1. Logging

S.No	Unique ID	Repeatable Steps	Expected Results	CWE	Actual Results	Total (0.75)
1	Available	Clear enough	Available	Available	The successful login is recorded in logs.	0.75
2	Available	Clear enough	Available	Available	The failed login is recorded in logs.	0.75
3	Available	Clear enough	Available	Available	The successful login is recorded in logs.	0.75
4	Available	Clear enough	Available	Available	The failed login is recorded in logs.	0.75
5	Available	Clear enough	Available	Available	The successful login is recorded in the logs, with an included timestamp for the given attempt.	0.75
6	Available	Clear enough	Available	Available	The failed logins are recorded in the logs, with an included timestamp for each attempt.	0.75
7	Available	Clear enough	Available	Available	The failed login is recorded in logs without executing the included script. The script is not neutralized though.	0.75
8	Available	Clear enough	Available	Available	The successful login is recorded in logs with time but without displaying the time zone.	0.75

Comments: Test cases process of 1,2 are same as 3,4, except the ASVS IDs.

Comment on the adequacy: The explanation looks good and contains valid information. (**2 marks**)

Total: 8/8

2. Attack Model:

Category	Points
Name 5 Attack Groups	2
Ten Techniques Per Attack Group with Techniques and Mitigations	1.5
Up to 5 Attack Trees	3
Up to 5 Defense Trees	3
Extra Credit	2
Total	**11.5/10**

3. Threat Modeling:

Threat Model Diagram: 2 points (interactor/external entity, process, data flow, trust boundary Available)

STRIDE per element: 2 points

Elevation of Privilege: 2 points

Cornucopia: 2 points

LINDDUN per element: 2 points

All 17 threats are Unique. Some Threats do not suggest a mitigation.

4. Seeker:

Black Box Test / OWASP ZAP Instructions

S.No	Unique ID	Repeatable steps	Expected Results	CWE	Actual Results
1	Available	Available	Available	Available	No results were returned from search. The SQL code is not executed.
2	Available	Available	Available	Available	The request went through. Last name is saved as **'); DROP TABLE Patients;--.** But the SQL query is not executed.
3	Available	Available	Available	Available	The comment is safely encoded as to not be executed.
4	Available	Available	Available	Available	The password change is rejected.
5	Available	Can't reproduce the issue mentioned in repeatable steps. Not clear enough.	Available	Available	–

Screenshots of Seeker are available.

Total for Black Box Tests - 5/5 points

Seek true positives test cases:

S.No	Unique ID	Repeatable Steps	Expected Results	CWE	Actual Results	Total (3)
1	Available	Clear enough	Available	Available	The GET request payload contains a userid	3
2	Available	Clear enough	Available	Available	The webpage allows an insecure connection	3
3	Available	Clear enough	Available	Available	The X-Frame-Options and Content-Security-Policy headers are missing	3
4	Available	Clear enough	Available	Available	The POST request contains the username in the URL	3
5	Available	Clear enough	Available	Available	The X-XSS-Protection header is missing	3

Seeker True Positive Screenshots - 5/5 points

Seeker True Positive Black Box Tests - 15/15 points

Time Taken & True Positives Per Hour - Present

Seeker Total - 25/25

5. WebInspect:

WebInspect true positive test cases:

S.No	Unique ID	Repeatable steps	Expected Results	CWE	Actual Results	True Positive Marks	Black Box TestPlan Marks
1	Available	Available	Available	Available	The HttpOnly attribute is not marked as true.	1	4
2	Available	Available	Available	Available	The content of sql.inc is visible in the browser.	1	4
3	Available	Available	Available	Available	The password change as “123456789” is not allowed as it does not meet password change requirements.(Not a true positive)	0	4
4	Available	Available	Available	Available	The session tokens for both the logins are different. (Not a true positive)	0	4
5	Available	Available	Available	Available	The password change with less than 12 characters is being allowed. For Example: “12345678@vV”	1	4
Total Marks: 23/25						3/5	20/20

Screenshots of WebInspect are available.
Comment on true positives: In the report we only have 3/5 true positives and the remaining two are false positives as the actual results are the same as the expected results.

Total : 23/25

WebInspect Report is Available.

6. Test Coverage:

All the 4 four test cases newly reported are to increase the coverage of controls which previously did not have a test case for.
Total : 8/8

Recomputing the test coverage is done.
Total : 2/2

Total marks for test coverage: 10/10