Perimeter Walk on njgop.org

FOR (PUBLIC EXAMPLE) ON OCTOBER 14, 2016

BY CYBERTICAL – CYBERSECURITY FOR POLITICAL CAMPAIGNS

RESULTS AND RECOMMENDATIONS

BACKGROUND

www.njgop.org is the official site of the New Jersey Republican Party (NJGOP). 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.njgop.org is a WordPress site that uses regular HTTP for most content and HTTPS for donations.

FINDINGS

This is the permanent home of the New Jersey Republican Party and it leverages the popular WordPress platform. The site is updated frequently but is beginning to lag behind with the PHP platform on which WordPress depends.

WordPress and its plug-ins are up-to-date. However, the site provides a complete list of all its users to anyone who asks, and the first user is the default "admin" account, which is frequently tested by hackers even if it isn't explicitly listed. The site's login page is also accessible to the Internet.

The underlying Apache web server displays its version in common headers (it's common to hide this information) but it's a properly updated version. HTTPS is present on the site and properly configured, but it is only used for donation content. The Akamai content distribution network also appears to be in use, a choice that has security ramifications because it can mitigate some denial-of-service attacks.

The donation form may have been built with WordPress-related Gravity Forms, which raises questions about the security of stored credit card information.

CYBERSECURITY GRADE

C-

Major negative factor(s): User enumeration, default admin still active

Ignored negative factor(s): HTTPS configuration not used for all content, PHP version is one major version behind and contains a handful of minor vulnerabilities, admin/login page is accessible

Mitigating positive factor(s): All software except PHP appears to be up-to-date, use of Akamai could mitigate low-level denial-of-service (DOS) attacks

RECOMMENDATIONS

The NJGOP should:

- 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 "admin" account, as well as any other admin accounts.

Finally, NJGOP may consider:

- Upgrading its PHP environment to the latest version (without vulnerabilities)
- Hiding the login/admin page
- Extending HTTPS protection to all content on the site. In addition to taking care of a number of privacy concerns, HTTPS-based sites may receive higher "SEO" ratings in Google searches.
- Double-checking where credit card "PAN" (primary account number) is actually stored or logged on the site – references to "gforms" on the page that handles credit-card donations would make many security professionals and auditors nervous.

If the first two bulleted recommendations were both applied, the site would earn a B cybersecurity grade. If all six 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

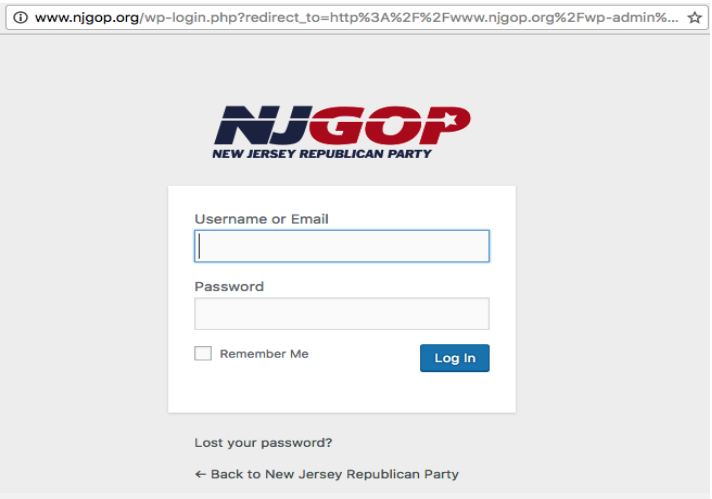
It is possible to manually enumerate usernames on the site. (Evidence: ?author=1, ?author=2…)

(In a contracted report, full usernames would be provided if you were the owner of the target. However, default, and therefore widely known, usernames are reported as is.)

- ?author=2 admin (admin - New Jersey Republican)
- ?author=2 n****
- ?author=3 r***
- ?author=4 p****

LOGIN PAGE

The regular WordPress login page is open to the Internet. (Evidence: /wp-login.php)



ADMINISTRATIVE ACCOUNT

The default WordPress author/user with an ID of 1 named "admin" is still present! (Evidence: user enumeration) All hackers would instantly know this user has special permissions, and many hackers will launch password-guessing attacks against an "admin" account before even confirming it was present on a WordPress system.

SELF-REGISTRATION

Self-registration was not possible on this site.

VERSION

The site appears to run version 4.6.1 (Evidence: /wp-links-opml.php, current).

PLUG-INS

- events-manager - v5.6.6.1 (current)
- gravity-forms-placeholders - v1.2.1 (current)
- soliloquy (unknown)

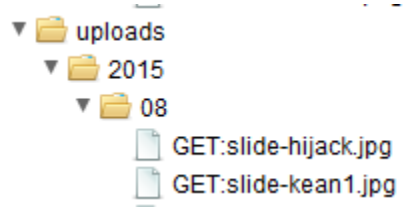
GENERAL INVESTIGATION

CONTENT DEVELOPER

Individual authors of the site are hard to identify as there seems to be heavy use of the common admin account, and few named accounts.

TECHNICAL DEVELOPER

The site was built by "Catch Digital Strategy" in August 2015. (Evidence: theme name, mention on Catch's site, month stamp on "content" folder.)



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 to the general Internet. Unfortunately, they are not. (Evidence: /robots.txt).

SITE HEADERS

The site runs Apache 2.4.23 (latest) and PHP 5.4.45 (from Sep 3, 2015, latest version of 5.4.*, 5.6.27 is latest, at least 6 known vulnerabilities). (Evidence: site headers returned on all pages. PHP 5.4 vulnerabilities: https://www.cloudlinux.com/cloudlinux-os-blog/entry/six-vulnerabilities-for-php-5-4-found)

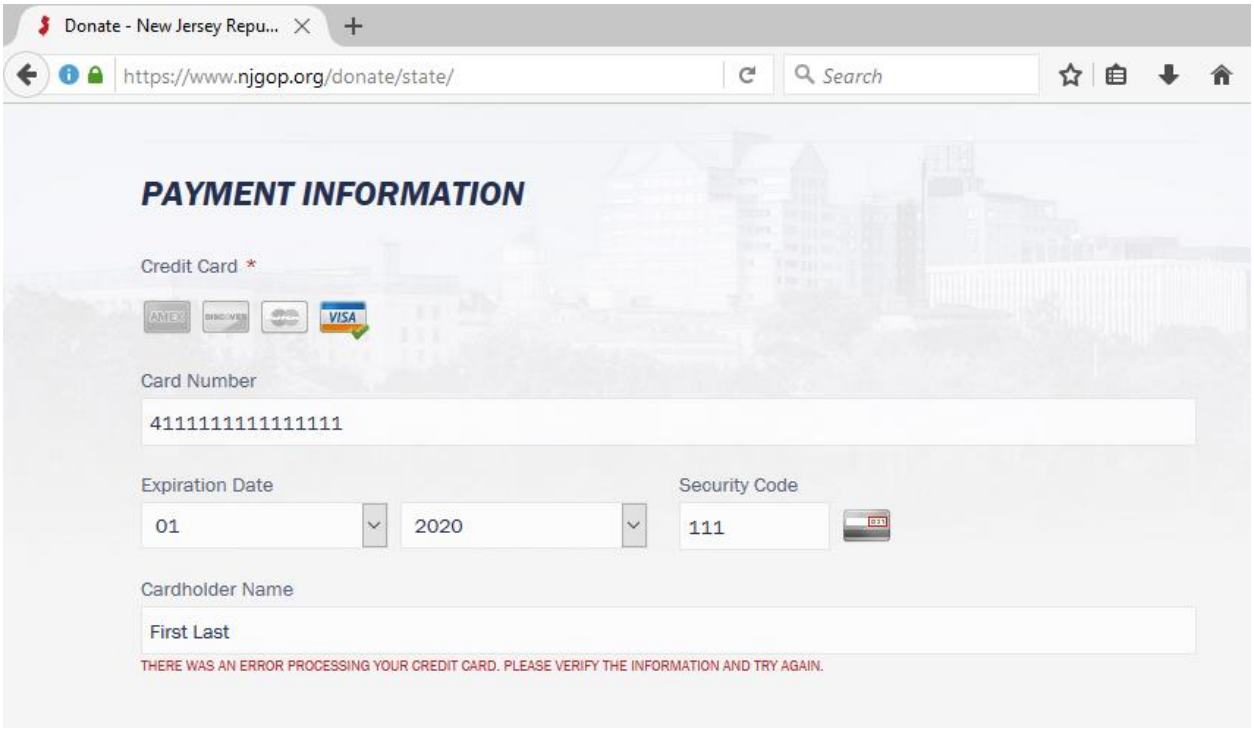
```
HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 02:26:45 GMT
Server: Apache/2.4.23
X-Powered-By: PHP/5.4.45
```

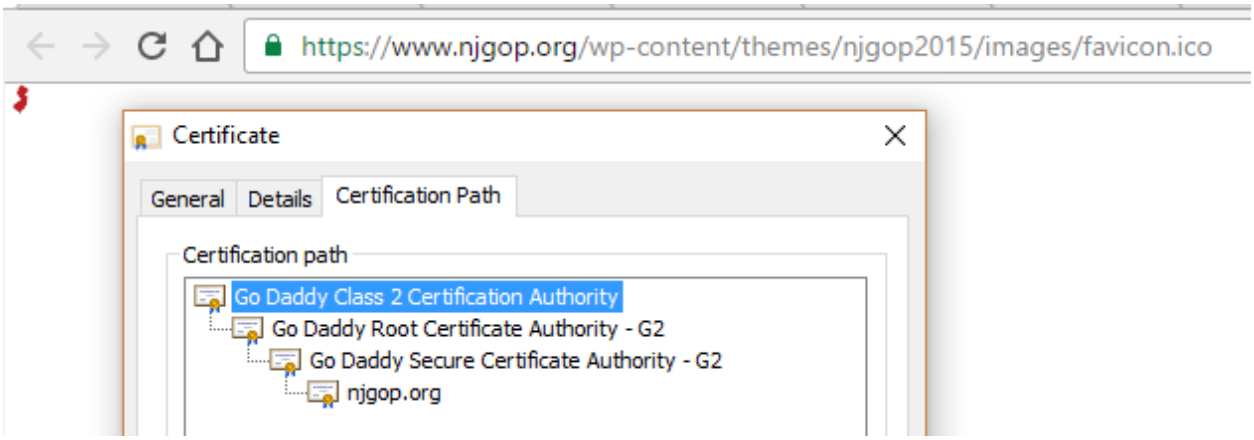
DNS AND HOSTING

- The site maps to multiple IP address depending on location.
  (Evidence: multiple lookups)
- The IP address does not appears to be dedicated to the site. (Evidence: connecting to the IP.)
- The site appears to be hosted or fronted by Akamai. (Evidence: online location lookup of IPs.)

HTTPS

The site does not use HTTPS and forces a redirect to HTTP immediately on non-donation content. (Evidence: direct observation.) HTTPS is set up and properly configured on the site, and it is used correctly to secure credit card submissions used for donations and specific files.





The X.509 certificate used to secure the site is a two-domain cert valid from September 5 2015 to September 5 2017 and issued by commercial CA GoDaddy, with a valid chain and strong hashing. There appears to be no extraneous information on the certificate. (Evidence: Chrome cert inspection).

CLOSELY RELATED SITES

DONATIONS

Donations are handled on the site, possibly through Gravity Forms (Evidence: "gform" entries in page source). While beyond the scope of this research, the target is advised to double-check that credit card numbers are not actually stored in local web storage or written to related logs.

STORE

n/a – there is no store

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.