

# Affected Items Report

Acunetix Security Audit

2022-06-26

# Scan of www.pornhub.com

## Scan details


|                    |                                  |
|--------------------|----------------------------------|
| Scan information   |                                  |
| Start time         | 2022-06-26T02:18:33.130504+00:00 |
| Start url          | www.pornhub.com                  |
| Host               | www.pornhub.com                  |
| Scan time          | 450 minutes, 10 seconds          |
| Profile            | Full Scan                        |
| Server information | openresty                        |
| Responsive         | True                             |
| Server OS          | Unknown                          |
| Application build  | 14.8.220606174                   |

## Threat level

### Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

## Alerts distribution

|   |    |
|---|----|
| Total alerts found  | 11 |
|  High          | 0  |
|  Medium        | 0  |
|  Low           | 8  |
|  Informational | 3  |

## Affected items

|                 |   |
|-----------------|---|
| Web Server      |   |
| Alert group     | Clickjacking: X-Frame-Options header  |
| Severity        | Low   |
| Description     | <p>Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.</p> <p>The server did not return an <b>X-Frame-Options</b> header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.</p>  |
| Recommendations | Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.  |
| Alert variants  |   |
| Details         | <p>Paths without secure XFO header:</p> <ul style="list-style-type: none"><li>• <a href="https://www.pornhub.com/_xa/">https://www.pornhub.com/_xa/</a></li><li>• <a href="https://www.pornhub.com/playlist/67613592">https://www.pornhub.com/playlist/67613592</a></li><li>• <a href="https://www.pornhub.com/information/rating">https://www.pornhub.com/information/rating</a></li><li>• <a href="https://www.pornhub.com/gif/40232491">https://www.pornhub.com/gif/40232491</a></li><li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox">https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox</a></li><li>• <a href="https://www.pornhub.com/user/discover/popular_verified_members">https://www.pornhub.com/user/discover/popular_verified_members</a></li><li>• <a href="https://www.pornhub.com/album/71010671">https://www.pornhub.com/album/71010671</a></li><li>• <a href="https://www.pornhub.com/pornstar/">https://www.pornhub.com/pornstar/</a></li><li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits">https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits</a></li></ul> |

GET /\_xa/ HTTP/1.1

Referer: https://www.pornhub.com/\_xa/

Cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc;  
bs=2nr1dz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570;  
fg\_fcf2e67d6468e8e1072596aead761f2b=64329.100000;  
fg\_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000;  
tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-  
f53353b6cfc6; atatusScript=hide; d\_fs=1; d\_b=1; RNLBSERVERID=ded4310; lang=cn; etavt=  
{ "ph6130deba91726": "1\_23\_NA\_NA|3", "ph6286bcb15f1a3": "1\_23\_NA\_NA|2", "ph626de171d928a": "1\_2  
3\_NA\_NA|1", "ph626c02d643fb7": "1\_23\_NA\_NA|0" }

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

| Web Server      |  |
|-----------------|--|
| Alert group     | Cookies with missing, inconsistent or contradictory properties (verified)  |
| Severity        | Low  |
| Description     | At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, or with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.   |
| Recommendations | Ensure that the cookies configuration complies with the applicable standards.  |
| Alert variants  |  |
| Details         | <p>List of cookies with missing, inconsistent or contradictory properties:</p> <ul style="list-style-type: none"><li>https://www.pornhub.com/<br/><br/>Cookie was set with:<br/><div>Set-Cookie: ua=09af53e829b1687c5db16483617c3ced; expires=Mon, 27</div><br/>This cookie has the following issues:<br/><div>- Cookie without SameSite attribute.<br/>When cookies lack the SameSite attribute, Web browsers may apply</div></li><li>https://www.pornhub.com/<br/><br/>Cookie was set with:<br/><div>Set-Cookie: platform=pc; expires=Sun, 03-Jul-2022 02:19:00 GMT; I</div><br/>This cookie has the following issues:</li></ul> |

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- <https://www.pornhub.com/>

Cookie was set with:

Set-Cookie: ss=986291158244780570; expires=Mon, 26-Jun-2023 02:1

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- <https://www.pornhub.com/>

Cookie was set with:

Set-Cookie: fg\_fcf2e67d6468e8e1072596aead761f2b=64329.100000; ex

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- <https://www.pornhub.com/>

Cookie was set with:

Set-Cookie: fg\_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000; ex

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID=2ae8ef641dd143f7a8c7bf1662a30654; Path=/; Do

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID\_v2=2ae8ef64-1dd1-43f7-a8c7-bf1662a30654; Pat

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/fla/log](https://www.pornhub.com/_xa/fla/log)

Cookie was set with:

Set-Cookie: RNLBSERVERID=ded4310; path=

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Cookie was set with:

Set-Cookie: tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat

This cookie has the following issues:

- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply

GET / HTTP/1.1

Referer: https://www.pornhub.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

## Web Server

### Alert group

**Cookies without HttpOnly flag set (verified)**

### Severity

Low

### Description

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

### Recommendations

If possible, you should set the HttpOnly flag for these cookies.

### Alert variants

### Details

Cookies without HttpOnly flag set:

- https://www.pornhub.com/

Set-Cookie: ua=09af53e829b1687c5db16483617c3ced; expires=Mon, 27

- https://www.pornhub.com/

Set-Cookie: platform=pc; expires=Sun, 03-Jul-2022 02:19:00 GMT; I

- https://www.pornhub.com/

Set-Cookie: bs=2nr1dz0g25ab5ok5ghhsqgn8yauyn0ne; expires=Wed, 23

- https://www.pornhub.com/

Set-Cookie: ss=986291158244780570; expires=Mon, 26-Jun-2023 02:1

- https://www.pornhub.com/

Set-Cookie: fg\_fcf2e67d6468e8e1072596aead761f2b=64329.100000; ex

- <https://www.pornhub.com/>

Set-Cookie: fg\_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000; ex

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID=2ae8ef641dd143f7a8c7bf1662a30654; Path=/; Do

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID\_v2=2ae8ef64-1dd1-43f7-a8c7-bf1662a30654; Pat

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat

- [https://www.pornhub.com/\\_xa/fla/log](https://www.pornhub.com/_xa/fla/log)

Set-Cookie: RNLBSERVERID=ded4310; path=

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat



GET / HTTP/1.1

Referer: https://www.pornhub.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

| Web Server      |   |
|-----------------|---|
| Alert group     | Cookies without Secure flag set (verified)  |
| Severity        | Low   |
| Description     | One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies. |
| Recommendations | If possible, you should set the Secure flag for these cookies.  |
| Alert variants  |   |
| Details         | <div>Cookies without Secure flag set:<ul style="list-style-type: none"><li>https://www.pornhub.com/_xa/fla/log</li></ul><div>Set-Cookie: RNLBSERVERID=ded4310; path=/<div></div></div></div>  |

```

GET /_xa/fla/log?
action=ad_view&ad_id=1053233971&campaign_id=1007400541&initial_zone_id=2184351&member_id=
402&zone_id=2184351 HTTP/1.1

Host: www.pornhub.com

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

accept-language: en-US

cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc;
bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570;
fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000;
fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000; atatusScript=hide;
tj_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; tj_UUID_v2=15f4e5fc-3ba9-4ecc-8f58-
f53353b6cfc6; d_fs=1; d_b=1

upgrade-insecure-requests: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-Dest: iframe

Referer: https://www.pornhub.com/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

```

|                        |   |
|------------------------|---|
| <b>Web Server</b>      |   |
| <b>Alert group</b>     | <b>HTTP Strict Transport Security (HSTS) not implemented</b>  |
| <b>Severity</b>        | Low   |
| <b>Description</b>     | HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response. |
| <b>Recommendations</b> | It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information  |
| <b>Alert variants</b>  |   |

|  |   |
|--|---|
| Details  | <p>URLs where HSTS is not enabled:</p> <ul style="list-style-type: none"> <li>• <a href="https://www.pornhub.com/playlist/67613592">https://www.pornhub.com/playlist/67613592</a></li> <li>• <a href="https://www.pornhub.com/information/rating">https://www.pornhub.com/information/rating</a></li> <li>• <a href="https://www.pornhub.com/gif/40232491">https://www.pornhub.com/gif/40232491</a></li> <li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox">https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox</a></li> <li>• <a href="https://www.pornhub.com/user/discover/popular_verified_members">https://www.pornhub.com/user/discover/popular_verified_members</a></li> <li>• <a href="https://www.pornhub.com/album/71010671">https://www.pornhub.com/album/71010671</a></li> <li>• <a href="https://www.pornhub.com/pornstar/">https://www.pornhub.com/pornstar/</a></li> <li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits">https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits</a></li> </ul> |
| <pre>GET /playlist/67613592 HTTP/1.1  Referer: https://www.pornhub.com/  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36  Cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc; bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570; fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000; fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000; tj_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; tj_UUID_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; atatusScript=hide; d_fs=1; d_b=1; RNLBSERVERID=ded4310; lang=cn; etavt= {"ph6130deba91726":"1_23_NA_NA 3"%2C"ph6286bcb15f1a3":"1_23_NA_NA 2"%2C"ph626de171d928a": "1_23_NA_NA 1"%2C"ph626c02d643fb7":"1_23_NA_NA 0"}  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Encoding: gzip,deflate,br  Host: www.pornhub.com  Connection: Keep-alive</pre> |   |

|                        |  |
|------------------------|--|
| <b>Web Server</b>      |  |
| <b>Alert group</b>     | <b>Sensitive pages could be cached</b>   |
| <b>Severity</b>        | Low  |
| <b>Description</b>     | One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified. |
| <b>Recommendations</b> | Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.  |
| <b>Alert variants</b>  |  |

|   |  |
|---|--|
| Details   | <p>List of pages that could be cached:</p> <ul style="list-style-type: none"> <li>https://www.pornhub.com/?from=pc_login_modal:index&amp;intended_action=1&amp;password=g00dPa\$\$w0rD&amp;redirect=h9wvaluzl5l0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J-RjuVnH61BKNm&amp;remember_me=on&amp;taste_profile=pHqghUme&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;user_id=pHqghUme&amp;username=pHqghUme</li> <li>https://www.pornhub.com/?authyId=94102&amp;authyIdHashed=94102&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;token2=94102&amp;username=pHqghUme&amp;verification_code=94102&amp;verification_modal=1</li> <li>https://www.pornhub.com/?from=pc_login_modal:index&amp;intended_action=1&amp;password=g00dPa\$\$w0rD&amp;redirect=h9wvaluzl5l0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J-RjuVnH61BKNm&amp;&amp;taste_profile=pHqghUme&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;user_id=pHqghUme&amp;username=pHqghUme</li> </ul> |
| <pre>GET /? from=pc_login_modal:index&amp;intended_action=1&amp;password=g00dPa%24%24w0rD&amp;redirect=h9wvaIuzI 5l0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J- RjuVnH61BKNm&amp;remember_me=on&amp;taste_profile=pHqghUme&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh- okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E- N8EYgNCB6E.&amp;user_id=pHqghUme&amp;username=pHqghUme HTTP/1.1  Referer: https://www.pornhub.com/  Cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc; bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570; fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000; fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36  Host: www.pornhub.com  Connection: Keep-alive</pre> |  |

|                 |  |
|-----------------|--|
| Web Server      |  |
| Alert group     | Session cookies scoped to parent domain (verified)   |
| Severity        | Low  |
| Description     | One ore more session cookies are scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and also by any other sub-domains of the parent domain. This could lead to security problems. |
| Recommendations | If possible, the session cookies should be scoped strictly to a sub-domain.  |
| Alert variants  |  |

- <https://www.pornhub.com/>

```
Set-Cookie: ua=09af53e829b1687c5db16483617c3ced; expires=Mon, 27
```

- <https://www.pornhub.com/>

```
Set-Cookie: platform=pc; expires=Sun, 03-Jul-2022 02:19:00 GMT; I
```

- <https://www.pornhub.com/>

```
Set-Cookie: bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; expires=Wed, 23
```

- <https://www.pornhub.com/>

```
Set-Cookie: ss=986291158244780570; expires=Mon, 26-Jun-2023 02:1
```

- <https://www.pornhub.com/>

```
Set-Cookie: fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000; ex
```

- <https://www.pornhub.com/>

```
Set-Cookie: fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000; ex
```

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

```
Set-Cookie: tj_UUID=2ae8ef641dd143f7a8c7bf1662a30654; Path=/; Do
```

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

```
Set-Cookie: tj_UUID_v2=2ae8ef64-1dd1-43f7-a8c7-bf1662a30654; Pat
```

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

```
Set-Cookie: tj_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do
```

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

```
Set-Cookie: tj_UUID_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat
```

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID=15f4e5fc3ba94ecc8f58f53353b6cfc6; Path=/; Do

- [https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)

Set-Cookie: tj\_UUID\_v2=15f4e5fc-3ba9-4ecc-8f58-f53353b6cfc6; Pat

GET / HTTP/1.1

Referer: <https://www.pornhub.com/>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

## Web Server

### Alert group

### Session token in URL

### Severity

Low

### Description

This application contains one or more pages with what appears to be a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

### Recommendations

The session should be maintained using cookies (or hidden input fields).

### Alert variants

|         |  |
|---------|--|
| Details | <p>Pages with session token in URL:</p> <ul style="list-style-type: none"> <li>https://www.pornhub.com/?from=pc_login_modal:index&amp;intended_action=1&amp;password=g00dPa\$\$w0rD&amp;redirect=h9wvaluzI5I0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J-RjuVnH61BKNm&amp;remember_me=on&amp;taste_profile=pHqghUme&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;user_id=pHqghUme&amp;username=pHqghUme (token)</li> <li>https://www.pornhub.com/?authyId=94102&amp;authyIdHashed=94102&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;token2=94102&amp;username=pHqghUme&amp;verification_code=94102&amp;verification_modal=1 (token)</li> <li>https://www.pornhub.com/?from=pc_login_modal:index&amp;intended_action=1&amp;password=g00dPa\$\$w0rD&amp;redirect=h9wvaluzI5I0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J-RjuVnH61BKNm&amp;&amp;taste_profile=pHqghUme&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E.&amp;user_id=pHqghUme&amp;username=pHqghUme (token)</li> <li>https://www.pornhub.com/front/set_mobile?redirect=9W_Ra4wgetwx6ikkCGwO_VSLpHro_yNkNLpzuNrPmWm0Tw0RVAHDSJ1n6tuk-_Q5&amp;token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-N8EYgNCB6E. (token)</li> </ul> |
|---------|--|

```

GET /?
from=pc_login_modal:index&intended_action=1&password=g00dPa%24%24w0rD&redirect=h9wvaIuzI
5I0YinsTCagxvsigdM_knMx-Yxmz0LlaqJXP2wQB-J-
RjuVnH61BKNm&remember_me=on&taste_profile=pHqghUme&token=MTY1NjIwOTk0MBRcil6ZzZ2hSDRovnh-
okvSNoWDF_fmKyKa1LEKJm8ZxR-DVxTRYRerAi75sdTFdJeRd0TxYO5E-
N8EYgNCB6E.&user_id=pHqghUme&username=pHqghUme HTTP/1.1

Referer: https://www.pornhub.com/

Cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc;
bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570;
fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000;
fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

```

|             |  |
|-------------|--|
| Web Server  |  |
| Alert group | Access-Control-Allow-Origin header with wildcard (*) value |
| Severity    | Informational  |

|                 |   |
|-----------------|---|
| Description     | <p>Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.</p> <p>If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to the site and access the responses.</p>  |
| Recommendations | Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.  |
| Alert variants  |   |
| Details         | <p>Affected paths (max. 25):</p> <ul style="list-style-type: none"><li>• /_xa/ads_batch</li></ul> <p>GET /_xa/ads_batch?<br/>ads=true&amp;channel[context_page_type]=home&amp;channel[site]=pornhub&amp;clientType=mobile&amp;data=[{"spots":[{"zone":5}]}]&amp;device_type=tablet&amp;dm=www.pornhub.com/_xa&amp;hc=A892BB70-5E78-440E-8006-2CAEAC682DF6&amp;site_id=2 HTTP/1.1</p> <p>Referer: https://www.pornhub.com/</p> <p>Cookie: ua=09af53e829b1687c5db16483617c3ced; platform=pc;<br/>bs=2nrldz0g25ab5ok5ghhsqgn8yauyn0ne; ss=986291158244780570;<br/>fg_fcf2e67d6468e8e1072596aead761f2b=64329.100000;<br/>fg_ee26b76392ae0c54fbcf7c635e3da0fa=39278.100000</p> <p>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</p> <p>Accept-Encoding: gzip,deflate,br</p> <p>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36</p> <p>Host: www.pornhub.com</p> <p>Connection: Keep-alive</p> |

|             |   |
|-------------|---|
| Web Server  |   |
| Alert group | Content Security Policy (CSP) not implemented |
| Severity    | Informational                                 |



|                 |   |
|-----------------|---|
| Description     | <p>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.</p> <p>Content Security Policy (CSP) can be implemented by adding a <b>Content-Security-Policy</b> header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:</p> <pre>Content-Security-Policy:     default-src 'self';     script-src 'self' https://code.jquery.com;</pre> <p>It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.</p>  |
| Recommendations | <p>It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the <b>Content-Security-Policy</b> HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.</p>   |
| Alert variants  |   |
| Details         | <p>Paths without CSP header:</p> <ul style="list-style-type: none"> <li>• <a href="https://www.pornhub.com/">https://www.pornhub.com/</a></li> <li>• <a href="https://www.pornhub.com/_xa/">https://www.pornhub.com/_xa/</a></li> <li>• <a href="https://www.pornhub.com/playlist/67613592">https://www.pornhub.com/playlist/67613592</a></li> <li>• <a href="https://www.pornhub.com/information/rating">https://www.pornhub.com/information/rating</a></li> <li>• <a href="https://www.pornhub.com/gif/40232491">https://www.pornhub.com/gif/40232491</a></li> <li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox">https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox</a></li> <li>• <a href="https://www.pornhub.com/user/discover/popular_verified_members">https://www.pornhub.com/user/discover/popular_verified_members</a></li> <li>• <a href="https://www.pornhub.com/album/71010671">https://www.pornhub.com/album/71010671</a></li> <li>• <a href="https://www.pornhub.com/pornstar/">https://www.pornhub.com/pornstar/</a></li> <li>• <a href="https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits">https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits</a></li> </ul> |

GET / HTTP/1.1

Referer: https://www.pornhub.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.pornhub.com

Connection: Keep-alive

## Web Server

### Alert group

**Subresource Integrity (SRI) not implemented**

### Severity

Informational

### Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the `<script>` HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

### Recommendations

Use the SRI Hash Generator link (from the References section) to generate a `<script>` element that implements Subresource Integrity (SRI).

For example, you can use the following `<script>` element to tell a browser that before executing the `https://example.com/example-framework.js` script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
      integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN
      crossorigin="anonymous"></script>
```

### Alert variants

|  |  |
|--|--|
| Details  | <p>Pages where SRI is not implemented:</p> <ul style="list-style-type: none"> <li>• <a href="https://www.pornhub.com/">https://www.pornhub.com/</a><br/>Script SRC: <b>https://ei.phncdn.com/www-static/js/lib/utls/mg_utils-1.0.0.js?cache=9261b2e60e</b></li> <li>• <a href="https://www.pornhub.com/">https://www.pornhub.com/</a><br/>Script SRC: <b>https://static.trafficjunky.com/ab/ads_test.js</b></li> </ul> |
| <pre>GET / HTTP/1.1  Referer: https://www.pornhub.com/  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36  Host: www.pornhub.com  Connection: Keep-alive</pre> |  |

## Scanned items (coverage report)

---

<https://www.pornhub.com/>  
[https://www.pornhub.com/\\_xa/](https://www.pornhub.com/_xa/)  
[https://www.pornhub.com/\\_xa/ads\\_batch](https://www.pornhub.com/_xa/ads_batch)  
[https://www.pornhub.com/\\_xa/fla/](https://www.pornhub.com/_xa/fla/)  
[https://www.pornhub.com/\\_xa/fla/log](https://www.pornhub.com/_xa/fla/log)  
<https://www.pornhub.com/album/>  
<https://www.pornhub.com/album/69530762>  
<https://www.pornhub.com/album/71010671>  
<https://www.pornhub.com/album/73027711>  
<https://www.pornhub.com/album/73039331>  
<https://www.pornhub.com/albums>  
<https://www.pornhub.com/albums/>  
<https://www.pornhub.com/albums/female-straight>  
<https://www.pornhub.com/albums/gay>  
<https://www.pornhub.com/blog>  
<https://www.pornhub.com/categories>  
<https://www.pornhub.com/categories/>  
<https://www.pornhub.com/categories/hentai>  
<https://www.pornhub.com/categories/teen>  
<https://www.pornhub.com/channels>  
<https://www.pornhub.com/channels/>  
<https://www.pornhub.com/channels/21sextury>  
<https://www.pornhub.com/channels/adventuresxxx>  
<https://www.pornhub.com/channels/allgirlmassage>  
<https://www.pornhub.com/channels/bellesa-plus>  
<https://www.pornhub.com/channels/brazzers>  
<https://www.pornhub.com/channels/cruel-media-tv>  
<https://www.pornhub.com/channels/family-strokes>  
<https://www.pornhub.com/channels/female-muscle-network>  
<https://www.pornhub.com/channels/full-porn-network>  
<https://www.pornhub.com/channels/got-my1f>  
<https://www.pornhub.com/channels/hot-guys-fuck>  
<https://www.pornhub.com/channels/les-worship>  
<https://www.pornhub.com/channels/milfswildholiday>  
<https://www.pornhub.com/channels/mom-swap>  
<https://www.pornhub.com/channels/mybros1f>  
<https://www.pornhub.com/channels/newsensations>  
<https://www.pornhub.com/channels/perv-mom>  
<https://www.pornhub.com/channels/perv-therapy>  
<https://www.pornhub.com/channels/sexso-24ore>  
<https://www.pornhub.com/channels/siri-pornstar>  
<https://www.pornhub.com/channels/sis-loves-me>  
<https://www.pornhub.com/channels/slayed>  
<https://www.pornhub.com/channels/teamskeet>  
<https://www.pornhub.com/community>  
<https://www.pornhub.com/content-removal>  
[https://www.pornhub.com/contest\\_hub](https://www.pornhub.com/contest_hub)  
[https://www.pornhub.com/contest\\_hub/](https://www.pornhub.com/contest_hub/)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice](https://www.pornhub.com/contest_hub/viewers_choice)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice/](https://www.pornhub.com/contest_hub/viewers_choice/)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice/horny69rabbits](https://www.pornhub.com/contest_hub/viewers_choice/horny69rabbits)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice/mybadreputation](https://www.pornhub.com/contest_hub/viewers_choice/mybadreputation)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice/serenity-cox](https://www.pornhub.com/contest_hub/viewers_choice/serenity-cox)  
[https://www.pornhub.com/contest\\_hub/viewers\\_choice/sweetie-fox](https://www.pornhub.com/contest_hub/viewers_choice/sweetie-fox)  
[https://www.pornhub.com/create\\_account\\_select](https://www.pornhub.com/create_account_select)  
<https://www.pornhub.com/explore>  
<https://www.pornhub.com/front/>  
<https://www.pornhub.com/front/authenticate>

[https://www.pornhub.com/front/lost\\_password](https://www.pornhub.com/front/lost_password)  
[https://www.pornhub.com/front/resend\\_confirmation\\_email](https://www.pornhub.com/front/resend_confirmation_email)  
[https://www.pornhub.com/front/set\\_mobile](https://www.pornhub.com/front/set_mobile)  
<https://www.pornhub.com/gay/>  
<https://www.pornhub.com/gay/categories>  
<https://www.pornhub.com/gayporn>  
<https://www.pornhub.com/gif/>  
<https://www.pornhub.com/gif/40232491>  
<https://www.pornhub.com/gif/40251871>  
<https://www.pornhub.com/gif/40351091>  
<https://www.pornhub.com/gif/40397921>  
<https://www.pornhub.com/gifgenerator>  
<https://www.pornhub.com/gifs>  
<https://www.pornhub.com/information/>  
<https://www.pornhub.com/information/2257>  
<https://www.pornhub.com/information/advertising>  
<https://www.pornhub.com/information/dmca>  
<https://www.pornhub.com/information/privacy>  
<https://www.pornhub.com/information/rating>  
<https://www.pornhub.com/information/terms>  
<https://www.pornhub.com/insights/>  
<https://www.pornhub.com/login>  
<https://www.pornhub.com/model/>  
<https://www.pornhub.com/model/angel>  
<https://www.pornhub.com/model/ayakayamamoto69>  
<https://www.pornhub.com/model/beamititik-beth>  
[https://www.pornhub.com/model/chris\\_dmnd](https://www.pornhub.com/model/chris_dmnd)  
<https://www.pornhub.com/model/closeupfantasy>  
<https://www.pornhub.com/model/daisybabytw>  
<https://www.pornhub.com/model/elymira>  
<https://www.pornhub.com/model/emiamateur>  
<https://www.pornhub.com/model/freyaairyc3>  
<https://www.pornhub.com/model/halloffame>  
<https://www.pornhub.com/model/hunnyandmylk>  
<https://www.pornhub.com/model/jadeenasty>  
<https://www.pornhub.com/model/jenny-lux>  
<https://www.pornhub.com/model/juicy-july>  
<https://www.pornhub.com/model/juliajoi>  
<https://www.pornhub.com/model/kissallisse>  
<https://www.pornhub.com/model/lewisharrell>  
<https://www.pornhub.com/model/liloostich>  
<https://www.pornhub.com/model/lodaddygetsdirty>  
<https://www.pornhub.com/model/mariana-martix>  
<https://www.pornhub.com/model/mikasax7>  
<https://www.pornhub.com/model/misslexa>  
<https://www.pornhub.com/model/mrpussylicking>  
<https://www.pornhub.com/model/nickmarxx>  
<https://www.pornhub.com/model/ooooop8>  
<https://www.pornhub.com/model/ponytw>  
<https://www.pornhub.com/model/porn-force>  
<https://www.pornhub.com/model/porn-force-compilations>  
<https://www.pornhub.com/model/sandra-bay>  
<https://www.pornhub.com/model/serenity-cox>  
<https://www.pornhub.com/model/solazola>  
<https://www.pornhub.com/model/stella-bianca>  
[https://www.pornhub.com/model/texas\\_milf\\_pov](https://www.pornhub.com/model/texas_milf_pov)  
<https://www.pornhub.com/model/white-venere>  
<https://www.pornhub.com/more>  
<https://www.pornhub.com/partners/>  
<https://www.pornhub.com/partners/cpp>  
<https://www.pornhub.com/partners/models>

<https://www.pornhub.com/playlist/>  
<https://www.pornhub.com/playlist/63226322>  
<https://www.pornhub.com/playlist/67613592>  
<https://www.pornhub.com/playlists>  
<https://www.pornhub.com/pornstar/>  
<https://www.pornhub.com/pornstar/blake-blossom>  
<https://www.pornhub.com/pornstar/candy-love>  
<https://www.pornhub.com/pornstar/chloe-cherry>  
<https://www.pornhub.com/pornstar/flesh-god>  
<https://www.pornhub.com/pornstar/kyle-balls-wca>  
<https://www.pornhub.com/pornstar/layla-london>  
<https://www.pornhub.com/pornstar/lexi-luna>  
<https://www.pornhub.com/pornstar/maya-johansson>  
<https://www.pornhub.com/pornstar/natasha-nice>  
<https://www.pornhub.com/pornstar/osa-lovely>  
<https://www.pornhub.com/pornstar/rick-angel>  
<https://www.pornhub.com/pornstar/skarlet-luvya>  
<https://www.pornhub.com/pornstar/skylar-vox>  
<https://www.pornhub.com/pornstar/violet-myers>  
<https://www.pornhub.com/pornstars>  
<https://www.pornhub.com/press>  
<https://www.pornhub.com/recaptcha/>  
<https://www.pornhub.com/recaptcha/api.js>  
<https://www.pornhub.com/recommended>  
<https://www.pornhub.com/robots.txt>  
<https://www.pornhub.com/rss>  
<https://www.pornhub.com/service-worker.js>  
<https://www.pornhub.com/sex/>  
<https://www.pornhub.com/sitemap>  
<https://www.pornhub.com/sitemaps.xml>  
<https://www.pornhub.com/support>  
<https://www.pornhub.com/transgender>  
<https://www.pornhub.com/upload/>  
<https://www.pornhub.com/upload/photo>  
<https://www.pornhub.com/user/>  
<https://www.pornhub.com/user/discover>  
<https://www.pornhub.com/user/discover/>  
[https://www.pornhub.com/user/discover/most\\_viewed\\_users](https://www.pornhub.com/user/discover/most_viewed_users)  
[https://www.pornhub.com/user/discover/popular\\_verified\\_members](https://www.pornhub.com/user/discover/popular_verified_members)  
<https://www.pornhub.com/user/search>  
<https://www.pornhub.com/users/>  
<https://www.pornhub.com/users/falsechair>  
<https://www.pornhub.com/video>  
<https://www.pornhub.com/video/>  
<https://www.pornhub.com/video/random>  
<https://www.pornhub.com/video/search>  
[https://www.pornhub.com/view\\_video.php](https://www.pornhub.com/view_video.php)  
<https://www.pornhub.com/webmasters>