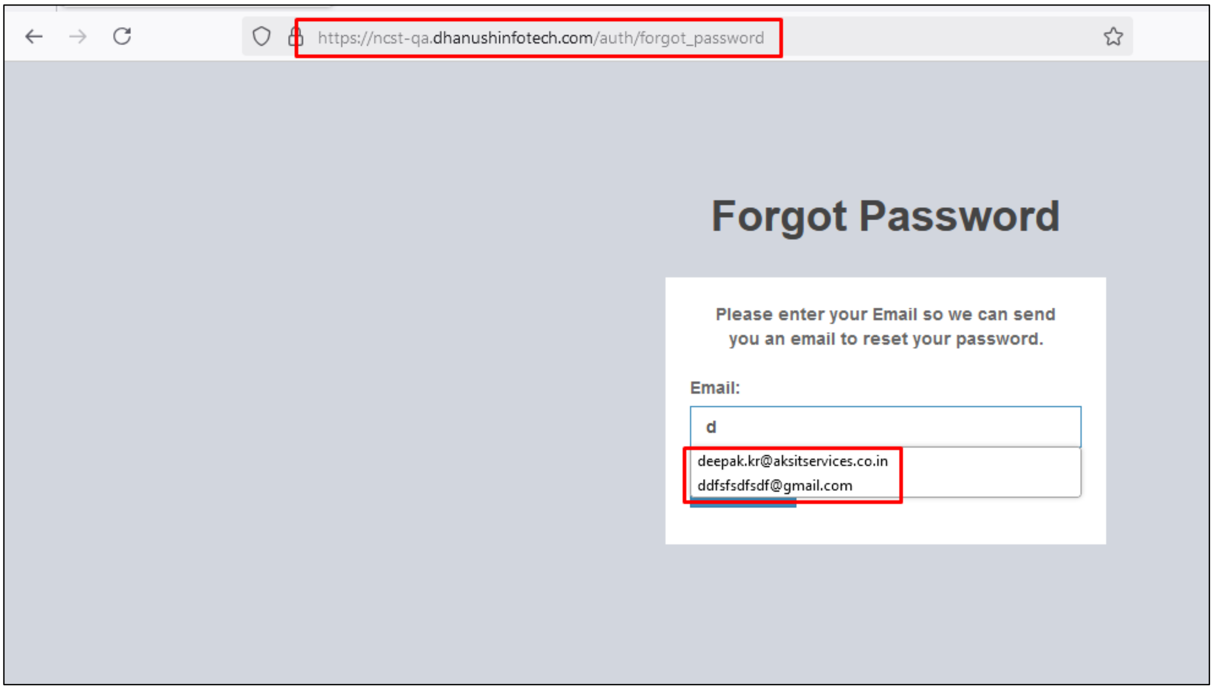
NCST Final Audit

1. Autocomplete Enabled (Already Reported)



https://ncst-qa.dhanushinfotech.com/auth/forgot_password

Forgot Password

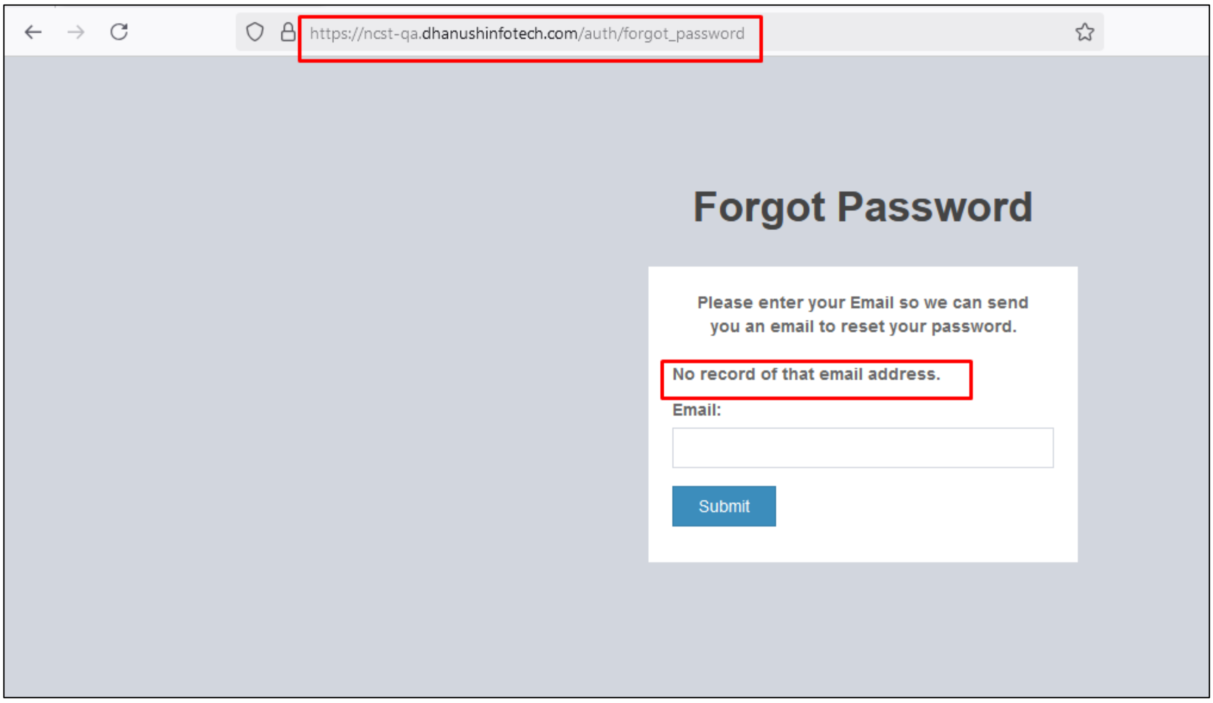
Please enter your Email so we can send you an email to reset your password.

Email: d

deepak.kr@aksitservices.co.in
ddfsfsdfsdf@gmail.com

Solution: Autocomplete:off

2. Username Enumeration



https://ncst-qa.dhanushinfotech.com/auth/forgot_password

Forgot Password

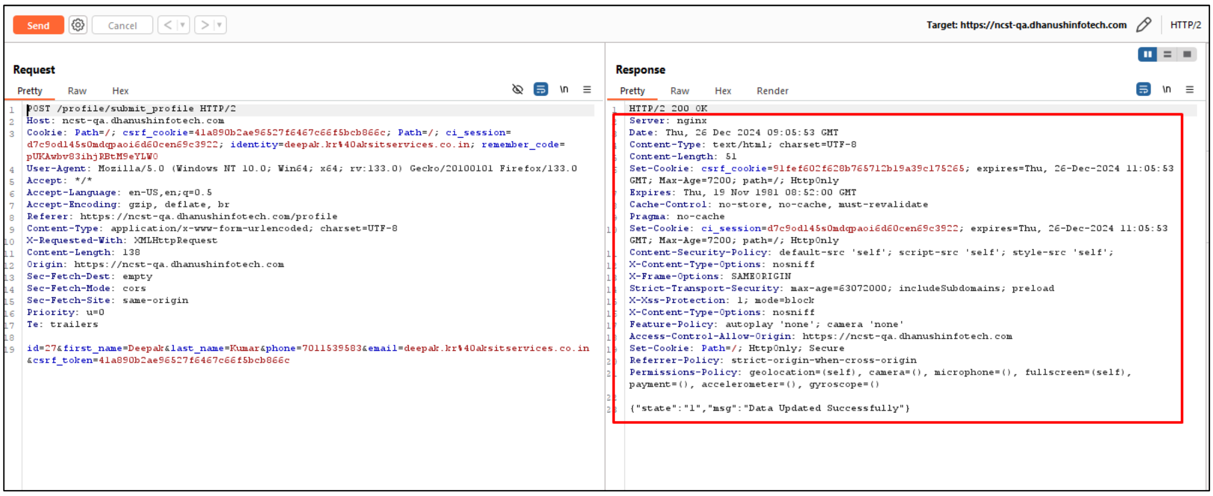
Please enter your Email so we can send you an email to reset your password.

No record of that email address.

Email:

Solution: Generic Message: If user is registered, OTP will be sent to email

3. CSP Not Implemented (Already Reported)

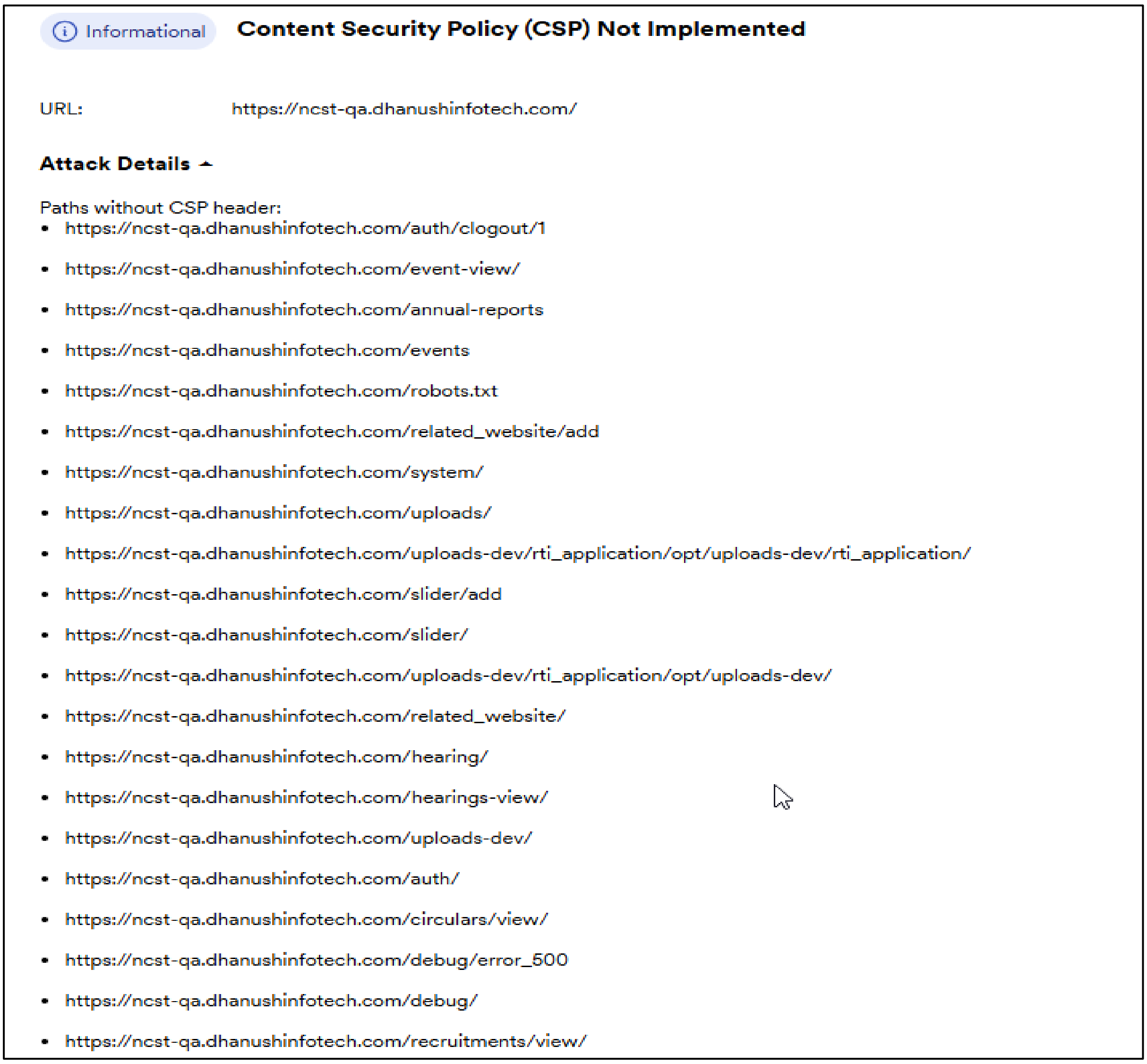


```
POST /profile/submit_profile HTTP/2
Host: ncst-qa.dhanushinfotech.com
Cookie: Path=/; csrf_cookie=41a890b2ae96527f6467c66f5bcb866c; Path=/; ci_session=
d7c9od145s0mdqpaoi6d60cen69c3922; identity=deepak.kr%40aksitservices.co.in; remember_code=
pUKAwbv83ihjRBtM9eYLW0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://ncst-qa.dhanushinfotech.com/profile
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 138
Origin: https://ncst-qa.dhanushinfotech.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

id=27&first_name=Deepak&last_name=Kumar&phone=7011539583&email=deepak.kr%40aksitservices.co.in
&csrf_token=41a890b2ae96527f6467c66f5bcb866c
```

```
HTTP/2 200 OK
Server: nginx
Date: Thu, 26 Dec 2024 09:05:53 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 51
Set-Cookie: csrf_cookie=91fef602f628b765712b19a39c175265; expires=Thu, 26-Dec-2024 11:05:53
GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=d7c9od145s0mdqpaoi6d60cen69c3922; expires=Thu, 26-Dec-2024 11:05:53
GMT; Max-Age=7200; path=/; HttpOnly
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self';
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Feature-Policy: autoplay 'none'; camera 'none'
Access-Control-Allow-Origin: https://ncst-qa.dhanushinfotech.com
Set-Cookie: Path=/; HttpOnly; Secure
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(self), camera=(), microphone=(), fullscreen=(self),
payment=(), accelerometer=(), gyroscope=()

{"state":"1","msg":"Data Updated Successfully"}
```



Content Security Policy (CSP) Not Implemented

URL: https://ncst-qa.dhanushinfotech.com/

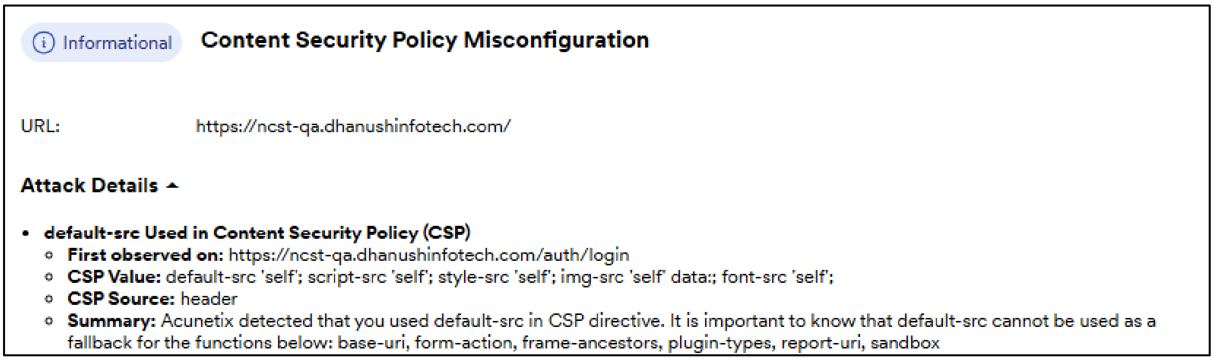
Attack Details

Paths without CSP header:

- https://ncst-qa.dhanushinfotech.com/auth/clogout/1
- https://ncst-qa.dhanushinfotech.com/event-view/
- https://ncst-qa.dhanushinfotech.com/annual-reports
- https://ncst-qa.dhanushinfotech.com/events
- https://ncst-qa.dhanushinfotech.com/robots.txt
- https://ncst-qa.dhanushinfotech.com/related_website/add
- https://ncst-qa.dhanushinfotech.com/system/
- https://ncst-qa.dhanushinfotech.com/uploads/
- https://ncst-qa.dhanushinfotech.com/uploads-dev/rti_application/opt/uploads-dev/rti_application/
- https://ncst-qa.dhanushinfotech.com/slider/add
- https://ncst-qa.dhanushinfotech.com/slider/
- https://ncst-qa.dhanushinfotech.com/uploads-dev/rti_application/opt/uploads-dev/
- https://ncst-qa.dhanushinfotech.com/related_website/
- https://ncst-qa.dhanushinfotech.com/hearing/
- https://ncst-qa.dhanushinfotech.com/hearings-view/
- https://ncst-qa.dhanushinfotech.com/uploads-dev/
- https://ncst-qa.dhanushinfotech.com/auth/
- https://ncst-qa.dhanushinfotech.com/circulars/view/
- https://ncst-qa.dhanushinfotech.com/debug/error_500
- https://ncst-qa.dhanushinfotech.com/debug/
- https://ncst-qa.dhanushinfotech.com/recruitments/view/

Solution: Implement CSP Header

4. CSP Misconfigured (Already Reported)



ⓘ Informational **Content Security Policy Misconfiguration**

URL: https://ncst-qa.dhanushinfotech.com/

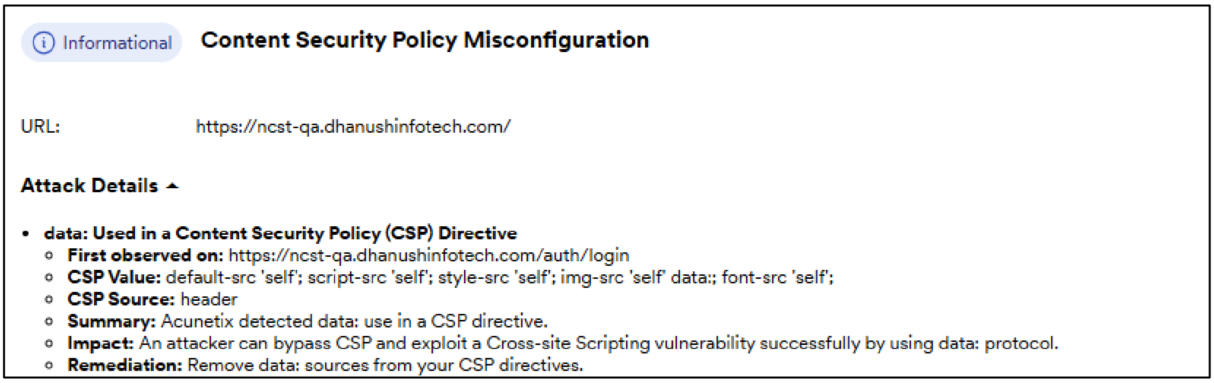
Attack Details ▴

- **default-src Used in Content Security Policy (CSP)**
  - **First observed on:** https://ncst-qa.dhanushinfotech.com/auth/login
  - **CSP Value:** default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:; font-src 'self';
  - **CSP Source:** header
  - **Summary:** Acunetix detected that you used default-src in CSP directive. It is important to know that default-src cannot be used as a fallback for the functions below: base-uri, form-action, frame-ancestors, plugin-types, report-uri, sandbox

1. **base-uri**: Controls the sources allowed for <base> tags.
2. **form-action**: Restricts URLs that can be used as form action targets.
3. **frame-ancestors**: Specifies valid parents that may embed the resource (via frames, iframes, etc.).
4. **plugin-types**: Defines allowed MIME types for plugins.
5. **report-uri**: Indicates the endpoint to which CSP violations should be reported.
6. **sandbox**: Applies restrictions on the resource's capabilities (e.g., preventing script execution).

Remidiation- You should explicitly define these directives in your CSP to ensure comprehensive security coverage. Here's an example CSP update:

Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:; font-src 'self'; base-uri 'self'; form-action 'self'; frame-ancestors 'none'; sandbox; report-uri /csp-violation-report-endpoint;

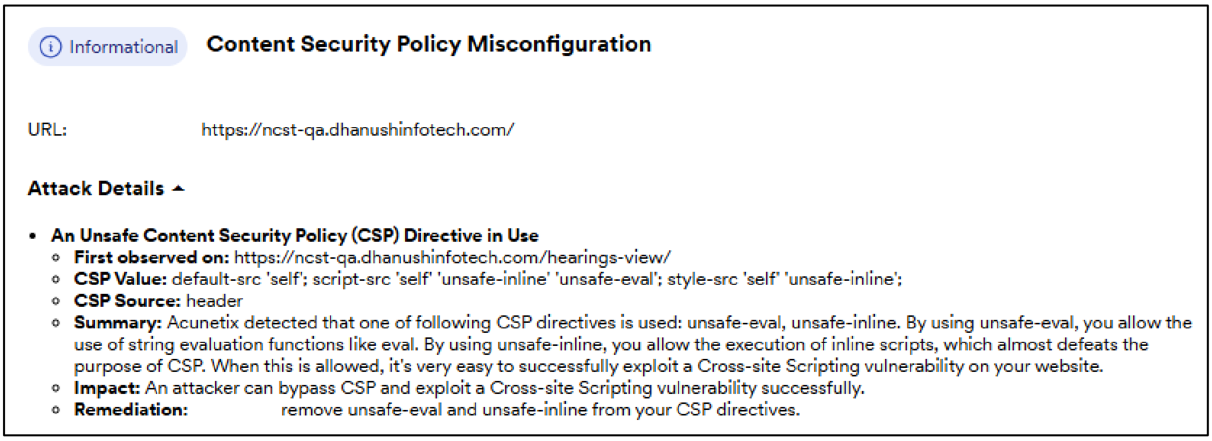


ⓘ Informational **Content Security Policy Misconfiguration**

URL: https://ncst-qa.dhanushinfotech.com/

Attack Details ▴

- **data: Used in a Content Security Policy (CSP) Directive**
  - **First observed on:** https://ncst-qa.dhanushinfotech.com/auth/login
  - **CSP Value:** default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:; font-src 'self';
  - **CSP Source:** header
  - **Summary:** Acunetix detected data: use in a CSP directive.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using data: protocol.
  - **Remediation:** Remove data: sources from your CSP directives.



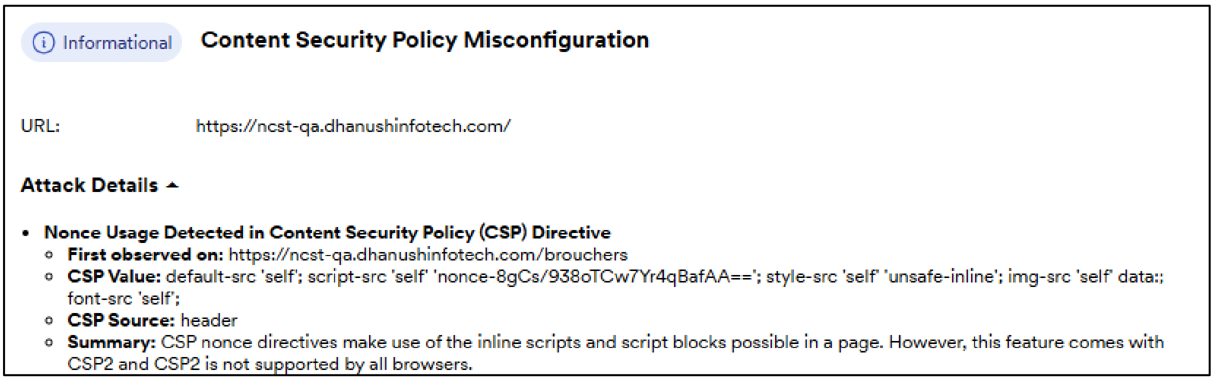
Informational

Content Security Policy Misconfiguration

URL: https://ncst-qa.dhanushinfotech.com/

Attack Details

- **An Unsafe Content Security Policy (CSP) Directive in Use**
    - **First observed on:** https://ncst-qa.dhanushinfotech.com/hearings-view/
    - **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline';
    - **CSP Source:** header
    - **Summary:** Acunetix detected that one of following CSP directives is used: unsafe-eval, unsafe-inline. By using unsafe-eval, you allow the use of string evaluation functions like eval. By using unsafe-inline, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.
    - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.
    - **Remediation:** remove unsafe-eval and unsafe-inline from your CSP directives.



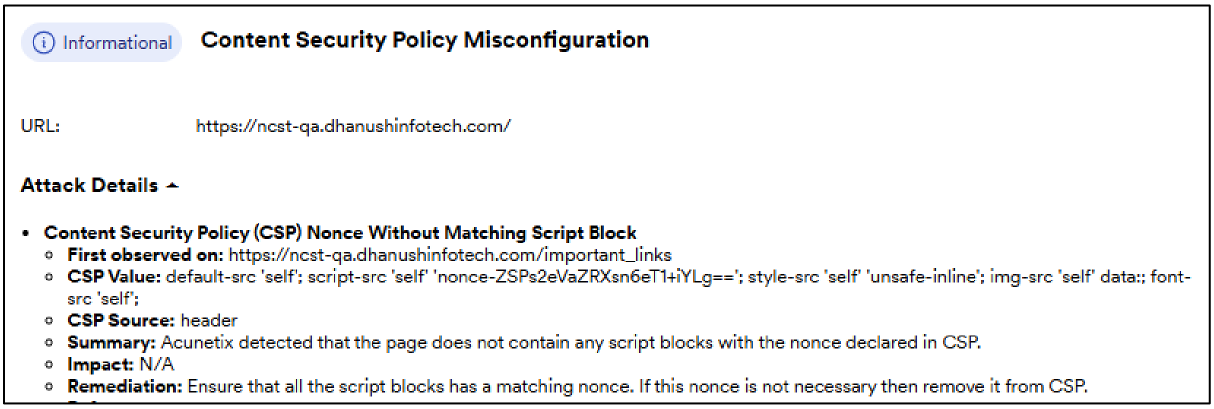
Informational

Content Security Policy Misconfiguration

URL: https://ncst-qa.dhanushinfotech.com/

Attack Details

- **Nonce Usage Detected in Content Security Policy (CSP) Directive**
    - **First observed on:** https://ncst-qa.dhanushinfotech.com/brouchers
    - **CSP Value:** default-src 'self'; script-src 'self' 'nonce-8gCs/938oTCw7Yr4qBafAA=='; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self';
    - **CSP Source:** header
    - **Summary:** CSP nonce directives make use of the inline scripts and script blocks possible in a page. However, this feature comes with CSP2 and CSP2 is not supported by all browsers.



Informational

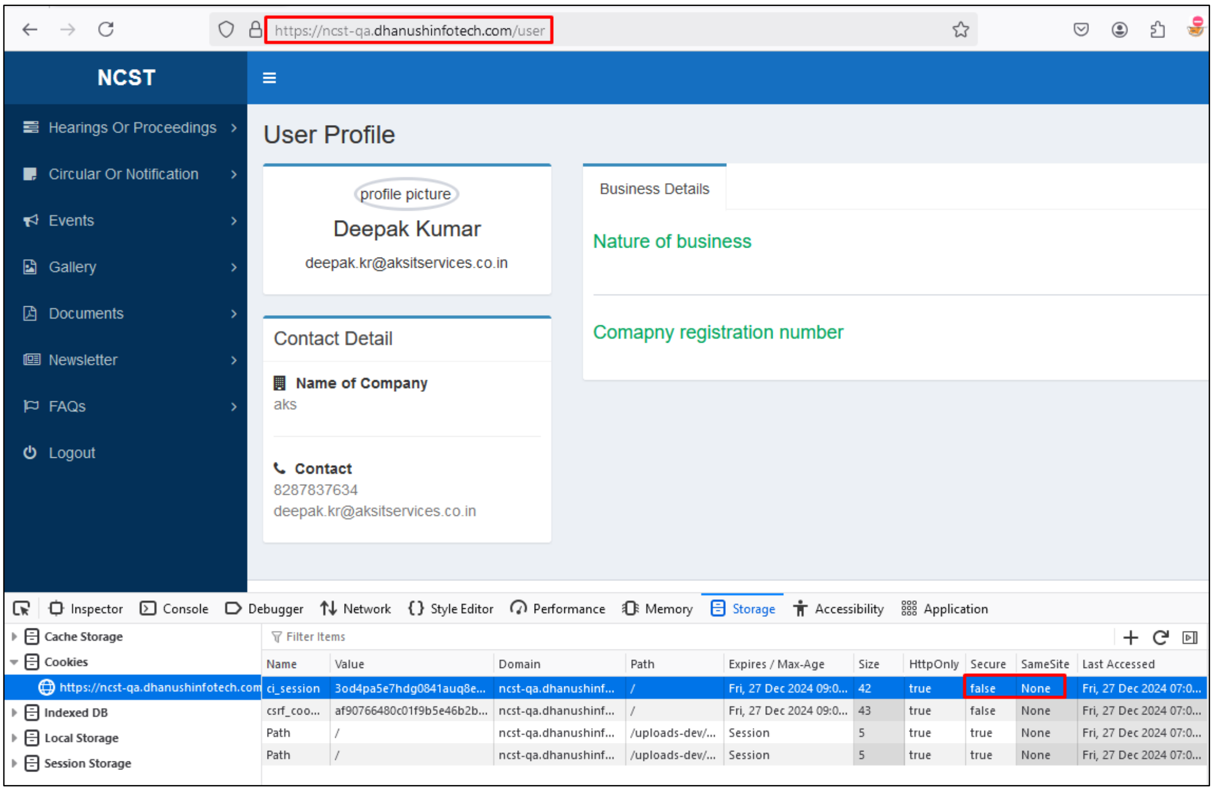
Content Security Policy Misconfiguration

URL: https://ncst-qa.dhanushinfotech.com/

Attack Details

- **Content Security Policy (CSP) Nonce Without Matching Script Block**
    - **First observed on:** https://ncst-qa.dhanushinfotech.com/important_links
    - **CSP Value:** default-src 'self'; script-src 'self' 'nonce-ZSPs2eVaZRXsn6eT1+iYLg=='; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self';
    - **CSP Source:** header
    - **Summary:** Acunetix detected that the page does not contain any script blocks with the nonce declared in CSP.
    - **Impact:** N/A
    - **Remediation:** Ensure that all the script blocks has a matching nonce. If this nonce is not necessary then remove it from CSP.

5. Missing Cookie Attributes (Already Reported)



User Profile

profile picture

Deepak Kumar

deepak.kr@aksitservices.co.in

Business Details

Nature of business

Comapny registration number

Contact Detail

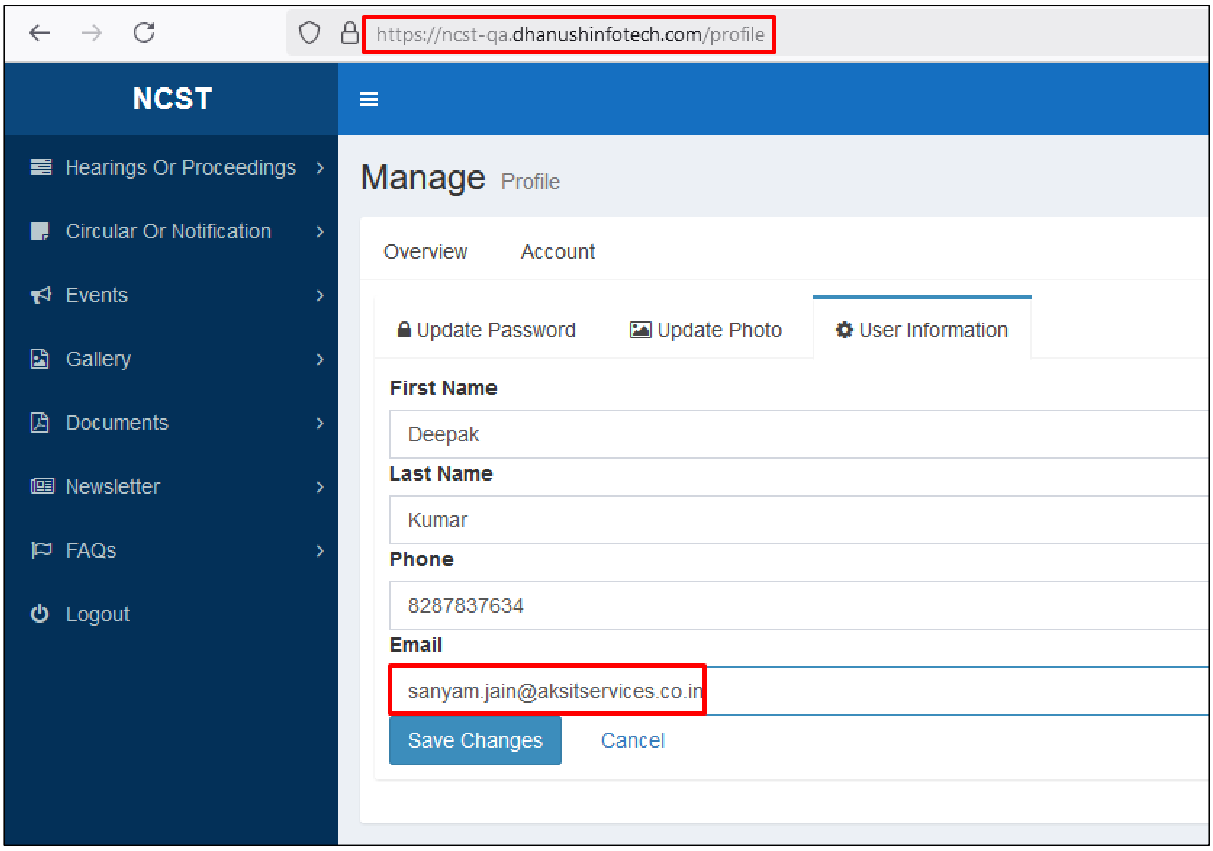
Name of Company
aks

Contact
8287837634
deepak.kr@aksitservices.co.in

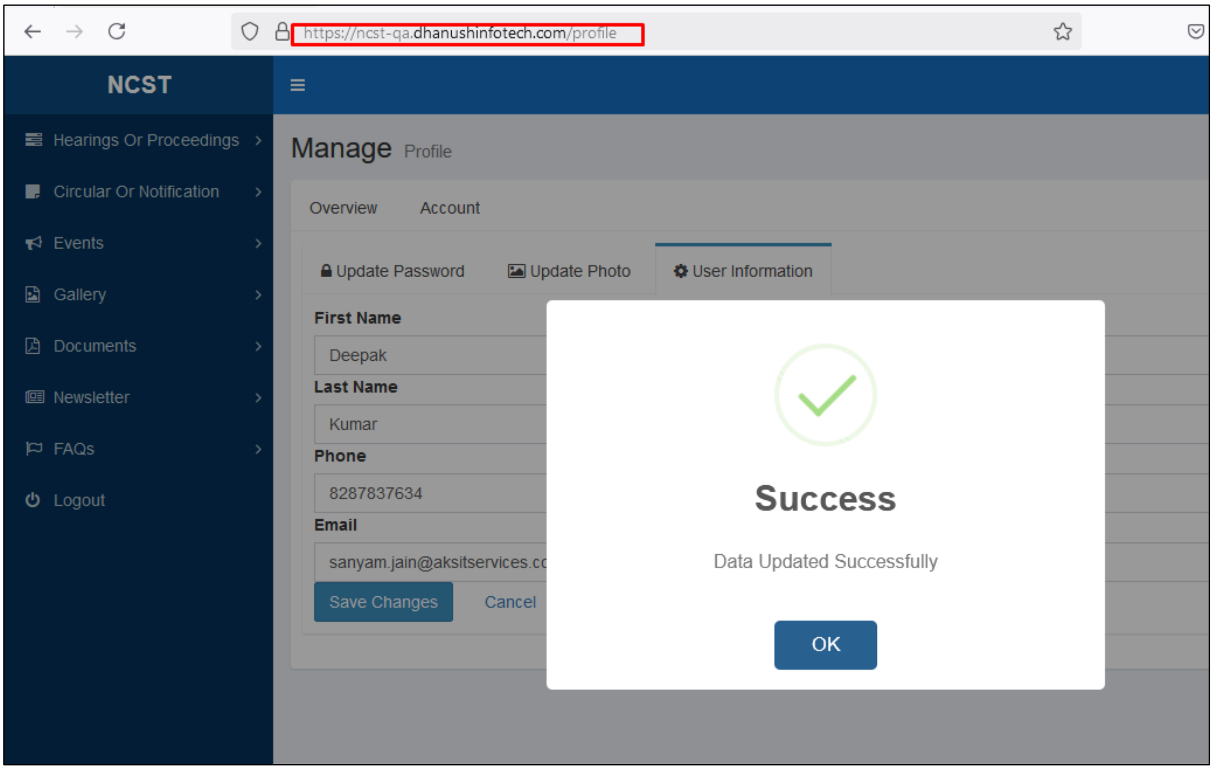
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ci_session	3od4pa5e7hdg0841auq8e...	ncst-qa.dhanushinf...	/	Fri, 27 Dec 2024 09:0...	42	true	false	None	Fri, 27 Dec 2024 07:0...
csrf_coo...	af90766480c01f9b5e46b2b...	ncst-qa.dhanushinf...	/	Fri, 27 Dec 2024 09:0...	43	true	false	None	Fri, 27 Dec 2024 07:0...
Path	/	ncst-qa.dhanushinf...	/uploads-dev/...	Session	5	true	true	None	Fri, 27 Dec 2024 07:0...
Path	/	ncst-qa.dhanushinf...	/uploads-dev/...	Session	5	true	true	None	Fri, 27 Dec 2024 07:0...

Solutions: Secure – True, Samesite – Lax/Strict

6. Unverified Email Change



First Name
Deepak
Last Name
Kumar
Phone
8287837634
Email
sanyam.jain@aksitservices.co.in



First Name
Deepak
Last Name
Kumar
Phone
8287837634
Email
sanyam.jain@aksitservices.co

Success

Data Updated Successfully

Solution: OTP Authentication mechanism should be there since the email address is used as username on login page.