2016 US Senate Race Cybersecurity

SUMMARY REPORT - NOVEMBER 3, 2016

BY CYBERTICAL – CYBERSECURITY FOR POLITICAL CAMPAIGNS

SUMMARY

Every two years almost seventy major candidates vie for Senate seats across the United States. Many of the candidates have or will soon have a major impact on policy and spending, and their campaign web sites are visited by millions of voters and other interested parties. 2016 has been the year of the political cyberattack, with hacked emails, phishing, insecure servers and even whispers of foreign penetration in the news.

Despite this backdrop, the cybersecurity of US Senate senatorial campaigns leaves much to be desired. On November 1, Cybertical employed a new tool to scan the sites of 67 major candidates and found unpatched vulnerabilities, administrative usernames and public entry points on many of them. To help communicate which candidates' sites were better or worse than others, every site scanned was awarded a "grade point average" (GPA) and a letter grade from A to F. *(See grade summary on next page.)*

Report Highlights:

- 3 Most Secure Candidates: Ron Wyden (Democratic Incumbent in Oregon), Todd Young (Republican Challenger in Indiana) and Foster Campbell (Democratic Challenger in Louisiana)
- 3 Least Secure Candidates: Patty Judge (Democratic Challenger in Iowa), Russ Feingold (Democratic Challenger in Wisconsin) and Patrick Wiesner (Democratic Challenger in Kansas)
- Just 33% of the sites require the use of HTTPS (also called "SSL" or "TLS") to protect privacy of the people who visit them
- 61% of Senate campaign sites run the popular WordPress "CMS" software, compared with just 25% of all sites on the Internet *(according to W3Times in November 2015)*
- 15% of all WordPress campaign sites were running old versions with 61 known vulnerabilities
- 99 account usernames (that could sign onto WordPress) were found as WordPress "authors" and 42 account usernames were found in WordPress "posts"
- A powerful administrative username was recovered from 56% of the WordPress sites
- A WordPress login form was exposed to the public on 78% of the WordPress sites, and 80% of the WordPress sites would tell a hacker if a specific username was on the system or not
- One of the WordPress sites allowed the public to register their own accounts
- It took Cybertical's tool about an hour to gather data from all the sites, or just less than a minute to gather the data from each site

CANDIDATE GPA/GRADE SUMMARY

The following chart summarizes the cybersecurity GPAs and letter grades for all major 2016 Senate candidates that had a website (one candidate did not).

State	Candidate	Party	GPA	Grade
Oregon	Ron Wyden	Democratic	3.90	A
Indiana	Todd Young	Republican	3.70	A-
Louisiana	Foster Campbell	Democratic	3.70	A-
Utah	Misty K. Snow	Democratic	3.70	A-
Florida	Marco Rubio	Republican	3.60	A-
Idaho	Jerry Sturgill	Democratic	3.60	A-
Nevada	Catherine Cortez	Democratic	3.60	A-
New York	Chuck Schumer	Democratic	3.60	A-
Ohio	Ted Strickland	Democratic	3.60	A-
Vermont	Patrick Leahy	Democratic	3.60	A-
Washington	Patty Murray	Democratic	3.60	A-
Georgia	Jim Barksdale	Democratic	3.50	A-
Ohio	Rob Portman	Republican	3.50	A-
Pennsylvania	Pat Toomey	Republican	3.50	A-
California	Loretta Sanchez	Democratic	3.40	B+
Connecticut	Dan Carter	Republican	3.40	B+
Florida	Patrick Murphy	Democratic	3.40	B+
Kentucky	Rand Paul	Republican	3.40	B+
Louisiana	Caroline Fayard	Democratic	3.40	B+
Missouri	Jason Kander	Democratic	3.40	B+
North Carolina	Deborah Ross	Democratic	3.40	B+
North Dakota	Eliot Glassheim	Democratic	3.40	B+
South Carolina	Thomas Dixon	Democratic	3.40	B+
South Dakota	Jay Williams	Democratic	3.40	B+
Arkansas	John Boozman	Republican	3.20	B+
Louisiana	John Kennedy	Republican	3.20	B+
Maryland	Kathy Szeliga	Republican	3.20	B+
North Dakota	John Hoeven	Republican	3.20	B+
Oklahoma	James Lankford	Republican	3.20	B+
South Dakota	John Thune	Republican	3.20	B+
Arizona	Ann Kirkpatrick	Democratic	3.10	B
Louisiana	Charles Boustan	Republican	3.00	B
Maryland	Chris Van Hollen	Democratic	3.00	B
Idaho	Mike Crapo	Republican	2.90	B

State	Candidate	Party	GPA	Grade
Iowa	Chuck Grassley	Republican	2.85	B-
Georgia	Johnny Isakson	Republican	2.80	B-
Hawaii	Brian Schatz	Democratic	2.70	B-
Illinois	Mark Kirk	Republican	2.70	B-
Alaska	Lisa Murkowski	Republican	2.65	B-
Indiana	Evan Bayh	Democratic	2.60	B-
Vermont	Scott Milne	Republican	2.40	C+
Hawaii	John Carroll	Republican	2.35	C+
Nevada	Joe Heck	Republican	2.30	C+
Utah	Mike Lee	Republican	2.25	C
Wisconsin	Ron Johnson	Republican	2.20	C
New York	Wendy Long	Republican	2.10	C
Pennsylvania	Kathleen McGint	Democratic	2.10	C
Missouri	Roy Blunt	Republican	2.05	C
Alabama	Ron Crumpton	Democratic	2.05	C
Illinois	Tammy Duckwor	Democratic	1.95	C-
Alaska	Ray Metcalfe	Democratic	1.85	C-
Colorado	Darryl Glenn	Republican	1.85	C-
Washington	Chris Vance	Republican	1.50	D+
North Carolina	Richard Burr	Republican	1.40	D+
Connecticut	Richard Blument	Democratic	1.20	D
Oregon	Mark Callahan	Republican	1.15	D
South Carolina	Tim Scott	Republican	1.15	D
Alabama	Richard Shelby	Republican	1.00	D-
Arizona	John McCain	Republican	1.00	D-
Kansas	Jerry Moran	Republican	0.90	D-
California	Kamala Harris	Democratic	0.65	F
Kentucky	Jim Gray	Democratic	0.65	F
Arkansas	Conner Eldridge	Democratic	0.58	F
Colorado	Michael Bennet	Democratic	0.53	F
Iowa	Patty Judge	Democratic	0.18	F
Wisconsin	Russ Feingold	Democratic	-0.26	F
Kansas	Patrick Wiesner	Democratic	-1.25	F

METHODOLOGY

APPROACH AND APPLICATION

Cybertical developed a new application to scan a list of target sites and look for attributes security experts (and hackers) frequently look for on potential targets.

The general approach used by the application was one used in manual reconnaissance operations by Cybertical founder Jonathan Lampe for years, and detailed in his application security presentation at the national CISSP conference ("(ISC)2 Congress") in 2015. The approach was also used by Lampe in a series of reports on presidential candidate cybersecurity when he led the Security Awareness product line at the InfoSec Institute. *(Visit Cybertical.com to download these materials.)*

Simply stated, Lampe's approach focused on using information freely available to the public to make security assumptions about a target. It was a "zero hacking" approach that sidesteps the hassle of requesting permission of targeted sites by avoiding unauthorized actions. In other words, this approach "looks really closely" without hacking. For example, Lampe would inspect the contents a site's "headers" (given freely when requesting any page) but would not try to exploit any possible vulnerabilities. Despite the limited scope of Lampe's approach, he could obtain a great deal of information about the security posture of a target, such as what software it ran, how often it was updated and whether a professional security team had been involved in the deployment.

Cybertical's new application automated key elements of this approach. This meant that the application could be used to quickly inspect multiple sites, and to inspect the same sites over time to track changes in their cybersecurity posture. The application was written in Python, a popular development environment in the cybersecurity community, and draws some inspiration from other (non-Python) information security tools such as nmap and wpScan.

INSPECTED ATTRIBUTES

The application inspected the following attributes on all sites using public-access calls:

- **Useful Server Header** – Helps hackers figure out what software is running so they can try the right exploits against it. A typical useful value for this field is "Apache/2.4.23".
- **Useful X-Powered-By** – Also helps hackers figure out what software is running so they can try the right exploits against it. A typical useful value for this field is "PHP/5.3.29".
- **HTTPS Is Available** – Whether the site was available (at all) using a secure HTTPS session (a.k.a. "SSL" or "TLS"). This is a positive attribute: HTTPS should be on.
- **HTTPS Is Required** – Whether the site automatically forced the use of HTTPS. This was an even more positive attribute: if HTTPS was available, it should also be required.
- **Site Runs WordPress** - Whether or not the site was powered by the popular "content management system" (CMS) software, software that often exposes with some additional security issues.

The application also inspected the following attributes on WordPress sites using public-access calls:

- **WordPress Version** – The apparent WordPress version, obtained by inspecting multiple URLs where the information is often exposed.
- **WordPress Login Page Is Exposed** – Whether the default login page is available to the public. This carries some risk because it means attackers could just try usernames and passwords against a friendly web form (no hacking skills needed).
- **WordPress Registration Page Is Exposed –** Whether the default account self-registration page is available to the public. This typically means that self-registration is enabled, and carries significant risk because it allows members of the public to create new accounts on what is often intended to be a closed server.
- **WordPress Author User Enumeration** – WordPress's built-in (and on-by-default) "posts for author" capability reveals a list of account username to anyone who asks. If this capability existed, it was logged as "**Allows WordPress Author User Enumeration**" and the number of usernames found was logged as "**WordPress Users Identified as Authors**".
- **WordPress Feed User Enumeration** – WordPress's built-in (and also on-by-default) "post feed" capability often reveals account usernames used to post articles, if account names were left to match their usernames. If this capability existed, it was logged as "**Allows WordPress Feed User Enumeration**" and the number of usernames found was logged as "**WordPress Users Identified In Posts**".

Since the application is still new, Cybertical also performed some manual operations to complete the data collection. (They may be automated in the future.) These operations included:

- Manual lookup of WordPress versions to determine if "**WordPress Out Of Date**" and how many "**WordPress Vulnerabilities**" might exist on the site

SCORING AND GRADING

Most collected attributes were first scored on a "0/1" binary scale. The three attributes that were scored on an integer scale instead were Age of WordPress Version In Days, WordPress Users Identified As Authors, and WordPress Users Identified In Posts.

Each attribute was given a weight. Negative weights were provided for negative attributes (e.g., Allows Author User Enumeration) and positive weights were provided for positive attributes (e.g., Requires HTTPS). The exact weights used in this report's grading are shown below.

Useful Server Header	Useful X-Powered-By	HTTPS Is Available	HTTPS Is Required	Site Runs Wordpress	Age of Wordpress Version In Days	Known Vulnerabilities in Wordpress Version
-0.2	-0.2	0.1	0.2	-0.3	-0.0014	-0.05

Wordpress Login Page Is Exposed	Wordpress Registration Page Is Exposed	Wordpress Lost Password Page Is Exposed	Wordpress Users Identified As Authors	Allows Wordpress Author User Enumeration
-0.1	-1	-0.3	-0.05	-0.5

Wordpress Users Identified In Posts	Allows Wordpress Feed User Enumeration	Using Default Wordpress admin	Other Wordpress Admin Account Likely Found
-0.05	-0.5	-1	-0.3

The attributes were summed for each site and added to a base value of 3.6 (an "A-"). This value was each site's grade point average (GPA).

Finally, letter grades were applied to each site (and average GPAs) using the following scale.

Min GPA	Max GPA	Letter Grade
4	1000	A+
3.8	**3.999**	**A**
3.5	3.799	A-
3.2	3.499	B+
2.9	**3.199**	**B**
2.6	2.899	B-
2.3	2.599	C+
2	**2.299**	**C**
1.7	1.999	C-
1.4	1.699	D+
1.1	**1.399**	**D**
0.8	1.099	D-
-1000	0.8	F

FINDINGS

SECURITY ATTRIBUTE SUMMARY

ALL SITES

The following results and analysis are based on all 67 candidate sites.

Attribute	% With It	Note
Useful Server Header	37%	Helps hackers figure what software is running so they can try the right exploits
Useful X-Powered-By	31%	Helps hackers figure what software is running so they can try the right exploits
HTTPS Is Available	43%	Server COULD protect privacy of users (this is a good start!)
HTTPS Is Required	33%	Server DOES protect privacy of users (this is great!)
Site Runs Wordpress	61%	Popular CMS that comes with some common security risks (see below)

Many sites provided headers that would be useful to hackers. Ideally these "Useful" percentages (37% and 31%) would be closer to zero because web sites that provide this type of information often become targets. (Hackers know that the first thing security experts typically do to a site is turn off these headers, so sites that still broadcast them are typically regarded as easier targets.)

In a positive step, a third of all sites used HTTPS to secure the browsing sessions of all visitors (by requiring HTTPS). This is an important security consideration that also offers "search engine optimization" (SEO) benefits (because Google reportedly boosts the search results of HTTPS sites).

However, another 10% of all sites offered but did not require HTTPS for the entire site. This type of configuration usually supports a handful of secure forms (for campaign contributions, volunteer registration, etc.), but a partially-configured HTTPS site is an anachronism that invites insecurity through accident in 2016. Instead, sites that support HTTPS should just use HTTPS throughout.

A large number of campaign sites (61%) ran WordPress. This figure is much higher than the 25% of sites that reportedly run WordPress worldwide, but it is actually lower than the percentage of major presidential candidate sites that ran WordPress in the 2016 campaign. *(See Cybertical.com for more information on 2016 presidential WordPress sites.)* Since most sites ran WordPress, Cybertical conducted additional investigation of these sites for this report.

WORDPRESS SITES

The following results and analysis are based on the 41 WordPress-based candidate sites.

Attribute	% With It	Note
Detected Wordpress Version	80%	Helps hackers figure what software is running so they can try the right exploits
Wordpress Out Of Date	15%	Exposes site to known vulnerabilities
Wordpress Login Page Is Exposed	78%	Lets low-skilled "hackers" try to sign onto the site
Wordpress Registration Page Is Exposed	2%	Lets the public register for their own accounts on the site (dangerous!)
Wordpress Lost Password Page Is Exposed	80%	Allows hackers to check whether or not certain users are on the system
Allows Wordpress Author User Enumeration	46%	Allows hackers to collect the names of all users on the site
Allows Wordpress Feed User Enumeration	46%	Allows hackers to collect the names of busy users (and see what they did)
Using Default Wordpress admin	24%	Opens site up to common scripted attacks against "admin" account
Other Wordpress Admin Account Likely Found	32%	Site suggests username of another administrator (besides "admin")

Attribute	Total	Note
Known Vulnerabilities in Wordpress Version	61	Total number of vulnerabilities discovered on all Wordpress sites
Wordpress Users Identified As Authors	99	Total number of users discovered as "authors" on all Wordpress sites
Wordpress Users Identified In Posts	42	Total number of users discovered in "posts" on all Wordpress sites

Cybertical's automated tool figured out the exact version of WordPress running on each site 80% of the time. Manual inspection (and future versions of the Cybertical tool) could boost this closer to 100%. The true version of WordPress is hard to obscure (even with WordPress security tools) because it leaks out in URLs, rarely-used fields, error messages, "readme" files and elsewhere. Since a determined hacker can usually get an accurate WordPress version from a target, it becomes even more essential for WordPress site owners to keep their software up-to-date.

Fortunately, only 15% of scanned sites were out-of-date. Most of the out-of-date sites were about four months behind, but Kansas Democrat challenger Patrick Wiesner appeared to be running a site almost two years out of date (and with 27 known vulnerabilities). Between all these out-of-date sites a total of 61 known vulnerabilities were suspected (or 34 vulnerabilities without Wiesner's).

WordPress campaign site authors often concentrate on the home page and pages/posts they create, but they often forget that WordPress also contains a number of built-in pages that reveal a surprising amount of information and access to the underlying WordPress application.

First, there is the WordPress login page. This page is what authors and administrators use to sign on to the system and make changes, but hackers can try to sign on too if this page is exposed to the Internet. This page was almost always (78%) enabled on the sites studied.

Second, there is the WordPress registration page. This page allows the public to register with their own accounts. It is rarely enabled on campaign sites, but Arizona Republican Senator John McCain's site appeared to have this dangerous function enabled.

Third, there is the WordPress "lost password" page. This page allows legitimate users to reset their passwords without bothering the site administrators. However, the way it has been implemented also allows hackers to try out different usernames to see if they exist on the site. (This occurs because the password reset function provides different responses when trying usernames that do or do not exist.) This page was also almost always (80%) enabled on the sites studied.

In addition to the built-in login, registration and lost password pages, other built-in pages list some or all of the account usernames on the system.

First, WordPress's "posts by author" revealed a complete list of account usernames on almost half (46%) of all sites studied, and a total of 99 different users were collected in this way.

Second, WordPress's "post feed" facility revealed a partial list of account usernames on almost half (46%) of all sites studied, and a total of 42 different users were collected in this way. This facility also tells interested parties which users were responsible for the most posts on the site, and this information can be used to guess which user is the administrator on the system when one user is responsible for most of the posts.

Some intelligence has to be applied to figure out the administrative username on each WordPress site. First, if any of the usernames is "admin", then that's the admin. Unfortunately, a site with an "admin" administrator is often susceptible to "script kiddies" who continually troll the Internet with automation that attempts to sign on as "admin" with a long list of common passwords. If there is no "admin" user, the first username in a list of authors is often the site administrator (since it's the first one that gets created). If the author list could not be obtained, then the busiest user listed in the feed post is often the site administrator.

After applying that intelligence, the username of a powerful administrative account could be determined on 56% of the sites. About half of those sites (24% of all WordPress sites) revealed the dangerous "admin" username, and the rest (32% of all WordPress sites) revealed other usernames.

US SENATE CANDIDATE SUMMARY

The complete results for all US Senate Candidate sites studied is provided below. The GPA and (letter) Grade fields were calculated using the methodology detailed above, and a list of factors that directly contributed to the GPA is listed in the "Reasons" column. (The list of Reasons is longer for poorly-scoring sites. However, remember that "HTTPS…" reasons are positive, not negative.)

State	Candidate	Party	Incum-bent	Site	GPA	Grade	Reasons
Oregon	Ron Wyden	Democratic	Yes	https://www.standtallforamerica.com	3.90	A	HTTPS Is Available, HTTPS Is Required,
Indiana	Todd Young	Republican	No	https://toddyoung.org/	3.70	A-	HTTPS Is Available,
Louisiana	Foster Campbell	Democratic	No	http://www.fostercampbell2016.com	3.70	A-	HTTPS Is Available,
Utah	Misty K. Snow	Democratic	No	http://www.mistyksnow.com	3.70	A-	HTTPS Is Available,
Florida	Marco Rubio	Republican	Yes	https://marcorubio.com	3.60	A-	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress,
Idaho	Jerry Sturgill	Democratic	No	http://sturgill4senate.com	3.60	A-	
Nevada	Catherine Cortez Masto	Democratic	No	http://catherinecortezmasto.com	3.60	A-	
New York	Chuck Schumer	Democratic	Yes	http://www.chuckschumer.com	3.60	A-	
Ohio	Ted Strickland	Democratic	No	http://www.tedstrickland.com	3.60	A-	
Vermont	Patrick Leahy	Democratic	Yes	http://www.leahyforvermont.com	3.60	A-	
Washington	Patty Murray	Democratic	Yes	http://www.pattymurray.com	3.60	A-	
Georgia	Jim Barksdale	Democratic	No	https://jimbarksdale.com	3.50	A-	Useful X-Powered-By, HTTPS Is Available,

Ohio	Rob Portman	Republican	Yes	https://www.robportman.com	3.50	A-	Useful Server Header, Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required,
Pennsylvania	Pat Toomey	Republican	Yes	https://www.toomeyforsenate.com	3.50	A-	Useful Server Header, Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required,
California	Loretta Sanchez	Democratic	No	http://www.loretta.org/	3.40	B+	Useful Server Header,
Connecticut	Dan Carter	Republican	No	http://www.carterforsenate.com	3.40	B+	Useful Server Header,
Florida	Patrick Murphy	Democratic	No	https://www.murphyforflorida.com	3.40	B+	Useful Server Header, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress,
Kentucky	Rand Paul	Republican	Yes	http://www.randpaul2016.com	3.40	B+	Useful X-Powered-By,
Louisiana	Caroline Fayard	Democratic	No	http://www.carolinefayard.com	3.40	B+	Useful Server Header,
Missouri	Jason Kander	Democratic	No	https://www.jasonkander.com	3.40	B+	Useful Server Header, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress,
North Carolina	Deborah Ross	Democratic	No	https://www.deborahross.com	3.40	B+	Useful Server Header, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress,
North Dakota	Eliot Glassheim	Democratic	No	http://www.eliot4nd.com	3.40	B+	Useful Server Header,
South Carolina	Thomas Dixon	Democratic	No	http://www.dixonforsc.com	3.40	B+	Useful Server Header,
South Dakota	Jay Williams	Democratic	No	http://www.jaywilliams2016.org	3.40	B+	Useful Server Header,
Arkansas	John Boozman	Republican	Yes	http://www.boozmanforarkansas.com	3.20	B+	Useful Server Header, Useful X-Powered-By,
Louisiana	John Kennedy	Republican	No	http://www.johnkennedy.com	3.20	B+	Useful Server Header, Useful X-Powered-By,

Maryland	Kathy Szeliga	Republican	No	http://www.kathyformaryland.com	3.20	B+	Useful Server Header, Useful X-Powered-By,
North Dakota	John Hoeven	Republican	Yes	http://www.hoevenforsenate.com	3.20	B+	Useful Server Header, Useful X-Powered-By,
Oklahoma	James Lankford	Republican	Yes	http://jameslankford.com	3.20	B+	Useful Server Header, Useful X-Powered-By,
South Dakota	John Thune	Republican	Yes	http://www.johnthune.com	3.20	B+	Useful Server Header, Useful X-Powered-By,
Arizona	Ann Kirkpatrick	Democratic	No	http://www.kirkpatrickforsenate.com	3.10	B	Useful Server Header, Site Runs Wordpress,
Louisiana	Charles Boustany	Republican	No	http://charlesboustany.com	3.00	B	HTTPS Is Available, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed,
Maryland	Chris Van Hollen	Democratic	No	https://vanhollen.org/	3.00	B	Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed,
Idaho	Mike Crapo	Republican	Yes	http://crapoforsenate.com	2.90	B	Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed,
Iowa	Chuck Grassley	Republican	Yes	https://grassleyworks.com	2.85	B-	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Georgia	Johnny Isakson	Republican	Yes	https://johnnyisakson.com	2.80	B-	Useful X-Powered-By, HTTPS Is Available, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed,

Hawaii	Brian Schatz	Democratic	Yes	http://brianschatz.com	2.70	B-	Useful X-Powered-By, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed,
Illinois	Mark Kirk	Republican	Yes	https://kirkforsenate.com	2.70	B-	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Alaska	Lisa Murkowski	Republican	Yes	https://www.lisamurkowski.com	2.65	B-	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Indiana	Evan Bayh	Democratic	No	http://evanbayhforindiana.com	2.60	B-	Site Runs Wordpress, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Vermont	Scott Milne	Republican	No	http://www.scottmilne.org	2.40	C+	Useful X-Powered-By, Site Runs Wordpress, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Hawaii	John Carroll	Republican	No	https://carroll4senate.wordpress.com	2.35	C+	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Nevada	Joe Heck	Republican	No	https://drjoeheck.com	2.30	C+	HTTPS Is Available, HTTPS Is Required, Site

							Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Utah	Mike Lee	Republican	Yes	https://www.leeforsenate.com	2.25	C	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Wisconsin	Ron Johnson	Republican	Yes	https://www.ronjohnsonforsenate.com	2.20	C	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
New York	Wendy Long	Republican	No	https://wendylong.com	2.10	C	Useful Server Header, Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Pennsylvania	Kathleen McGinty	Democratic	No	https://katiemcginty.com	2.10	C	Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is

							Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Missouri	Roy Blunt	Republican	Yes	https://www.royblunt.com	2.05	C	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration,
Alabama	Ron Crumpton	Democratic	No	http://crumptonforalabama.com	2.05	C	Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Illinois	Tammy Duckworth	Democratic	No	http://tammyduckworth.com	1.95	C-	Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Alaska	Ray Metcalfe	Democratic	No	http://metcalfeforussenate.com	1.85	C-	Useful X-Powered-By, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Colorado	Darryl Glenn	Republican	No	https://electdarrylglenn.com	1.85	C-	Useful Server Header, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress

							Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Washington	Chris Vance	Republican	No	https://chrisvanceforsenate.com	1.50	D+	Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
North Carolina	Richard Burr	Republican	Yes	https://www.burrforsenate.com	1.40	D+	HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Connecticut	Richard Blumenthal	Democratic	Yes	http://richardblumenthal.com	1.20	D	Useful Server Header, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,

Oregon	Mark Callahan	Republican	No	https://callahanfororegon.com	1.15	D	Useful Server Header, Useful X-Powered-By, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Using Default Wordpress admin,
South Carolina	Tim Scott	Republican	Yes	http://votetimscott.com	1.15	D	Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,
Alabama	Richard Shelby	Republican	Yes	http://www.shelbyforsenate.com	1.00	D-	Useful Server Header, Useful X-Powered-By, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,
Arizona	John McCain	Republican	Yes	http://www.johnmccain.com	1.00	D-	Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Registration Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Other Wordpress Admin Account Likely Found,

Kansas	Jerry Moran	Republican	Yes	https://www.moranforkansas.com	0.90	D-	Useful Server Header, HTTPS Is Available, HTTPS Is Required, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,
California	Kamala Harris	Democratic	No	http://www.kamalaharris.org/	0.65	F	HTTPS Is Available, Site Runs Wordpress, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Using Default Wordpress admin,
Kentucky	Jim Gray	Democratic	No	http://grayforkentucky.com	0.65	F	Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Using Default Wordpress admin,
Arkansas	Conner Eldridge	Democratic	No	https://connerforarkansas.com	0.58	F	Useful Server Header, Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts,

							Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,
Colorado	Michael Bennet	Democratic	Yes	http://bennetforcolorado.com	0.53	F	Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Using Default Wordpress admin,
Iowa	Patty Judge	Democratic	No	http://pattyjudgeforiowa.com	0.18	F	Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,
Wisconsin	Russ Feingold	Democratic	No	http://russfeingold.com	-0.26	F	Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified As Authors, Allows Wordpress Author User Enumeration, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,

Kansas	Patrick Wiesner	Democratic	No	http://www.wiesnerforsenate.com	-1.25	F	Useful X-Powered-By, Site Runs Wordpress, Age of Wordpress Version In Days, Known Vulnerabilities in Wordpress Version, Wordpress Login Page Is Exposed, Wordpress Lost Password Page Is Exposed, Wordpress Users Identified In Posts, Allows Wordpress Feed User Enumeration, Using Default Wordpress admin,

IGNORED CANDIDATE

Mike Workman, the Democratic challenger in Oklahoma, was ignored in this report because his campaign did not appear to have a website. (Workman instead relied on a Facebook page for his Internet presence.)

POLITICAL PARTY AND INCUMBENT STATUS ANALYSIS

Cybertical analyzed the average GPA of two different candidate groupings:

- Political Party (Republican or Democrat)
- Incumbent Status (whether each candidate was an incumbent or not)

Surprisingly there was little difference between either of the two groups in the two different groupings.

REPUBLICAN VS. DEMOCRAT

Democratic	2.44	C+
Republican	2.51	C+
AVERAGE	2.51	C+

The average GPA of Republicans and Democrats was similar, with Republicans holding a slight edge. This finding was even more unexpected because of the greater volatility of Democratic cybersecurity GPAs (the three least secure and two of the most secure candidates were all Democrats).

INCUMBENT VS. CHALLENGERS

Incumbent	2.56	C+
Not an Incumbent	2.41	C+
AVERAGE	2.51	C+

The average GPA of Incumbents and Challengers was similar, with Incumbents holding a slight edge. This finding was expected, as Incumbents often have more resources and time to prepare than challengers (especially in non-competitive races).

DISCLAIMERS

As noted throughout this report, no attempt to gain unauthorized access to any target server was made, no "hacking" was performed, and Cybertical does not endorse or encourage any act that attempts to gain unauthorized access or "hack" any target, or violate any law or regulation.

CONTACT

Visit Cybertical.com for more information about out political cybersecurity services, past reports and presentations. Complete information (or the application) used to create this report may be available for a nominal fee, or a reduced or waived fee for certain uses. Detailed extracts (e.g., for a specific candidate or race) and additional background information are typically available at no charge. Report sponsorship and republication/distribution rights may also be available.

Please submit all inquiries to info@cybertical.com.