Time taken 5 mins 35 secs Marks 14.00/15.00 Grade 93.33 out of 100.00 In the following vulnerable code, what type of attack can be performed? ('ping \${req.body.host}', (error, stdout, stderr) => {}}); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In the solid provided of the second of the sec	State Finished Monday, 17 March 2025, 3:38 PM Monday, 17 March 2025, 3:38 PM March 2025, 3:38 PM 14.00/15.00 March 2025 3:33 out of 100.00 March 2025 3:33 out of 100.00 March 2025 March 202	State Finished Completed on Monday, Time taken 5 mins 35 Marks 14.00/15.0 Grade 93.33 out Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (error of the following out of the following out of the following vulnerable coexec(`ping \${req.body.host}`, (error of the following out of the following out of the following vulnerable coexec(`ping \${req.body.host}`, (error of the following out of the following out of the following out of the following vulnerable coexec(`ping \${req.body.host}`, (error of the following out of the following o	17 March 2025, 3:38 PM secs 00 of 100.00 ode, what type of attack can be performed? or, stdout, stderr) => { });
Time taken 5 mins 35 secs Marks 14.00/15.00 Grade 93.33 out of 100.00 In the following vulnerable code, what type of attack can be performed? (*ping \$(req.body.host)*, (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In the store Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Time taken 5 mins 35 secs Marks 14.00/15.00 Question 1 Complete Mark 1.00 out of 1.00 Case SQL Injection Cross-Site Scripting (XSS) Cross-Site Scripting (XSS) How can Broken Access Control be exploited? By making too many API requests C. By logging in with the wrong password d. By using a strong password Glove the sale of the sale	Completed on Monday, Time taken 5 mins 35 Marks 14.00/15.0 Grade 93.33 out Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (error of the coexec) of the coexec of	secs 20 20 20 20 20 20 20 20 20 20 20 20 20
Time taken 5 mins 35 secs Marks 14.00/15.00 Grade 93.33 out of 100.00 In the following vulnerable code, what type of attack can be performed? ('ping \$\text{freq.body.host}', (error, stdout, stderr) => {}); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed? In the following vulnerable code, what type of attack can be performed	Time taken	Time taken 5 mins 35 Marks 14.00/15.0 Grade 93.33 out Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (error of the coexec) of the coexec of the coex	secs 20 20 20 20 20 20 20 20 20 20 20 20 20
Marks 14.00/15.00 Grade 93.33 out of 100.00 In the following vulnerable code, what type of attack can be performed? (ping \$(req.body.host); (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In the solid provided i	Mark: 14.00/15.00 Grade 93.33 out of 100.00 Question 1 Complete Mark: 1.00 out of 1.00 Given the following vulnerable code, what type of attack can be performed? exec(ping \${req.body.host}; (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark: 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Marks 14.00/15.0 Grade 93.33 out Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (error a. CSRF Attack b. Command Injection c. SQL Injection	ode, what type of attack can be performed? or, stdout, stderr) => { });
Grade 93.33 out of 100.00 In the following vulnerable code, what type of attack can be performed? ('ping S(req.body.host)', (error, stdout, stderr) => { }}); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In the solid process of the second	Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable code, what type of attack can be performed? exec(*)ping \${req.body.host}*, (error, stdout, stderr) => {}); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Grade 93.33 out Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (error a. CSRF Attack b. Command Injection c. SQL Injection	ode, what type of attack can be performed? or, stdout, stderr) => { });
n the following vulnerable code, what type of attack can be performed? ('ping \${req.body.host}', (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) and 2 te e e e e e e e e e e e e e e e e e e	Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable code, what type of attack can be performed? exec(ping \${req.body.host}, (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Question 1 Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (errollowing by the coexec of the co	ode, what type of attack can be performed? or, stdout, stderr) => { });
te 00 out of 1.00 In the following vulnerable code, what type of attack can be performed? (('ping \${req.body.host}', (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) In 2 te 00 out of 1.00 It can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Given the following vulnerable code, what type of attack can be performed? exec('ping \${req.body.host}', (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (errollowing by the complete of the complete o	or, stdout, stderr) => { });
nt the following vulnerable code, what type of attack can be performed? ((ping \${req.body.host})^*, (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) and 2 te end of the property of	Complete Mark 1.00 out of 1.00 Given the following vulnerable code, what type of attack can be performed? exec('ping \${req.body.host}', (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Complete Mark 1.00 out of 1.00 Given the following vulnerable coexec(`ping \${req.body.host}`, (errollowing by the complete of the complete o	or, stdout, stderr) => { });
n the following vulnerable code, what type of attack can be performed? ('ping \$(req.body.host)', (error, stdout, stderr') => { })); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) are 2 te 200 out of 1.00 are an Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Given the following vulnerable code, what type of attack can be performed? exec('ping \$(req.body.host)', (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Given the following vulnerable coexec('ping \${req.body.host}`, (errown a. CSRF Attack b. Command Injection c. SQL Injection	or, stdout, stderr) => { });
n the following vulnerable code, what type of attack can be performed? ('ping \$(req.body.host)', (error, stdout, stderr) => { }); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) a. 2 tee 00 out of 1.00 a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Given the following vulnerable code, what type of attack can be performed? exec(ping \${req.body.host}', (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Given the following vulnerable coexec(`ping \${req.body.host}`, (errollowing vulnerable coexec(`ping \${req.body.host}`, (errollowing vulnerable coexec(`ping \${req.body.host}`, (errollowing vulnerable coexec). a. CSRF Attack b. Command Injection c. SQL Injection	or, stdout, stderr) => { });
(Cping \${req.body.host}`, (error, stdout, stderr) => {}); a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	exec(`ping \${req.body.host}`, (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	exec(`ping \${req.body.host}`, (error a. CSRF Attack b. Command Injection c. SQL Injection	or, stdout, stderr) => { });
(Cping \${req.body.host}`, (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) a. 2 tee 00 out of 1.00 a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	exec(`ping \${req.body.host}`, (error, stdout, stderr) => { }}; a. CSRF Attack b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	exec(`ping \${req.body.host}`, (error a. CSRF Attack b. Command Injection c. SQL Injection	or, stdout, stderr) => { });
b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) on 2 te e e e e e e e e e e e e e e e e e e	 b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password Question 3	b. Command Injectionc. SQL Injection	
b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) on 2 te e e e e e e e e e e e e e e e e e e	 b. Command Injection c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password Question 3	b. Command Injectionc. SQL Injection	
c. SQL Injection d. Cross-Site Scripting (XSS) on 2 te 00 out of 1.00 r can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	c. SQL Injection d. Cross-Site Scripting (XSS) Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	c. SQL Injection	
d. Cross-Site Scripting (XSS) an 2 te 2 te 200 out of 1.00 a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password		
to an Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Question 2 Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	a. Cross-site scripting (XSS	.1
a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password		
a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Complete Mark 1.00 out of 1.00 How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	Question 2	
a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password		
a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	How can Broken Access Control be exploited? a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password	•	
 a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password 	 a. By modifying JWT tokens or accessing restricted APIs b. By making too many API requests c. By logging in with the wrong password d. By using a strong password 		
 b. By making too many API requests c. By logging in with the wrong password d. By using a strong password 	 b. By making too many API requests c. By logging in with the wrong password d. By using a strong password Question 3	How can Broken Access Control b	pe exploited?
c. By logging in with the wrong password d. By using a strong password	 c. By logging in with the wrong password d. By using a strong password Question 3	a. By modifying JWT token	s or accessing restricted APIs
c. By logging in with the wrong password d. By using a strong password	 c. By logging in with the wrong password d. By using a strong password Question 3	b. By making too many API	requests
d. By using a strong password	d. By using a strong passwordQuestion 3		
on 3	Question 3		
		a. By asing a strong passwi	
te te	Complete	Question 3	
00 out of 1.00	Mark 1.00 out of 1.00	Question 3 Complete	
	Complete Mark 1.00 out of 1.00	b. By making too many APIc. By logging in with the w	requests rong password

O b. By sending an empty request body

c. By making multiple requests at the same timed. By injecting shell commands in the plateNumber field

Question 4	
Complete	
Mark 1.00 o	ut of 1.00
If a user	r inputs `ABC123 && rm -rf /`, what will happen on a Linux server?
О а.	
b.	The entire file system could be deleted
○ c.	The server will shut down immediately
O d.	The vehicle tracking system will show an error
Question 5	;
Mark 1.00 o	ut of 1.00
What co	ommand could an attacker enter in the `/track-vehicle` endpoint to delete files on a Windows system?
a.	ABC123 && del C:\Windows\System32
	ABC123 && mv /etc/passwd /dev/null
	ABC123 && shutdown -h now
	ABC123; rm -rf /
o u.	7.65 (125, 111 11)
Question 6)
Complete	
Mark 1.00 o	ut of 1.00
What is	the best way to prevent command injection attacks?
О а.	Use an insecure API to execute shell commands
b.	Allow user input directly in system commands
C.	Use parameterized queries and sanitize input
O d.	Use eval() to process user input
Question 7	,
Complete	
Mark 1.00 o	ut of 1.00
What is	the correct way to restrict access to admin users only?
a.	if (!decoded.role) return res.status(403).json({ error: 'Forbidden' });
O b.	if (decoded.role !== 'user') return res.status(403).json({ error: 'Forbidden' });
O c.	if (decoded.id === 1) return res.status(403).json({ error: 'Forbidden' });
d.	if (decoded.role !== 'admin') return res.status(403).json({ error: 'Forbidden' });

Question 8		
Complete		
Mark 1.00 out of 1.00		
What is the impact of Broken Access Control on an application?		
a. Attackers can execute arbitrary commands on the server		
○ b. It allows Cross-Site Scripting (XSS)		
c. Unauthorized users can access restricted information or perform admin actions		
d. The database gets automatically deleted		
Question 9		
Complete		
Mark 1.00 out of 1.00		
What is the primary cause of command injection vulnerabilities in applications?		
a. Poor network security configuration		
b. Lack of input validation when executing system commands		
○ c. Using HTTPS instead of HTTP		
d. Incorrect use of loops in JavaScript		
Question 10		
Complete		
Mark 1.00 out of 1.00		
THEIR LOOP CALL OF LOOP		
What is the safest way to execute system commands in Node.js?		
Consistential user input into system commands		
a. Concatenating user input into system commands		
b. Using eval()		

- o. Using execFile() with sanitized input
- od. Using exec() with user input

Question 11 Complete Mark 1.00 out of 1.00

What security flaw exists in the following '/users' endpoint?

```
app.get('/users', (req, res) => {
  const token = req.headers.authorization;
  jwt.verify(token, SECRET_KEY, (err, decoded) => {
    db.query('SELECT id, username, role FROM users', (err, results) => {
      res.json({ users: results });
    });
  });
});

a. It does not store passwords securely
    b. It does not verify the user's role before returning data
    c. It is vulnerable to SQL injection
```

Question 12

Complete

Mark 0.00 out of 1.00

What would happen if an attacker modified a JWT token to escalate their privileges?

- a. The token would expire immediately
- igcup b. They could access admin-only features
- oc. The server would detect the modification and reject the request
- od. They would get logged out

od. It does not return JSON data

Question 13

Complete

Mark 1.00 out of 1.00

Which function is the most dangerous when handling user input in Node.js?

- a. parseInt()
- b. exec()
- c. JSON.stringify()
- d. console.log()

Question 14 Complete Mark 1.00 out of 1.00

Which of the following is an effective way to prevent Broken Access Control?

- a. Validate user roles and permissions before processing requests
- Ob. Allow users to modify their own JWT tokens
- oc. Remove authentication from sensitive endpoints
- O d. Store JWT tokens in Local Storage without encryption

Question 15

Complete

Mark 1.00 out of 1.00

```
Why is the following endpoint a security risk?
app.get('/users', (req, res) => {
    db.query('SELECT id, username, role FROM users', (err, results) => {
      res.json({ users: results });
    });
});

    a. It uses HTTPS instead of HTTP
    b. It is vulnerable to CSRF
    c. It allows SQL Injection
```

od. It exposes all users' details without authentication