



## 2 Security headers missed on https://acme-validation.jamieweb.net/

Share:

State ○ Resolved (Closed)

Disclosed **March 28, 2019 6:21am +0530**

Reported To [JamieWeb](#)

Asset [acme-validation.jamieweb.net](#)  
(Domain)

Weakness Violation of Secure Design Principles

Severity □□□ Medium (4 ~ 6.9)

Participants

Visibility Disclosed (Full)

[Collapse](#)

### SUMMARY BY JAMIEWEB



The reporter identified that the X-DNS-Prefetch-Control, X-Download-Options and Public-Key-Pins headers were missing.

X-Download-Options and Public-Key-Pins are deprecated/of limited use, so these have not been implemented. However, the X-DNS-Prefetch-Control header has now been implemented on all of my live sites in order to avoid the risk of information disclosure via this feature.

### TIMELINE



[mik317](#) submitted a report to [JamieWeb](#).

Feb 25th (about 1 month ago)

#### Summary:

Hi JamieWeb team,

the `https://acme-validation.jamieweb.net/` domain doesn't present some important security headers.

The `X-DNS-Prefetch-Control` header isn't specified with value `off`, so is enabled by default on modern web browsers, and can lead to `information disclosure` (<https://security.stackexchange.com/questions/121796/what-security-implications-does-dns-prefetching-have>).

Additionally, the `X-Download-Options` isn't present, while a good security implication would be `noopen` (here is explained why is important in certain circumstances: <https://github.com/Fyrd/caniuse/issues/3388>).

Finally, the `Public-Key-Pins` header isn't present. It is very helpful because tells to the web browser to associate a public key with a certain web server to prevent `MITM attacks` using `rogue and forged X.509 certificates`. This protects users in case a certificate authority is compromised. Is useful also for the validation of the `SSL` certificate.

#### Steps To Reproduce:

1. Add a `X-DNS-Prefetch-Control: off` header
2. Add a `X-Download-Options: noopen` header
3. Add a `Public-Key-Pins` header (for calculate its value follow the <https://scotthelme.co.uk/hpkp-http-public-key-pinning/> article)

If you don't consider this a valid issue, let me know it and I'll autoclose by myself as N/A :)

#### Impact

Some security headers missed can lead to prevention of certain attacks that can be exploited using reflected attacks in the local network either in remote contexts.



[jamieonubuntu](#) changed the status to ○ Triaged.

Feb 25th (about 1 month ago)

Hi [@mik317](#),

Thanks for your report.

Good spot here - I'm going to add 'X-DNS-Prefetch-Control: off' to all responses and test it in my staging environment. Then hopefully it will be pushed out to the public site either tonight or later in the week.

Public-Key-Pins is a deprecated header and also quite risky to implement, so I'm going to leave it out. X-Download-Options also seems to be applicable only to older IE versions, so I will also leave it out, however I do have it noted as one to keep an eye on, as there does seem to be an ongoing feature request for this to be implemented in Edge. With Edge soon to be switching to Chromium as the engine though, this may mean that the feature request won't be fulfilled.

I will resolve this report once I have implemented the changes on the live website.

Thanks,  
Jamie



jamieonubuntu posted a comment.

Feb 25th (about 1 month ago)

Change has been implemented in staging - deployment to production is planned for Monday night/Tuesday morning GMT.



mik317 posted a comment.

Feb 25th (about 1 month ago)

Hi @jamieonubuntu ,  
thank you so much :).

I'm going to report the same issue also for the other websites:)  
Best, Mik



jamieonubuntu closed the report and changed the status to Resolved.

Feb 26th (about 1 month ago)

Hi @mik317,

I have now implemented the X-DNS-Prefetch-Control header on all of my live sites.

Thanks again for your help,  
Jamie



jamieonubuntu requested to disclose this report.

Feb 26th (about 1 month ago)



mik317 posted a comment.

Mar 16th (12 days ago)

Hi @jamieonubuntu ,  
before report another invalid header, can I know if you're interested in X-Permitted-Cross-Domain-Policies ?  
If yes, let me know it and I'll open another report :)

Best, Mik



jamieonubuntu posted a comment.

Mar 17th (11 days ago)

Hi @mik317,

If you have an attack scenario for the lack of that header, please feel free to report it.

My current thoughts are that any attack would be limited to edge-case information disclosure. For example, a site running a malicious Flash file may be able to determine that somebody had previously visited my site (and maybe even which pages by querying the local cache?), however this header may not even protect against that.

However, if somebody wants to use an old built-in PDF reader or other plugin to access my site, they are welcome to do that, so I'd prefer not to unnecessarily restrict access unless there is a security reason to do so.

Also, in 2019 there would be easier ways to carry out that attack, for example some malicious JavaScript could probably determine based on response times whether my site was in the local DNS cache, or perhaps even by making some requests to try to see whether there are cached Strict-Transport-Security and Expect-CT policies, indicating that the site has been visited previously.

Thanks for your help,  
Jamie




mik317 posted a comment.

Mar 17th (11 days ago)

Thank for the response full of informations :)

Best, Mik

 This report has been disclosed.

Mar 28th (5 hrs ago)