Easy Challenges

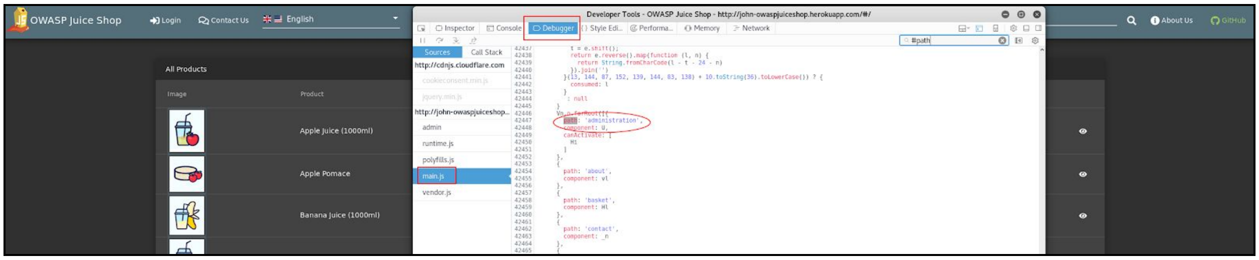
Admin Section - Access the administration section of the store

Prerequisite ⇒ Complete the ‘*Login as Admin*’ beforehand

1. Right-click on any of the page and select “Inspect Page”

2. In the Developer Tools, go to “Debugger” tab (“Sources”, in Chrome) and select the file “main.js”

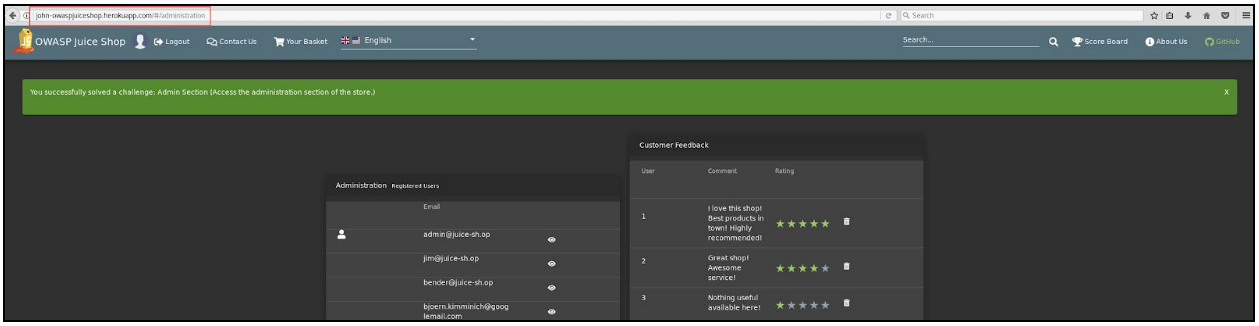
3. Search for the word “Administration” to figure out the path to the page



```
      t = e.shift();
      return e.reverse().map(function (l, n) {
        return String.fromCharCode(l - t - 24 - n)
      }).join('')
    }(13, 144, 87, 152, 139, 144, 83, 138) + 10.toString(36).toLowerCase()) ? {
      consumed: l
    }
     : null
  }
  Vn.o.forRoot([{
    path: 'administration',
    component: U,
    canActivate: [
      Hi
    ]
  },
  {
    path: 'about',
    component: vl
  },
  {
    path: 'basket',
    component: Hl
  },
  {
    path: 'contact',
    component: _n
  },
  {
```

4. If you are not logged in as admin, the web application will display a 403 Error briefly and then redirect to the main page.

5. Login as admin and access the page.



You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration Registered Users

Email
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@googlemail.com

Customer Feedback

User	Comment	Rating
1	I love this shop! Best products in town! Highly recommended!	★★★★★
2	Great shop! Awesome service!	★★★★☆
3	Nothing useful available here!	★☆☆☆☆

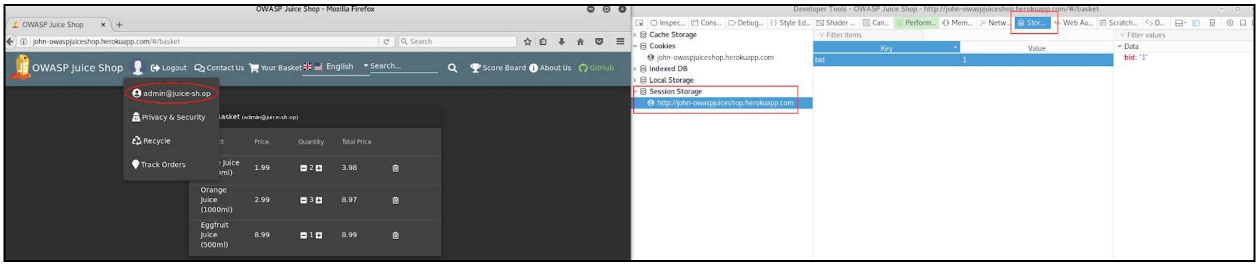
Written by Jonathan Harijanto

Basket Access Tier 1 - View another user's shopping basket.

1. On the home page, login as any user (in this case, logged-in as admin)

2. Go to the “Your Basket” page

3. Open the Developer Tools (right-click > Inspect Page) and click on the “Storage” tab. Then, select the “Session Storage” option and memorize the value of the “bid” variable (basket ID)



OWASP Juice Shop - Mozilla Firefox

john-owaspjuiceshop.herokuapp.com/#/basket

admin@juice-sh.op

Basket (admin@juice-sh.op)

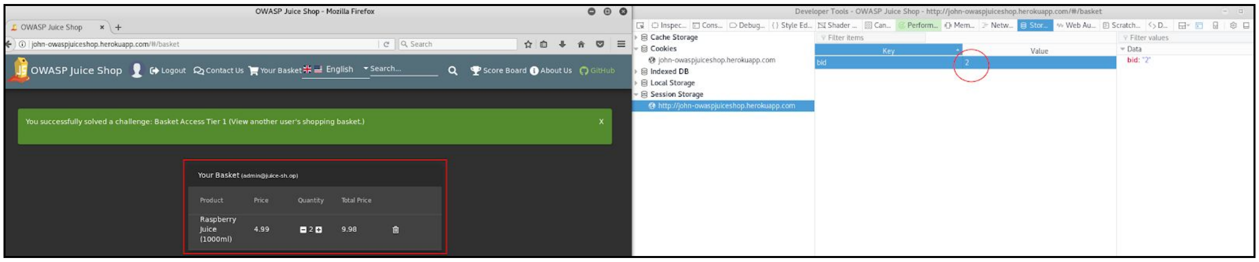
ct	Price	Quantity	Total Price
Juice ml)	1.99	2	3.98
Orange Juice (1000ml)	2.99	3	8.97
Eggfruit Juice (500ml)	8.99	1	8.99

Session Storage: http://john-owaspjuiceshop.herokuapp.com

Key	Value
bid	1

Data
bid: "1"

4. Replace the value of “bid” from 1 to 2 (or any other number) and refresh the page. The “Your Basket” page will show a different item (order).



OWASP Juice Shop - Mozilla Firefox

john-owaspjuiceshop.herokuapp.com/#/basket

You successfully solved a challenge: Basket Access Tier 1 (View another user's shopping basket.)

Your Basket (admin@juice-sh.op)

Product	Price	Quantity	Total Price
Raspberry Juice (1000ml)	4.99	2	9.98

Session Storage: http://john-owaspjuiceshop.herokuapp.com

Key	Value
bid	2

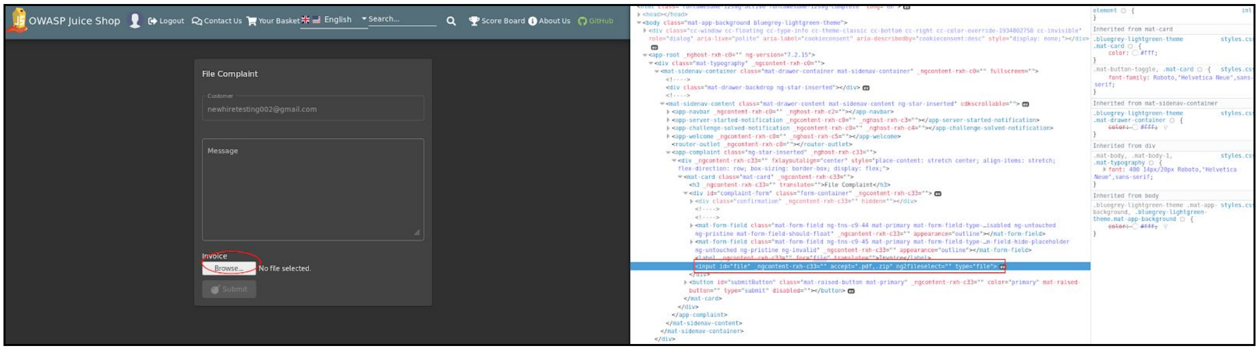
Data
bid: "2"

Written by Jonathan Harijanto

Deprecated Interface - Use a deprecated B2B interface that was not properly shut down

1. On the home page, login as any user

2. Go to the “File Complaint” page and do right-click on the “Browse…” button. Observe that it only accepts .pdf or .zip file



File Complaint

Customer
newhiretesting002@gmail.com

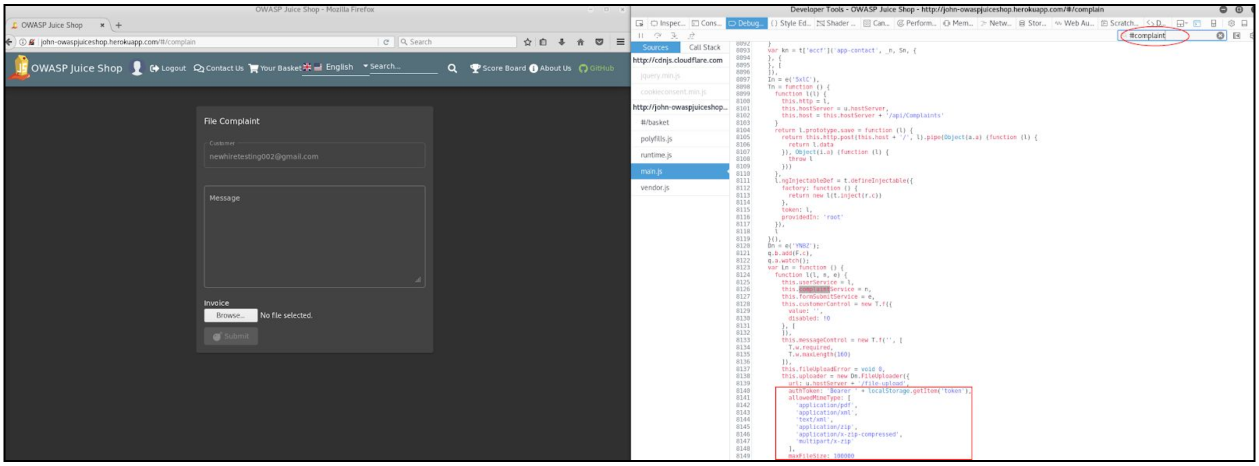
Message

Invoice
Browse... No file selected.

Submit

```
<head></head>
<body class="mat-app-background bluegrey-lightgreen-theme">
  <div class="cc-window cc-floating cc-type-info cc-theme-classic cc-bottom cc-right cc-color-override-1934802758 cc-invisible" role="dialog" aria-live="polite" aria-label="cookieconsent" aria-describedby="cookieconsent:desc" style="display: none;"></div>
  <app-root _nghost-rxh-c0="" ng-version="7.2.15">
    <div class="mat-typography" _ngcontent-rxh-c0="">
      <mat-sidenav-container class="mat-drawer-container mat-sidenav-container" _ngcontent-rxh-c0="" fullscreen="">
        <!---->
        <div class="mat-drawer-backdrop ng-star-inserted"></div>
        <!---->
        <mat-sidenav-content class="mat-drawer-content mat-sidenav-content ng-star-inserted" cdkscrollable="">
          <app-navbar _ngcontent-rxh-c0="" _nghost-rxh-c2=""></app-navbar>
          <app-server-started-notification _ngcontent-rxh-c0="" _nghost-rxh-c3=""></app-server-started-notification>
          <app-challenge-solved-notification _ngcontent-rxh-c0="" _nghost-rxh-c4=""></app-challenge-solved-notification>
          <app-welcome _ngcontent-rxh-c0="" _nghost-rxh-c5=""></app-welcome>
          <router-outlet _ngcontent-rxh-c0=""></router-outlet>
          <app-complaint class="ng-star-inserted" _nghost-rxh-c33="">
            <div _ngcontent-rxh-c33="" fxlayoutalign="center" style="place-content: stretch center; align-items: stretch;
            flex-direction: row; box-sizing: border-box; display: flex;">
              <mat-card class="mat-card" _ngcontent-rxh-c33="">
                <h3 _ngcontent-rxh-c33="" translate="">File Complaint</h3>
                <div id="complaint-form" class="form-container" _ngcontent-rxh-c33="">
                  <div class="confirmation" _ngcontent-rxh-c33="" hidden=""></div>
                  <!---->
                  <!---->
                  <mat-form-field class="mat-form-field ng-tns-c9-44 mat-primary mat-form-field-type-…isabled ng-untouched
                  ng-pristine mat-form-field-should-float" _ngcontent-rxh-c33="" appearance="outline"></mat-form-field>
                  <mat-form-field class="mat-form-field ng-tns-c9-45 mat-primary mat-form-field-type-…n-field-hide-placeholder
                  ng-untouched ng-pristine ng-invalid" _ngcontent-rxh-c33="" appearance="outline"></mat-form-field>
                  <label _ngcontent-rxh-c33="" for="file" translate="">Invoice</label>
                  <input id="file" _ngcontent-rxh-c33="" accept=".pdf,.zip" ng2fileselect="" type="file">
                </div>
                <button id="submitButton" class="mat-raised-button mat-primary" _ngcontent-rxh-c33="" color="primary" mat-raised-
                button="" type="submit" disabled=""></button>
              </mat-card>
            </div>
          </app-complaint>
        </mat-sidenav-content>
      </mat-sidenav-container>
    </div>
```

3. On the same Developer Tools, go to the “Debugger” tab and select the file “main.js”. Search for the word “complaint”. Notice that there’s a list of accepted file extension accepted, one of them is .xml (hidden).



john-owaspjuiceshop.herokuapp.com/#/complain

Developer Tools - OWASP Juice Shop - http://john-owaspjuiceshop.herokuapp.com/#/complain

#complaint

File Complaint

Customer
newhiretesting002@gmail.com

Message

Invoice
Browse... No file selected.

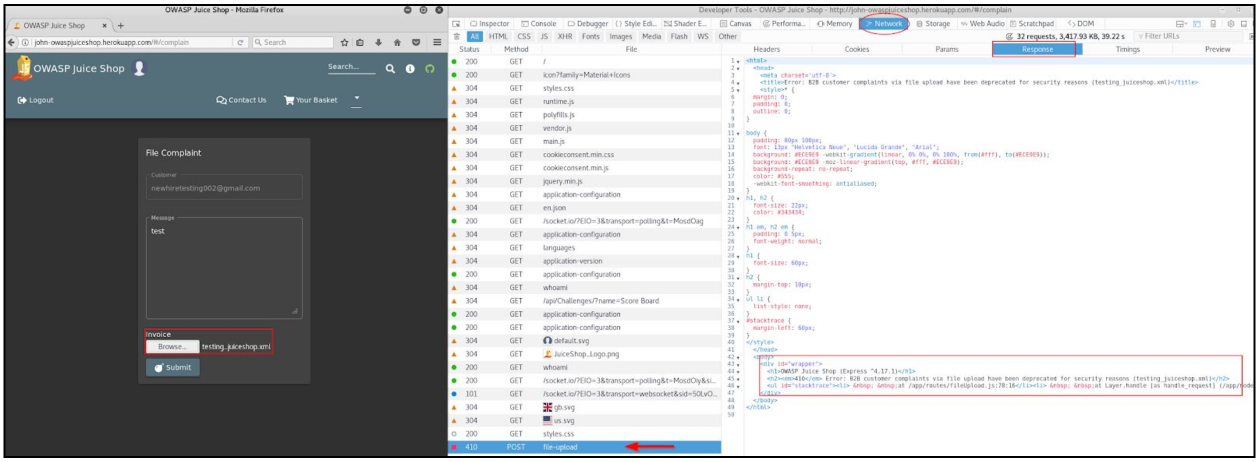
Submit

```
}
var kn = t['eccf']('app-contact', _n, Sn, {
}, {
}, [
]),
In = e('5xlC'),
Tn = function () {
  function l(l) {
    this.http = l,
    this.hostServer = u.hostServer,
    this.host = this.hostServer + '/api/Complaints'
  }
  return l.prototype.save = function (l) {
    return this.http.post(this.host + '/', l).pipe(Object(a.a) (function (l) {
      return l.data
    }), Object(i.a) (function (l) {
      throw l
    }))
  },
  l.ngInjectableDef = t.defineInjectable({
    factory: function () {
      return new l(t.inject(r.c))
    },
    token: l,
    providedIn: 'root'
  }),
  l
}(),
Dn = e('YNBZ');
q.b.add(F.c),
q.a.watch();
var Ln = function () {
  function l(l, n, e) {
    this.userService = l,
    this.complaintService = n,
    this.formSubmitService = e,
    this.customerControl = new T.f({
      value: '',
      disabled: !0
    }, [
    ]),
    this.messageControl = new T.f('', [
      T.w.required,
      T.w.maxLength(160)
    ]),
    this.fileUploadError = void 0,
    this.uploader = new Dn.FileUploader({
      url: u.hostServer + '/file-upload',
      authToken: 'Bearer ' + localStorage.getItem('token'),
      allowedMimeType: [
        'application/pdf',
        'application/xml',
        'text/xml',
        'application/zip',
        'application/x-zip-compressed',
        'multipart/x-zip'
      ],
      maxFileSize: 100000
```

4. Create a random .xml file and upload it on the “File Complaint” page.

Written by Jonathan Harijanto

5. Open the Developer Tools and navigate to the “Network” tab. An error message will appear saying that B2B customer complaints via file upload have been deprecated for security reasons.



File Complaint

Customer: newhiretesting002@gmail.com

Message: test

Invoice: testing_juiceshop.xml

```
Status  Method  File
200     GET     /
200     GET     icon?family=Material+Icons
304     GET     styles.css
304     GET     runtime.js
304     GET     polyfills.js
304     GET     vendor.js
304     GET     main.js
304     GET     cookieconsent.min.css
304     GET     cookieconsent.min.js
304     GET     jquery.min.js
304     GET     application-configuration
304     GET     en.json
200     GET     /socket.io/?EIO=3&transport=polling&t=MosdOag
304     GET     application-configuration
304     GET     languages
304     GET     application-version
200     GET     application-configuration
304     GET     whoami
304     GET     /api/Challenges/?name=Score Board
200     GET     application-configuration
200     GET     application-configuration
304     GET     default.svg
304     GET     JuiceShop_Logo.png
200     GET     whoami
200     GET     /socket.io/?EIO=3&transport=polling&t=MosdOiy&si...
101     GET     /socket.io/?EIO=3&transport=websocket&sid=50LvO...
304     GET     gb.svg
304     GET     us.svg
200     GET     styles.css
410     POST    file-upload
```

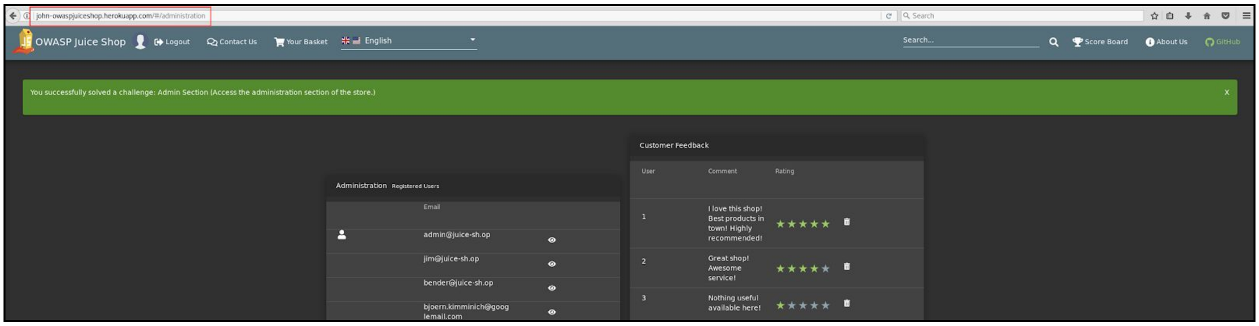
```
<html>
  <head>
    <meta charset='utf-8'>
    <title>Error: B2B customer complaints via file upload have been deprecated for security reasons (testing_juiceshop.xml)</title>
    <style>* {
  margin: 0;
  padding: 0;
  outline: 0;
}

body {
  padding: 80px 100px;
  font: 13px "Helvetica Neue", "Lucida Grande", "Arial";
  background: #ECE9E9 -webkit-gradient(linear, 0% 0%, 0% 100%, from(#fff), to(#ECE9E9));
  background: #ECE9E9 -moz-linear-gradient(top, #fff, #ECE9E9);
  background-repeat: no-repeat;
  color: #555;
  -webkit-font-smoothing: antialiased;
}
h1, h2 {
  font-size: 22px;
  color: #343434;
}
h1 em, h2 em {
  padding: 0 5px;
  font-weight: normal;
}
h1 {
  font-size: 60px;
}
h2 {
  margin-top: 10px;
}
ul li {
  list-style: none;
}
#stacktrace {
  margin-left: 60px;
}
</style>
  </head>
  <body>
    <div id="wrapper">
      <h1>OWASP Juice Shop (Express ^4.17.1)</h1>
      <h2><em>410</em> Error: B2B customer complaints via file upload have been deprecated for security reasons (testing_juiceshop.xml)</h2>
      <ul id="stacktrace"><li> &nbsp; &nbsp;at /app/routes/fileUpload.js:78:16</li><li> &nbsp; &nbsp;at Layer.handle [as handle_request] (/app/node
    </div>
  </body>
</html>
```

Written by Jonathan Harijanto

Five-Star Feedback - Get rid of all 5-star customer feedback

1. Login as Admin and visit the /administration page

2. Scan through the “Customer Feedback” and remove the 5-star review(s)



john-owaspjuiceshop.herokuapp.com/#/administration

You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration Registered Users

	Email	
👤	admin@juice-sh.op	👁
	jim@juice-sh.op	👁
	bender@juice-sh.op	👁
	bjoern.kimminich@googlemail.com	👁

Customer Feedback

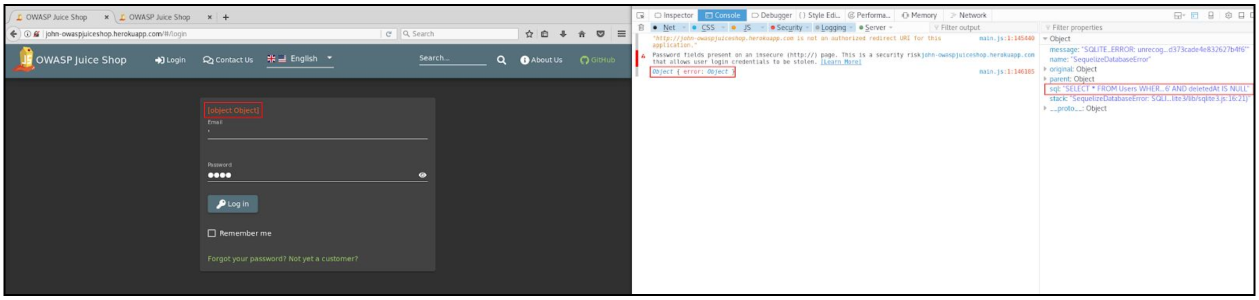
User	Comment	Rating	
1	I love this shop! Best products in town! Highly recommended!	★★★★★	🗑
2	Great shop! Awesome service!	★★★★☆	🗑
3	Nothing useful available here!	★☆☆☆☆	🗑

Written by Jonathan Harijanto

Login Admin - Log in with the administrator's user account

1. Go to the Login page and open the Developer Tools. Navigate to the “Console” tab.

2. Perform a simple “injection” where Email==’ && Password==test. Observe what’s displayed on the UI and also the Console window. Yes, the author included the SQL query.



```
"http://john-owaspjuiceshop.herokuapp.com is not an authorized redirect URI for this     main.js:1:145440
application."
Password fields present on an insecure (http://) page. This is a security riskjohn-owaspjuiceshop.herokuapp.com
that allows user login credentials to be stolen. [Learn More]
Object { error: Object }                                                                  main.js:1:146185
```

```
Object
  message: "SQLITE_ERROR: unrecog...d373cade4e832627b4f6'"
  name: "SequelizeDatabaseError"
  original: Object
  parent: Object
  sql: "SELECT * FROM Users WHER...6' AND deletedAt IS NULL"
  stack: "SequelizeDatabaseError: SQLI...lite3/lib/sqlite3.js:16:21)"
  __proto__: Object
```

3. The query retrieved from “Console” window:

    "SELECT * FROM Users WHERE email = ''' AND password = '098f6bcd4621d373cade4e832627b4f6' AND deletedAt IS NULL"

4. Perform the real injection by doing:

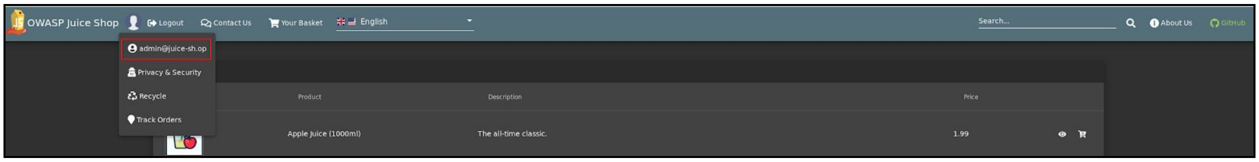
    Email: ‘ OR true
    Password: test

5. The injection didn’t work. But, notice the change in the SQL query:

    “SELECT * FROM Users WHERE email = '' OR true' AND password = '098f6bcd4621d373cade4e832627b4f6' AND deletedAt IS NULL"

6. Try another injection using double-dash (it is used to out-comment a query in SQL language):

    Email: ‘ OR true --
    Password: test



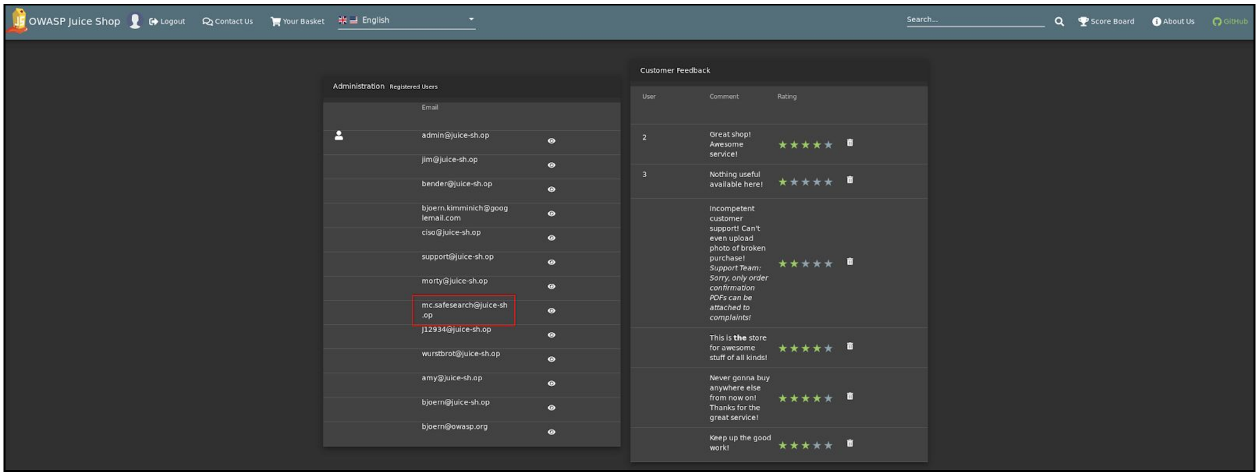
Product	Description	Price
Apple Juice (1000ml)	The all-time classic.	1.99

Source:
https://stackoverflow.com/questions/31288409/double-hyphen-dash-in-sql-injection-what-are-they-used-for

Written by Jonathan Harijanto

Login MC SafeSearch - Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass

1. Login as an Admin and go to the "/administration" page. Look for the user "mc.safesearch". The only missing piece is the password!



Administration Registered Users

Email
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@googlemail.com
ciso@juice-sh.op
support@juice-sh.op
morty@juice-sh.op
mc.safesearch@juice-sh.op
J12934@juice-sh.op
wurstbrot@juice-sh.op
amy@juice-sh.op
bjoern@juice-sh.op
bjoern@owasp.org

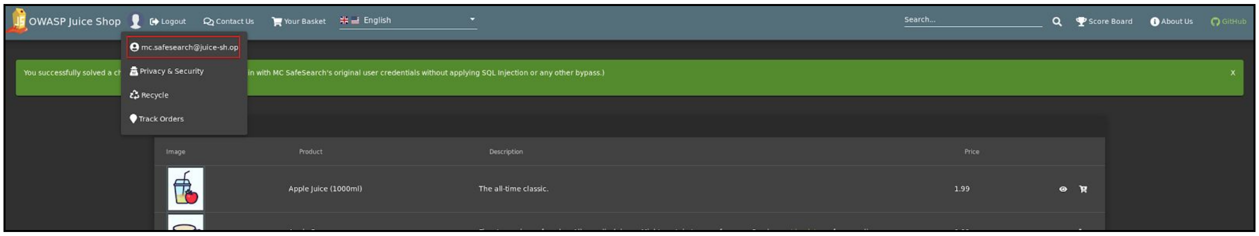
Customer Feedback

User	Comment	Rating
2	Great shop! Awesome service!	★★★★☆
3	Nothing useful available here!	★☆☆☆☆
	Incompetent customer support! Can't even upload photo of broken purchase! *Support Team: Sorry, only order confirmation PDFs can be attached to complaints!*	★★☆☆☆
	This is **the** store for awesome stuff of all kinds!	★★★★☆
	Never gonna buy anywhere else from now on! Thanks for the great service!	★★★★☆
	Keep up the good work!	★★★☆☆

2. Google the name "MC SafeSearch". One of the search results will be from Youtube (https://www.youtube.com/watch?v=v59CX2DiX0Y)

3. At :35 seconds in the video, the rapper says "Why not use the first name of your favorite pet? Mine is my dog, Mr. Noodle." And, at :45 seconds, the rapper adds "replace some vowels with zeroes".

Email: mc.safesearch@juice-sh.op
Password: Mr. N00dles



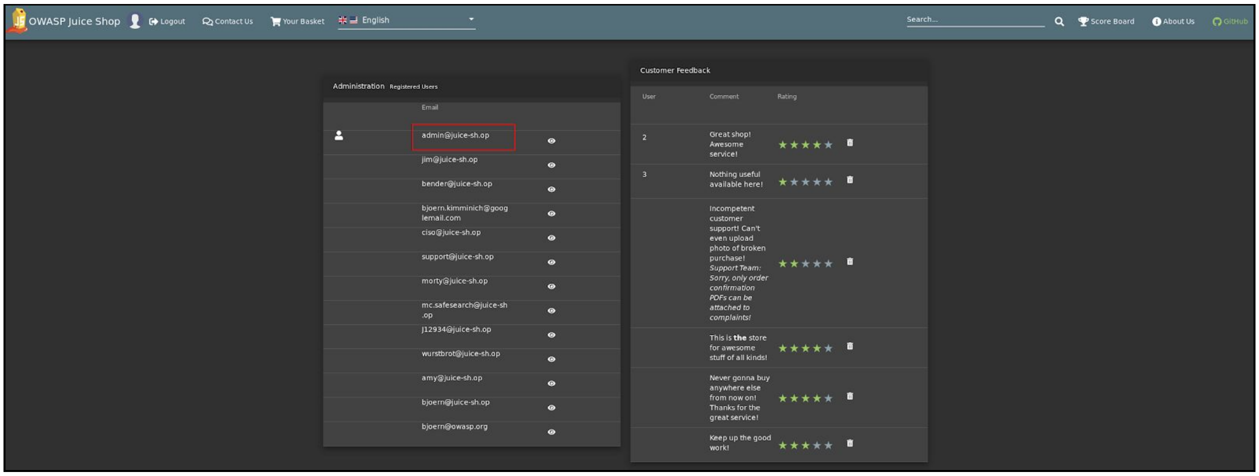
You successfully solved a ch in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.)

Image	Product	Description	Price
	Apple Juice (1000ml)	The all-time classic.	1.99

Written by Jonathan Harijanto

Password Strength - Log in with the administrator's user credentials without previously changing them or applying SQL Injection

1. Login as an Admin via SQL injection and go to the “/administration” page



Administration Registered Users

Email
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@googlemail.com
ciso@juice-sh.op
support@juice-sh.op
morty@juice-sh.op
mc.safesearch@juice-sh.op
J12934@juice-sh.op
wurstbrot@juice-sh.op
amy@juice-sh.op
bjoern@juice-sh.op
bjoern@owasp.org

Customer Feedback

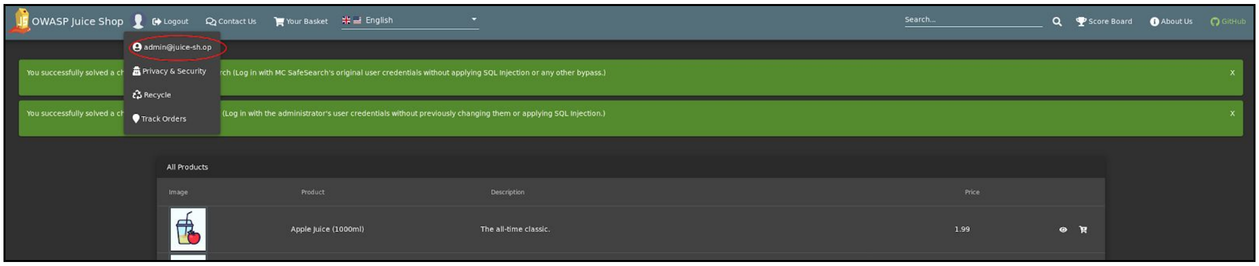
User	Comment	Rating
2	Great shop! Awesome service!	★★★★☆
3	Nothing useful available here!	★☆☆☆☆
	Incompetent customer support! Can't even upload photo of broken purchase! *Support Team: Sorry, only order confirmation PDFs can be attached to complaints!*	★★☆☆☆
	This is **the** store for awesome stuff of all kinds!	★★★★☆
	Never gonna buy anywhere else from now on! Thanks for the great service!	★★★★☆
	Keep up the good work!	★★★☆☆

2. The email address is admin@juice-sh.op. The only missing piece is the password.

3. Go to Google and search for the keywords “Basic Administrator Password” ⇒ https://www.darkreading.com/attacks-breaches/top-10-admin-passwords-to-avoid/d/d-id/1128615

4. Try all of the possible passwords.

Username: admin@juice-sh.op
Password: admin123



You successfully solved a ch… rch (Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.) X

You successfully solved a ch… (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.) X

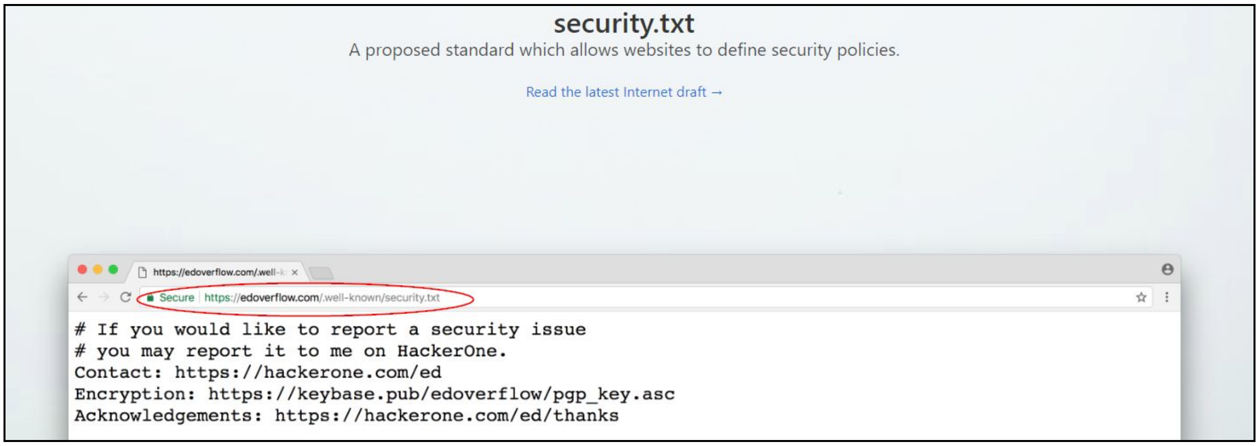
All Products

Image	Product	Description	Price
	Apple Juice (1000ml)	The all-time classic.	1.99

Written by Jonathan Harijanto

Security Policy - Behave like any "white-hat" should

1. Google the keyword “security.txt” (https://securitytxt.org/). It’s supposed to be the standard at every website about it’s security policies.



security.txt

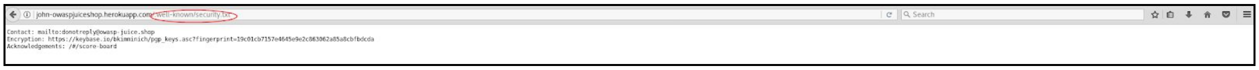
A proposed standard which allows websites to define security policies.

Read the latest Internet draft →

https://edoverflow.com/.well-k
Secure
https://edoverflow.com/.well-known/security.txt

```
# If you would like to report a security issue
# you may report it to me on HackerOne.
Contact: https://hackerone.com/ed
Encryption: https://keybase.pub/edoverflow/pgp_key.asc
Acknowledgements: https://hackerone.com/ed/thanks
```

2. Apply the same concept to the JuiceShop website (http://john-owaspjuiceshop.herokuapp.com/.well-known/security.txt)



```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda
Acknowledgements: /#/score-board
```

3. The content of that address looks like this:

```
Contact: mailto:donotreply@owasp-juice.shop
Encryption:
https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda
Acknowledgements: /#/score-board
```

Written by Jonathan Harijanto

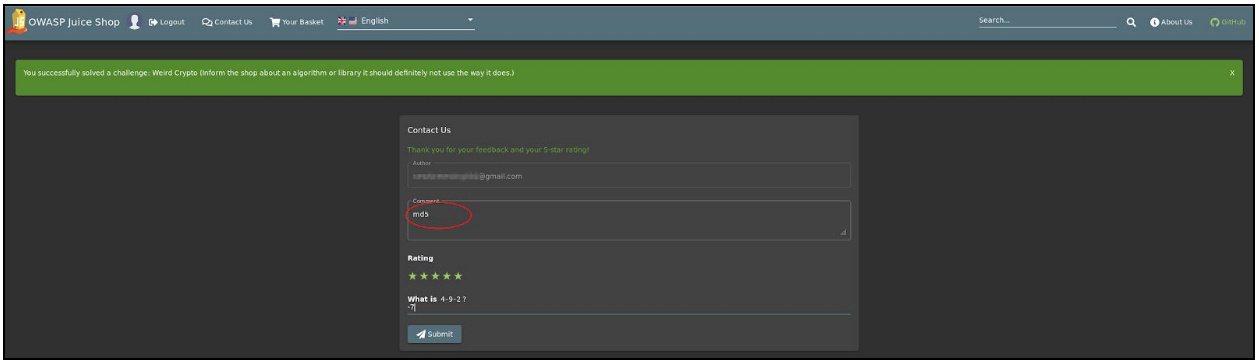
Weird Crypto - Inform the shop about an algorithm or library it should definitely not use the way it does

1. Analyze the hint. It says:

> *To fulfil this challenge you must identify a cryptographic algorithm (or crypto library) that either*
>
> - *should not be used at all*
> - *or is a bad choice for a given requirement*
> - *or is used in an insecure way.*
>
> *Use the Contact Us form to submit a feedback mentioning the abused algorithm or library.*

2. One of the obvious insecure cryptographic algorithms is md5.

3. Login as any user. Go to the “Contact Us” page and type “md5” as the comment. Hit Submit.



You successfully solved a challenge: Weird Crypto (Inform the shop about an algorithm or library it should definitely not use the way it does.)

Contact Us

Thank you for your feedback and your 5-star rating!

Author: [redacted]@gmail.com

Comment: md5

Rating: ★★★★★

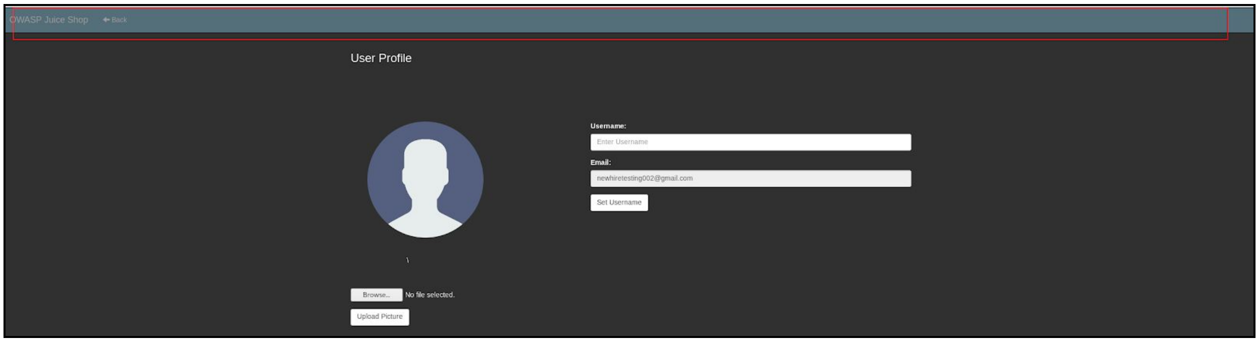
What is 4-9-2 ? -7

Written by Jonathan Harijanto

XSS Tier 1.5 - Perform an XSS attack with <script>alert(`xss`)</script> on a legacy page within the application

1. The title of the challenge says “legacy page” which provides a small hint that the target page must look outdated compared with all others.

2. Login with any user and go to the “User Profile” page. Notice that it looks “older” than the rest of the pages in the Web App.

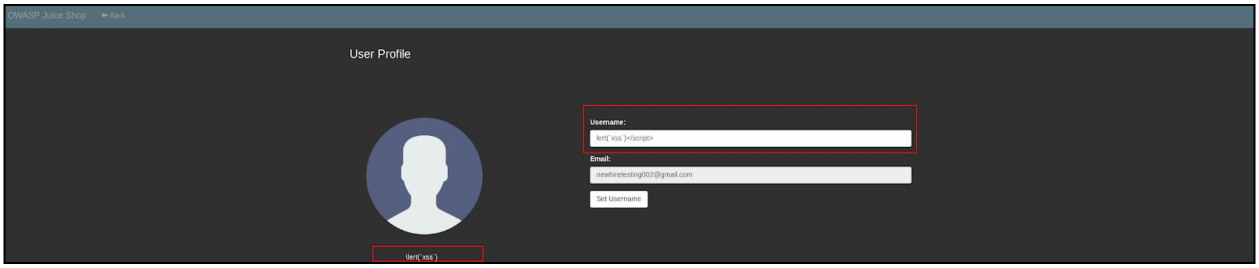


Username: Enter Username

Email: newhiretesting002@gmail.com

\

3. Copy-paste the payload string into the “Username” field. Observe the way this page parses the input. The username below the profile picture becomes “lert(`xss`)”, whereas the Username field becomes “lert(`xss`)</script>”.



Username: lert(`xss`)</script>

Email: newhiretesting002@gmail.com

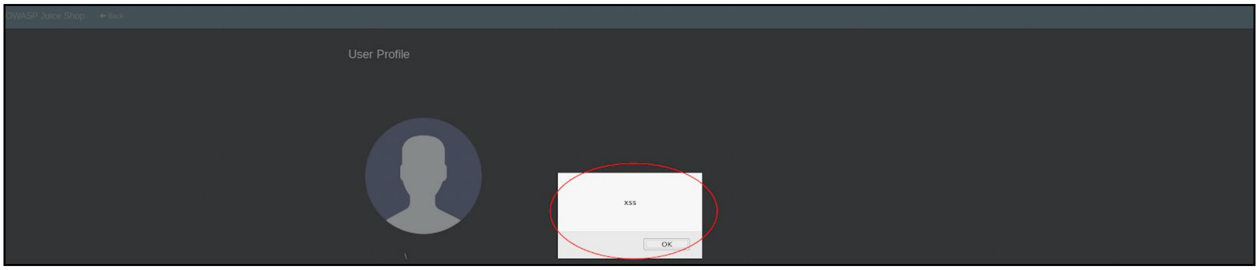
\lert(`xss`)

4. This shows that the input is sanitized, but it still has some loopholes.

Written by Jonathan Harijanto

5. Play around with the input in the “Username” field. These are what I tried:

Input	Output (result)
<a><script>alert(`xss`)</script>	cript>alert(`xss`)</script>
<<a>script>alert(`xss`)</script>	<cript>alert(`xss`)</script>
<<a>sscript>alert(`xss`)</script>	*pop-up appears*



User Profile

xss