Cybersecurity

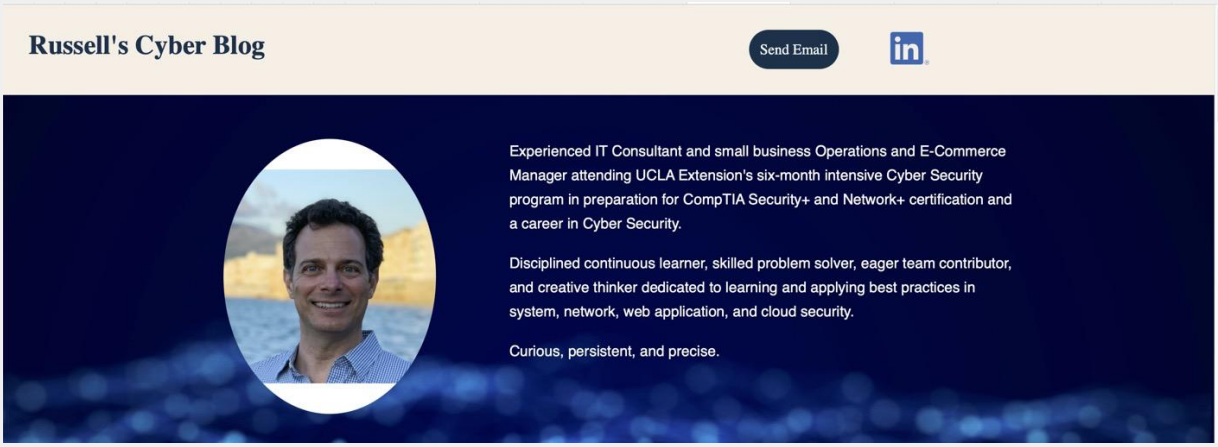
Project 1 Technical Brief

Your Web Application

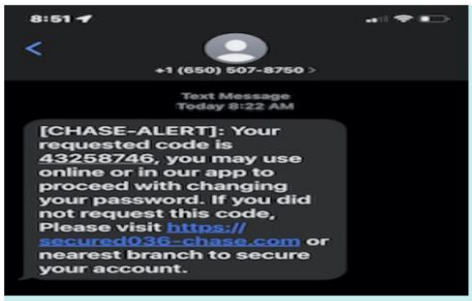
Enter the URL for the web application that you created:

```
https://rjgsecurityresume.azurewebsites.net
```

Paste screenshots of your website created (Be sure to include your blog posts):



Blog Posts



Smishing on the Rise

This morning I received a "smishing" (SMS-based phishing) attempt sent to my phone. I don't have an active Chase account, but I have in the past, so it gave me pause. What if one of my IT clients who DO have active Chase accounts had received this message? What could they do to investigate (or, more likely, ask me to do on their behalf)?

I put on my cyber Sherlock Holmes hat and put some energy into the thought exercise.

The URL includes the words "chase.com," but after a hyphen so it was clear that the TLD (top level domain) was not, in fact, coming from chase.com. That, and a quick internet search for "chase-alert text scam," turned up enough articles and examples to make me confident that this was a smishing attempt and something about which to warn my clients.

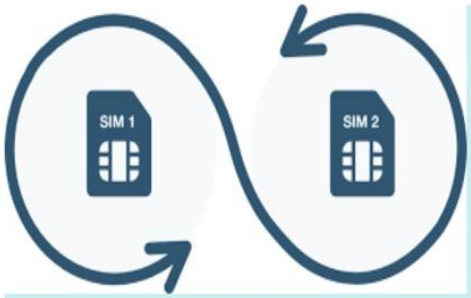
What are these "smishers" trying to do? Typically, the link included in the text redirects one to a fake website which has been made to look official but which is designed to harvest login credentials or other PII (Personally Identifiable Information). The website may even try to get the user to download malware for future tracking or even keylogging.

The problem is huge. Proofpoint reported in 2020 that 84% of organizations had been subjected to smishing, and "the FBI has reported that losses from phishing and other scams topped more than $3.5 billion to individual and business victims in 2019."

The vast majority of people in the U.S. are not even aware of this problem. It has been estimated that "only 23% of users over 55 had been able to correctly define smishing" and "millennials didn't do much better, with only 34% of people 23-38 years old" able to define what the term means.

Text-based scams were estimated to cost Americans over $10 billion in 2021 alone.

So, this problem is costly, widespread, and unknown to many Americans. It's clear that much education needs to be done, by technology companies such as phone makers and phone carriers, but also by myself and other consultants with clients who trust us to keep them informed and safe.



2FA via SMS Authentication Has Got to Go

In my previous post "Smishing on the Rise," I explored the increasing incidence and danger of SMS-based phishing attempts. This got me thinking further about mobile phone related vulnerabilities.

For many years, companies have required two-factor authentication (2FA) via SMS message as an additional security layer in the login process for their web applications. It's simple: one types in login credentials and a code (usually six digits) is sent to one's phone. This code, along with the login credentials, grants access to one's account. Even if a user's login credentials have been compromised, an unauthorized person can't log in without physical access to that phone.

Except now they can.

There are multiple reasons why 2FA via SMS authentication is no longer considered a secure MFA (multi-factor authentication) method. Forrester says that "SMS 2FA only stops 76 % of attacks" and is "susceptible to man-in-the-middle attacks, social engineering, and SIM swapping."

SMS messages are in plain text, not encrypted (unlike Apple's iMessages or WhatsApp messages), so they can be intercepted and read if a user's phone has been compromised with malware which can watch for security codes.

SIM swapping, in which a hacker gets a phone carrier to issue a new SIM for a target user's phone is a more sophisticated tactic that does not require any interaction with a phone user. The hacker just calls a phone carrier pretending to be a user who has lost or damaged their SIM card. They use PII (personally identifiable information) gathered via social engineering, phishing, or purchased from criminal data brokers to to convince the phone company to port the victim's phone number to a new SIM card possessed by the hacker. Or they just bribe the phone carrier employee to give them the information they need. Once the hacker has ported a valid user's mobile number to a new phone, they can intercept calls and texts, including 2FA codes.

Even more sophisticated cybercriminals use RDP (remote desktop protocol) tools to gain access to a phone carrier's system to get the information they need for SIM swapping. They trick employees at a phone carrier to install or activate RDP software and then dig into that employee's computer to gain tools for porting a legit phone user's phone number to a new SIM controlled by the hacker.

So, what is one to do?

There are now more secure methods of 2FA, including hardware authentication via a dedicated physical device such as fobs like YubiKey which generate a new code at regular, brief intervals. The same function is now possible via software using apps like Authy, Google Authenticator, or Microsoft Authenticator which change codes every 30 seconds. Those can be mobile apps on one's phone or browser based for one's desktop computer. For corporate security, IP-based controls can be placed on user accounts restricting access using whitelists of approved IP addresses. Combining methods like IP-based controls with a 2FA app adds even more security.

The increasing prevalence of remote work, BYOD (bring your own device) policies, and the sheer amount of data and systems more easily accessible from mobile devices means these devices pose a dangerously large (and increasing) cybersecurity attack surface. While the convenience of 2FA via SMS authentication is high, those responsible for cybersecurity within an organization or providing consulting advice to companies and individuals have a responsibility to move users to more sophisticated (and, hopefully, layered) MFA approaches. The "keys to the kingdom" are getting shinier and more powerful by the day, and they must be better secured.

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
Azure free domain
```

2. What is your domain name?

```
rjgsecurityresume.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.40.202.29
```

2. What is the location (city, state, country) of your IP address?

```
Des Moines, Iowa, US
```

3. Run a DNS lookup on your website. What does the NS record show?

```
rjg@RJG-iMac-2015:~$ nslookup rjgsecurityresume.azurewebsites.net
Server:             1.1.1.1
Address:      1.1.1.1#53

Non-authoritative answer:
rjgsecurityresume.azurewebsites.net      canonical name = waws-prod-dm1-
235.sip.azurewebsites.windows.net.
waws-prod-dm1-235.sip.azurewebsites.windows.net canonical name = waws-prod-dm1-235-
4298.centralus.cloudapp.azure.com.
Name:  waws-prod-dm1-235-4298.centralus.cloudapp.azure.com
Address: 20.40.202.29
```

Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

```
PHP 7.4 which works on the back end is an open source scripting language
well suited for web development
```

2. Inside the `/var/www/html` directory, there was another directory called assets. Explain what was inside that directory.

```
Two directories with resources (stylesheet language and images) used to
build the website in a client's browser:
   css
   images
The css directory contains an external stylesheet file with a .css
extension. This is the most common and useful method of bringing CSS to a
```

document. It is basically a template for how elements should look on an HTML formatted page.

The images directory contains images to be used by index.html (the HTML for my web app) such as the LinkedIn logo, “Robert Smith’s” photo, and two stock images for Blog Posts 1 and 2.

3. Consider your response to the above question. Does this work with the front end or back end?

These assets are being served to the front end (so the browser can build the page on a user’s screen).

Cloud Questions

1. What is a cloud tenant?

An SaaS provider’s customer using cloud computing architecture that allows them to share computer resources in a public/private cloud but whose data is isolated from and invisible to other tenants.

In a private cloud, tenants might be different individuals in a single company. In a public cloud, different organizations may safely share their server space.

2. Why would an access policy be important on a key vault?

According to the principle of least privilege, only users who need access should be given access so as to reduce the threat surface to bad actors. An access policy following that principle would limit which users, groups, or applications could make use of the secrets, certificates, and keys in a key vault. Additionally, users and groups should be given the least amount of access (privilege) needed to perform their tasks.

3. Within the key vault, what are the differences between keys, secrets, and certificates?

Key Vault allows one to not need to store security information in applications which eliminates the need to make this information part of the code, increasing security. Key Vault holds three categories of information:

Keys involve cryptographic material imported or generated when requested of the key vault; in Azure Key Vault, they are either an RSA key or an Elliptic Curve (EC) key. Keys encrypt information without giving a user the private

```
key. They are represented as JSON Web Key [JWK] objects.

Secrets are encrypted sequences of octets (with a maximum size of 25k bytes
each) like connection strings, authentication keys, storage account keys, or
the passwords for PFX; basically, anything that is sensitive that is not an
asymmetric key or certificate.

Certificates are digital certificates that authenticate a website's identity
and enable an encrypted connection. They have two parts: managed X.509 v3
certificates and their associated private keys.
```

Cryptography Questions

1. What are the advantages of a self-signed certificate?

```
They are free and suitable for internal network websites and
development/testing environments. Both encryption and decryption uses same
ciphers used by paid SSL certificates.
```

2. What are the disadvantages of a self-signed certificate?

```
They are risky, because they have no validation from a third-party authority
(usually a Trusted SSL Certificate Company) and won't be trusted by browsers
(and users will not see a "lock" symbol next to the URL).

Attackers can generate self-signed certificates for use in man-in-the-middle
(MITM) attacks.
```

3. What is a wildcard certificate?

```
A single certificate with a wildcard character (*) in the domain name field
which allows the certificate to secure multiple sub domain names (hosts)
pertaining to the same base domain more efficiently (which could save
costs).
```

4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

```
To ensure the safety of the users, Microsoft completely disabled SSL 3.0 in
Azure Websites by default to protect customers from the vulnerability
commonly known as POODLE that could allow for unauthorized information
disclosure. TLS, however, is modern and secure.
```

5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

    a. Is your browser returning an error for your SSL certificate?

```
No, because I am using Azure App Services which provides a trusted
certificate for my domain.
```

    b. What is the validity of your certificate (date range)?

```
2022-03-14 11:39:55 AM PDT to 2023-03-09 10:39:55 AM PDT
```

    c. Do you have an intermediate certificate? If so, what is it?

```
Yes: Microsoft Azure TLS Issuing CA 01
```

    d. Do you have a root certificate? If so, what is it?

```
Yes: DigiCert Global Root G2
```

    e. Does your browser have the root certificate in its root store?

```
DigiCert Global Root G2 is visible in the information Safari provides on the
certificate, but in macOS, the root store is in the Keychain Access
application.
```

    f. List one other root CA in your browser's root store.

```
DigiCert Assured ID Root CA
```

Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

```
Similarities:
   • Reside in front of the web app
   • Work on OSI Application Layer (7)
   • Primary solution is a load balancer
   • Can incorporate a WAF (web application firewall) to protect against
     web vulnerabilities
   • Have additional features such as URL path-based routing and SSL/TLS
```

termination
Differences:
- The Web Application Gateway is more **regional**, to protect a web app in a single region in one's cloud
- The Azure Front Door is more **global** and is better suited when one has a variety of regions in a cloud environment
- The Azure Front Door is simpler to implement

2. A feature of the Web Application Gateway and Front Door is "SSL Offloading." What is SSL offloading? What are its benefits?

SSL Offloading uses a load balancer between the browser and the server to handle the encryption and decryption tasks using the server's existing SSL certificate. There are two types of SSL Offloading: SSL Termination and SSL Bridging.

In SSL Termination, the load balancer decrypts data from the browser then passes that unencrypted data to the server. The server sends back a response in plaintext to the load balancer which encrypts this data using the session key and sends it to the client which decrypts the data using the same session key. The benefit of this process is improved server speed. A main risk is that the unencrypted traffic between the load balancer and the server is vulnerable to data theft, session hijacking, and MitM attacks.

In SSL Bridging, a load balancer between the client and the server is also used to decrypt the data, but before passing it on to the server, it does a deep-packet inspection for all the HTTPS traffic and blocks anything suspicious (like viruses, spyware, and other forms of malware). Then it re-encrypts the data and forwards it to the server. The main advantages are that data security is maintained because the data remains encrypted during transmission and servers can be protected from common web app attacks like DDoS attacks, SQL injections, and cross-site request forgeries.

3. What OSI layer does a WAF work on?

Application Layer (7)

4. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

A WAF managed rule to prevent directory traversal (aka file path traversal) stops attackers from reaching the root directory in order to gain access to restricted directories and files which would allow them to do things like modify programs or libraries, download password files, execute commands on the web server, or expose web application source code.

5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

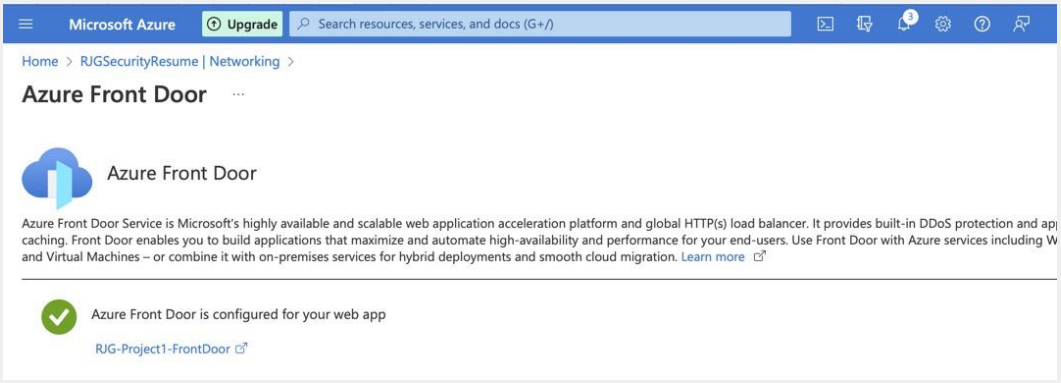
No. In the DefaultRuleSet_1.0 that is enabled for Azure Front Door, there are two managed rules that block Path Traversal Attacks (aka directory traversal attacks).

6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

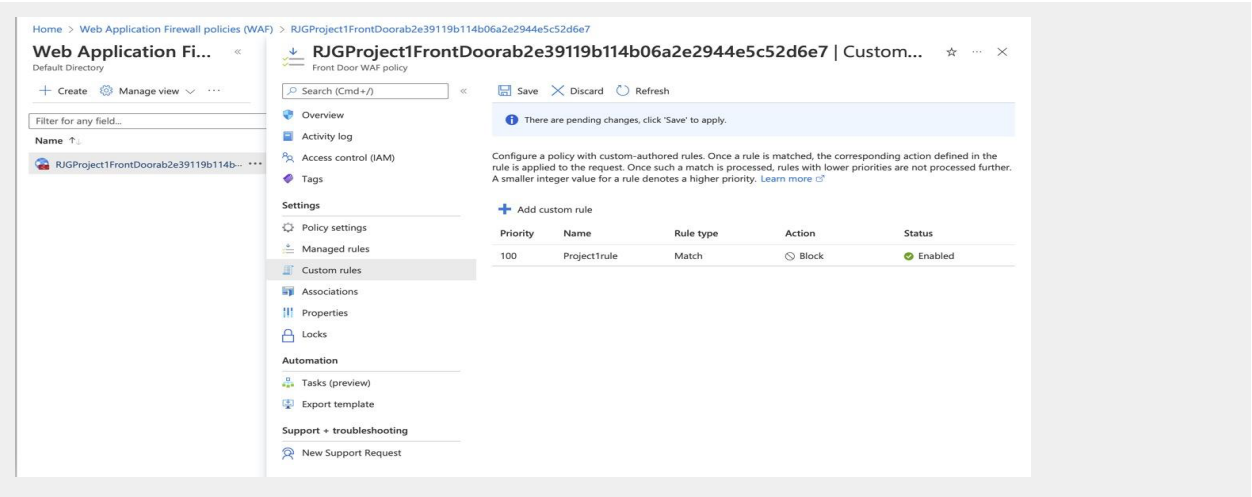
In general, yes, but not always. WAF rules using geo matching use lists of **known** IP addresses for regions. It's possible that a Canadian resident could have an IP address that is not a known address for Canada which would escape the WAF rule blacklist. Also, those in Canada using a VPN to route their traffic through another country's range of IP addresses could possibly get access to the website.

7. Include screenshots below to demonstrate that your web app has the following:

    a. Azure Front Door enabled



    b. A WAF custom rule



Note: There were no security center recommendations by Microsoft Defender for my web application