# Security Scan 01

Scan completed 12/05/2017

Target: Authentication dummy set up on localhost:3000

Vulnerabilities found: 4

## X-Frame-Options Header Not Set

URL: <http://localhost:3000/>

Risk: Medium

Confidence: Medium

Parameter: X-Frame-Options

CWE ID: 16

WASC ID: 15

Source: Passive

X-Frame-Options header is not included in the HTTP response to protect against ‘ClickJacking’ attacks.

### Vulnerable Code



### Found scan information

HTTP/1.1 200 OK

X-Powered-By: Express

Content-Type: text/html; charset=utf-8

Content-Length: 55

ETag: W/"37-u0h2k2epSRIeypX8Y2Av0FqlX68"

set-cookie: connect.sid=s%3ABVxS7oPl9UiljVMymS2xJbjbvUeTlhkZ.zrMm%2FAmqbAxwvLVha5hQRBXccueF7226uzzXyy1yJHw; Path=/; HttpOnly

Date: Fri, 12 May 2017 04:18:13 GMT

Connection: keep-alive

## Password Autocomplete in Brower

URL: <http://localhost:3000/login>

Risk: Low

Confidence: Medium

Parameter: password

Evidence: <input type=”password” name=”password” />

CWE ID: 525

WASC ID: 15

Source: Passive

The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.

### Vulnerable Code

### 

### Found scan information

HTTP/1.1 200 OK

X-Powered-By: Express

Content-Type: text/html; charset=utf-8

Content-Length: 266

ETag: W/"10a-gRQiPcE1LDDlxhjuhGu3u3KJpgg"

set-cookie: connect.sid=s%3AzV4oJGpOJfVemuXyB9inUXHpoR3FOVbs.2JQ09NYI7nZ9opFBkSM%2Bh5S5FmC2s5FcTISdsqoosmY; Path=/; HttpOnly

Date: Fri, 12 May 2017 04:18:13 GMT

Connection: keep-alive

## Web Browser XSS Protection Not Enabled

URL: <http://localhost:3000/>

Risk: Low

Confidence: Medium

Parameter: X-XSS-Protection

CWE ID: 933

WASC ID: 14

Source: Passive

Web Brower XSS Protection is not enabled, or is disabled by the configuration of the ‘X-XSS-Protection’ HTTP response header on the web server.

### Vulnerable Code



### Found scan information

HTTP/1.1 200 OK

X-Powered-By: Express

Content-Type: text/html; charset=utf-8

Content-Length: 55

ETag: W/"37-u0h2k2epSRIeypX8Y2Av0FqlX68"

set-cookie: connect.sid=s%3ABVxS7oPl9UiljVMymS2xJbjbvUeTlhkZ.zrMm%2FAmqbAxwvLVha5hQRBXccueF7226uzzXyy1yJHw; Path=/; HttpOnly

Date: Fri, 12 May 2017 04:18:13 GMT

Connection: keep-alive

## X-Content-Type-Options Header Missing

URL: <http://localhost:3000/>

Risk: Low

Confidence: Medium

Parameter: X-Content-Type-Options

CWE ID: 16

WASC ID: 15

Source: Passive

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to ‘nosniff’. 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 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.

### Vulnerable Code



### Found scan information

HTTP/1.1 200 OK

X-Powered-By: Express

Content-Type: text/html; charset=utf-8

Content-Length: 55

ETag: W/"37-u0h2k2epSRIeypX8Y2Av0FqlX68"

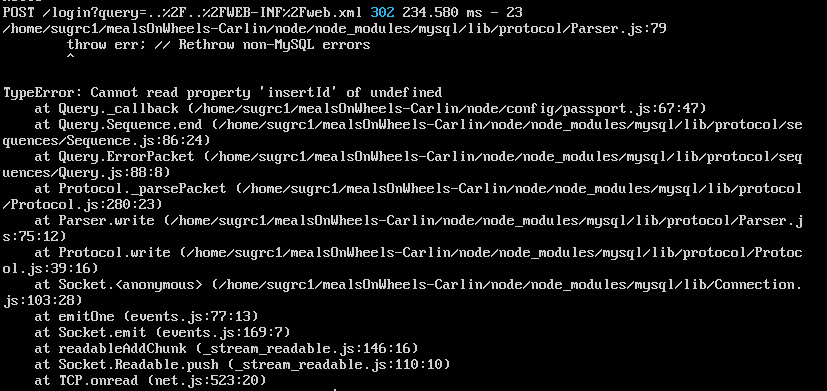
set-cookie: connect.sid=s%3ABVxS7oPl9UiljVMymS2xJbjbvUeTlhkZ.zrMm%2FAmqbAxwvLVha5hQRBXccueF7226uzzXyy1yJHw; Path=/; HttpOnly

Date: Fri, 12 May 2017 04:18:13 GMT

Connection: keep-alive

Security Scan 02 – 2/06/2017

Server Crash error thrown



SkipFish

- 192.168.19.128 -00:32.171, 137 kB in, 86 kB out (7.8 kB/s) ps

- 192.168.19.128 -00:36.987, 150 kB in, 102 kB out (7.8 kB/s) s

Scan statistics:: 0:00:42.886, 159 kB in, 115 kB out (7.4 kB/s) s

Scan statistics:: 0:00:48.598, 164 kB in, 126 kB out (6.8 kB/s) s

Scan time : 0:00:52.382, 170 kB in, 136 kB out (6.3 kB/s) s

Scan time : 0:00:54.335, 183 kB in, 149 kB out (6.4 kB/s) s

HTTP requests : 465 (8.6/s), 186 kB in, 160 kB out (6.4 kB/s) s val

Compression : 0 kB in, 0 kB out (0.0% gain) etried, 0 drops val

HTTP faults : 84 net errors, 0 proto errors, 13 retried, 0 dropsal

TCP handshakes : 97 total (4.8 req/conn) purgeddict 5 par, 0 val

TCP faults : 0 failures, 0 timeouts, 0 purgeddict 5 par, 0 val

External links : 96 skipped1 done (10.00%) 3 dict 5 par, 0 val

Reqs pending : 0 1 done (10.00%) 2 dict 5 par, 0 val

Database statistics: total, 1 done (10.00%) 2 dict 5 par, 0 val

Database statistics: total, 1 done (10.00%) 2 dict 5 par, 0 val

Pivots : 10 total, 1 done (10.00%) 2 dict 5 par, 0 val

Pivots : 10 total, 1 done (10.00%) 1 dict 5 par, 0 val

In progress : 0 pending, 1 init, 7 attacks, 1 dict 5 par, 0 val

Missing nodes : 1 spotted dir, 0 file, 0 pinfo, 0 unkn, 5 par, 0 val

Node types : 1 serv, 4 dir, 0 file, 0 pinfo, 0 unkn, 5 par, 0 val

Issues found : 16 info, 9 warn, 0 low, 6 medium, 0 high impact

Dict size : 7 words (7 new), 0 extensions, 78 candidates

Signatures : 77 total

[+] Copying static resources...

[+] Sorting and annotating crawl nodes: 10

[+] Looking for duplicate entries: 10

[+] Counting unique nodes: 10

[+] Saving pivot data for third-party tools...

[+] Writing scan description...

[+] Writing crawl tree: 10

[+] Generating summary views...

[+] Report saved to '3000/index.html' [0xe72e4487].

[+] This was a great day for science!

Skipfish take 2 (not /login)

- 192.168.19.128 -01:05.108, 301 kB in, 206 kB out (7.8 kB/s) s val

- 192.168.19.128 -01:08.555, 319 kB in, 224 kB out (8.4 kB/s) s val

Scan statistics:: 0:01:14.063, 329 kB in, 240 kB out (8.3 kB/s) s val

Scan statistics:: 0:01:16.086, 334 kB in, 250 kB out (7.9 kB/s) s val

Scan time : 0:01:18.338, 377 kB in, 262 kB out (8.4 kB/s) s val

Scan time : 0:01:21.441, 394 kB in, 278 kB out (8.6 kB/s) s val

HTTP requests : 730 (9.1/s), 404 kB in, 297 kB out (8.6 kB/s) s val

Compression : 0 kB in, 0 kB out (0.0% gain) etried, 0 drops val

HTTP faults : 7 net errors, 0 proto errors, 16 retried, 0 dropsval

TCP handshakes : 34 total (24.3 req/conn) purgeddict 5 par, 0 val

TCP faults : 0 failures, 0 timeouts, 1 purgeddict 5 par, 0 val

External links : 162 skipped done (23.08%) 0 dict 5 par, 0 val

Reqs pending : 96 3 done (23.08%) 0 dict 5 par, 0 val

Database statistics: total, 3 done (23.08%) 0 dict 5 par, 0 val

Database statistics: total, 3 done (23.08%) 0 dict 5 par, 0 val

Pivots : 13 total, 3 done (23.08%) 2 dict 5 par, 0 val

Pivots : 13 total, 3 done (23.08%) 1 dict 5 par, 0 val

In progress : 0 pending, 0 init, 10 attacks, 0 dict par, 0 val

Missing nodes : 0 spotted dir, 0 file, 0 pinfo, 0 unkn, 5 par, 0 val

Node types : 1 serv, 7 dir, 0 file, 0 pinfo, 0 unkn, 5 par, 0 val

Issues found : 16 info, 10 warn, 0 low, 12 medium, 0 high impact

Dict size : 7 words (7 new), 0 extensions, 85 candidates

Signatures : 77 total