Application Sample Scenario

CREST Certification Examination – Example Examination Paper

Application – Scenario

This is an example of a CREST Certified Tester (Application) examination paper, designed to give candidates an understanding of the structure of the Scenario component of the CCT Application examination.

Candidates should use this to aid examination preparation, but should **not** use this as an indication of the technical content and capability required. Candidates should refer to the syllabus to understand the breadth and depth of the required knowledge and capability.

Table of Contents

1 Introduction 3
1.1 Marking 3
1.2 Late Delivery Penalty 3
2 Rules of Engagement 4
2.1 Application 4
3 Scenario Question (150 marks, 150 minutes) 5
3.1 Background 5
3.2 Risk Summary 5
3.3 Test Scope and Methodology 5
3.4 Vulnerability List From Zenicarna 6
3.5 Web Application Details 7
3.6 Application Server Details 7
3.7 Reporting 8
3.8 Answer 9
3.9 Tasks (145 marks) 10
3.10 Report Deliverables (5 marks) 12

Application Sample Scenario

1 Introduction

You will be given **15 minutes** before the examination starts to read through the requirements for this part of the exam. This is purely for you to get familiar with the requirements of the scenario component of the Application Certification Examination; no examination activities are permitted during this time.

The application examination comprises two parts; this is the first and requires you to complete a scenario question which involves practical work and reporting, based on the concept of a retest. The second part, which you will attempt after this one, is based on a practical penetration test. You must achieve the minimum pass mark in both parts.

There is no requirement to complete the individual sections in the order that they are given in this worksheet: feel free to complete them as you wish, provided that you do so within the allotted time.

You should upload your deliverables to **\\crestanswers\Scenario** before the end of the examination, and are advised to save your work as you go along.

1.1 Marking

Written answers to these questions should be of a similar quality to a report supplied as a client deliverable by a CREST company. Candidates should be aware that the following will not attract marks:

- Lack of a form and style of writing appropriate to purpose, or appropriate to the audience.
- Unclear or ambiguous answers.
- Incorrect technical information (e.g. incorrect findings or incorrect terminology)
- Poor sentence construction.
- An excessive number of spelling or grammatical errors, or casual language which would not be suitable in a professional report.
- Overly vague, generic, incorrect or irrelevant content included as part of the answer which adds no meaningful value to the report.
- An absence of contextualisation of the findings.

1.2 Late Delivery Penalty

You have 150 minutes to complete the scenario portion of this exam including delivery of your output. It is suggested you ensure that you can deliver the output as required prior to the end of the 150 minutes.

Output submitted after the 150 minutes elapses is subject to a penalty (5 marks per minute overdue). You may also lose access to **\\crestanswers\Scenario** after this time, so ensure that any deliverables have been correctly saved in good time.

2 Rules of Engagement

2.1 Application

The purpose of the rules and information below is to help you during the examination, and prevent you from attacking the wrong targets or wasting time on hosts that will be much more difficult to attack successfully.

- You should be able to obtain an IPv4 address by DHCP – this will be in the range **172.29.240.0/20** and you must **not** attack systems outside this range.
- You may need to configure your DNS server manually to **172.29.253.254**.
- You may need to configure your DNS suffix manually to **elements.crest**.
- You may make any legitimate DNS queries to **172.29.253.254**.
- The examination answers host (**\\crestanswers**) is provided for you to upload your deliverables. There is nothing to be gained by attempting to compromise this host; no correct answers are stored on it. It is simply a file share designed for electronic submission of your examination answers.

For this part, you may ONLY interact with:

- The DHCP server (legitimate DHCP traffic only)
- The DNS server (legitimate DNS queries only)
- The application that you have been specifically asked to review.
- The examination answers share (\\crestanswers) - legitimate requests only.

No interaction is permitted with ANY other system or IP address.

Any other interaction may result in immediate termination of your examination.

3 Scenario Question (150 marks, 150 minutes)

3.1 Background

Zenicarna, a fictional pharmaceuticals company, have engaged you to conduct an application assessment against one of their internal applications for annual compliance purposes. The application is sensitive in nature as it holds payroll data and associated human resources records.

The application has undergone an annual assessment through automated scanners but this year Zenicarna would like a manual assessment of specific issues to be conducted. Previous scans of the application indicated to the customer that several serious risks were present but the third party developers stated that the risks were only theoretical and any practical attack attempts would fail.

Zenicarna's primary aim is to obtain an impartial insight into the security risks reported by automated tooling against the application, which will then be presented to both technical and business leaders in the organisation where a view will be taken on any future work required.

Zenicarna have provided a list of vulnerabilities reported by the automated tooling and require them to be retested by a CREST Certified Applications consultant. This list of vulnerabilities has been reproduced in Section 3.4. Note a full test of all functionality is not required as this will be conducted at a later date.

3.2 Risk Summary

The primary concern of Zenicarna surrounds the sensitive data in the application, as there is a duty of care and legal obligations around holding payroll and employees' personal information. Confidentiality is a critical requirement whilst integrity of the data is also key to ensuring the business can meet its functional requirements. The availability of data is less of a concern as there is a backup human resources system instance and the hosting provider has extensive failover ability (including to the dataset in the application).

3.3 Test Scope and Methodology

Zenicarna understand that a full test of the application is not viable in the time allocated. They have instead opted for a specific retest of issues identified through automated tooling. This will be using a "white-box" approach against the issues shared. These issues are shared in Section 3.4. Specifically this means that you do not need to identify or comment on any other vulnerabilities that may be present in the application.

Two accounts have been provisioned, one at a standard user level to simulate employee access and one which has administrative access that replicates the access rights of the Human Resources Director. These and the applications details can be found in Section 3.5.

There is also a set of local administrative credentials to the server hosting the application should server access to the application hosting server be needed. These, as well as the host server details, can be found in Section 3.6.

3.4 Vulnerability List From Zenicarna

Vulnerability ID	Vulnerability Title	Summary	Risk Rating
ZEN-APP-1	CGI Generic Command Execution	The remote web server hosts a CGI script (cgi-bin/ping.pl) that fails to adequately sanitise request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.	High
ZEN-APP-2	Apache 2.4.x Multiple Vulnerabilities	The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities.	High
ZEN-APP-3	Apache Tomcat Manager Bruteforced	Scanner successfully authenticated on the target Apache Tomcat manager interface by using weak or predictable credentials.	Medium
ZEN-APP-4	LDAP Injection Authentication Bypass	Scanner was able to detect a page that is vulnerable to LDAP injection based on known error messages. This injection was detected as scanner was able to bypass the authentication mechanism and access the authenticated web application.	Medium
ZEN-APP-5	Cross-Site Request Forgery	Scanner detected a request (update-salary), available only to authenticated users, where all parameters within are known or predictable. The request may therefore be vulnerable to CSRF attacks.	Low

3.5 Web Application Details

Application URL		**http://hrportal.zeninf.internal**
Low Privileged User Credentials	Username	pentest
	Password	password
Administrative User Credentials	Username	admin-pentest
	Password	Password

3.6 Application Server Details

Server Type	Web Server
Server FQDN	hrportal.zeninf.internal
Server OS	Windows Server 2022
Administrator Username	Administrator
Administrator Password	Adminpassword!
Remote Management	RDP, SMB

3.7 Reporting

Zenicarna expect a report in PDF format to be delivered at or before the deadline containing the sections below:

- A management summary, intended for Zenicarna's Head of Compliance (HOC). This role ultimately owns and is accountable for Zenicarna's risk. The HOC would like to understand the strategic themes and requires the technical findings to be translated into business risk. In particular, she would like to understand the extent to which the vulnerabilities would allow for the data inside the application to be stolen or manipulated. She is **not** a technical specialist and is very keen that the entire report is contextualised to Zenicarna's situation.
- A technical summary, intended for Zenicarna's Global Application Development Director, who has a technical background and is responsible for the overall delivery of all application in the business. A description of whether each issue is applicable or not as well as a likelihood of any vulnerabilities being exploited, explaining if a combination of vulnerabilities could form a path which results in a serious compromise, would be extremely welcome.
- Vulnerability descriptions, intended for Zenicarna's application developers, who will need a clear technical understanding of any issues that you discover. They require clear instructions on how to replicate and exploit any issues that you discover and specific recommendations. The content must be sufficiently detailed to allow a technically competent individual who does not have prior knowledge of this particular issue to be able to understand and reproduce it.

3.8 Answer

Your answers should be delivered as a single client report which contains, as a minimum, each of the deliverables detailed in section 3.7, and should be uploaded to **\\crestanswers\Scenario** before the end of the examination as **scenario.pdf**.

A report template layout is detailed in section 3.10. If you use report generation software or have corporate reporting templates, you may use them as long as the output is presented in a similar format and meets all criteria. Additional unrelated content included due to the reporting software or template will be disregarded without penalty as long as it is possible to easily identify the elements that are requested section 3.7.

You must present your report as an **A4 PDF** which does not include active scripting or other dynamic content. No other format will be accepted.

3.9 Tasks (145 marks)

ID	Task	Marks
1	Assess each of the 5 vulnerabilities. Your documentation for each valid issue should include: • A technical description of the issue, including risk rating & analysis • Reproduction instructions • Supporting evidence (e.g. screenshots or code output with the relevant part clearly marked) • Recommendations or remedial action. Your documentation for each false positive issue should include: • A description of the testing that occurred. • Supporting evidence (e.g. screenshots or code output with the relevant part clearly marked). It is accepted that it is not always possible to prove a negative, but take reasonable steps to show why you believe the issue has been reported falsely by the automated tooling. Zenicarna have asked that this part of the report is specific to their systems, and remedial action specific to their environment. In other words, they will not be satisfied with a report solely comprising a generic 'copy and paste' of vulnerability scanner or tool output with no contextualised examples and explanation. In addition, they will not be satisfied with recommendation examples that do not apply to their environment, for example due to a mismatched operating system or server software; you should aim to ensure that the report reproduction instructions are actionable, as far as is reasonably possible, within the constraints of their specific environment. For example, providing remediation instructions specific to a UNIX operating system would be of no benefit to Zenicarna.	100 Marks
2	Provide a technical summary of your findings, intended for Zenicarna's Global Application Development Director, who has a technical background and is responsible for the overall delivery of all application in the business. This must include a table of each of the tested issues, showing whether the issue is a false positive or not, and should explain any underlying root causes if any vulnerabilities is valid. She is very keen to understand the effect of the vulnerabilities and, if possible, how and why they occurred including the likelihood they'll be exploited. **Simply duplicating the answers to task 1 will not attract high marks.**	20 marks

ID	Task	Marks
3	Provide a management summary (an executive summary) of your findings. This summary is intended for Zenicarna's Head of Compliance (HOC). The HOC would like to understand the strategic themes and requires the technical findings to be translated into business risk. In particular, she would like to understand the extent to which the vulnerabilities would allow for the data inside the application to be stolen or manipulated. She is not a technical specialist and is very keen that the entire report is contextualised to Zenicarna's situation. **Simply duplicating the answers to tasks 1 & 2 will not attract high marks.**	25 marks

3.10 Report Deliverables (5 marks)

This section provides an example of the report format that is required. You are free to use any reporting software or adjuncts provided that the output is generated in the format and structure below. Key requirements for the report include:

- The report must contain page numbers.
- The author must be named on the report.
- There must be clear sections that relate to the tasks and deliverables in Section 3.7.
- There must be a table which allows the documentation for each vulnerability to be clearly identified. This can be by using a unique section number or a page number, but it must be possible to quickly and intuitively cross-reference or find specific vulnerabilities.
- It must be exported in PDF format and uploaded to **\\crestanswers\Scenario** before the end of the examination as **scenario.pdf**. It cannot be dynamic (i.e. it cannot include or rely on active scripting).

Application Sample Scenario

An example of the report structure required is shown below. Note that the spacing between each of the sections **is not indicative of the level of detail or length of answer required**:

Page 1 of 2 Candidate Name

Contents

Management Summary.....1
Technical Summary.....1
Vulnerabilities.....2

Management Summary

Answer here.

Technical Summary

Answer here.

ID	Name	Rating	Status	Page
			RESOLVED	2
			UNRESOLVED	2
				2
				2
				2

Application Sample Scenario

 Candidate Name

Vulnerability 1 Name

Vulnerability 2 Name

Vulnerability 3 Name

Vulnerability 4 Name

Vulnerability 5 Name