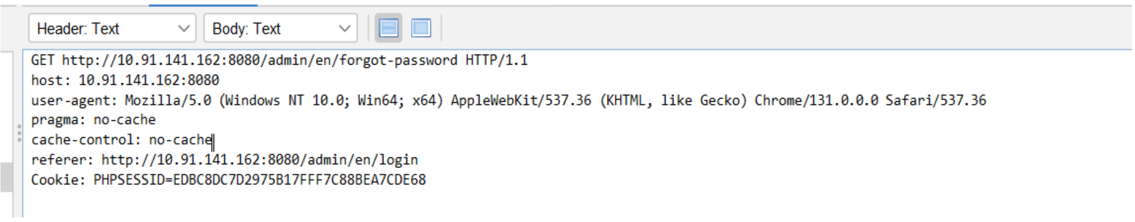
VAPT Report

Finding #1: Content Security Policy (CSP) Header Not Set

- **Severity:** Medium
- **Risk:** High (can lead to exploitation via XSS, data injection, content hijacking)
- **Affected URL:** `http://10.91.141.162:8080/admin/en/forgot-password`
- **Parameter:** N/A (applies at HTTP header level)
- **Input Vector:** Passive (Header Missing)
- **Alert Reference:** 10038-1
- **CWE ID:** 693 (Protection Mechanism Failure)
- **WASC ID:** 15 (Application Misconfiguration)
- **Evidence:**
  - Request:



```
GET http://10.91.141.162:8080/admin/en/forgot-password HTTP/1.1
host: 10.91.141.162:8080
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://10.91.141.162:8080/admin/en/login
Cookie: PHPSESSID=EDBC8DC7D2975B17FFF7C88BEA7CDE68
```

  - Response headers did not include `Content-Security-Policy`.

Description:
The application does not set the `Content-Security-Policy (CSP)` header in HTTP responses.
CSP is a critical security control that helps mitigate **Cross-Site Scripting (XSS)**, **Clickjacking**, and other injection-based attacks by restricting the sources of content that can be executed in the browser.
Without CSP, attackers may be able to inject malicious scripts or resources that execute in the user's browser.

Impact:

- Increased risk of **Cross-Site Scripting (XSS)** attacks.
- Attackers could steal session tokens, cookies, or sensitive user data.
- Possible defacement or malware injection through vulnerable third-party scripts.

Recommendation (Solution):

- Configure the web server / application server to include a strong CSP header in all responses.
- Example secure CSP policy (adjust based on your application needs):

-
  ```
  Content-Security-Policy: default-src 'self';
  script-src 'self' https://trusted.cdn.com;
  style-src 'self';
  frame-ancestors 'none';
  object-src 'none';
  ```
- Regularly review and tighten CSP policies to restrict execution only to trusted sources.
- Test policies in **report-only** mode before enforcing, to avoid breaking application functionality.

Remediation Priority:
● Apply in **next patch cycle** (before next release).

Nice one ✅ You've shared another **CSP header missing** finding, but this time for a different endpoint:

```
http://10.91.141.162:8080/tl/vulnerability?...
```

I'll document it professionally and then we'll expand your **Findings Table**.

Finding #2: Content Security Policy (CSP) Header Not Set

- **Severity:** Medium
- **Risk:** High (client-side exploitation possible)
- **Affected URL:**
- `http://10.91.141.162:8080/tl/vulnerability?captcha=ZAP&email=zaproxy%40example.com&message=...`
- **Parameter:** N/A (Header missing)
- **Input Vector:** Passive (Header Missing)
- **Alert Reference:** 10038-1
- **CWE ID:** 693 (Protection Mechanism Failure)
- **WASC ID:** 15 (Application Misconfiguration)

Evidence:

- The HTTP response from the above endpoint did not include a `Content-Security-Policy` header.

Description:
The application does not set a `Content-Security-Policy (CSP)` header in HTTP responses. Without CSP, browsers do not restrict the sources of executable content. This increases the risk of client-side injection attacks such as **Cross-Site Scripting (XSS)**.

Impact:

- Increased likelihood of successful XSS attacks.
- Possible theft of session tokens, cookies, or other sensitive data.
- Injection of malicious scripts or content from untrusted domains.

Recommendation:

- Configure a strict CSP policy at the web server or application level. Example:
- `Content-Security-Policy: default-src 'self'; script-src 'self' https://trusted.cdn.com; style-src 'self'; frame-ancestors 'none'; object-src 'none';`
- Test the CSP in **report-only mode** before enforcing to prevent application breakage.
- Regularly review and refine CSP policies.

Remediation Priority:
□ Apply within the **next patch cycle**.

📊 Updated Summary of Findings

Severity	Vulnerability	Affected Asset	CWE/WASC	Status
Medium	Content Security Policy (CSP) Header Not Set	`http://10.91.141.162:8080/admin/en/forgot-password`	CWE-693 / WASC-15	Open
Medium	Content Security Policy (CSP) Header Not Set	`http://10.91.141.162:8080/tl/vulnerability?captcha=ZAP&email=...&uploadFile=...`	CWE-693 / WASC-15	Open

---

Contents