Security Report Of

Shothik.AI

Information Scanning:

```
Other addresses for beta.shothik.ai (not scanned): 172.67.178.36 2606:4700:3032::ac43:b224 2606:4700:3034::6815:2b6a
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy
```

```
[sudo] password for faisal:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 08:42 +06
Nmap scan report for beta.shothik.ai (104.21.43.106)
Host is up (0.058s latency).
Other addresses for beta.shothik.ai (not scanned): 172.67.178.36 2606:4700:3034::6815:2b6a 2606:4700:3032::ac43:b224
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: cloudflare
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp  open  ssl/http Cloudflare http proxy
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: cloudflare
| http-enum:
|   /blog/: Blog
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /robots.txt: Robots file
|   /manifest.json: Manifest JSON File
|   /account/: Potentially interesting folder
|   /payment/: Potentially interesting folder
|_  /tools/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8080/tcp open  http     Cloudflare http proxy
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
```

```
8080/tcp open  http      Cloudflare http proxy
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-server-header: cloudflare
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
8443/tcp open  ssl/http Cloudflare http proxy
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 584.73 seconds

┌──(faisal㉿kali)-[~]
└─$
```

```
1  POST /v1/accounts:signInWithPassword?key=AIzaSyAE-xtJmH6HTc4XQZSYjdRQtsRYoaIS_lo HTTP/2
2  Host: identitytoolkit.googleapis.com
3  Content-Length: 87
4  Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5  X-Firebase-Gmpid: 1:259331281661:web:5d89590c720a60fd1e2494
6  Content-Type: application/json
7  X-Client-Version: Chrome/JsCore/9.17.1/FirebaseCore-web
8  Sec-Ch-Ua-Mobile: ?0
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
10 Sec-Ch-Ua-Platform: "Linux"
11 Accept: */*
12 Origin: https://beta.shothik.ai
13 X-Client-Data: CNTxygE=
14 Sec-Fetch-Site: cross-site
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
20 {
     "returnSecureToken":true,
     "email":"teacher7@teacher.com",
     "password":"alfkjsldfjasldfj"
   }
```

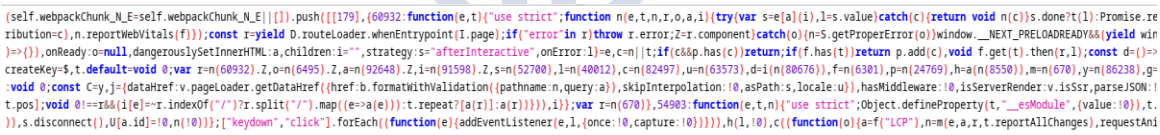
1. Application Error Disclosure

Severity: Medium

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Evidence:

```
HTTP/1.1 200 OK
Date: Tue, 16 May 2023 22:59:09 GMT
Content-Type: text/javascript; charset=utf-8
Connection: keep-alive
Cache-Control: max-age=14400
etag: W/"2d768a75ef95b0ea7dba695f5ba895db92866991e39d58bb5b75f18bc271c757"
last-modified: Thu, 11 May 2023 20:25:15 GMT
strict-transport-security: max-age=31556926
x-served-by: cache-qpg1243-QPG
x-cache: HIT
x-cache-hits: 1
x-timer: S1684277949.348064,VS0,VE1
vary: x-fh-requested-host, accept-encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: MISS
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Z0TaShskEfA%2FUhIMysQcw8uVSfh3s7Zv1ZY8D%2Bg7pl5XNOxnDxQMJGDFyZzwWqiwo3hEbeSsEGB%2F%2B359zUmylpSF0W9PmiHLVtLimW0nWB71%
2BaVUc10EjfLFQRcwmUuK7Ck%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 7c873abf4cdd3df5-SIN
Content-Length: 91424
```



```
(self.webpackChunk_N_E=self.webpackChunk_N_E||[]).push([[179],{60932:function(e,t){"use strict";function n(e,t,n,r,o,a,i){try{var s=e[a](i),l=s.value}catch(c){return void n(c)}s.done?t(l):Promise.re
ribution=c),n.reportWebVitals(f)});const r=yield D.routeLoader.whenEntrypoint(I.page);if("error"in r)throw r.error;Z=r.component}catch(o){n=S.getProperError(o)}window.__NEXT_PRELOADREADY&&(yield win
)=>{}),onReady:o=null,dangerouslySetInnerHTML:a,children:i="",strategy:s="afterInteractive",onError:l}=e,c=n||t;if(c&&p.has(c))return;if(f.has(t))return p.add(c),void f.get(t).then(r,l);const d=()=>
createKey=$,t.default=void 0;var r=n(60932).Z,o=n(6495).Z,a=n(92648).Z,i=n(91598).Z,s=n(52700),l=n(40012),c=n(82497),u=n(63573),d=i(n(80676)),f=n(6301),p=n(24769),h=a(n(8550)),m=n(670),y=n(86238),g=
:void 0;const C=y,j={dataHref:v.pageLoader.getDataHref({href:b.formatWithValidation({pathname:n,query:a}),skipInterpolation:!0,asPath:s,locale:u}),hasMiddleware:!0,isServerRender:v.isSsr,parseJSON:!
t.pos];void 0!==r&&(i[e]=~r.indexOf("/")?r.split("/").map((e=>a(e))):t.repeat?[a(r)]:a(r))))),i}};var r=n(670)},54903:function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0}),t.
)),s.disconnect(),U[a.id]=!0,n(!0)});["keydown","click"].forEach((function(e){addEventListener(e,l,{once:!0,capture:!0})}))},h(l,!0),c((function(o){a=f("LCP"),n=m(e,a,r,t.reportAllChanges),requestAni
```


Impact: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. Because this information can be used to launch further attacks against the web application.

Solution: Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

2. Content Security Policy (CSP) Header Not Set

Severity: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Evidence:

Impact: There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

3. Missing Anti-Clickjacking Header

Severity: Medium

Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'Clickjacking' attacks.

Evidence:

```
HTTP/1.1 200 OK
Date: Tue, 16 May 2023 22:59:07 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: max-age=3600
last-modified: Thu, 11 May 2023 20:25:15 GMT
strict-transport-security: max-age=31556926
x-served-by: cache-qpg1256-QPG
x-cache: HIT
x-cache-hits: 1
x-timer: S1684277947.034792,VS0,VE1
vary: x-fh-requested-host, accept-encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=4iaXrbs4aEWgQyYtE%2FJ83Y%2FYArC9JfXyviQoLLIS6%2BSEh%2BoU8fBGybSXnAEdDlRaWPfU%2B3mFhnOXGFfPzFPFLBeOsLCFrKkMG3okbJd8y%
2BFUxsvQAVWrftKabgNCwF%2BMlYU%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 7c873ab0d94c6b9e-SIN
Content-Length: 10626
```

```
<!DOCTYPE html><html lang="en" class="__className_ad314c"><head><meta charset="utf-8" /><meta name="viewport" content="initial-scale=1, width=device-width" /><title>Shothik AI : The future of writin
```

Impact: Missing X-Frame-Options header means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.
If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

4. Strict-Transport-Security Header Not Set

Severity: Low

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Evidence:

```
HTTP/1.1 200 OK
Date: Tue, 16 May 2023 22:59:09 GMT
Content-Type: application/javascript
Content-Length: 12332
Connection: keep-alive
Last-Modified: Fri, 12 May 2023 12:05:41 GMT
ETag: "645e2b95-302c"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LO7bfKlWWUmZVSMxQnbPnamJgBX%2FzbPg%2FODNixMHD3e5%2F7aEU%2BbMWqgcuVFT2xV%2FzAnqMq1%2B%2BkfCQ%2FBt8j%
2FDNLIjnE433I7ZPAybiXr3fe4VLULoBd%2BhYqILWX0xNRoaK4%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 7c873ac2cb274488-SIN
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Expires: Thu, 18 May 2023 22:59:09 GMT
Cache-Control: max-age=172800
Cache-Control: public
Accept-Ranges: bytes
```

```
!function(){"use strict";function t(){return"cf-marker-"+Math.random().toString().slice(2)}function e(){for(var t=[],e=0;e<arguments.length;e++)t[e]=arguments[e];(n=console.warn||console.log).call.
```

Impact: Why “Strict-Transport-Security Header Not Set” can be dangerous. The missing Strict-Transport-Security header results in communication over HTTP being allowed to the specified domain. That makes the website vulnerable to man-in-the-middle attacks, presenting a fake login page being one of the options.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

5. Timestamp Disclosure - Unix

Severity: Low

Description: A timestamp was disclosed by the application/web server - Unix. Like 1540483477, which evaluates to: 2018-10-25 22:04:37

Evidence:

```
HTTP/1.1 200 OK
Date: Tue, 16 May 2023 22:59:09 GMT
Content-Type: text/javascript; charset=utf-8
Content-Length: 1088963
Connection: keep-alive
Cache-Control: max-age=14400
Cf-Bgj: minify
Cf-Polished: origSize=1088969
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
etag: "719946783e33232d284e2fe7ab6f82de2ce120f70f77a8328576e6ac5867add3"
last-modified: Thu, 11 May 2023 20:25:15 GMT
strict-transport-security: max-age=31556926
vary: x-fh-requested-host, accept-encoding
x-cache: HIT
x-cache-hits: 1
x-served-by: cache-qpg1243-QPG
x-timer: S1684139926.625132,VS0,VE3
CF-Cache-Status: REVALIDATED
Accept-Ranges: bytes
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0sqgxh23n%2FKqVxfx0sene%2FA1Y9kwTiLYB8J7L1WfmusLmX%2BrI49hUpSHSbGpd%2BbfG%2F2v%2Fv%2BTy4rX0EddcXn5f2flrWp%2F2inghbHCh%
2BLZnwwgt8QdWx%2Fvwy2OymqHS%2FTIh74%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 7c873abfefcd44c3-SIN

(self.webpackChunk_N_E=self.webpackChunk_N_E||[]).push([[2888],{26077:function(e,t,n){"use strict";n.d(t,{Z:function(){return y}});var r=function(){function e(e){var t=this;this._insertTag=function
style),c=(0,r.Z)({},n,i,o);return e.length>0&&(c.className=e),Object.keys(t).length>0&&(c.style=t),{props:c,internalRef:void 0}}const u=function(e,t=[]){if(void 0===e)return{};const n={};return Obj
  0% {
    transform: scale(0);
    opacity: 0.1;
  }

  100% {
    transform: scale(1);
    opacity: 0.3;
  }
`)),D=(0,k.F4)(I||(I=A`
  0% {
    opacity: 1;
  }

  100% {
    opacity: 0;
  }
`)),N=(0,k.F4)(R||(R=A`
  0% {
    transform: scale(1);
  }

  50% {
    transform: scale(0.92);
  }

  100% {
    transform: scale(1);
  }
`)),M=(0,c.ZP)("span",{name:"MuiTouchRipple",slot:"Root"})({overflow:"hidden",pointerEvents:"none",position:"absolute",zIndex:0,top:0,right:0,bottom:0,left:0,borderRadius:"inherit"}),L=(0,c.ZP)(E,{
  opacity: 0;
```

Impact: The security implications of a timestamp disclosure are significant. If a timestamp is disclosed, it can be used to gain access to a system or to modify or delete data. It can also be used to track user activity, as the timestamp can be used to determine when a user logged into a system or when a file was created.

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

6. X-Content-Type-Options Header Missing

Severity: Low

Description: The Anti-MIME-Sniffing Header X-Content-Type-Options was not set to 'no sniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Evidence:

Impact: Why “X-Content-Type-Options Header Missing” can be dangerous. The missing "X-Content-Type-Options" http header enables a browser (mostly Internet Explorer) to perform MIME sniffing when the Content-Type header is not set or its value seems inappropriate.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'no sniff' for all web pages.
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.