Sri Lanka Institute of Information Technology

Missing Content Security Policy (CSP) Header and Potential Clickjacking Vulnerability

IE2062 - Web Security

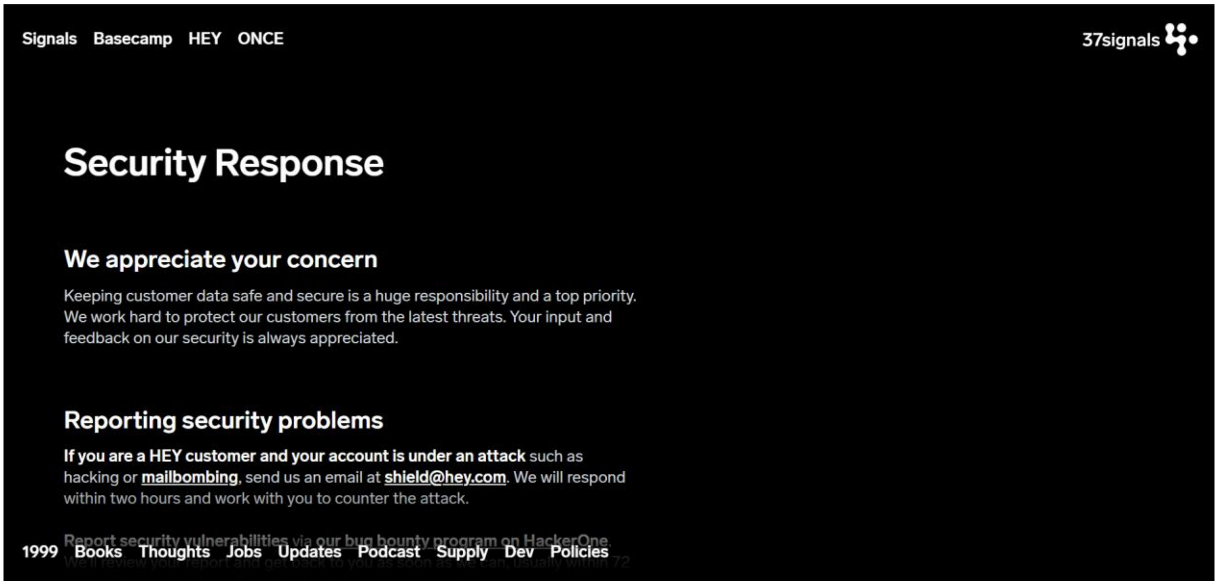
IT23269484 - T. H. Ranasinghe

Missing Content Security Policy (CSP) Header and Potential Clickjacking Vulnerability

1. Vulnerability Title

Missing Content Security Policy (CSP) Header and Potential Clickjacking Vulnerability on Basecamp Security Response Page

2. Vulnerability Description



Security Response

We appreciate your concern

Keeping customer data safe and secure is a huge responsibility and a top priority. We work hard to protect our customers from the latest threats. Your input and feedback on our security is always appreciated.

Reporting security problems

If you are a HEY customer and your account is under an attack such as hacking or **mailbombing**, send us an email at **shield@hey.com**. We will respond within two hours and work with you to counter the attack.

Report security vulnerabilities via **our bug bounty program on HackerOne**. We'll review your report and get back to you as soon as we can, usually within 72

During a security assessment of the website **https://basecamp.com/about/policies/security/response**, I identified that the page lacks two critical security headers **Content-Security-Policy (CSP)** and **X-Frame-Options**. The absence of a CSP header may allow unintended content sources to load, weakening the site's security posture. Similarly, the missing X-Frame-Options header indicates a potential vulnerability to **clickjacking**, where an attacker could embed the page in a malicious iframe to trick users into performing unintended actions.

I used multiple tools to assess these issues:

- OWASP ZAP: Flagged the absence of CSP and X-Frame-Options headers during a passive scan.
- Nikto: Confirmed the missing security headers.
- Nmap: Identified that the site uses Cloudflare for protection, but the headers remain unset.

While the missing headers suggest potential vulnerabilities, I conducted tests to determine if the site is exploitable for clickjacking. By attempting to embed the page in an iframe, I confirmed it is frameable, but the page's static content and lack of actionable elements (e.g., forms or buttons) prevented any exploitable actions. Despite the missing headers, the site appears resilient to immediate exploitation, likely due to Cloudflare's protections and the page's design.

3. Affected Components

- **URL**: https://basecamp.com/about/policies/security/response
- **Missing Headers**:
  - Content-Security-Policy
  - X-Frame-Options
- **CWE ID**: 693 - Protection Mechanism Failure
- **WASC ID**: 15 - Application Misconfiguration

4. Impact Assessment

- **Risk Level**: Medium

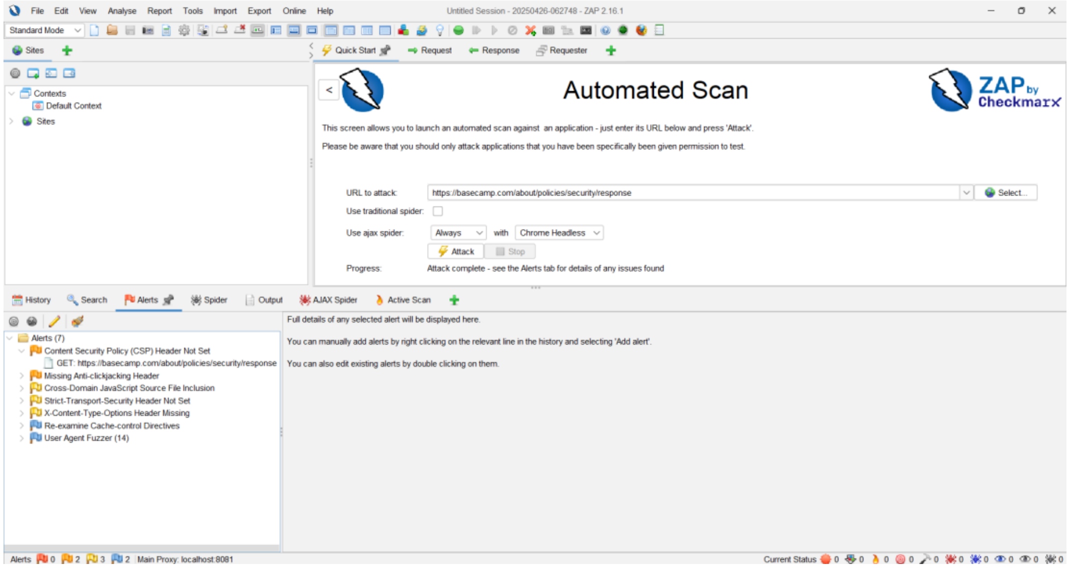
The missing CSP header could allow unintended content to load if other protections fail, potentially weakening the site's security. The missing X-Frame-Options header suggests a risk of clickjacking, where an attacker could embed the page in an iframe and overlay deceptive elements to capture user clicks. Potential impacts include:

- Tricking users into performing unintended actions (e.g., clicking a hidden button).
- Combining with other vulnerabilities to amplify attacks.

However, the tested page is primarily informational, with no interactive elements like forms or buttons that could be exploited via clickjacking. Testing confirmed no exploitable actions, reducing the immediate risk. Adding these headers would further strengthen the site’s security posture.

5. Steps to Reproduce

1. **CSP Header Check with OWASP ZAP**:
   - Scanned https://basecamp.com/about/policies/security/response using OWASP ZAP’s passive scan.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://basecamp.com/about/policies/security/response

Use traditional spider: □

Use ajax spider: Always with Chrome Headless

Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (7)
- Content Security Policy (CSP) Header Not Set
  - GET: https://basecamp.com/about/policies/security/response
- Missing Anti-clickjacking Header
- Cross-Domain JavaScript Source File Inclusion
- Strict-Transport-Security Header Not Set
- X-Content-Type-Options Header Missing
- Re-examine Cache-control Directives
- User Agent Fuzzer (14)

Full details of any selected alert will be displayed here.

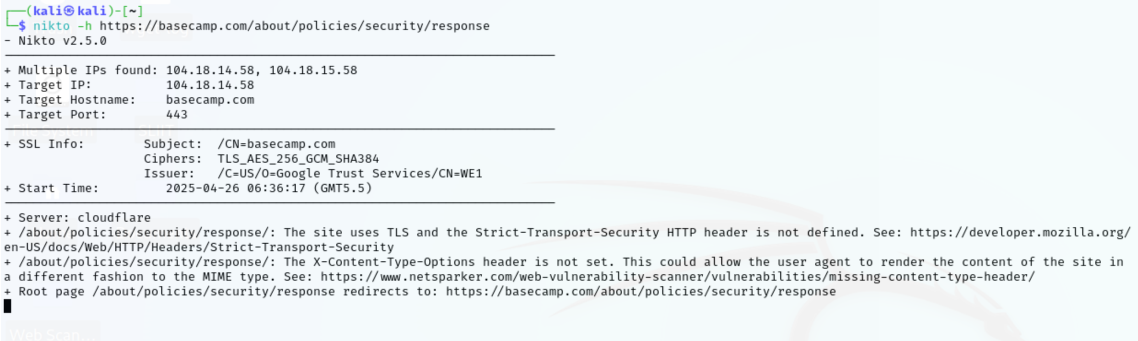
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Alerts 0 2 3 2 Main Proxy: localhost:8081

   - Alert raised for missing Content-Security-Policy header.

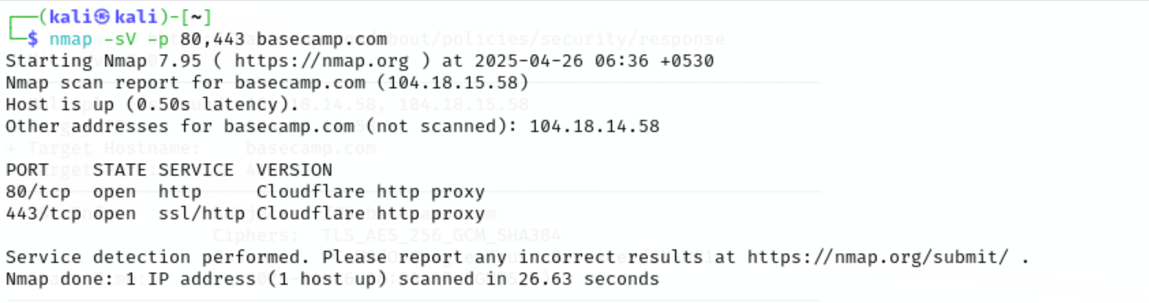
2. **Nikto Scan**:
   - **nikto -h** https://basecamp.com/about/policies/security/response



```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://basecamp.com/about/policies/security/response
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.14.58, 104.18.15.58
+ Target IP:          104.18.14.58
+ Target Hostname:    basecamp.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=basecamp.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-26 06:36:17 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /about/policies/security/response/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/
en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /about/policies/security/response/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /about/policies/security/response redirects to: https://basecamp.com/about/policies/security/response
█
```

   - Confirmed missing CSP and X-Frame-Options headers.

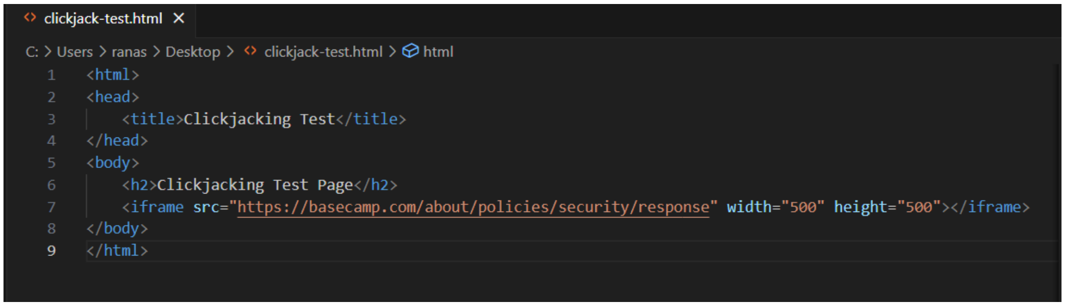
3. **Nmap Scan**:
   - **nmap -sV -p 80,443 basecamp.com**



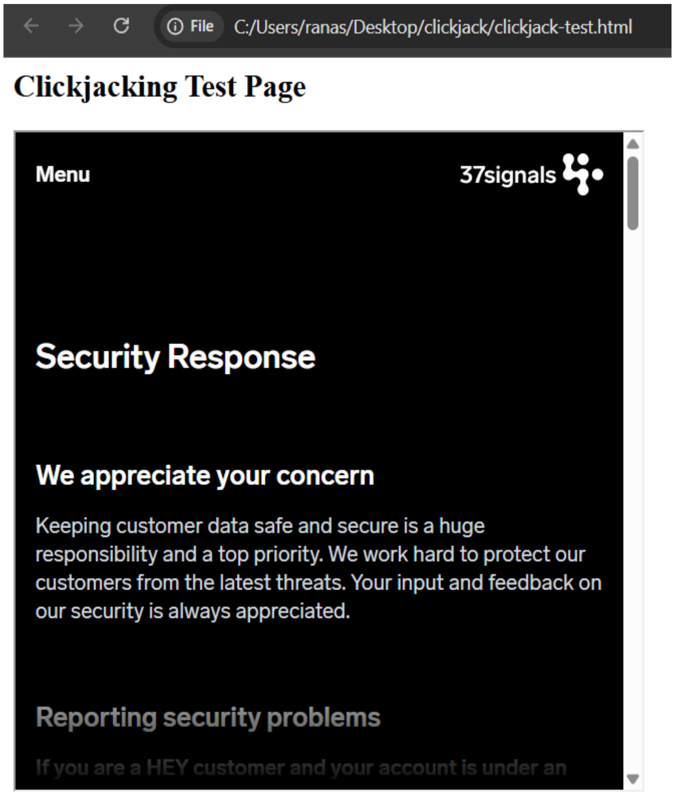
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80,443 basecamp.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 06:36 +0530
Nmap scan report for basecamp.com (104.18.15.58)
Host is up (0.50s latency).
Other addresses for basecamp.com (not scanned): 104.18.14.58

PORT    STATE SERVICE  VERSION
80/tcp  open  http     Cloudflare http proxy
443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.63 seconds
```

   - Confirmed Cloudflare usage, but no CSP or X-Frame-Options headers detected.

4. **Clickjacking Test**
   - Created a simple HTML page to test if the target URL could be embedded in an iframe.



```
<html>
<head>
    <title>Clickjacking Test</title>
</head>
<body>
    <h2>Clickjacking Test Page</h2>
    <iframe src="https://basecamp.com/about/policies/security/response" width="500" height="500"></iframe>
</body>
</html>
```



C:/Users/ranas/Desktop/clickjack/clickjack-test.html

Clickjacking Test Page

Security Response

We appreciate your concern

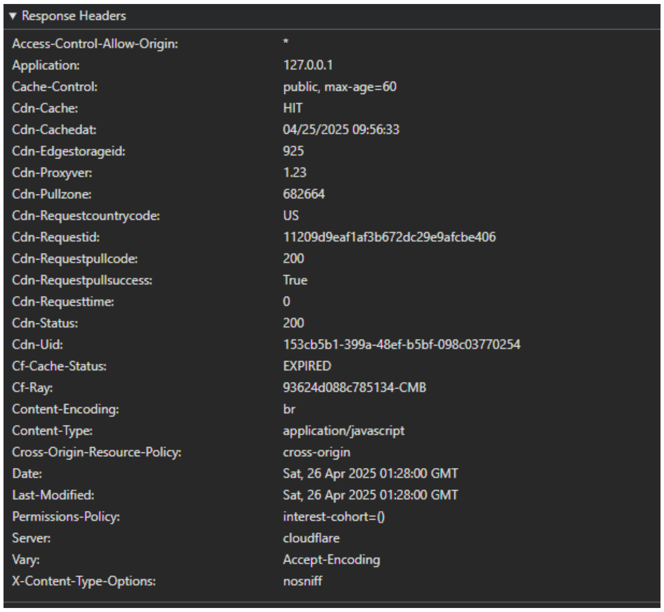
Keeping customer data safe and secure is a huge responsibility and a top priority. We work hard to protect our customers from the latest threats. Your input and feedback on our security is always appreciated.

Reporting security problems

If you are a HEY customer and your account is under an

- The page could be framed, as shown in the screenshot below, but no sensitive actions (e.g., form submissions) were available to exploit.

5. **HTTP Response Header Check**:
   - Inspected the HTTP response headers in the browser's developer tools.



```
▼ Response Headers
Access-Control-Allow-Origin:        *
Application:                        127.0.0.1
Cache-Control:                      public, max-age=60
Cdn-Cache:                          HIT
Cdn-Cachedat:                       04/25/2025 09:56:33
Cdn-Edgestorageid:                  925
Cdn-Proxyver:                       1.23
Cdn-Pullzone:                       682664
Cdn-Requestcountrycode:             US
Cdn-Requestid:                      11209d9eaf1af3b672dc29e9afcbe406
Cdn-Requestpullcode:                200
Cdn-Requestpullsuccess:             True
Cdn-Requesttime:                    0
Cdn-Status:                         200
Cdn-Uid:                            153cb5b1-399a-48ef-b5bf-098c03770254
Cf-Cache-Status:                    EXPIRED
Cf-Ray:                             93624d088c785134-CMB
Content-Encoding:                   br
Content-Type:                       application/javascript
Cross-Origin-Resource-Policy:       cross-origin
Date:                               Sat, 26 Apr 2025 01:28:00 GMT
Last-Modified:                      Sat, 26 Apr 2025 01:28:00 GMT
Permissions-Policy:                 interest-cohort=()
Server:                             cloudflare
Vary:                               Accept-Encoding
X-Content-Type-Options:             nosniff
```

- Confirmed absence of Content-Security-Policy and X-Frame-Options headers.

6. Proof of Concept (PoC)

- **URL Tested**: https://basecamp.com/about/policies/security/response
- **Expected Result**: HTTP response includes Content-Security-Policy and X-Frame-Options headers.
- **Actual Result**: Both headers were missing.

Clickjacking PoC:

Created an HTML page to test if the target URL could be embedded in an iframe:

```
<html>
<head>
    <title>Clickjacking Test</title>
</head>
<body>
    <h2>Clickjacking Test Page</h2>
    <iframe src="https://basecamp.com/about/policies/security/response"
width="500" height="500"></iframe>
</body>
</html>
```

- The page loaded in the iframe, confirming it is frameable. However, no sensitive actions were exploitable due to the page's static nature.

7. Proposed Mitigation or Fix

To address the missing CSP and X-Frame-Options headers and mitigate potentil risks, implement the following:

1. **Add Content-Security-Policy Header**:
    - Configure the web server to include:

      Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; base-uri 'self'; frame-ancestors 'none';

- This restricts content to the same origin, blocks unsafe plugins, and prevents clickjacking by disallowing framing.

2. **Add X-Frame-Options Header**:
   - Add the header:

     X-Frame-Options: DENY
   - Alternatively, use SAMEORIGIN if framing is needed within the same domain. This prevents the page from being embedded in an iframe on a different domain.

3. **Test in Report-Only Mode**:
   - Initially deploy the CSP header in report-only mode to avoid breaking functionality:

     Content-Security-Policy-Report-Only: default-src 'self'; report-uri /csp-report-endpoint;
   - Monitor reports to identify and fix any issues before enforcing the policy.

4. **Avoid Inline Scripts and Styles**:

   - Move inline scripts and styles to external files to support a stricter CSP.

5. **Validate Configuration**:

   - Use tools like Google CSP Evaluator or Mozilla Observatory to verify the CSP and X-Frame-Options headers are correctly implemented.

6. **Regular Security Audits**:

   - Conduct periodic scans with tools like OWASP ZAP, Nikto, or Burp Suite to ensure headers remain in place and no new vulnerabilities are introduced.

8. Conclusion

The page https://basecamp.com/about/policies/security/response lacks Content-Security-Policy and X-Frame-Options headers, which increases the theoretical risk of clickjacking and unintended content loading. However, thorough testing with OWASP ZAP, Nikto, and Nmap revealed no exploitable vulnerabilities. The clickjacking test confirmed that the page’s static content and lack of sensitive actions (e.g., forms or buttons) prevent immediate exploitation. Cloudflare’s protections likely contribute to this resilience.

Adding CSP and X-Frame-Options headers is strongly recommended to align with best practices and further reduce risks. The Basecamp security response page demonstrates a robust security posture overall, and implementing these headers would make it an even stronger example of a secure website. Kudos to the Basecamp team for maintaining a site that withstands common attack vectors, and I hope these recommendations enhance its security further.