Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Fix Recommendations

- Config your server to use the "X-XSS-Protection" header with value '1' (enabled)
- Correctly set the "autocomplete" attribute to "off"
- Do not allow sensitive information to leak.
- Enforce the use of HTTPS when sending sensitive information
- Implement the HTTP Strict-Transport-Security policy with a long "max-age"
- Remove e-mail addresses from the website
- Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Advisories

- Cross-Site Request Forgery
- Autocomplete HTML Attribute Not Disabled for Password Field
- Check for SRI (Subresource Integrity) support
- Direct Access to Administration Pages
- Encryption Not Enforced
- Missing "Content-Security-Policy" header
- Missing or insecure "X-XSS-Protection" header
- Missing or insecure HTTP Strict-Transport-Security Header
- Unnecessary Http Response Headers found in the Application
- Unsafe third-party link (target="_blank")
- Application Error
- Email Address Pattern Found

Application Data

- Cookies
- JavaScripts
- Parameters
- Comments
- Visited URLs
- Failed Requests
- Filtered URLs

Introduction

This report contains the results of a web application security scan performed by HCL AppScan Standard.

Medium severity issues:	1
Low severity issues:	43
Informational severity issues:	6
Total security issues included in the report:	50
Total security issues discovered in the scan:	50

General Information

Scan file name:	heroku
Scan started:	10/27/2021 8:28:36 AM
Test policy:	Application-Only
Test optimization level:	Normal

Host	xtreme-fitness.herokuapp.com
Port	443
Operating system:	Unknown
Web server:	Unknown
Application server:	Any

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Enabled
In-session pattern:	`>Logout<`

Tracked or session ID cookies:	`csrftoken`
	`m`
	`__stripe_mid`
	`__stripe_sid`
	`sessionid`

Tracked or session ID parameters:	`csrfmiddlewaretoken`
	`pb`
	`callback`
	`callback`

Login sequence:

```
https://xtreme-fitness.herokuapp.com/
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://js.stripe.com/v3/m-outer-
f7902241893e7a497417843cb15dc858.html
https://m.stripe.network/inner.html
https://m.stripe.com/6
https://xtreme-fitness.herokuapp.com/accounts/login/
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://m.stripe.com/6
https://m.stripe.com/6
https://xtreme-fitness.herokuapp.com/accounts/login/
https://xtreme-fitness.herokuapp.com/
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://js.stripe.com/v3/m-outer-
f7902241893e7a497417843cb15dc858.html
https://m.stripe.com/6
https://m.stripe.com/6
https://www.google.com/maps/embed?
pb=!1m18!1m12!1m3!1d2461.947587459914!2d-
8.474601348764978!3d51.89842058975903!2m3!1f0!2f0!3f0!3m2!1i1024!2i7
68!4f13.1!3m3!1m2!1s0x484490104a24174d:0xb8772718995a199f!2sSt
Patrick's St, Centre,
Cork!5e0!3m2!1sen!2sie!4v1632403818716!5m2!1sen!2sie
https://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewp
ortInfo?1m6=&1m2=&1d51.88800343557756=&2d-
8.503126122798246=&2m2=&1d51.908526396478116=&2d-
8.44221927109337=&2u16=&4sen=&5e0=&6sm@578000000=&7b0=&8e0=&11e289=&
12e2=&callback=_xdc_._lj4gto&client=google-maps-embed&token=106352
https://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewp
ortInfo?1m6=&1m2=&1d51.885773724014214=&2d-
8.492258223400762=&2m2=&1d51.91072964447354=&2d-
8.452811768481183=&2u12=&4sen=&5e2=&7b0=&8e0=&11e289=&12e2=&callback
=_xdc_._lpttjz&client=google-maps-embed&token=86400
https://maps.googleapis.com/maps/api/js/AuthenticationService.Authen
ticate?1shttps://www.google.com/maps/embed=&2sgoogle-maps-
embed=&callback=_xdc_._c3oema&client=google-maps-embed&token=17743
https://xtreme-fitness.herokuapp.com/about/
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://m.stripe.com/6
https://m.stripe.com/6
https://xtreme-fitness.herokuapp.com/products/?category=back_attack
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://m.stripe.com/6
https://m.stripe.com/6
https://xtreme-fitness.herokuapp.com/products/?category=apparel
https://unpkg.com/sweetalert/dist/sweetalert.min.js
https://m.stripe.com/6
https://m.stripe.com/6
```

Summary

Issue Types 12

TOC

	Issue Type	Number of Issues
M	Cross-Site Request Forgery	1
L	Autocomplete HTML Attribute Not Disabled for Password Field	1
L	Check for SRI (Subresource Integrity) support	17
L	Direct Access to Administration Pages	1
L	Encryption Not Enforced	1
L	Missing "Content-Security-Policy" header	1
L	Missing or insecure "X-XSS-Protection" header	1
L	Missing or insecure HTTP Strict-Transport-Security Header	1
L	Unnecessary Http Response Headers found in the Application	1
L	Unsafe third-party link (target="_blank")	19
I	Application Error	5
I	Email Address Pattern Found	1

Vulnerable URLs 19

TOC

	URL	Number of Issues
M	https://xtreme-fitness.herokuapp.com/products/	5
L	https://xtreme-fitness.herokuapp.com/accounts/login/	3
L	https://xtreme-fitness.herokuapp.com/	9
L	https://xtreme-fitness.herokuapp.com/about/	2
L	https://xtreme-fitness.herokuapp.com/bag/	2
L	https://xtreme-fitness.herokuapp.com/blog/	2
L	https://xtreme-fitness.herokuapp.com/blog/post-2/	2
L	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	2
L	https://xtreme-fitness.herokuapp.com/contact/	2
L	https://xtreme-fitness.herokuapp.com/products/1/	2
L	https://xtreme-fitness.herokuapp.com/products/2/	2
L	https://xtreme-fitness.herokuapp.com/products/4/	2
L	https://xtreme-fitness.herokuapp.com/products/8/	2

L	https://xtreme-fitness.herokuapp.com/products/add/	2
L	https://xtreme-fitness.herokuapp.com/products/edit/3/	2
L	https://xtreme-fitness.herokuapp.com/profile/	2
L	https://xtreme-fitness.herokuapp.com/subscribe/	2
L	https://xtreme-fitness.herokuapp.com/bag/add/1/	3
L	https://xtreme-fitness.herokuapp.com/bag/adjust/6/	2

Fix Recommendations 12

TOC

	Remediation Task	Number of Issues
M	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form	1
L	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"	19
L	Add to each third-party script/link element support to SRI(Subresource Integrity).	17
L	Apply proper authorization to administration scripts	1
L	Config your server to use the "Content-Security-Policy" header with secure policies	1
L	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)	1
L	Correctly set the "autocomplete" attribute to "off"	1
L	Do not allow sensitive information to leak.	1
L	Enforce the use of HTTPS when sending sensitive information	1
L	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	1
L	Remove e-mail addresses from the website	1
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	5

Security Risks 8

TOC

	Risk	Number of Issues
M	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	1
L	It may be possible to bypass the web application's authentication mechanism	1
L	In case the third-party server is compromised, the content/behavior of the site will change	17
L	It might be possible to escalate user privileges and gain administrative permissions over the web application	1
L	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	1
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	5
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	22
I	It is possible to gather sensitive debugging information	5

Causes 8

TOC

	Cause	Number of Issues
M	Insufficient authentication method was used by the application	1
L	Insecure web application programming or configuration	6
L	SRI (Subresource Integrity) not supported	17
L	The web server or application server are configured in an insecure way	1
L	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted	1
L	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object	19
I	Proper bounds checking were not performed on incoming parameter values	5
I	No validation was done in order to make sure that user input matches the data type expected	5

WASC Threat Classification

TOC

Threat	Number of Issues
Abuse of Functionality	19
Cross-site Request Forgery	1
Information Leakage	12
Predictable Resource Location	1
Remote File Inclusion	17

Issues Sorted by Issue Type

M Cross-Site Request Forgery 1

TOC

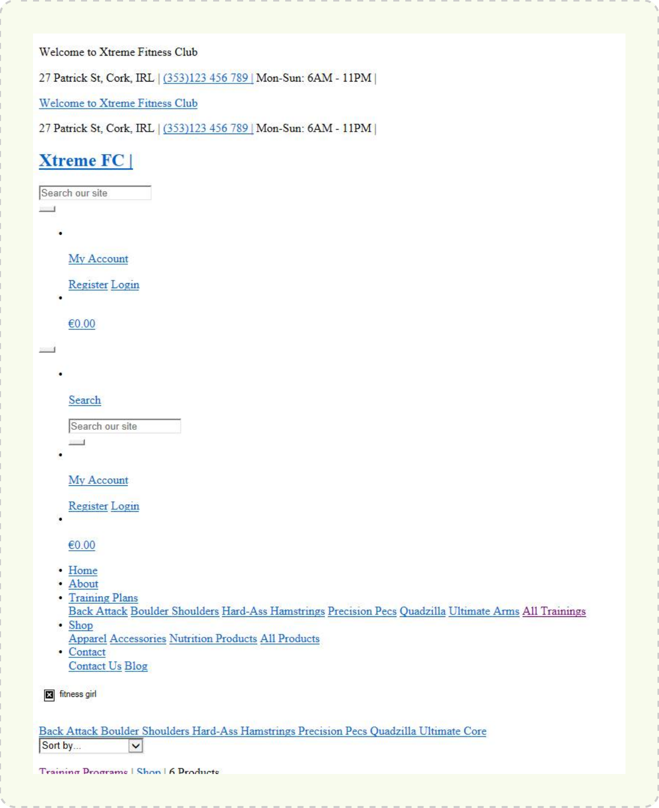
Issue 1 of 1

TOC

Cross-Site Request Forgery	
Severity:	Medium
CVSS Score:	6.4
URL:	https://xtreme-fitness.herokuapp.com/products/
Entity:	(Page)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Original Response **Test Response**



Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Xtreme FC |

Search our site

-

  My Account

  Register Login
-

  €0.00

-

  Search

  Search our site
-

  My Account

  Register Login
-

  €0.00

- Home
- About
- Training Plans
  Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Arms All Trainings
- Shop
  Apparel Accessories Nutrition Products All Products
- Contact
  Contact Us Blog

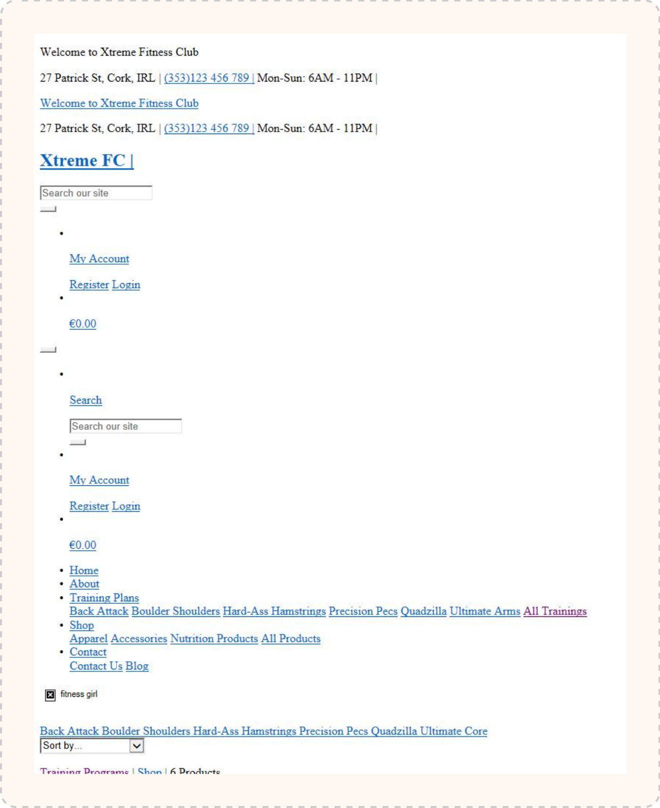
☒ fitness girl

Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Core

Sort by...

Training Programs | Shop | 6 Products

≈



Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Xtreme FC |

Search our site

My Account

Register Login

€0.00

Search

Search our site

My Account

Register Login

€0.00

- Home
- About
- Training Plans
  Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Arms All Trainings
- Shop
  Apparel Accessories Nutrition Products All Products
- Contact
  Contact Us Blog

☒ fitness girl

Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Core

Sort by...

Training Programs | Shop | 6 Products

L Autocomplete HTML Attribute Not Disabled for Password Field 1 TOC

Issue 1 of 1 TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/accounts/login/
Entity:	(Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Raw Test Response:

```
...

<div id="div_id_login" class="form-group"> <label for="id_login" class=" requiredField">
          Login<span class="asteriskField">*</span> </label> <div class=""> <input type="text" name="login"
placeholder="Username or e-mail" autofocus="autofocus" class="textinput textInput form-control" required id="id_login">
</div> </div> <div id="div_id_password" class="form-group"> <label for="id_password" class=" requiredField">
          Password<span class="asteriskField">*</span> </label> <div class=""> <input type="password" name="password"
placeholder="Password" class="textinput textInput form-control" required id="id_password"> </div> </div> <div class="form-
group"> <div id="div_id_remember" class="form-check"> <input type="checkbox" name="remember" class="checkboxinput form-
check-input" id="id_remember"> <label for="id_remember" class="form-check-label">
          Remember Me
          </label> </div> </div>
...
```

L Check for SRI (Subresource Integrity) support 17 TOC

Issue 1 of 17 TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/8/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 2 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/accounts/login/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 3 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/subscribe/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 4 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/2/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 5 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/about/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 6 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/contact/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...

...


      <!--EmailJs-->
      <script src="https://xtreme-fitness.s3.amazonaws.com/static/js/sendEmail.js"></script>
...
```

Issue 7 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...

...


      <!--EmailJs-->
      <script src="https://xtreme-fitness.s3.amazonaws.com/static/js/sendEmail.js"></script>
...
```

Issue 8 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 9 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/1/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 10 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/edit/3/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 11 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/profile/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...

      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">

    <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/profiles/css/profile.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...

...



      <!--Back to top btn-->
      <script type="text/javascript">
          $('.btt-link').click(function(e) {
          window.scrollTo(0,0)
          })
      </script>

    <script type="text/javascript" src="https://xtreme-fitness.s3.amazonaws.com/static/profiles/js/countryfield.js">
</script>
...
```

Issue 12 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/post-2/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 13 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 14 of 17

TOC

### Check for SRI (Subresource Integrity) support	
Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 15 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/4/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 16 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/add/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

Issue 17 of 17

TOC

Check for SRI (Subresource Integrity) support

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/bag/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	SRI (Subresource Integrity) not supported
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...


      <link rel="stylesheet"
          href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css">
      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css"/>
      <link rel="stylesheet" href="https://xtreme-fitness.s3.amazonaws.com/static/css/base.css">
      <!--Favicon-->
      <link rel="apple-touch-icon" sizes="180x180" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-
touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
32x32.png">
      <link rel="icon" type="image/png" sizes="16x16" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/favicon-
16x16.png">
      <!-- <link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest"> -->
...

...


      <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">



      <!--Bootstarp-->
      <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js"></script>
      <!--Stripe-->
      <script src="https://js.stripe.com/v3/"></script>
      <!--Anime js-->
      <script src="https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js"></script>
      <!--Email JS-->
      <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js"></script>
      <script>
          (function() {
          emailjs.init("user_kubWAs5UzOaovudWdYgFm");
          })();
      </script>
      <!--SweetAlert-->
      <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>


...
```

L Direct Access to Administration Pages 1 TOC

Issue 1 of 1

Direct Access to Administration Pages

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	(Page)
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	The web server or application server are configured in an insecure way
Fix:	Apply proper authorization to administration scripts

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; W
OW64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/89.0.4389.114 Safari/537.36
Referer: https://xtreme-fitness.herokuapp.
com/accounts/login/
Cookie: sessionid=ot6avhrclasg7qjbp662mn0s
fx94zgxw; csrftoken=4MpDyRCC59z5zSSxKODnCa
8rrVmzEbB94OGWK27Ng1chuMCIyValex41YzESu8CZ
Host: xtreme-fitness.herokuapp.com
Accept: text/html,application/xhtml+xml,ap
plication/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
...
GET /admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; W
OW64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/89.0.4389.114 Safari/537.36
Referer: https://xtreme-fitness.herokuapp.
com/accounts/login/
Cookie: sessionid=ot6avhrclasg7qjbp662mn0s
fx94zgxw; csrftoken=4MpDyRCC59z5zSSxKODnCa
8rrVmzEbB94OGWK27Ng1chuMCIyValex41YzESu8CZ
Host: xtreme-fitness.herokuapp.com
Accept: text/html,application/xhtml+xml,ap
plication/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 11624
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-cache, no-sto
re, must-revalidate, private
Referrer-Policy: same-origin

...

...



          <a href="/">View site</a> /






          <a href="/admin/password_change/
">Change password</a> /

          <a href="/admin/logout/">Log out
</a>

        </div>



    </div>
    <!-- END Header -->
...
```

L Encryption Not Enforced 1

TOC

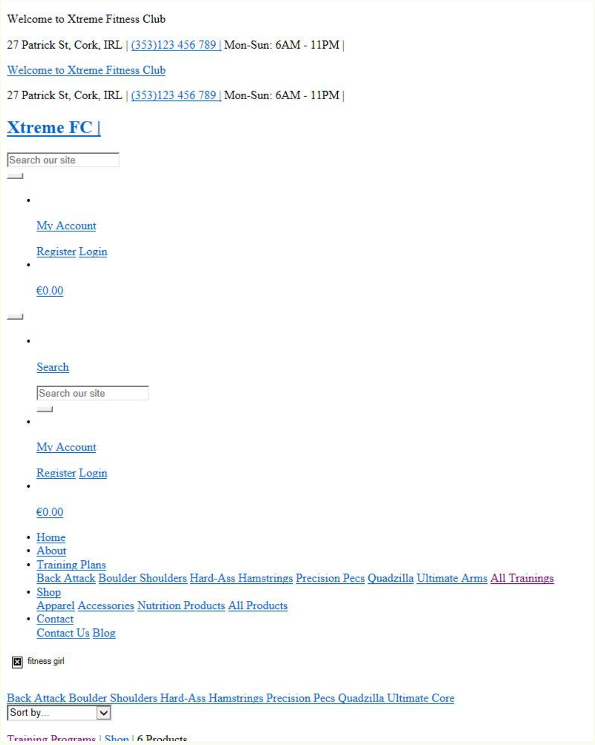
Issue 1 of 1

TOC

Encryption Not Enforced	
Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	xtreme-fitness.herokuapp.com (Page)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Original Response



Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Xtreme FC |

Search our site

-

  My Account

  Register Login
-

  €0.00

-

  Search

  Search our site
-

  My Account

  Register Login
-

  €0.00

- Home
- About
- Training Plans
  Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Arms All Trainings
- Shop
  Apparel Accessories Nutrition Products All Products
- Contact
  Contact Us Blog

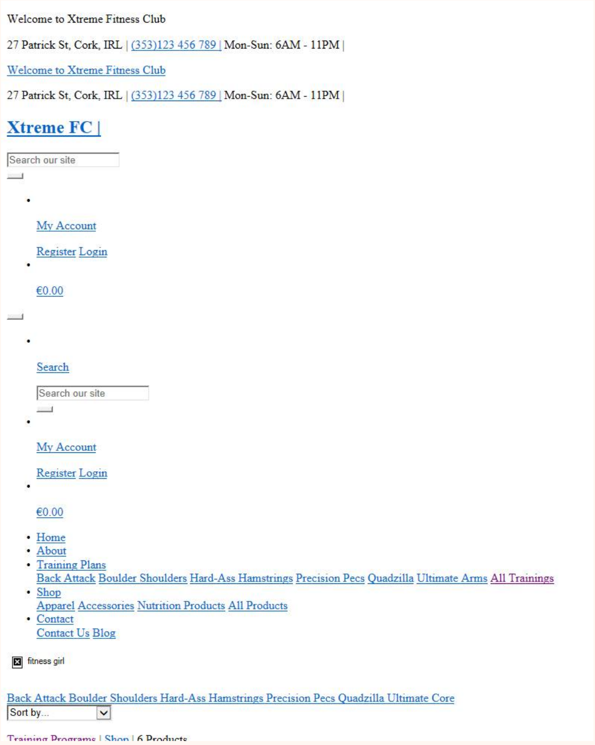
☒ fitness girl

Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Core
Sort by...

Training Programs | Shop | 6 Products

≈

Test Response



Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Welcome to Xtreme Fitness Club

27 Patrick St, Cork, IRL | (353)123 456 789 | Mon-Sun: 6AM - 11PM |

Xtreme FC |

Search our site

-

  My Account

  Register Login
-

  €0.00

-

  Search

  Search our site
-

  My Account

  Register Login
-

  €0.00

- Home
- About
- Training Plans
  Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Arms All Trainings
- Shop
  Apparel Accessories Nutrition Products All Products
- Contact
  Contact Us Blog

☒ fitness girl

Back Attack Boulder Shoulders Hard-Ass Hamstrings Precision Pecs Quadzilla Ultimate Core
Sort by...

Training Programs | Shop | 6 Products

L Missing "Content-Security-Policy" header 1

TOC

Issue 1 of 1

TOC

Missing "Content-Security-Policy" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	xtreme-fitness.herokuapp.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```
HTTP/1.1 200 OK
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 22607
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: csrftoken=FIJI8VJ3MPCW7BalodHbWE4ObMEe23po3PJptmrpr3JvpmVv21yIGKHhKR20A7Uk; expires=Wed, 26 Oct 2022 15:15:48
GMT; Max-Age=31449600; Path=/; SameSite=Lax
Date: Wed, 27 Oct 2021 15:15:48 GMT
Referrer-Policy: same-origin
Content-Type: text/html; charset=utf-8

...
```

L Missing or insecure "X-XSS-Protection" header 1

TOC

Issue 1 of 1

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	xtreme-fitness.herokuapp.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```
...

Host: xtreme-fitness.herokuapp.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document


HTTP/1.1 200 OK
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Content-Length: 22607
Vary: Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: csrftoken=4MpDyRCC59z5zSSxKODnCa8rrVmzEbB94OGWK27Ng1chuMCIyValex41YzESu8CZ; expires=Wed, 26 Oct 2022 15:35:55
GMT; Max-Age=31449600; Path=/; SameSite=Lax
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:35:55 GMT
Content-Type: text/html; charset=utf-8


...
```

L Missing or insecure HTTP Strict-Transport-Security Header 1

TOC

Issue 1 of 1

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	xtreme-fitness.herokuapp.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Content-Length: 22607
Vary: Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: csrftoken=4MpDyRCC59z5zSSxKODnCa8rrVmzEbB94OGWK27Ng1chuMCIyValex41YzESu8CZ; expires=Wed, 26 Oct 2022 15:35:55
GMT; Max-Age=31449600; Path=/; SameSite=Lax
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:35:55 GMT
Content-Type: text/html; charset=utf-8

...
```

L Unnecessary Http Response Headers found in the Application 1

TOC

Issue 1 of 1

TOC

Unnecessary Http Response Headers found in the Application

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	products/ (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Raw Test Response:

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document


HTTP/1.1 200 OK
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 49349
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:44:38 GMT
Content-Type: text/html; charset=utf-8


...
```

L Unsafe third-party link (target="_blank") 19

TOC

Issue 1 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/bag/adjust/6/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
```

```
            <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
            <span class="sr-only">Instagram</span>
            </a>
            <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
            <span class="sr-only">YouTube</span>
            </a>
            <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
            ...

...
```

Issue 2 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/1/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

      <div>
          <img class="img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg" alt="fitness girl">
      </div>
      <div class="container-fluid mt-md-5 pt-4">
          <div class="row">
          <div class="col-12 col-md-6 col-lg-4 offset-lg-2">
          <h1 class="mb-0 text-center text-uppercase d-block d-md-none">Back Attack</h1>
          <div class="image-container my-5">

          <a href="https://xtreme-fitness.s3.amazonaws.com/media/1.jpg" target="_blank">
          <img class="card-img-top img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/media/1.jpg" alt="Back Attack">
          </a>

          </div>
          </div>
          <div class="col-12 col-md-6 col-lg-4">
          <div class="product-details-container mb-5 mt-md-5">
          <h1 class="mb-0 text-center text-uppercase d-none d-md-block">Back Attack</h1>
          <p class="mt-3">A big, strong back can take you far in your athletic endeavors. The back muscles help you to
twist your torso, pull your arms in and down from overhead, a
...

...
...            <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 3 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/accounts/login/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 4 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/edit/3/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...         <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 5 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/about/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <div class="team-social">
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter fa-2x" aria-
hidden="true"></i>
          ...

...

...
...          <div class="team-social">
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter fa-2x" aria-
hidden="true"></i>
          ...

...

...
...          <div class="team-social">
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube fa-2x" aria-
hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter fa-2x" aria-
hidden="true"></i>
          ...

...

...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          ...
```

Issue 6 of 19 TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>

          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>

          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 7 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 8 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/2/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```

...

      <div>
          <img class="img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg" alt="fitness girl">
      </div>
      <div class="container-fluid mt-md-5 pt-4">
          <div class="row">
          <div class="col-12 col-md-6 col-lg-4 offset-lg-2">
          <h1 class="mb-0 text-center text-uppercase d-block d-md-none">Boulder Shoulders</h1>
          <div class="image-container my-5">

          <a href="https://xtreme-fitness.s3.amazonaws.com/media/2.jpg" target="_blank">
          <img class="card-img-top img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/media/2.jpg" alt="Boulder
Shoulders">
          </a>

          </div>
          </div>
          <div class="col-12 col-md-6 col-lg-4">
          <div class="product-details-container mb-5 mt-md-5">
          <h1 class="mb-0 text-center text-uppercase d-none d-md-block">Boulder Shoulders</h1>
          <p class="mt-3">More than a fundamental component to a complete workout routine, the best shoulder exercises
bring you one step closer to that desirable V-shape. Indeed,
...

...
```

```
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 9 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/contact/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 10 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 11 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/bag/add/1/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

      <div>
          <img class="img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg" alt="fitness girl">
      </div>
      <div class="container-fluid mt-md-5 pt-4">
          <div class="row">
          <div class="col-12 col-md-6 col-lg-4 offset-lg-2">
          <h1 class="mb-0 text-center text-uppercase d-block d-md-none">Back Attack</h1>
          <div class="image-container my-5">

          <a href="https://xtreme-fitness.s3.amazonaws.com/media/1.jpg" target="_blank">
          <img class="card-img-top img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/media/1.jpg" alt="Back Attack">
          </a>

          </div>
          </div>
          <div class="col-12 col-md-6 col-lg-4">
          <div class="product-details-container mb-5 mt-md-5">
          <h1 class="mb-0 text-center text-uppercase d-none d-md-block">Back Attack</h1>
          <p class="mt-3">A big, strong back can take you far in your athletic endeavors. The back muscles help you to
twist your torso, pull your arms in and down from overhead, a
...

...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 12 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
```

```
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 13 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/profile/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 14 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/4/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

      <div>
          <img class="img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg" alt="fitness girl">
      </div>
      <div class="container-fluid mt-md-5 pt-4">
          <div class="row">
          <div class="col-12 col-md-6 col-lg-4 offset-lg-2">
          <h1 class="mb-0 text-center text-uppercase d-block d-md-none">Precision Pecs</h1>
          <div class="image-container my-5">

          <a href="https://xtreme-fitness.s3.amazonaws.com/media/4.jpg" target="_blank">
          <img class="card-img-top img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/media/4.jpg" alt="Precision
Pecs">
          </a>

          </div>
          </div>
          <div class="col-12 col-md-6 col-lg-4">
          <div class="product-details-container mb-5 mt-md-5">
          <h1 class="mb-0 text-center text-uppercase d-none d-md-block">Precision Pecs</h1>
          <p class="mt-3">For most guys, a chest workout involves alternating between three chest exercises: bench press
completed in the flat, incline and decline positions. But i
...

...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 15 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/8/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

      <div>
          <img class="img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg" alt="fitness girl">
      </div>
      <div class="container-fluid mt-md-5 pt-4">
          <div class="row">
          <div class="col-12 col-md-6 col-lg-4 offset-lg-2">
          <h1 class="mb-0 text-center text-uppercase d-block d-md-none">ADAPT SEAMLESS SPORTS BRA</h1>
          <div class="image-container my-5">

          <a href="https://xtreme-fitness.s3.amazonaws.com/media/8.jpeg" target="_blank">
          <img class="card-img-top img-fluid" src="https://xtreme-fitness.s3.amazonaws.com/media/8.jpeg" alt="ADAPT
SEAMLESS SPORTS BRA">
          </a>

          </div>
          </div>
          <div class="col-12 col-md-6 col-lg-4">
          <div class="product-details-container mb-5 mt-md-5">
          <h1 class="mb-0 text-center text-uppercase d-none d-md-block">ADAPT SEAMLESS SPORTS BRA</h1>
          <p class="mt-3">The Pursue Fitness women&#x27;s ADAPT seamless sports bra. Ready for your biggest workout or your
well deserved rest day.&lt;br /&gt; - Removable padding&
...

...
...          <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 16 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/blog/post-2/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...         <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 17 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/subscribe/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...           <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 18 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/products/add/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...           <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

Issue 19 of 19

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://xtreme-fitness.herokuapp.com/bag/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...
...           <span>Follow on Socials</span>
          <a href="http://www.facebook.com" target="_blank" rel="noopener"><i class="fab fa-facebook" aria-hidden="true">
</i>
          <span class="sr-only">Facebook</span>
          </a>
          <a href="http://www.instagram.com" target="_blank" rel="noopener"><i class="fab fa-instagram" aria-hidden="true">
</i>
          <span class="sr-only">Instagram</span>
          </a>
          <a href="http://www.youtube.com" target="_blank" rel="noopener"><i class="fab fa-youtube" aria-hidden="true"></i>
          <span class="sr-only">YouTube</span>
          </a>
          <a href="http://www.twitter.com" target="_blank" rel="noopener"><i class="fab fa-twitter" aria-hidden="true"></i>
          ...

...
```

I Application Error 5

TOC

Issue 1 of 5

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/bag/add/1/
Entity:	quantity (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...

Origin: https://xtreme-fitness.herokuapp.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document
Content-Type: application/x-www-form-urlencoded

csrfmiddlewaretoken=AIQJxqsdASfdF5C4odRBag4gvhTd4MpcAK72JBXoLKSpAZmfckozMD0Q2VbwUJq2&quantity=%00&redirect_url=%2Fproducts%
2F1%2F

HTTP/1.1 500 Internal Server Error
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 145
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:36:51 GMT

...
```

Issue 2 of 5

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/bag/add/1/
Entity:	redirect_url (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...

Origin: https://xtreme-fitness.herokuapp.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document
Content-Type: application/x-www-form-urlencoded

csrfmiddlewaretoken=AIQJxqsdASfdF5C4odRBag4gvhTd4MpcAK72JBXoLKSpAZmfckozMD0Q2VbwUJq2&quantity=1&redirect_url.=%2Fproducts%2
F1%2F

HTTP/1.1 500 Internal Server Error
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 145
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:36:51 GMT

...
```

Issue 3 of 5

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/products/
Entity:	category (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...

Host: xtreme-fitness.herokuapp.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document


HTTP/1.1 500 Internal Server Error
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 145
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:36:51 GMT

...
```

Issue 4 of 5

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/products/
Entity:	q (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...

Host: xtreme-fitness.herokuapp.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document
```

```
HTTP/1.1 500 Internal Server Error
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 145
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:36:51 GMT

...
```

Issue 5 of 5

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/bag/adjust/6/
Entity:	quantity (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...

Origin: https://xtreme-fitness.herokuapp.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document
Content-Type: application/x-www-form-urlencoded

csrfmiddlewaretoken=AIQJxqsdASfdF5C4odRBag4gvhTd4MpcAK72JBXoLKSpAZmfckozMD0Q2VbwUJq2&quantity=

HTTP/1.1 500 Internal Server Error
Via: 1.1 vegur
Connection: keep-alive
Server: gunicorn
Vary: Cookie
Content-Length: 145
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Date: Wed, 27 Oct 2021 15:36:51 GMT

...
```

I Email Address Pattern Found 1

TOC

Issue 1 of 1

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://xtreme-fitness.herokuapp.com/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...

          </li>
          <li>
          <span class="icon"><i class="fas fa-phone-alt"></i></span>
          <strong>Contact</strong>
          <a href="tel:+353123456789"> +(353)123 456 789</a>
          </li>
          <li>
          <span class="icon"><i class="fas fa-at"></i></span>
          <strong>Email</strong>
          <a href="mailto:xtremefitnessclub@gmail.com">Xtremefitnessclub@gmail.com</a>
          </li>
          </ul>
          </div>
          </div>
          </div>
          </div>
      </div>
</section>
<!--End Contact Map Section-->
...
```

Fix Recommendations

M Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form TOC

Issue Types that this task fixes

- Cross-Site Request Forgery

General

Set all session and authentication cookies to include the `SameSite` attribute, setting it to `Strict` or `Lax`. When setting this attribute to `Lax` ensure that no sensitive action can be performed via a `GET` request, as per the HTTP standard.
Use built-in CSRF protection provided by the platform or framework, and ensure to activate it appropriately whether in configuration or code.
If your platform does not provide a built-in anti-CSRF mechanism, consider integrating a well-vetted library to implement the protection, such as OWASP CSRFGuard.
Avoid building a custom anti-CSRF implementation, as this can be complicated to achieve correctly without allowing trivial bypass. If you absolutely must do so due to lack of standard library support, you should generate a secure, random and non-predictable token (e.g. GUID v4) on the server and embed it in each HTML form, while binding it to the user's session. Upon receiving the submitted form, verify that the included form token matches the token previously bound to the user. It is also feasible to embed the CSRF token in a designated cookie ('double-submitted cookie'), or even better use a custom request header - when the server receives these together with the submitted form token, it is simple to validate that they match (instead of storing in the user's session).
An alternative approach would be to require user reauthentication for specific actions, to ensure the user's active confirmation. Note that this would substantially impact user experience, so this should be used sparingly and only for especially sensitive actions.
Verify the source of the request by validating the `Origin` header if present, or at least the `Referer` header. Discard sensitive requests that originate from a different site.

L Add the attribute rel = "noopener noreferrer" to each link element with target="_blank" TOC

Issue Types that this task fixes

- Unsafe third-party link (target="_blank")

General

Add rel="noopener noreferrer" to every link tag with source not in your domain
More detailed fix recomendation can be found in the Advisory's References and Relevant Links

L Add to each third-party script/link element support to SRI(Subresource Integrity). TOC

Issue Types that this task fixes

- Check for SRI (Subresource Integrity) support

General

Add Subresource Integrity to every script/link with source not in your domain
W3C Subresource Integrity:
https://www.w3.org/TR/SRI/
SRI Hash Generator:
https://srihash.org
Sample Script Element Not Supporting SRI:

```
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
```

Sample Script Element Supporting SRI:

```
<script src="https://example.com/example-framework.js" integrity="sha384-
oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>
```

L Apply proper authorization to administration scripts TOC

Issue Types that this task fixes

- Direct Access to Administration Pages

General

Do not allow access to administration scripts without proper authorization, as it may allow an attacker to gain privileged rights.

L Config your server to use the "Content-Security-Policy" header with secure policies TOC

Issue Types that this task fixes

- Missing "Content-Security-Policy" header

General

Configure your server to send the "Content-Security-Policy" header.

It is recommended to configure Content-Security-Policy header with secure values for its directives as below:
For 'default-src', 'script-src' and 'object-src', secure values such as 'none', 'self', https://any.example.com and 'unsafe-inline' or 'unsafe-eval' with nonce or hash-algorithm were expected.
For 'frame-ancestors', secure values such as 'self', 'none' or https://any.example.com were expected.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

L Config your server to use the "X-XSS-Protection" header with value '1' (enabled) TOC

Issue Types that this task fixes

- Missing or insecure "X-XSS-Protection" header

General

Configure your server to send the "X-XSS-Protection" header with value "1" (i.e. Enabled) on all outgoing requests.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

L Correctly set the "autocomplete" attribute to "off" TOC

Issue Types that this task fixes

- Autocomplete HTML Attribute Not Disabled for Password Field

General

If the "autocomplete" attribute is missing in the "password" field of the "input" element, add it and set it to "off".
If the "autocomplete" attribute is set to "on", change it to "off".
For example:
Vulnerable site:
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" /><br /> Password: <input type="password" name="lastname" /> <input type="submit" value="Submit" /> <form>
Non-vulnerable site:
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" /><br /> Password: <input type="password" name="lastname" autocomplete="off"/> <input type="submit" value="Submit" /> <form>

L Do not allow sensitive information to leak. TOC

Issue Types that this task fixes

- Unnecessary Http Response Headers found in the Application

General

Configure your server to remove the default "Server" header from being sent to all outgoing requests.
IIS
Set IIS response headers
For nginx, see:
Set nginx response headers
For Weblogic, see:
Set Weblogic response headers
For Apache, see:
Set Apache response headers

L Enforce the use of HTTPS when sending sensitive information TOC

Issue Types that this task fixes

- Encryption Not Enforced

General

You should always transmit all data over a TLS/SSL connection only. This includes all external communications, including browsers, backend connections such as databases, third party APIs, and other services.
In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site.
Always enforce the use of an encrypted connection (e.g. TLS/SSL), and do not allow any access to sensitive information using unencrypted HTTP.
Use TLS 1.2 or TLS 1.3 and use strong cryptographic hashing algorithms and cipher suites.

L Implement the HTTP Strict-Transport-Security policy with a long "max-age" TOC

Issue Types that this task fixes

- Missing or insecure HTTP Strict-Transport-Security Header

General

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.
For more information please see
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

L Remove e-mail addresses from the website TOC

Issue Types that this task fixes

- Email Address Pattern Found

General

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

L Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions TOC

Issue Types that this task fixes

- Application Error

General

[1] Check incoming requests for the presence of all expected parameters and values. When a parameter is missing, issue a proper error message or use default values.
[2] The application should verify that its input consists of valid characters (after decoding). For example, an input value containing the null byte (encoded as %00), apostrophe, quotes, etc. should be rejected.
[3] Enforce values in their expected ranges and types. If your application expects a certain parameter to have a value from a certain set, then the application should ensure that the value it receives indeed belongs to the set. For example, if your application expects a value in the range 10..99, then it should make sure that the value is indeed numeric, and that its value is in 10..99.
[4] Verify that the data belongs to the set offered to the client.
[5] Do not output debugging error messages and exceptions in a production environment.
In order to disable debugging in ASP.NET, edit your web.config file to contain the following:

```
<compilation
debug="false"
/>
```

For more information, see "HOW TO: Disable Debugging for ASP.NET Applications" in:
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157
You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, testing for valid dates or values within a range), plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.
To make sure that all the required parameters exist in a request, use the "RequiredFieldValidator" validation control. This control ensures that

the user does not skip an entry in the web form.

To make sure user input contains only valid values, you can use one of the following validation controls:

[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Test for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Test for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field

[2] Field data type (all HTTP request parameters are Strings by default)

[3] Field length

[4] Field range

[5] Field options

[6] Field pattern

[7] Cookie values

[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field

Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }

A good practice is to convert all HTTP request parameters to their respective data types. For example, store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...

The primary Java data types that the application should handle:

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength) { String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength && validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if

```
(Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }
```

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >=
min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if
(Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) {
// numberOfChoices is valid, continue processing request ... } } }
```

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options,
Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch
(Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"); // Verify that the user selection
is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) {
// valid user selection, continue processing request ... }
```

[6] Field pattern

Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

```
^[a-zA-Z0-9]*$
```

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support.

Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import
org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String
value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); }
return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if
(Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import
java.util.regex.Pattern; import java.util.regexe.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String
expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }
```

[7] Cookie value

Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

```
// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies =
request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { //
validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }
```

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:

< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null)
{ return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<':
result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case '\'': result.append("'"); break; case '%':
result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&':
result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } ... // Filter the
HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response));
out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter
all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest
request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter();
ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw
= new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html");
response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends
HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public
CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){
return new PrintWriter(output); } } } }
```

[8-2] Secure the cookie

When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user", "sensitive"); cookie.setSecure(true); response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:

required: succeeds if the field contains any characters other than white space.

mask: succeeds if the value matches the regular expression given by the mask attribute.

range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).

maxLength: succeeds if the field is length is less than or equal to the max attribute.

minLength: succeeds if the field is length is greater than or equal to the min attribute.

byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.

date: succeeds if the value represents a valid date. A date pattern may be provided.

creditCard: succeeds if the value could be a valid credit card number.

e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
```

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:

validate_doublerange: registers a DoubleRangeValidator on a component

validate_length: registers a LengthValidator on a component

validate_longrange: registers a LongRangeValidator on a component

validate_required: registers a RequiredValidator on a component

validate_stringrange: registers a StringRangeValidator on a component

validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):

input_date: accepts a java.util.Date formatted with a java.text.Date instance

output_date: displays a java.util.Date formatted with a java.text.Date instance

input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance

output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance

input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat

input_text: accepts a text string of one line.

output_text: displays a text string of one line.

input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance

output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance

input_hidden: allows a page author to include a hidden variable in a page

input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed

input_textarea: accepts multiple lines of text

output_errors: displays error messages for an entire page or error messages associated with a specified client identifier

output_label: displays a nested component as a label for a specified input field

output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /><p> </h:form> </f:use_faces>
```

REFERENCES

Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html

Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors

Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // -
ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String
ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC =
"error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final
String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements
Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and
array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String
getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private
Object[] values = null; }
```

- Errors: encapsulates a Collection of errors

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is
the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the
Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors =
(ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); }
propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for
the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new
HashMap(); }
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName =
request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name",
new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-
zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check
validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if
the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new
Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for
specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE); } } // set the
errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...
```

[2] Reporting Errors

There are two ways to report web-tier application errors:

(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism

A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
// Example to forward to the userInput.jsp following user validation errors RequestDispatcher rd =
getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.

Example to return a HTTP error:

```
// Example to return a HTTP error code RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) {
// messages is a resource bundle with all message keys and values
response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism

JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

```
<%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors

The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:
(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles

Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
################################################# # ErrorMessages.properties
################################################# # required user name error message error.username.required=User name field is
required # invalid user name format error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one ...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting

The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters String pattern = "User name {0} already exists, please choose
another one"; String userName = request.getParameter("user_name"); Object[] args = new Object[1]; args[0] = userName; String message =
MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file) // Utility class to retrieve locale-specific error
messages public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale public String
getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key
in the specified locale public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns
a formatted error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Object[] args, Locale
locale) { // Get localized ErrorMessageResource ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages",
locale); // Get localized error message String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the
message using the specified placeholders args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default
environment locale private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale Locale userLocale =
request.getLocale(); // Check if there were any validation errors Errors errors = (Errors)request.getAttribute("errors"); if (errors != null &&
errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property ArrayList userNameErrors =
errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object Error error
= (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage
+ "\r\n"); } }
```

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping

Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-
type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-
code>500</exception-type> <location>/errors/internalError.html</error-page> </error-page> <error-page> ... </error-page> ...
```

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:

[1] Jakarta Commons Validator (integrated with Struts 1.1)

The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired"
msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask"
msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case
insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg
name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-
value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld"
prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right">
<html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username"
size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right">
<html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>
```

[2] JavaServer Faces Technology

JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-
login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean"
scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20"
modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display
errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit"
commandName="submit" /><p> </h:form> </f:use_faces>
```

REFERENCES

Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:

[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options

[6] Field pattern
[7] Cookie values
[8] HTTP Response
A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.
Example of how to validate required fields:
// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0){ $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +
PHP includes some automatic sanitization utility functions, such as htmlentities():
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:
<?php header('Content-Type: text/html; charset=UTF-8'); ?>

[8-2] Secure the cookie
When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.
You can use the following code example, for securing the cookie:
<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>
In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).
The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES
[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Advisories

Cross-Site Request Forgery

TOC

Test Type:

Application

Threat Classification:

Cross-site Request Forgery

Causes:

Insufficient authentication method was used by the application

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

CWE:

352

References:

OWASP CSRF Cheat Sheet
OWASP CSRFGuard

Technical Description:

This vulnerability arises because the application allows the user to perform some sensitive action without verifying that the request was sent intentionally.
An attacker can cause a victim's browser to emit an HTTP request to an arbitrary URL in the application. When this request is sent from an authenticated victim's browser, it will include the victim's session cookie or authentication header. The application will accept this as a valid request from an authenticated user.
When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, an attacker may be able to trick a client into making an unintentional request from a different site, which will be treated as an authentic request by the application. This can be done by submitting a form, loading an image, sending an XMLHttpRequest in JavaScript, and more.
For example, this IMG tag can be embedded in an attacker's webpage, and the victim's browser will submit a request to retrieve the image. This valid request will be processed by the application, and the browser will not display a broken image. `<img src="https://myapp.com/transfer?acct=VICTIM&amount=10000" width=0 height=0 border=0>`. As a result, money is transferred from the victim's account to the attacker, using the victim’s session.

An attacker can exploit this vulnerability to perform sensitive actions in another user's account, or using their privileges.
It may be possible to abuse a customer's session, which could be used to effectively impersonate a legitimate user. This would allow the attacker to alter user records and to perform transactions as that user.
If the user is currently logged-in to the victim site, the request will automatically use the user's credentials such as session cookies, IP address, and other browser authentication methods. Using this method, the attacker forges the victim's identity and submits actions on their behalf.
The severity of this vulnerability depends on the affected functionality in context of the application. For example, a CSRF attack on a search

page is less severe than a CSRF attack on a money-transfer or profile-update page.

Autocomplete HTML Attribute Not Disabled for Password Field

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

It may be possible to bypass the web application's authentication mechanism

Affected Products:

CWE:

522

Technical Description:

Insecure web application programming or configuration

It may be possible to bypass the web application's authentication mechanism
The "autocomplete" attribute has been standardized in the HTML5 standard. W3C's site states that the attribute has two states, "on" and "off", and that omitting it altogether is equivalent to setting it to "on".
This page is vulnerable since it does not set the "autocomplete" attribute to "off" for the "password" field in the "input" element.
This may enable an unauthorized user (with local access to an authorized client) to autofill the username and password fields, and thus log in to the site.

Check for SRI (Subresource Integrity) support

TOC

Test Type:

Application

Threat Classification:

Remote File Inclusion

Causes:

SRI (Subresource Integrity) not supported

Security Risks:

In case the third-party server is compromised, the content/behavior of the site will change

Affected Products:

CWE:

829

References:

Vendor site
Explanation

Technical Description:

There is no support to Subresource Integrity.

The user-agent can't verify scripts from third-party services. In case of compromise of the third-party service, the user is not protected.
script and link tags with src from another domain are not supporting integrity check.
This can be exploited if the service that have the script is compromise.
Sample Script Element Not Supporting SRI:
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
Sample Script Element Supporting SRI:
<script src="https://example.com/example-framework.js" integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7" crossorigin="anonymous"></script>

Direct Access to Administration Pages

TOC

Test Type:

Application

Threat Classification:

Predictable Resource Location

Causes:

The web server or application server are configured in an insecure way

Security Risks:

It might be possible to escalate user privileges and gain administrative permissions over the web application

CWE:

306

Technical Description:

The web server or application server are configured in an insecure way

It might be possible to escalate user privileges and gain administrative permissions over the web application
A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked).

An attacker may be able to access these pages by guessing their name, e.g. admin.php, admin.asp, admin.cgi, admin.html, etc.
Example request for a script named "admin.php":
http://[SERVER]/admin.php
Access to administration scripts should not be allowed without proper authorization, as it may allow an attacker to gain privileged rights.
Sample Exploit:
http://[SERVER]/admin.php
http://[SERVER]/admin.asp
http://[SERVER]/admin.aspx
http://[SERVER]/admin.html
http://[SERVER]/admin.cfm
http://[SERVER]/admin.cgi

Encryption Not Enforced

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Security Risks:

It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

CWE:

319

References:

OWASP - TLS Cipher String Cheat Sheet
OWASP - Transport Layer Protection Cheat Sheet

Technical Description:

The application does not use a secure channel, such as TLS/SSL, to exchange sensitive information.
An attacker with access to the network traffic can eavesdrop on packets over the connection. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels.

Any information sent to the server as clear text may be stolen over the network and used later for identity theft or user impersonation.
It may be possible to intercept sensitive data such as user login information (usernames and passwords), credit card numbers, social security numbers etc. that are sent unencrypted.
It may be possible to perform man in the middle (MitM) attacks, which would give an attacker full control of the communication, including changing content, stealing data, or impersonating the user to the server.

Missing "Content-Security-Policy" header

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

CWE:

1032

References:

List of some secure Headers
An Introduction to Content Security Policy
MDN web docs - Content-Security-Policy

Technical Description:

Insecure web application programming or configuration

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of CSP can cause the web application being vulnerable to XSS, clickjacking, etc.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:
Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.
For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Missing or insecure "X-XSS-Protection" header

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

CWE:

200

References:

List of useful HTTP headers
IE XSS Filter

Technical Description:

Insecure web application programming or configuration

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The "X-XSS-Protection" header with value '1' forces the Cross-Site Scripting filter into Enable mode, even if disabled by the user.
This filter is built into most recent web browsers (IE 8+, Chrome 4+), and is usually enabled by default. Although it is not designed as first and only defense against Cross-Site Scripting, it acts as an additional layer of protection.

Missing or insecure HTTP Strict-Transport-Security Header

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

CWE:

200

References:

OWASP "HTTP Strict Transport Security"
HSTS Spec

Technical Description:

Insecure web application programming or configuration

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.
It is important to set the 'max-age' to a high enough value to prevent falling back to an insecure connection prematurely.
The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Unnecessary Http Response Headers found in the Application

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

CWE:

200

References:

Fingerprinting
Preventing Information Leakage

Technical Description:

Insecure web application programming or configuration

It is possible to gather sensitive information about the web server type, version, OS and more.
AppScan detected a Http response header that is unnecessary.
For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.
The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.
The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.
These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Unsafe third-party link (target="_blank")

TOC

Test Type:

Application

Threat Classification:

Abuse of Functionality

Causes:

The page that is linked to with the target=_blank link gains partial access to the linking page window object via the window.opener object

Security Risks:

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

CWE:

0

References:

The most underestimated vulnerability ever - Explanation, example and fix recomendation

Technical Description:

The rel attribute in the link element is not set to "noopener noreferrer".

The linked page gains partial access to the opening page window object.

The target="_blank" attribute is added to link elements to make the link open in a new window.
link tags of this kind(i.e. with target="_blank" attribute) expose parts of the window object of the original page to the linked page via window.opener object.
This can be exploited for phishing attacks if the linked page is malicious.
Attention: if links can be added by users and propogate to pages visable by other users this threat should be treated as HIGH severity

Application Error

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

- Proper bounds checking were not performed on incoming parameter values
- No validation was done in order to make sure that user input matches the data type expected

Security Risks:

It is possible to gather sensitive debugging information

Affected Products:

CWE:

550

References:

An example for using apostrophe to hack a site can be found in "How I hacked PacketStorm (by Rain Forest Puppy), RFP's site"
"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
CERT Advisory (CA-1997-25): Sanitizing user-supplied data in CGI scripts

Technical Description:

Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

It is possible to gather sensitive debugging information
If an attacker probes the application by forging a request that contains parameters or parameter values other than the ones expected by the application (examples are listed below), the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request, which information may be exploited to locate application weaknesses.
For example, if the parameter field should be an apostrophe-quoted string (e.g. in an ASP script or SQL query), the injected apostrophe symbol will prematurely terminate the string stream, thus changing the normal flow/syntax of the script.
Another cause of vital information being revealed in error messages, is when the scripting engine, web server, or database are misconfigured.
Here are some different variants:
[1] Remove parameter
[2] Remove parameter value
[3] Set parameter value to null
[4] Set parameter value to a numeric overflow (+/- 99999999)
[5] Set parameter value to hazardous characters, such as ' " \' \") ;
[6] Append some string to a numeric parameter value
[7] Append "." (dot) or "[]" (angle brackets) to the parameter name

Email Address Pattern Found

TOC

Test Type:

Application

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

CWE:

359

References:

Definition of Spambot (Wikipedia)

Technical Description:

Insecure web application programming or configuration

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).
AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail
Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Application Data

Visited URLs 30

TOC

URL
https://xtreme-fitness.herokuapp.com/accounts/login/
https://xtreme-fitness.herokuapp.com/accounts/login/
https://xtreme-fitness.herokuapp.com/contact/
https://xtreme-fitness.herokuapp.com/products/?category=back_attack,boulder_shoulders,hard_ass_hamstrings,precision_pecs,quadzilla,ultimate_core
https://xtreme-fitness.herokuapp.com/products/?category=quadzilla
https://xtreme-fitness.herokuapp.com/
https://xtreme-fitness.herokuapp.com/
https://xtreme-fitness.herokuapp.com/products/1/
https://xtreme-fitness.herokuapp.com/bag/add/1/
https://xtreme-fitness.herokuapp.com/products/
https://xtreme-fitness.herokuapp.com/products/2/
https://xtreme-fitness.herokuapp.com/products/edit/3/
https://xtreme-fitness.herokuapp.com/products/4/
https://xtreme-fitness.herokuapp.com/products/8/
https://xtreme-fitness.herokuapp.com/subscribe/
https://xtreme-fitness.herokuapp.com/subscribe/
https://xtreme-fitness.herokuapp.com/about/
https://xtreme-fitness.herokuapp.com/blog/
https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/
https://xtreme-fitness.herokuapp.com/blog/post-2/
https://xtreme-fitness.herokuapp.com/products/add/
https://xtreme-fitness.herokuapp.com/profile/
https://xtreme-fitness.herokuapp.com/bag/
https://xtreme-fitness.herokuapp.com/bag/remove/5/
https://xtreme-fitness.herokuapp.com/bag/adjust/6/
https://xtreme-fitness.herokuapp.com/products/1/
https://xtreme-fitness.herokuapp.com/bag/
https://xtreme-fitness.herokuapp.com/accounts/login/
https://xtreme-fitness.herokuapp.com/products/?q=1234
https://xtreme-fitness.herokuapp.com/products/?q=

Parameters 18

TOC

Name	Value	URL	Type
body	testing	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	TextArea
csrfmiddlewaretoken	fkMFeE1292L8pwsjQCZP90VlSQpuCGoGxM4WbNhD68DrZW7CrVgHG3rzyIXpLfNz	https://xtreme-fitness.herokuapp.com/bag/adjust/6/	Hidden
csrfmiddlewaretoken	GslptlPjYUI7P64yWzGaAq4q5Dvq3f0v4zl6OMxFD8PG7RPIAnxHkwHTEITcBjvrZPNxbFJLSDNzjlTCxC5U8R7VqQX5bqIwhu7Losp08e8ginAsTjOo5OaHR9pIhm4a	https://xtreme-fitness.herokuapp.com/accounts/login/	Hidden
password	**CONFIDENTIAL 0**	https://xtreme-fitness.herokuapp.com/accounts/login/	Password
csrfmiddlewaretoken	nJ78ICOTq8NDxNcCHj5bqOmZZGJvDcMWFbppFL4uneFW7dRViCm3XRSdFyhqMLbP	https://xtreme-fitness.herokuapp.com/subscribe/	Hidden
email	test@test.com	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	Body
product_size		https://xtreme-fitness.herokuapp.com/bag/remove/5/	Body
q	1234	https://xtreme-fitness.herokuapp.com/products/?q=1234	Text
csrfmiddlewaretoken	S4bLbzijlGxK8DXohfmJtJ0gHn9YA6FCawt28IyUiMp3I3CHSyDB0MwunfHTJF4v	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	Hidden
quantity	1	https://xtreme-fitness.herokuapp.com/bag/adjust/6/	Body
redirect_url	/products/1/	https://xtreme-fitness.herokuapp.com/bag/add/1/	Hidden
name	test	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	Text
csrfmiddlewaretoken	ub8mUbJhieXkZZ78bz3uKGsLGOycOOKRMDqDRkZSfkPDzpMrMSkmhJYZmG67Xn9K	https://xtreme-fitness.herokuapp.com/bag/remove/5/	Hidden
category	back_attack,boulder_shoulders,hard_ass_hamstrings,precision_pecs,quadzilla,ultimate_core quadzilla	https://xtreme-fitness.herokuapp.com/products/?category=back_attack,boulder_shoulders,hard_ass_hamstrings,precision_pecs,quadzilla,ultimate_core	Simple Link
login	szilvia	https://xtreme-fitness.herokuapp.com/accounts/login/	Text
email	test@test.com	https://xtreme-fitness.herokuapp.com/subscribe/	Body
quantity	1	https://xtreme-fitness.herokuapp.com/bag/add/1/	Body
csrfmiddlewaretoken	THEIumuz5MBZDFHGMj3KwO8dRKULwxyub9WZrvKa2Stid5mZnCkC3RErxCsGF6Xn	https://xtreme-fitness.herokuapp.com/bag/add/1/	Hidden

Failed Requests 0

TOC

URL	Reason

Filtered URLs 189

TOC

URL	Reason
https://xtreme-fitness.s3.amazonaws.com/media/2.jpg	Untested Web Server
https://code.jquery.com/jquery-3.6.0.min.js	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/membership-card.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/author-1.jpeg	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/css/bootstrap.min.css	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/css/base.css	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/favicon/apple-touch-icon.png	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/about-2.jpg	Untested Web Server
http://www.facebook.com/	Untested Web Server
http://www.instagram.com/	Untested Web Server
http://www.youtube.com/	Untested Web Server
http://www.twitter.com/	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/contact-02.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/1.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/5.jpg	Untested Web Server
https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d2461.947587459914!2d-8.474601348764978!3d51.89842058975903!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x484490104a24174d%3A0xb8772718995a199f!2sSt Patrick's St%2C Centre%2C Cork!5e0!3m2!1sen!2sie!4v1632403818716!5m2!1sen!2sie	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/carousel-img01.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/carousel-img02.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/award.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/about-1.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/3.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/4.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/6.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/author-2.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/author-3.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/author-4.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/info.jpeg	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js	Untested Web Server
https://js.stripe.com/v3/	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js	Untested Web Server
https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js	Untested Web Server
https://unpkg.com/sweetalert/dist/sweetalert.min.js	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/js/sendEmail.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/	Likely Similar DOM
https://xtreme-fitness.s3.amazonaws.com/static/profiles/js/countryfield.js	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/profiles/css/profile.css	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/15.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/16.jpeg	Untested Web Server
https://xtreme-fitness.herokuapp.com/products/5/	Similar Body
https://xtreme-fitness.s3.amazonaws.com/media/27.jpeg	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/9.jpeg	Untested Web Server

https://xtreme-fitness.s3.amazonaws.com/media/10.jpeg	Untested Web Server
https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/	Similar DOM
https://xtreme-fitness.s3.amazonaws.com/static/about-lowerbody-2.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/28.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/43.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/38.jpeg	Untested Web Server
https://code.jquery.com/jquery-3.6.0.min.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/bag/remove/1/	Similar Body
https://xtreme-fitness.s3.amazonaws.com/media/39.jpeg	Untested Web Server
https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.6.0/js/bootstrap.min.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/bag/remove/2/	Similar Body
https://cdnjs.cloudflare.com/ajax/libs/animejs/3.2.1/anime.min.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/bag/remove/3/	Similar Body
https://cdn.jsdelivr.net/npm/emailjs-com@3/dist/email.min.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/bag/remove/4/	Similar Body
https://xtreme-fitness.s3.amazonaws.com/media/8.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/subscribe01.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/7.jpeg	Untested Web Server
https://images.unsplash.com/photo-1616803689943-5601631c7fec?ixid=MnwxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&ixlib=rb-1.2.1&auto=format&fit=crop&w=1770&q=80	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/about-4.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/about-gym-fitness.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/about-core.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/muscles.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/stopwatch.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/pizza.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/throphy.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/hearth.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/trainer.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/trainer-3.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/trainer.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/trainer-2.jpg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/training.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/healthy.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/nutrition.png	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/benefit-1.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/benefit-2.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/benefit-3.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/benefit-4.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/11.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/12.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/13.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/14.jpeg	Untested Web Server
https://images.unsplash.com/photo-1522898467493-49726bf28798?ixid=MnwxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&ixlib=rb-1.2.1&auto=format&fit=crop&w=1770&q=80	Untested Web Server
https://images.unsplash.com/photo-1571019614242-c5c5dee9f50b?ixid=MnwxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&ixlib=rb-1.2.1&auto=format&fit=crop&w=1770&q=80	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/17.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/18.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/19.jpeg	Untested Web Server

https://xtreme-fitness.s3.amazonaws.com/media/20.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/21.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/22.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/23.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/24.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/25.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/26.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/29.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/30.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/31.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/32.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/33.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/34.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/35.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/36.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/37.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/40.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/41.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/42.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/44.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/45.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/46.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/47.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/48.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/49.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/50.jpeg	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/media/51.jpeg	Untested Web Server
https://xtreme-fitness.herokuapp.com/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=back_attack	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=boulder_shoulders	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=hard_ass_hamstrings	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=precision_pecs	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=ultimate_core	Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/1/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/2/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/2/	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/3/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/3/	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/3/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/4/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/4/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/5/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/5/	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/6/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/6/	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/6/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/8/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/7/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/add/7/	Similar DOM

https://xtreme-fitness.herokuapp.com/products/edit/7/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/9/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/edit/9/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=apparel	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=accessories	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=nutrition-products	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=apparel,accessories,nutrition-products	Likely Similar DOM
https://xtreme-fitness.herokuapp.com/blog/post-1/	Similar DOM
https://unpkg.com/sweetalert/dist/sweetalert.min.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/bag/adjust/6/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/remove/6/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/remove/8/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/adjust/7/	Similar DOM
https://xtreme-fitness.herokuapp.com/bag/remove/7/	Similar DOM
https://unpkg.com/sweetalert@2.1.2/dist/sweetalert.min.js	Untested Web Server
https://xtreme-fitness.s3.amazonaws.com/static/js/sendEmail.js	Untested Web Server
https://js.stripe.com/v3/	Untested Web Server
https://js.stripe.com/v3/m-outer-f7902241893e7a497417843cb15dc858.html	Untested Web Server
https://js.stripe.com/v3/fingerprinted/js/m-outer-639174098ea8fe7fede6fa654790e8ec.js	Untested Web Server
https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d2461.947587459914!2d-8.474601348764978!3d51.89842058975903!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x484490104a24174d:0xb8772718995a199f!2sSt Patrick's St, Centre, Cork!5e0!3m2!1sen!2sie!4v1632403818716!5m2!1sen!2sie	Untested Web Server
https://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en&region=ie&callback=onApiLoad	Untested Web Server
https://csp.withgoogle.com/csp/geo-maps-api/1	Untested Web Server
https://m.stripe.network/inner.html	Untested Web Server
https://m.stripe.network/out-4.5.41.js	Untested Web Server
https://m.stripe.com/6	Untested Web Server
https://xtreme-fitness.herokuapp.com/	Similar Body
https://m.stripe.com/6	Untested Web Server
https://maps.gstatic.com/maps-api-v3/embed/js/46/10/init_embed.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/common.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/map.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/overlay.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/onion.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/util.js	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/search_impl.js	Untested Web Server
https://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewportInfo?1m6&1m2&1d51.885773724014214&2d-8.492258223400762&2m2&1d51.91072964447354&2d-8.452811768481183&2u12&4sen&5e2&7b0&8e0&11e289&12e1&13shttps://www.google.com/maps/embed&14b1&callback=_xdc_._9i4964&client=google-maps-embed&token=1164	Untested Web Server
https://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewportInfo?1m6&1m2&1d51.88800343557756&2d-8.513718618746921&2m2&1d51.908526396478116&2d-8.431626775144695&2u16&4sen&5e0&6sm@578000000&7b0&8e0&11e289&12e1&13shttps://www.google.com/maps/embed&14b1&callback=_xdc_._q6c5by&client=google-maps-embed&token=124935	Untested Web Server
https://maps.googleapis.com/maps/api/js/AuthenticationService.Authenticate?1shttps://www.google.com/maps/embed&2sgoogle-maps-embed&7m1&1e0&callback=_xdc_._lkdbea&client=google-maps-embed&token=78567	Untested Web Server
https://maps.googleapis.com/maps/api/js/QuotaService.RecordEvent?1shttps://www.google.com/maps/embed&2sgoogle-maps-embed&7s9oe4rq&10e1&callback=_xdc_._x3jrq&client=google-maps-embed&token=61780	Untested Web Server
https://www.google.com/maps/vt?pb=!1m4!1m3!1i16!2i31223!3i21676!1m4!1m3!1i16!2i31223!3i21677!1m4!1m3!1i16!2i31223!3i21678!1m4!1m3!1i16!2i31224!3i21676!1m4!1m3!1i16!2i31224!3i21677!1m4!1m3!1i16!2i31225!3i21676!1m4!1m3!1i16!2i31225!3i21677!1m4!1m3!1i16!2i31224!3i21678!1m4!1m3!1i16!2i31225!3i21678!1m4!1m3!1i	Untested Web Server

16!2i31226!3i21676!1m4!1m3!1i16!2i31226!3i21677!1m4!1m3!1i16!2i31227!3i21676!2m3!1e0!2sm!3i578304112!2m38!1e2!2sspotlight!5i1!8m34!1m2!12m1!20e1!2m7!1s0x484490104a24174d:0xb8772718995a199f!2sSt+Patrick's+St,+Centre,+Cork!4m2!3d51.8984173!4d-8.4724073!5e3!6b1!11e11!13m14!2sa!14b1!18m7!5b0!6b0!9b1!12b1!16b0!20b1!21b1!22m3!6e2!7e3!8e2!19u12!19u14!19u29!19u37!19u30!19u61!19u70!3m12!2sen!3sIE!5e289!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e3!12m1!5b1&client=google-maps-embed&token=53513	
https://www.google.com/maps/vt?pb=!1m4!1m3!1i16!2i31227!3i21677!1m4!1m3!1i16!2i31226!3i21678!1m4!1m3!1i16!2i31227!3i21678!1m4!1m3!1i16!2i31228!3i21676!1m4!1m3!1i16!2i31228!3i21677!1m4!1m3!1i16!2i31228!3i21678!2m3!1e0!2sm!3i578304112!2m38!1e2!2sspotlight!5i1!8m34!1m2!12m1!20e1!2m7!1s0x484490104a24174d:0xb8772718995a199f!2sSt+Patrick's+St,+Centre,+Cork!4m2!3d51.8984173!4d-8.4724073!5e3!6b1!11e11!13m14!2sa!14b1!18m7!5b0!6b0!9b1!12b1!16b0!20b1!21b1!22m3!6e2!7e3!8e2!19u12!19u14!19u29!19u37!19u30!19u61!19u70!3m12!2sen!3sIE!5e289!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e3!12m1!5b1&client=google-maps-embed&token=98699	Untested Web Server
https://maps.googleapis.com/maps-api-v3/api/js/46/10/controls.js	Untested Web Server
https://xtreme-fitness.herokuapp.com/products/	Similar Body
https://xtreme-fitness.herokuapp.com/	Similar DOM
https://xtreme-fitness.herokuapp.com/accounts/login/	Similar DOM
https://xtreme-fitness.herokuapp.com/about/	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=back_attack	Similar DOM
https://xtreme-fitness.herokuapp.com/products/?category=apparel	Likely Similar DOM

Comments 59

TOC

URL	Comment
https://xtreme-fitness.herokuapp.com/products/	<!DOCTYPE html>
https://xtreme-fitness.herokuapp.com/products/	Favicon
https://xtreme-fitness.herokuapp.com/products/	<link rel="manifest" href="https://xtreme-fitness.s3.amazonaws.com/static/favicon/site.webmanifest">
https://xtreme-fitness.herokuapp.com/products/	Bootstarp
https://xtreme-fitness.herokuapp.com/products/	Stripe
https://xtreme-fitness.herokuapp.com/products/	Anime js
https://xtreme-fitness.herokuapp.com/products/	Email JS
https://xtreme-fitness.herokuapp.com/products/	SweetAlert
https://xtreme-fitness.herokuapp.com/products/	footer-widgets
https://xtreme-fitness.herokuapp.com/products/	widget-column
https://xtreme-fitness.herokuapp.com/products/	footer-bottom
https://xtreme-fitness.herokuapp.com/products/	Bootstrap toast
https://xtreme-fitness.herokuapp.com/products/	navbar color change on scrolling
https://xtreme-fitness.herokuapp.com/products/	Back to top btn
https://xtreme-fitness.herokuapp.com/	Start Carousel
https://xtreme-fitness.herokuapp.com/	End Carousel
https://xtreme-fitness.herokuapp.com/	Start Service Block
https://xtreme-fitness.herokuapp.com/	Service Block 1
https://xtreme-fitness.herokuapp.com/	Service Block 2
https://xtreme-fitness.herokuapp.com/	Service Block 3
https://xtreme-fitness.herokuapp.com/	End Sevice Block
https://xtreme-fitness.herokuapp.com/	Start About Section
https://xtreme-fitness.herokuapp.com/	Content-Column
https://xtreme-fitness.herokuapp.com/	Section Title

https://xtreme-fitness.herokuapp.com/	Featured Block 1
https://xtreme-fitness.herokuapp.com/	Featured Block 2
https://xtreme-fitness.herokuapp.com/	Image-Column
https://xtreme-fitness.herokuapp.com/	End About Section
https://xtreme-fitness.herokuapp.com/	Start Membership Section
https://xtreme-fitness.herokuapp.com/	End Membership Section
https://xtreme-fitness.herokuapp.com/	Start Testimonial Section
https://xtreme-fitness.herokuapp.com/	Carousel Wrapper
https://xtreme-fitness.herokuapp.com/	Slides
https://xtreme-fitness.herokuapp.com/	Controls
https://xtreme-fitness.herokuapp.com/	End Testimonial Section
https://xtreme-fitness.herokuapp.com/	Start Contact Map Section
https://xtreme-fitness.herokuapp.com/	map box
https://xtreme-fitness.herokuapp.com/	Column 1
https://xtreme-fitness.herokuapp.com/	Column 2
https://xtreme-fitness.herokuapp.com/	End Contact Map Section
https://xtreme-fitness.herokuapp.com/	Start Contact-form Section
https://xtreme-fitness.herokuapp.com/	Title Column
https://xtreme-fitness.herokuapp.com/	Form Column
https://xtreme-fitness.herokuapp.com/	Form
https://xtreme-fitness.herokuapp.com/	End Contact-form Section
https://xtreme-fitness.herokuapp.com/	EmailJs
https://xtreme-fitness.herokuapp.com/contact/	Start Header Image Section
https://xtreme-fitness.herokuapp.com/contact/	End Header Image Section
https://xtreme-fitness.herokuapp.com/about/	Start Services Section
https://xtreme-fitness.herokuapp.com/about/	End Services Section
https://xtreme-fitness.herokuapp.com/about/	Start Trainning Section
https://xtreme-fitness.herokuapp.com/about/	End Trainning Section
https://xtreme-fitness.herokuapp.com/about/	Start Motivation Icons Section
https://xtreme-fitness.herokuapp.com/about/	End Motivation Icons Section
https://xtreme-fitness.herokuapp.com/about/	Start Trainers Section
https://xtreme-fitness.herokuapp.com/about/	End Trainers Section
https://xtreme-fitness.herokuapp.com/about/	Start Benefit Section
https://xtreme-fitness.herokuapp.com/about/	End Benefit Section
https://xtreme-fitness.herokuapp.com/about/	Start

JavaScripts 11

TOC

URL / Code

https://xtreme-fitness.herokuapp.com/products/

```
    (function() {
    emailjs.init("user_kubWAs5UzOaovudWdYgFm");
    })();
```

https://xtreme-fitness.herokuapp.com/products/

```
document.write(new Date().getFullYear());
```

https://xtreme-fitness.herokuapp.com/products/

```
          $('.toast').toast('show');
```

https://xtreme-fitness.herokuapp.com/products/

```
          $(window).scroll(function() {
          $('.bg-color').toggleClass('scrolled', $(this).scrollTop() > 50)
          });
```

https://xtreme-fitness.herokuapp.com/products/

```
          $('.btt-link').click(function(e) {
          window.scrollTo(0,0)
          })
```

https://xtreme-fitness.herokuapp.com/products/

```
          $('#sort-selector').change(function() {
          var selector = $(this);
          var currentUrl = new URL(window.location);

          var selectedVal = selector.val();
          if(selectedVal != "reset"){
          var sort = selectedVal.split("_")[0];
          var direction = selectedVal.split("_")[1];

          currentUrl.searchParams.set("sort", sort);
          currentUrl.searchParams.set("direction", direction);

          window.location.replace(currentUrl);
          } else {
          currentUrl.searchParams.delete("sort");
          currentUrl.searchParams.delete("direction");

          window.location.replace(currentUrl);
          }
          })
```

https://xtreme-fitness.herokuapp.com/

```
return sendMail(this);
```

https://xtreme-fitness.herokuapp.com/products/1/

```
// Disable +/- buttons outside 1-99 range
function handleEnableDisable(itemId) {
    var currentValue = parseInt($(`#id_qty_${itemId}`).val());
    var minusDisabled = currentValue < 2;
    var plusDisabled = currentValue > 98;
    $(`#decrement-qty_${itemId}`).prop('disabled', minusDisabled);
    $(`#increment-qty_${itemId}`).prop('disabled', plusDisabled);
}

// Ensure proper enabling/disabling of all inputs on page load
var allQtyInputs = $('.qty_input');
for(var i = 0; i < allQtyInputs.length; i++){
    var itemId = $(allQtyInputs[i]).data('item_id');
    handleEnableDisable(itemId);
}

// Check enable/disable every time the input is changed
$('.qty_input').change(function() {
    var itemId = $(this).data('item_id');
    handleEnableDisable(itemId);
});

// Increment quantity
$('.increment-qty').click(function(e) {
    e.preventDefault();
    var closestInput = $(this).closest('.input-group').find('.qty_input')[0];
    var currentValue = parseInt($(closestInput).val());
    $(closestInput).val(currentValue + 1);
    var itemId = $(this).data('item_id');
    handleEnableDisable(itemId);
});

// Decrement quantity
$('.decrement-qty').click(function(e) {
    e.preventDefault();
    var closestInput = $(this).closest('.input-group').find('.qty_input')[0];
    var currentValue = parseInt($(closestInput).val());
    $(closestInput).val(currentValue - 1);
    var itemId = $(this).data('item_id');
    handleEnableDisable(itemId);
});
```

https://xtreme-fitness.herokuapp.com/bag/

```
// Update quantity on click
$('.update-link').click(function(e) {
    var form = $(this).prev('.update-form');
    form.submit();
})

// Remove item and reload on click
$('.remove-item').click(function(e) {
    var csrfToken = "INovXP2x9Ub3vBwtYQOnWzGnLfsZkd3j0fGMUYi8603m51bMz95ftCcBr70UtMsc";
    var itemId = $(this).attr('id').split('remove_')[1];
    var size = $(this).data('product_size');
    var url = `/bag/remove/${itemId}/`;
    var data = {'csrfmiddlewaretoken': csrfToken, 'product_size': size};

    $.post(url, data)
     .done(function() {
      location.reload();
     });
})
```

https://xtreme-fitness.herokuapp.com/products/edit/3/

```
        $('#new-image').change(function() {
          var file = $('#new-image')[0].files[0];
          $('#filename').text(`Image will be set to: ${file.name}`);
        });
```

https://xtreme-fitness.herokuapp.com/bag/

```
    // Update quantity on click
    $('.update-link').click(function(e) {
        var form = $(this).prev('.update-form');
        form.submit();
    })

    // Remove item and reload on click
    $('.remove-item').click(function(e) {
        var csrfToken = "SyntDRHKqUElms1iKgxT4Z0M5wVBTrcza0FKA0Xln0wEWSGBlzOLB2w0Lotw20Bs";
        var itemId = $(this).attr('id').split('remove_')[1];
        var size = $(this).data('product_size');
        var url = `/bag/remove/${itemId}/`;
        var data = {'csrfmiddlewaretoken': csrfToken, 'product_size': size};

        $.post(url, data)
         .done(function() {
          location.reload();
         });
    })
```

Cookies 42

TOC

Name	First Set	Domain	Secure	HTTP Only	Same Site	JS Stack Trace
Value	Requested URL		Expires			
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/blog/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/4/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/add/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/about/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/bag/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91	https://xtreme-fitness.herokuapp.com/subscribe					

e-eb9601d8aa95735d41	/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/accounts/login/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/bag/remove/5/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/edit/3/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/blog/post-2/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/profile/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/2/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/bag/add/1/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/bag/adjust/6/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/1/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/?category=back_attack,boulder_shoulders,hard_ass_hamstrings,precision_pecs,quadzilla,ultimate_core					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/contact/					
__stripe_mid			False	False		
0ea5f847-12bb-45dd-a91e-eb9601d8aa95735d41	https://xtreme-fitness.herokuapp.com/products/8/					
__stripe_mid	https://xtreme-fitness.herokuapp.com/products/?q=1234	xtreme-fitness.herokuapp.com	True	False	Strict	at he (https://js.stripe.com/v3/:1:74600) at e.value (https://js.stripe.com/v3/:1:80345) at https://js.stripe.com/v3/:1:77268
048bbaca-77b4-4a02-84ca-efa4acda1fe2397296	https://xtreme-fitness.herokuapp.com/		10/27/2022 3:32:05 PM			
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/bag/add/1/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/profile/					
__stripe_sid			False	False		

d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/blog/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/2/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/bag/remove/5/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/blog/warm-up-post-3/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/blog/post-2/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/?category=back_attack,boulder_shoulders,hard_ass_hamstrings,precision_pecs,quadzilla,ultimate_core					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/edit/3/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/4/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/1/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/add/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/products/8/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/accounts/login/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/about/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/bag/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/subscribe/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/bag/adjust/6/					
__stripe_sid			False	False		
d6715eca-2dbc-4cb4-bc52-782e8fbc52db243281	https://xtreme-fitness.herokuapp.com/contact/					
__stripe_sid	https://xtreme-fitness.herokuapp.com/products/	xtreme-fit	True	False	Strict	at he (https://js.stripe.com/v

	?q=1234	ness.herokuapp.com				3/:1:74600) at e.value (https://js.stripe.com/v3/:1:80599) at https://js.stripe.com/v3/:1:77290
cdbd45d0-4deb-4556-bc95-2d4e710c5c5c7c5525	https://xtreme-fitness.herokuapp.com/		10/27/2021 4:02:05 PM			
csrftoken	https://xtreme-fitness.herokuapp.com/accounts/login/	xtreme-fitness.herokuapp.com	False	False	Lax	
epRG5HWomqCqX4ge63T2bK2QoxF4xELHvdYBJMLw0hoBodmw03PpAqarg93FO0sI	https://xtreme-fitness.herokuapp.com/accounts/login/		10/26/2022 3:31:38 PM			
sessionid	https://xtreme-fitness.herokuapp.com/accounts/login/	xtreme-fitness.herokuapp.com	False	True	Lax	
ji30vypqzanzvsvxu92qf97xm8fe8aok	https://xtreme-fitness.herokuapp.com/contact/					