František Malina
fmalina@gmail.com

27 February 2015

NHS.uk security vulnerability

protection from http-accept header forgery

SECURITY REPORT:
STRICTLY CONFIDENTIAL
UNTIL ACTIONED AND FULLY FIXED

This document contains a proof of concept code to help developer test for this issue on local development server. **Do not run it agains the live site.** Author is not responsible for any damage caused by misuse of this report.

This report is provided by the author "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this report, even if advised of the possibility of such damage.

Introduction

While researching family planning I noticed a random webpage of NHS choices does not render, only returns code. See Figure 1.

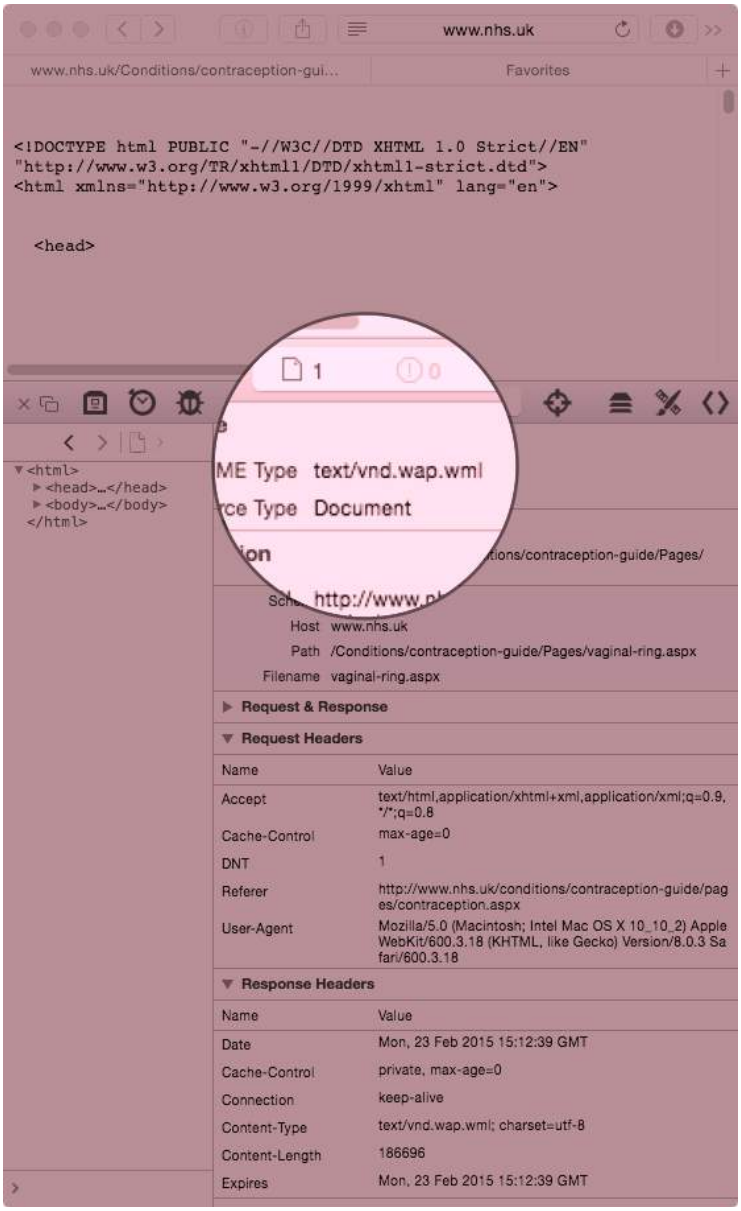
It's an interesting problem, because HTTP Content-Type header for the page looks correct: "Content-Type: text/html", when checked using "curl -i" and the error does not expose itself. This is misleading. The Content-Type header a user agent gets when the error appears is: "Content-Type: text/vnd.wap.wml"

So what is broken

This is due to broken/badly implemented IIS/ASP.NET behaviour where it tries to accommodate for old feature phones, and BREAKS things when such response happens to get cached and subsequently fed to users who were expecting "text/html".

This bug opens a security issue for caches generated on demand because an insisting crawler (or just wget --recursive) with forged http accept header (full code below) can mislead the NHS.uk to regenerate broken cache and take the site down.

Figure 1


www.nhs.uk
www.nhs.uk/Conditions/contraception-gui...
Favorites
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en">
<head>
1
0
ME Type text/vnd.wap.wml
rce Type Document
ion
tions/contraception-guide/Pages/
Host www.nhs.uk
Path /Conditions/contraception-guide/Pages/vaginal-ring.aspx
Filename vaginal-ring.aspx
Request & Response
Request Headers
Name
Value
Accept
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cache-Control
max-age=0
DNT
1
Referer
http://www.nhs.uk/conditions/contraception-guide/pages/contraception.aspx
User-Agent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/600.3.18 (KHTML, like Gecko) Version/8.0.3 Safari/600.3.18
Response Headers
Name
Value
Date
Mon, 23 Feb 2015 15:12:39 GMT
Cache-Control
private, max-age=0
Connection
keep-alive
Content-Type
text/vnd.wap.wml; charset=utf-8
Content-Length
186696
Expires
Mon, 23 Feb 2015 15:12:39 GMT

How to fix it

Specify content-type explicitly.

E.g. change the content-type in the _ViewStart.cshtml (or other shared view start)

```
Response.ContentType = "text/html";
```

your actual views can still override this:

```
@{
 Layout = null;
 Response.ContentType = "application/atom+xml";
}
```

To test for this issue on your local development server
(with a clean cache to avoid false results by previous cached data), use wget or curl:

```
wget yourpage --header="Accept: text/vnd.wap.wml"
  --server-response
  --header="Accept-Encoding: gzip, deflate"
```

and look for:

```
Content-Type: text/vnd.wap.wml; charset=utf-8
```

Source: stackoverflow.com/questions/1261144