Perimeter Walk on demconvention.com

FOR (PUBLIC EXAMPLE) ON OCTOBER 14, 2016

BY CYBERTICAL – CYBERSECURITY FOR POLITICAL CAMPAIGNS

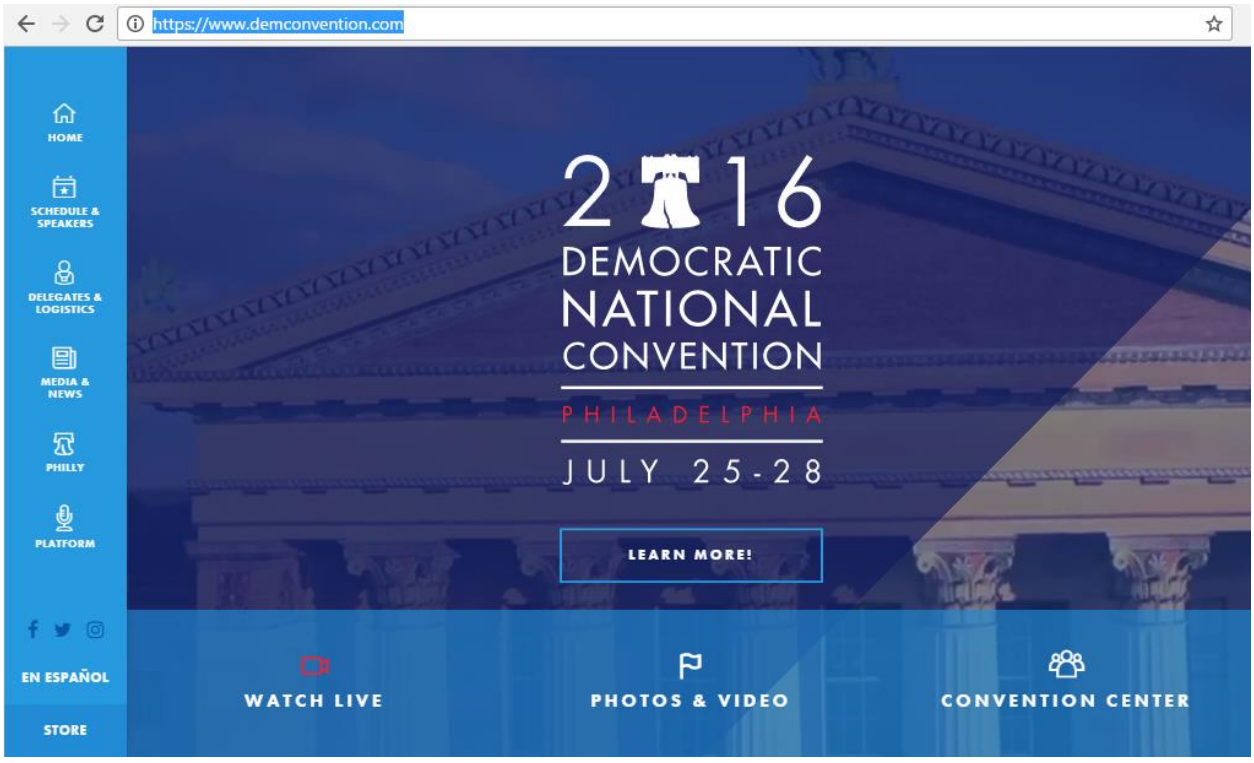
RESULTS AND RECOMMENDATIONS

BACKGROUND

www.demconvention.com is the official site of the 2016 Democratic Convention held July 25-28 by the Democratic National Committee. To demonstrate how Cybertical's non-invasive "Perimeter Walk" service works, Cybertical analyzed the site using information that would be freely available to anyone browsing the site, but from a hacker's perspective.

TARGET

www.demconvention.com is a WordPress site that can only be accessed using HTTPS ("SSL" or "TLS").

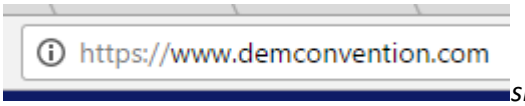


FINDINGS

This is an "event" site that was put up quickly using the popular WordPress content management systems (CMS) but fortunately doesn't try to do too much. The site does not appear to have been updated since the event and at least four known "medium" vulnerabilities are currently known for the versions of software it runs. If the site is left unattended it will likely continue to accrue more known vulnerabilities as they are discovered and fixed in newer (but not applied) versions.

WordPress appears to have been partially secured on this site. On the positive side the usual login page is not accessible and the default administrator appears to have been renamed. However, on the negative side the site provides a complete list of all its accounts (we call this "user enumeration"), and the name of the current administrator is probably the first name on that list.

The underlying "Apache" web server and the "SSL" certificate and encryption settings used to secure access to the site all appear to be correct and properly secured. The site is also almost configured for HTTPS correctly: while it forces HTTPS connections for all its own site traffic, it still pulls in one insecure (HTTP) image that causes web browsers to see the site as a "mixed" site and HIDE the expected "lock icon" when people view the site. (The site will also appear as "not secure" for people drill down on the browser icon where the HTTPS lock should be).



should look like:


An ancillary site used for the store is still active but appears to have been secured by outsourcing the ecommerce engine and store hosting entirely.

CYBERSECURITY GRADE

C

Major negative factor(s): User enumeration, old versions with "medium" known vulnerabilities, site no longer appears to be receiving updates

Ignored negative factor(s): Broken HTTPS configuration

Mitigating positive factor(s): signs of effort on "SSL certificate" and web server security, vulnerabilities can generally only be exploited by authenticated users

RECOMMENDATIONS

Since this site was designed for a single event and it is no longer being updated, the DNC should decide to either take the site down soon or convert it to a "static" site that removes the use of the underlying WordPress engine. Leaving it up indefinitely without updates could lead to an eventually compromise.

In the meantime, the DNC should:

- Update the vulnerable Wordpress engine and the vulnerable plug-in. This is a process that, including back-ups, should take less than a hour, and can be partially updated (with notifications or automatic updates) in the future.
- Turn off "user enumeration" on the site. There are a number of free and commercial WordPress plug-ins with names like "Stop User Enumeration" that can do this.
- Create a new administrative account and delete the original "d***" account, as well as any other admin accounts.

Finally, to address the annoying lack-of-a-lock on its otherwise well-configured HTTPS connections, the DNC may consider:

- Changing the reference to its one HTTP-based "Thank You" image

If the first three bulleted recommendations were both applied, the site would earn a "B+" cybersecurity grade. If all four bulleted recommendations were applied, it would earn an "A-". (The minus on the "A" would still be there due to the choice of the takes-work-to-keep-secure WordPress platform as the underlying engine.)

DETAILED RESEARCH

SITE IDENTIFICATION

This is a WordPress site. (Evidence: view source, see "wp-…" folder references.)

WORDPRESS-SPECIFIC SITE INVESTIGATION

AUTHOR/USERNAME ENUMERATION

It is possible to manually enumerate usernames on the site. (Evidence: ?author=1, ?author=2…)

(In a contracted report, full usernames would be provided if you were the owner of the target.)

- ?author=1 d***
- ?author=3 (blank)
- ?author=4 k**** (Kelli Klein)
- ?author=5 (blank)
- ?author=8 o**** (Olivia Chow)
- ?author=9 (blank)
- ?author=10 h******* (Heather Barmore)
- ?author=12 j****** (Jessica Torres)
- ?author=13 (blank)
- ?author=15 c*******
- ?author=17 k**********
- ?author=18 (blank)
- ?author=20 m**********
- ?author=23 j******
- ?author=26 s**********
- ?author=28 a*****
- ?author=29 d******1
- ?author=31 d******media
- ?author=32 d******2
- ?author=35 d******3
- ?author=37 d******4
- ?author=38 d******5
- ?author=39 anonymous******866
- ?author=42 j*******
- ?author=44 s*********
- ?author=45 e********
- ?author=46 b********
- ?author=51 m****** (Megan Meehan)
- ?author=53 anonymous******795

- ?author=55 n****** (Nick Cat)
- ?author=57 c******** (Chris Frommann)
- ?author=60 h******* (Hayley Richard)
- ?author=62 a***** (Jared James)
- ?author=63 s********** (Sam Waldenburg)
- ?author=64 a**** (Ayanna Gill)
- ?author=65 anonymous******485
- ?author=67 anonymous******455
- ?author=69 anonymous******845
- ?author=71 anonymous******397
- ?author=73 anonymous******650
- ?author=74 j******* (Juan D. Pachon)
- ?author=75 g***** (gab adams)

LOGIN PAGE

The usual WordPress login pages have been obscured or removed. (Evidence: missing /wp-admin and /wp-login.php)

ADMINISTRATIVE ACCOUNT

There is a Wordpress author/user with an ID of 1 named "d***". (Evidence: user enumeration) Most hackers would speculate that the "d***" account is an administrative account.

(In a contracted report, full usernames would be provided if you were the owner of the target.)

SELF-REGISTRATION

Self-Registration was not possible on this site.

VERSION

The site appears to run version 4.5.3 (Evidence: /wp-links-opml.php, released Jun 18, current is 4.6.1). As of October 14, 2016, this version is known to harbor three "medium" vulnerabilities.

- Authenticated Denial of Service (DoS)
- Authenticated Stored Cross-Site Scripting via Image Filename
- Path Traversal in Upgrade Package Uploader

"Authenticated" means a user has to be signed on to take advantage of the vulnerability.

PLUG-INS

- ravnur 4.3 (current)
- wp-super-cache 1.4.8 (current)
- wordpress-seo 3.3.4 (latest is 3.7.0, contains a "medium" vulnerability)
    - Authenticated Stored Cross-Site Scripting (XSS)

GENERAL INVESTIGATION

CONTENT DEVELOPER

Four of the authors/users appear would appear to be most active on the site, if the following article detailing the "digital team" in charge of the site is credible:

Clockwise from top left: Olivia Chow, Kelli Klein, Heather Barmore and Jess Torres.
Source: Celeste Katz

TECHNICAL DEVELOPER

The site was built by "Wide Eye Creative" in 2016. (Evidence: prominent comment in home page source, explicit link on "author" pages)

ROBOTS FILE

The "robots.txt" file that suggests which folders and files search engines should allow and ignore contains puzzling references to "/wp-admin/" and "/wp-admin/admin-ajax.php" – administrative logins that should not be accessible. Fortunately, they are not. (Evidence: /robots.txt).

SITE HEADERS

No site headers other than "Apache" (a common type of web server) and "ETag" (which usually indicates that a site claiming to be "Apache" actually is) were seen.

DNS AND HOSTING

- The site maps to a single IP address:
  Evidence:

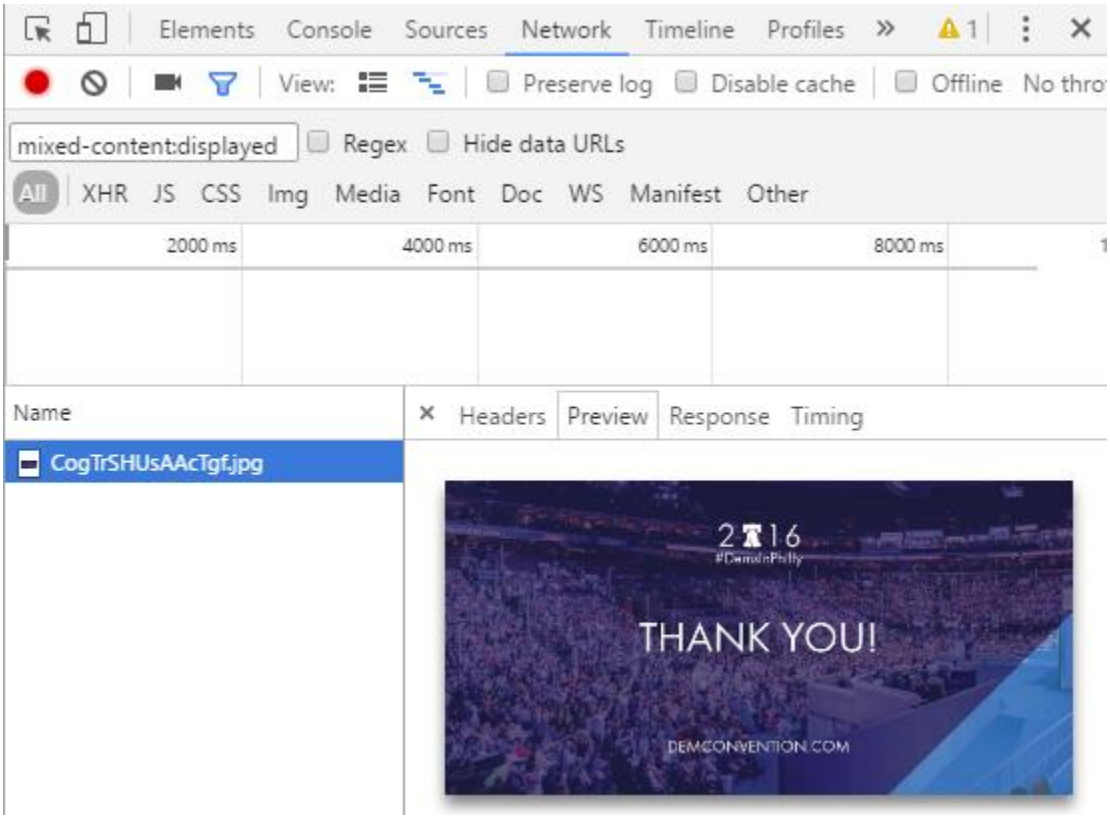
```
www.demconvention.com.   59      IN      CNAME   demconvention.com.
demconvention.com.       59      IN      A       13.89.38.161
```

- The IP address appears to be dedicated to the site. (Evidence: connecting to the IP.)
- The site appears to be hosted on Apache in a Microsoft Azure cloud instance, possibly located in Iowa. (Evidence: online location lookup of IP.)

HTTPS

The site requires HTTPS and forces a redirect to it immediately on insecure content. (Evidence: direct observation)

The site used "mixed content" (using https content and http from other sites). (Evidence: Chrome network info). The content appears limited to a single image (below).



The X.509 certificate used to secure the site is a wildcard cert valid from June 30 2016-July 5 2017 and issued by commercial CA Digicert, with a valid chain and strong hashing. There appears to be no extraneous information on the certificate. (Evidence: Chrome cert inspection).

CLOSELY RELATED SITES

STORE

A related store is hosted offsite on a branded myshopify site at https://democratic-national-convention-store.myshopify.com

ETHICAL DISCLOSURE

The research for this report was conducted on October 14, 2016. This site and a similar site from the major opposition party were selected to demonstrate Cybertical's "Perimeter Walk" service. The report was completed on October 17, 2016 and was immediately sent to three different party contacts with ties to the targeted web site. This report was posted on October 24, 2016 after providing the site owner time to address the issues.

Additional questions can be submitted to info@cybertical.com.