

# Rubber Duckies FTW

Astro Pryor and Grant Stautzenberger

# Who are we?

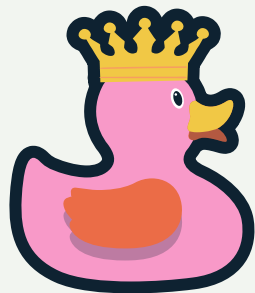
**We are Rubber Duckies FTW.**

**We are your one stop shop for buy and creating personalized rubber ducks for everything from your desk to your bath.**



# How it works

- Our website creates a place for customers to come and get personalized rubber ducks to own. As programmers many of us keep a rubber duck on our desk to read off our code to help us find where we need to tweak our creations.
- Having a place to buy and create a customized rubber feathered desk companion allows you to have a little bit of your own personality sitting on your desk to liven up your day.
- Our website acts as a medium to allow you to do just that. We have prebuilt ducks for sale. However we also have created a place where you can design your own duck.



.....

.....

# How does she look?

.....

.....



# Ain't she pretty?

We created a User friendly interface on our client side that is used for browsing our selection of rubber duck themed merchandise, personalising the merch and purchasing said merch.

## Ducks

We have a wide variety of already-made ducks. From cowboys to shark-themed, we have everything you could need to fit your rubber duck desires. We also offer custom ducks, which can be found on the custom ducks page or press the button below.

[Custom Duck!](#)

Below are the different already made ducks that we offer!

In addition to our amazing rubber duck collection, we also offer multiple different designs of towels, pajamas and blankets. To see those Please press the button below!

[More Products!](#)



Custom Duck

\$10.00

[Add to cart](#)



Soldier Duck

\$5.00

[Add to cart](#)



Jurassic Park Duck

\$6.00

[Add to cart](#)



[Log In](#) [Create account](#) [Ducks](#) [Pants](#) [Blankets and Towels](#) [Cart](#) [Log Out](#)

# ***RUBBERDUCKIESFTW***

Your one-stop shop for your personalized duck friend.

We offer products ranging from small rubber ducks to large rubber ducks. We offer Rubber duck themed sheets, towels and even clothes.



## Pants, Blankets and Towels

This is our amazing collection of towels, blankets and pajama bottoms.



**Blanket #3**

\$20.00

Add to cart



**Blanket #2**

\$20.00

Add to cart



**Blanket #1**

\$20.00

Add to cart



**Pajama #4**

\$20.00

Add to cart



**Pajama #3**

\$15.00

Add to cart



**Pajama #2**

\$20.00

Add to cart



**Pajama #1**

\$30.00

Add to cart



**Towel #3**

\$30.00

Add to cart




**Towel #2**

\$15.00

Add to cart



## Cart

PRODUCT	TOTAL
<div> Blanket #2 \$20.00</div> <div><div>- 1 +</div><div><a href="#">Remove item</a></div></div>	\$20.00

### CART TOTALS

Add a coupon	▼
Subtotal	\$20.00

**Total** **\$20.00 USD**

WOO PAY

G Pay VISA \*\*\*\* 2962

OR

Proceed to Checkout

[Refund Policy](#)

Crafted with that [WordPress](#) heat 🔥





Username or Email Address

unt.astro.pryor@gmail.com

Password

.....



Prove your humanity

7 + 5 = 13

☐ Remember Me



Your login confirmation code for Rubber Duckies FTW

Inbox x

Register

**wp2fa** wp2fa@rubberduckiesftw.wpcomstaging.com via b.atomicsites.net to me ▼

Enter **509477** to log in.

Thank you.

Email sent by [WP 2FA plugin](#).



One Time Password (i.e. 2FA)

(check your OTP app to get this password)

Log In

7 + 5 = 13

Lost your password?

to Rubber Duckies FTW

# Inside and out!



phpMyAdmin - Server: 527.8.8.1 - Database: 154833608

Structure SQL Search Query Export Import Operations Routines Events Triggers Designer

Filters

Containing the word

Table	Action	Rows	Type	Collation	Size	Overhead
wp_actionscheduler_actions	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	120	InnoDB	latin1_swedish_ci	288.0 K	-
wp_actionscheduler_claims	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	32.0 K	-
wp_actionscheduler_groups	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	9	InnoDB	latin1_swedish_ci	32.0 K	-
wp_actionscheduler_logs	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	336	InnoDB	latin1_swedish_ci	332.0 K	-
wp_comments	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	12	InnoDB	latin1_swedish_ci	48.0 K	-
wp_defender_email_log	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	2	InnoDB	latin1_swedish_ci	112.0 K	-
wp_defender_email_log	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	96.0 K	-
wp_defender_email_log	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	3	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_lockout	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	97	InnoDB	latin1_swedish_ci	88.0 K	-
wp_defender_lockout_log	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	164	InnoDB	latin1_swedish_ci	128.0 K	-
wp_defender_scan	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	1	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_scan_item	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	48.0 K	-
wp_defender_unlockout	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	88.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	9	InnoDB	latin1_swedish_ci	64.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	26	InnoDB	latin1_swedish_ci	64.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	1	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	28	InnoDB	latin1_swedish_ci	88.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	88.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	10	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	603	InnoDB	latin1_swedish_ci	1.2 M	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	28	InnoDB	latin1_swedish_ci	64.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	4	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	103	InnoDB	latin1_swedish_ci	352.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	256	InnoDB	latin1_swedish_ci	576.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	1	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	2	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	16.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	9	InnoDB	latin1_swedish_ci	48.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	27	InnoDB	latin1_swedish_ci	48.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	72	InnoDB	latin1_swedish_ci	32.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	27	InnoDB	latin1_swedish_ci	48.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	273	InnoDB	latin1_swedish_ci	256.0 K	-
wp_defender_views	[Browse] [Structure] [Search] [Insert] [Empty] [Drop]	0	InnoDB	latin1_swedish_ci	64.0 K	-

Utilizing the features provided through Wordpress out back end server handles authentication, secure payment gateways and product management. These features include Wordpress' hosting environment with PHP and MySQL backend.

# Plus She's Smart



We used WP2FA, Defender, WooCommerce and some editing plugins.

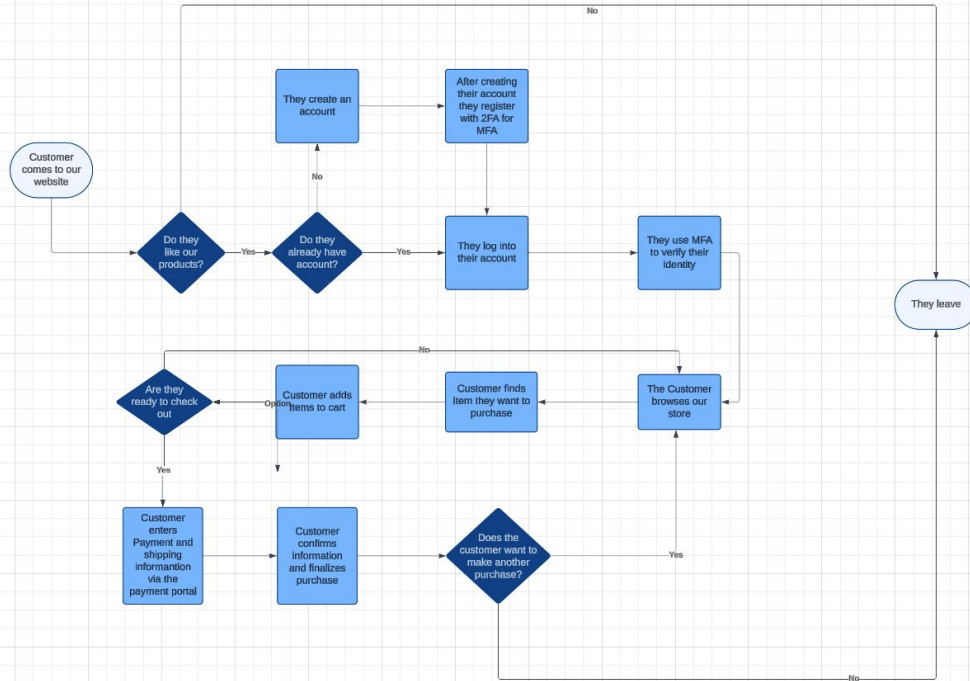
The data is stored in Wordpress databases systems using encrypted credentials and the products and stock management data is managed using WooCommerce.



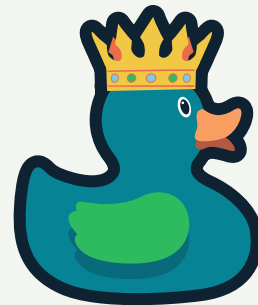
<input type="checkbox"/>	<b>Defender</b> <a href="#">Dashboard</a>   <a href="#">Docs</a>   <a href="#">Upgrade For 80% Off!</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Forminator</b> <a href="#">Dashboard</a>   <a href="#">Docs</a>   <a href="#">Upgrade For 80% Off!</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Jetpack</b> <a href="#">My Jetpack</a>   <a href="#">Settings</a>
	Jetpack is automatically managed for you.
<input type="checkbox"/>	<b>Jetpack Protect</b> <a href="#">My Jetpack</a>   <a href="#">Dashboard</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Login Logout Menu</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Login-Logout</b> <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>LoginPress</b> <a href="#">Settings</a>   <a href="#">Customize</a>   <a href="#">Opt Out</a>   <a href="#">Deactivate</a>   <a href="#">Upgrade Pro</a>
<input type="checkbox"/>	<b>My wpdb</b> <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Page Optimize</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
	This plugin was installed by WordPress.com and provides f
<input type="checkbox"/>	<b>Participants Database</b> <a href="#">Deactivate</a>   <a href="#">Settings</a>

<input type="checkbox"/>	<b>SQL Buddy</b> <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Stripe Tax - Sales tax automation for WooCommerce</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>Two Factor Authentication</b> <a href="#">User settings</a>   <a href="#">Plugin settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>WooCommerce</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>WooCommerce Custom Add To Cart Button</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>WooPayments</b> <a href="#">Settings</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>WP 2FA - Two-factor authentication for WordPress</b> <a href="#">Configure 2FA Settings</a>   <a href="#">Upgrade to Premium</a>   <a href="#">Deactivate</a>
<input type="checkbox"/>	<b>WP Migrate Lite</b> <a href="#">Migrate</a>   <a href="#">Settings</a>   <a href="#">Deactivate</a>   <a href="#">Upgrade</a>
<input type="checkbox"/>	<b>WPForms Lite</b> <a href="#">Get WPForms Pro</a>   <a href="#">Settings</a>   <a href="#">Docs</a>   <a href="#">Deactivate</a>

# Data Flow



# Results and Analysis



We have implemented a secure login and logout system that involves multi factor authentication.

We have installed a secure payment gateway to ensure the user's information won't get stolen.



The website is completely functioning.

For the vulnerability assessment we used Qualys, HostedScan, Security Headers and Nessus and there were minimal security problems. All of them were low or medium severity risks.



# Results and Analysis



Overall there were only 4 big vulnerabilities

- Missing security headers
    - Content security policy, anti CSRF tokens, CORD misconfiguration
  - Insecure cookies
    - Missing HttpOnly, secure and SameSite attributes
  - Network vulnerabilities
  - Open TCP ports (80 and 443)
  - SSL/TLS configuration issues
    - HSTS preload not enabled
- 
- 



# Results and Analysis

To remedy these vulnerabilities, we would need to make these changes

- Implement a CSP header to restrict content sources
  - Add anti-CSRF tokens to submission forms for secure submissions
  - Update the CORS policy to allow only trusted domains
  - Add HttpOnly, Secure and SameSite attributes to all cookies
  - Disable ICMP timestamp replies or block it via firewall
  - Submit the domain for HSTS preloading for better and enhanced HTTPS enforcement
- 
- 







# Results and Analysis

We faced a lot of different challenges during this project. These include

- Setting up multi factor authentication
- Verifying authentication
- Restarting from scratch because our first website couldn't implement all the features that we wanted
- Not knowing the proper plugins to add to the website to get the features we needed

We overcame these challenges by

- Creating a new website weeks before the due date
  - Spent a good amount of time researching and testing different 2 factor authentication tools
  - Implementing the different plugins that we found and testing them
- 
- 

192.0.78.20



Vulnerabilities

Total: 9

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	85805	HTTP/2 Cleartext Detection
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	-	106375	nginx HTTP Server Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown

## Total Risks

0

0

3

8

0

27%

73%

### Passive Web Application Vulnerabilities

#### Severity

#### First Detected

#### Last Detected

Cross-Domain Misconfiguration

Medium

7 days ago

7 days ago

Absence of Anti-CSRF Tokens

Medium

7 days ago

7 days ago

Content Security Policy (CSP) Header Not Set

Medium

7 days ago

7 days ago

Cookie No HttpOnly Flag

Low

7 days ago

7 days ago

Cookie Without Secure Flag

Low

7 days ago

7 days ago

Cross-Domain JavaScript Source File Inclusion

Low

7 days ago

7 days ago

X-Content-Type-Options Header Missing

Low

7 days ago

7 days ago

Cookie without SameSite Attribute

Low

7 days ago

7 days ago

### Network Vulnerabilities

#### Severity

#### First Detected

#### Last Detected

ICMP Timestamp Reply Information Disclosure  
cvss score: 2.1

Low

7 days ago

7 days ago

### Open TCP Ports

#### Severity

#### First Detected

#### Last Detected

Open TCP Port: 80

Low

7 days ago

7 days ago

Open TCP Port: 443

Low

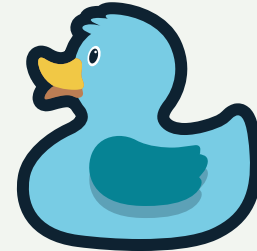
7 days ago

7 days ago

# Conclusion

In the end, we created a secure and user friendly ecommerce platform using wordpress. We implemented several safety features without coding them thanks to Wordpresses plugins.

Overall, we gained proficiency in using wordpress and how websites function on the front and backend. Selecting the correct plugin and doing research on the ones that we did add was essential and enhanced our skills for website vulnerability testing and optimizing Wordpress for the best performance.





# Video of Website

