various debugging information, including the `SECRET_KEY` environment variable.

```
<tr>
  <td class="e">
    SECRET_KEY
  </td>
  <td class="v">
    kwwb2hvw0bxx711senacmccau9f7n1q
  </td>
</tr>
```

9. Go back to the lab, click "Submit solution", and enter the `SECRET_KEY` to solve the lab.