THAGHARAT

شركة صائد الثغرات

Penetration Test Report

Web application and API penetration test of the customer portal

Prepared for	Example Trading Company
Report date	27 October 2026
Version	1.1
Reference	TH-2026-000
Statement of Work	TH-2026-000, 3 September 2026

SAMPLE REPORT. The client, the systems and the findings in it are fictional.

This sample shows the report that every Thagharat client receives. Example Trading Company does not exist: its systems and the findings were written for this sample, and the names of people are left out.

شركة صائد الثغرات · CR 7055275007 · Riyadh · info@thagharat.com

SAMPLE

Document control

Version	Date	Description	Author
1.0	20 September 2026	Final report	Engagement lead
1.1	27 October 2026	Retest results added (section 7)	Engagement lead

Distribution

Name	Organisation	Role
Named in the client's copy	Example Trading Company	Head of Information Technology
Named in the client's copy	شركة صائد الثغرات	Engagement lead

Engagement team

Name	Role	Qualifications
Named in the client's copy	Engagement lead	Listed in the client's copy
Named in the client's copy	Tester	Listed in the client's copy

Delivery	Delivered through the client's secure file portal on 27 October 2026. The password was given separately to the Head of Information Technology by phone. A spreadsheet of the findings is delivered with this report for your ticketing system.
Quality review	Reviewed by a reviewer named in the client's copy, who did not carry out the testing, on 26 October 2026.
Handling	This report describes weaknesses in your systems. Share it only with people who need it to fix them or to assess compliance, and keep it encrypted. Thagharat destroys its engagement data 30 days after issuing the closure letter.
Contact	Thagharat engagement lead, info@thagharat.com, +966 50 601 6914

SAMPLE

Contents

Document control 2

1. Executive summary 4

2. Scope and approach 5

3. Findings summary 5

4. Detailed findings 6

TH-01 Any customer can download every other customer's invoice 6

TH-02 Password reset emails can carry a link to an attacker's site 7

TH-03 The sign-in accepts unlimited password guesses 9

TH-04 A crafted link runs an attacker's script inside the portal 10

TH-05 Any customer can list the staff accounts, with email addresses and roles 11

TH-06 Signing out does not end the session on the server 13

TH-07 Browser security headers are missing 14

5. Remediation roadmap 16

6. Compliance mapping 16

7. Retest results 16

8. Next steps 17

Appendix A. Risk ratings 18

Appendix B. Testing timeline 19

Appendix C. Test coverage 19

SAMPLE

1. Executive summary

Example Trading Company engaged Thagharat to test its customer portal and the API behind it between 13 September 2026 and 15 September 2026, to assess the security of the portal and of the personal data it holds. Testing followed the agreed scope and rules of engagement under Statement of Work TH-2026-000.

Overall risk	**Critical**: any customer could download every other customer's invoice, with names, addresses and mobile numbers (TH-01).
Retest results	Fixed: 4 · Partially fixed: 1 · Not fixed: 1 · Risk accepted: 1 (section 7)

Findings at a glance

Risk	Number of findings
Critical	1
High	2
Medium	2
Low	1
Informational	1
Total	7



Main risks

- Any customer can download every other customer's invoice by changing a number in the address. Each invoice shows a name, an address, a mobile number and what was bought (TH-01).
- An attacker can take over an account, a staff account included, in two ways: when its owner clicks a password reset link that the portal itself sends (TH-02), or by guessing the password with no limit on attempts (TH-03).
- A link sent to a signed-in customer runs the attacker's script inside the portal, where it acts as that customer (TH-04).

What to fix first

- Check on the server that an invoice belongs to the signed-in customer before returning it (TH-01).
- Build password reset links from a fixed address, and limit sign-in attempts for each account and each source address (TH-02, TH-03).
- Encode the search text before showing it, and restrict the staff list to staff (TH-04, TH-05).

What is working well

- All traffic uses HTTPS with a modern TLS configuration, and plain HTTP is redirected to it.
- Orders are protected: a customer could not read or change another customer's order.
- The payment step never handles card numbers inside the portal: it hands over to the page hosted by the payment provider.
- Malformed input produced no database or server error messages, and no SQL injection was found in any input that was tested.

SAMPLE

2. Scope and approach

#	Target	Type	Environment
1	https://portal.example.com	Web application	Production
2	https://api.example.com	API	Production

Out of scope	The payment page hosted by the payment provider, and tests of availability.
Testing window	13 to 15 September 2026, 09:00 to 17:00
Source IP addresses	203.0.113.24
Approach	Grey box; test accounts: two customer accounts and one staff account, created by Example Trading Company for the test

Method

Web testing followed the OWASP WSTG, and mobile testing followed OWASP MASVS and MASTG. The test followed the four phases of NIST SP 800-115: planning, discovery, attack and reporting. Thagharat uses AI tools that run on its own hardware to help map the attack surface, sort scan output and review code. A tester confirmed every finding in this report.

Limitations

This is a point-in-time assessment of the systems in scope during the testing window. It does not guarantee that every vulnerability was found or that the systems are secure. The staff account arrived on the second day, so the staff area was tested on 14 and 15 September only.

3. Findings summary

ID	Finding	Risk	CVSS	Asset	Status
TH-01	Any customer can download every other customer's invoice	Critical	6.5	Portal API	Fixed
TH-02	Password reset emails can carry a link to an attacker's site	High	8.1	Portal API	Fixed
TH-03	The sign-in accepts unlimited password guesses	High	7.4	Portal API	Partially fixed
TH-04	A crafted link runs an attacker's script inside the portal	Medium	6.1	Portal	Fixed
TH-05	Any customer can list the staff accounts, with email addresses and roles	Medium	4.3	Portal API	Fixed
TH-06	Signing out does not end the session on the server	Low	4.8	Portal API	Risk accepted
TH-07	Browser security headers are missing	Informational	0.0	Portal	Not fixed

SAMPLE

4. Detailed findings

TH-01 Any customer can download every other customer's invoice

Risk	**Critical**: likelihood High, business impact High (Appendix A)
CVSS 3.1	6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
Likelihood	High: needs only a customer account, which anyone can create, and invoice numbers run in sequence.
Business impact	High: exposes the name, address, mobile number and purchases of every customer, which is personal data at scale.
Affected asset	https://api.example.com/v1/invoices/{number}/pdf
Category	OWASP Top 10 2025 A01: Broken Access Control; OWASP API Security Top 10 2023 API1: Broken Object Level Authorization; CWE-639
Found on	13 September 2026
Fix effort	Low
Status	**Fixed**

Description

The invoice endpoint returns the PDF of any invoice whose number is in the address. It checks that the request carries a valid session, but not that the invoice belongs to the signed-in customer. Invoice numbers run in sequence, so the next customer's invoice is one number away.

Impact

Anyone who registers on the portal can download every invoice the company has issued. Each invoice shows the customer's name, delivery address and mobile number, and what they bought.

This is a disclosure of personal data at scale. It could require notifying the competent authority and the affected customers under the Personal Data Protection Law, and it would damage customers' trust.

The team proved the flaw with its two test accounts only. It did not request the invoice of any real customer.

Steps to reproduce

1. Sign in as test customer A and open one of its invoices. The browser requests `/v1/invoices/104217/pdf`.
2. Send the same request again with the number changed to `104218`, an invoice of test customer B.
3. The response is the invoice of test customer B.

Evidence

```
GET /v1/invoices/104218/pdf HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 200 OK
Content-Type: application/pdf
Content-Disposition: attachment; filename="invoice-104218.pdf"
```

The file returned is the invoice of test customer B. Both accounts were created for this test.

Recommendation

Before returning an invoice, check on the server that it belongs to the signed-in customer. Answer `404` both for an invoice that does not exist and for one that belongs to someone else, so that the answer does not reveal which

numbers are in use.

- Apply the same check to every address that takes the number of an invoice, an order or a customer.
- Add an automated test that requests another account's invoice and expects `404`.
- Because the flaw was live, review the access logs for accounts that requested many invoice numbers.

References

- OWASP API Security Top 10 2023, API1 Broken Object Level Authorization: https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- OWASP Insecure Direct Object Reference Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
- CWE-639: https://cwe.mitre.org/data/definitions/639.html

Compliance mapping

- PDPL: Article 19 (protecting personal data)
- NCA ECC: 2-2, 2-15 (identity and access management; web application security)
- ISO 27001: A.8.3 (information access restriction)

TH-02 Password reset emails can carry a link to an attacker's site

Risk	**High**: likelihood Medium, business impact High (Appendix A)
CVSS 3.1	8.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)
Likelihood	Medium: needs no account, but the victim must click the link in the email, which comes from the portal's own address.
Business impact	High: gives control of any account whose owner clicks, staff accounts included, and one staff account can read every customer's orders.
Affected asset	https://api.example.com/v1/auth/password-reset
Category	OWASP Top 10 2025 A07: Authentication Failures; OWASP API Security Top 10 2023 API2: Broken Authentication; CWE-640
Found on	14 September 2026
Fix effort	Low
Status	**Fixed**

Description

When someone asks for a password reset, the portal emails a link to the address of the account. It builds that link from the `X-Forwarded-Host` header of the request instead of its own fixed address. An attacker who asks for a reset of someone else's account can therefore choose the site the link points to.

The email is genuine: it comes from the portal, and the link carries the real reset token.

Impact

If the owner of the account clicks the link, the token goes to the attacker's site. The attacker then sets a new password and controls the account.

For a customer, this exposes their orders and invoices. For a member of staff, it exposes every customer's orders and contact details, which is personal data at scale under the Personal Data Protection Law.

Steps to reproduce

1. Ask for a password reset for test customer B, adding the header `X-Forwarded-Host: attacker.example` to the request.
2. Open the email that arrives in the mailbox of test customer B. The reset link points to `attacker.example`.
3. Take the token from that link and send it to `/v1/auth/password-reset/confirm` with a new password. The password of test customer B changes.

Evidence

```
POST /v1/auth/password-reset HTTP/1.1
Host: api.example.com
X-Forwarded-Host: attacker.example
Content-Type: application/json

{"email": "customer-b@example.com"}

HTTP/1.1 202 Accepted
```

The link in the email that test customer B received:

```
https://attacker.example/reset?token=(removed, ending 7d2e)
```

Recommendation

Build the reset link from a fixed address in the server's configuration, never from a header of the request.

- Refuse any request whose `Host` or `X-Forwarded-Host` header is not one of the portal's own names.
- Keep reset tokens short-lived and usable once.
- Add an automated test that sends a forged `X-Forwarded-Host` header and expects the link to keep the portal's address.

References

- PortSwigger Web Security Academy, Password reset poisoning: https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning
- OWASP Forgot Password Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html
- CWE-640: https://cwe.mitre.org/data/definitions/640.html

Compliance mapping

- PDPL: Article 19 (protecting personal data)
- NCA ECC: 2-2, 2-15 (identity and access management; web application security)
- ISO 27001: A.8.5 (secure authentication)

SAMPLE

TH-03 The sign-in accepts unlimited password guesses

Risk	**High**: likelihood Medium, business impact High (Appendix A)
CVSS 3.1	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
Likelihood	Medium: needs no account, but works only against accounts with a guessable password, which the six-character minimum allows.
Business impact	High: staff sign in through the same form, and one staff account can read every customer's orders and contact details.
Affected asset	https://api.example.com/v1/auth/login
Category	OWASP Top 10 2025 A07: Authentication Failures; OWASP API Security Top 10 2023 API2: Broken Authentication; CWE-307
Found on	13 September 2026
Fix effort	Medium
Status	**Partially fixed**

Description

The sign-in endpoint answers every attempt at once, however many have failed before. There is no delay, no temporary lock and no extra check after repeated failures, either for the account or for the address the attempts come from.

The portal also accepts passwords of six characters and does not compare them with lists of common passwords.

Impact

An attacker can try thousands of common passwords against any account. The team sent 5,000 attempts in under four minutes against its own test account without being slowed, and found the weak password it had set for the test.

Accounts with weak passwords will fall, and staff accounts use the same form. Together with TH-05, which gives an attacker the email addresses of the staff, this is a direct path to a staff account.

Steps to reproduce

1. Use the email address of test customer A, whose password was set to a common six-character word for this test.
2. Send 5,000 sign-in requests to `/v1/auth/login`, each with a different password from a public list.
3. Every wrong attempt is answered `401` in about 40 milliseconds. No attempt is refused or delayed, and the correct password is answered `200`.

Evidence

```
POST /v1/auth/login HTTP/1.1
Host: api.example.com
Content-Type: application/json

{"email": "customer-a@example.com", "password": "(guess 1 to 5,000)"}

Attempts sent           5,000 in 3 minutes 41 seconds
Answered 401            4,999
Answered 200            1 (attempt 3,112)
Answered 429 or locked  0
```

Recommendation

Limit failed sign-ins for each account and for each source address. For example, slow the answers after five failures, lock the account for 15 minutes after ten, and tell its owner by email.

- Apply the limit in the API itself, so that it covers every application that signs in through it.
- Require passwords of at least 12 characters, and refuse those found in lists of common or leaked passwords.
- Offer a second factor to customers and require it for staff.
- Verify by repeating the steps above and expecting the account to lock.

References

- OWASP Authentication Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- OWASP API Security Top 10 2023, API2 Broken Authentication: https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
- CWE-307: https://cwe.mitre.org/data/definitions/307.html

Compliance mapping

- PDPL: Article 19 (protecting personal data)
- NCA ECC: 2-2, 2-15 (identity and access management; web application security)
- ISO 27001: A.8.5 (secure authentication)

TH-04 A crafted link runs an attacker's script inside the portal

Risk	**Medium**: likelihood Medium, business impact Medium (Appendix A)
CVSS 3.1	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Likelihood	Medium: a signed-in customer must open a link that the attacker sends.
Business impact	Medium: the script acts as that one customer: it can read their orders and invoices and change their details.
Affected asset	https://portal.example.com/orders?search=
Category	OWASP Top 10 2025 A05: Injection; CWE-79
Found on	14 September 2026
Fix effort	Low
Status	**Fixed**

Description

The order search page shows the search text back to the user without encoding it. Text that contains HTML is therefore treated as part of the page, and a script inside it runs in the visitor's browser with the portal's own rights.

Impact

An attacker sends a customer a link to the real portal, with a script in the search text. If the customer is signed in and opens it, the script can read the sign-in token that the portal keeps in the browser and send it to the attacker. The attacker can then use the account until the token expires: read the customer's orders and invoices, and change their details.

TH-06 makes this worse, because signing out does not cancel the token. The page exists only in the customer area, so staff accounts are not exposed through it.

Steps to reproduce

1. Sign in as test customer A.
2. Open `https://portal.example.com/orders?search=<img src=x onerror=alert(document.domain)>`.
3. The page shows a dialog with `portal.example.com`, which means the script ran inside the portal.

Evidence

```
GET /orders?search=%3Cimg%20src%3Dx%20onerror%3Dalert(document.domain)%3E HTTP/1.1
Host: portal.example.com

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

<p class="results-title">Results for <img src=x onerror=alert(document.domain)></p>
```

Recommendation

Encode the search text for HTML before writing it into the page: use the automatic escaping of the template engine, and remove the unescaped output on this page.

- Search the code for other places that write values from the request without encoding them.
- Add a Content Security Policy that forbids inline scripts, as a second layer (TH-07).
- Add an automated test that requests the page with `<script>` in the search text and expects it to come back encoded.

References

- OWASP Cross Site Scripting Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
- CWE-79: https://cwe.mitre.org/data/definitions/79.html

Compliance mapping

- PDPL: Article 19 (protecting personal data)
- NCA ECC: 2-15 (web application security)
- ISO 27001: A.8.28 (secure coding)

TH-05 Any customer can list the staff accounts, with email addresses and roles

Risk	**Medium**: likelihood High, business impact Low (Appendix A)
CVSS 3.1	4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
Likelihood	High: needs only a customer account, which anyone can create, and one request.
Business impact	Low: discloses the names, work email addresses and roles of staff: no customer data, but it tells an attacker whom to target.
Affected asset	https://api.example.com/v1/staff
Category	OWASP Top 10 2025 A01: Broken Access Control; OWASP API Security Top 10 2023 API5: Broken Function Level Authorization; CWE-862
Found on	14 September 2026
Fix effort	Low
Status	**Fixed**

SAMPLE

Description

The staff directory endpoint is meant for the staff area, but it answers any signed-in account. A customer who requests it receives the name, work email address and role of every member of staff.

Impact

The list holds no customer data. Its value to an attacker is in what it makes possible: it names the accounts worth attacking and shows which of them are administrators.

It makes TH-03 and TH-02 practical against staff, and it helps an attacker write convincing phishing emails to them.

Steps to reproduce

1. Sign in as test customer A and copy the token from any request to the API.
2. Request `/v1/staff` with that token.
3. The response lists every staff account.

Evidence

```
GET /v1/staff HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 200 OK
Content-Type: application/json

{"staff": [
  {"name": "(removed)", "email": "(removed)", "role": "admin"},
  {"name": "(removed)", "email": "(removed)", "role": "support"},
  (9 more accounts)
]}
```

Recommendation

Require the staff role on `/v1/staff` and on every other address of the staff area, and check it on the server for each request.

- Review the addresses of the API against the roles allowed to call them.
- Add an automated test that calls each staff address with a customer's token and expects `403`.

References

- OWASP API Security Top 10 2023, API5 Broken Function Level Authorization: https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/
- CWE-862: https://cwe.mitre.org/data/definitions/862.html

Compliance mapping

- PDPL: Article 19 (protecting personal data)
- NCA ECC: 2-2 (identity and access management)
- ISO 27001: A.8.3 (information access restriction)

TH-06 Signing out does not end the session on the server

Risk	**Low**: likelihood Low, business impact Medium (Appendix A)
CVSS 3.1	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
Likelihood	Low: the attacker must first obtain a user's token, through another weakness or from the user's device.
Business impact	Medium: gives the use of one account for up to 12 hours after its owner signed out.
Affected asset	https://api.example.com/v1/auth/logout
Category	OWASP Top 10 2025 A07: Authentication Failures; CWE-613
Found on	15 September 2026
Fix effort	Medium
Status	**Risk accepted**

Description

When a user signs out, the web application deletes the sign-in token from the browser, but the server keeps accepting that token until it expires, 12 hours after it was issued. Changing the password does not cancel earlier tokens either.

Impact

A token that has been copied stays usable after its owner signs out or changes their password, so neither step locks an attacker out. A token can be copied by a script in the page (TH-04), from a shared computer or from the logs of a proxy.

The finding gives no access on its own, which is why its likelihood is low.

Steps to reproduce

1. Sign in as test customer A and note the token in the `Authorization` header.
2. Sign out in the web application.
3. Send `GET /v1/orders` with the token you noted. The server still answers `200` with the customer's orders.

Evidence

```
POST /v1/auth/logout HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 204 No Content


GET /v1/orders HTTP/1.1
Host: api.example.com
Authorization: Bearer (the same token, after signing out)

HTTP/1.1 200 OK
```

Recommendation

Keep a record on the server of the tokens that were cancelled, or of the session behind each token, and refuse a token once its user signs out or changes their password.

- Shorten the life of the token to 30 minutes or less, and renew it with a refresh token that the server can cancel.
- Verify by repeating the three steps above and expecting `401`.

SAMPLE

References

- OWASP Session Management Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
- CWE-613: https://cwe.mitre.org/data/definitions/613.html

Compliance mapping

- NCA ECC: 2-15 (web application security)
- ISO 27001: A.8.5 (secure authentication)

TH-07 Browser security headers are missing

Risk	**Informational**: likelihood Low, business impact Low (Appendix A)
CVSS 3.1	0.0
Likelihood	Low: another weakness is needed first: missing headers cannot be attacked on their own.
Business impact	Low: no direct harm: the headers would limit the damage of other weaknesses, such as TH-04.
Affected asset	https://portal.example.com
Category	OWASP Top 10 2025 A02: Security Misconfiguration; CWE-693
Found on	13 September 2026
Fix effort	Low
Status	**Not fixed**

Description

The portal's responses do not set three headers that ask browsers to apply extra protection: `Content-Security-Policy`, `X-Content-Type-Options` and `Referrer-Policy`.

The portal does send `Strict-Transport-Security`, which is good.

Impact

There is no direct impact. With a Content Security Policy in place, a weakness such as TH-04 is much harder to turn into a working attack, so the headers are an inexpensive second layer.

Steps to reproduce

1. Request `https://portal.example.com/` and read the headers of the response.
2. `Content-Security-Policy`, `X-Content-Type-Options` and `Referrer-Policy` are absent.

Evidence

```
GET / HTTP/1.1
Host: portal.example.com

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cache-Control: no-store
```

SAMPLE

Recommendation

Send `X-Content-Type-Options: nosniff` and `Referrer-Policy: strict-origin-when-cross-origin` with every response.

- Introduce a Content Security Policy in report-only mode first, remove inline scripts as the reports show them, then enforce the policy.
- Verify with the browser's developer tools that every page carries the three headers.

References

- OWASP HTTP Security Response Headers Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html
- OWASP Secure Headers Project: https://owasp.org/www-project-secure-headers/

Compliance mapping

- NCA ECC: 2-15 (web application security)
- ISO 27001: A.8.9 (configuration management)

SAMPLE

5. Remediation roadmap

Priority	Findings	Suggested timeframe	Owner
Immediately	TH-01	Within 7 days	Development team
Next	TH-02, TH-03	Within 30 days	Development team
Planned	TH-04, TH-05	Within 90 days	Development team
Routine	TH-06, TH-07	Next release cycle	Development team, Infrastructure team

6. Compliance mapping

The table shows which controls each finding affects in the frameworks you report against. It is evidence for your compliance team, not an audit opinion or a certification.

Finding	PDPL	NCA ECC	ISO 27001
TH-01	Article 19	2-2, 2-15	A.8.3
TH-02	Article 19	2-2, 2-15	A.8.5
TH-03	Article 19	2-2, 2-15	A.8.5
TH-04	Article 19	2-15	A.8.28
TH-05	Article 19	2-2	A.8.3
TH-06	-	2-15	A.8.5
TH-07	-	2-15	A.8.9

7. Retest results

ID	Finding	Status on retest	Retest date	Notes
TH-01	Any customer can download every other customer's invoice	**Fixed**	25 October 2026	The endpoint now answers `404` for an invoice of another account. Tested with both test accounts.
TH-02	Password reset emails can carry a link to an attacker's site	**Fixed**	25 October 2026	The link now always carries the portal's own address, and a forged header is ignored.
TH-03	The sign-in accepts unlimited password guesses	**Partially fixed**	25 October 2026	The limit works on `/v1/auth/login`: the account locked after ten failures. The older address `/v1/login`, which the mobile site still calls, accepted 1,000 guesses with no limit.
TH-04	A crafted link runs an attacker's script inside the portal	**Fixed**	25 October 2026	The search text is now encoded, and the test strings appear as plain text.
TH-05	Any customer can list the staff accounts, with email addresses and roles	**Fixed**	25 October 2026	The endpoint now answers `403` to customer accounts.

SAMPLE

ID	Finding	Status on retest	Retest date	Notes
TH-06	Signing out does not end the session on the server	**Risk accepted**	25 October 2026	The client shortened the life of the token from 12 hours to 30 minutes, and decided in writing on 20 October 2026 to accept the remaining risk until it replaces the sign-in component.
TH-07	Browser security headers are missing	**Not fixed**	25 October 2026	The three headers were still absent. The client plans to add them in its next front-end release.

8. Next steps

- Closure letter: issued with this version of the report. It records the status of each finding on the retest date.
- Still open: TH-03 is partially fixed and TH-07 is not fixed. The retest results say what remains for each.
- Engagement data: Thagharat destroys it 30 days after issuing the closure letter and confirms the destruction in writing.

SAMPLE

Appendix A. Risk ratings

Each finding's risk combines the likelihood of exploitation with the impact on your business, as in the OWASP Risk Rating Methodology. The CVSS base score, in the version set in the Statement of Work, is given alongside it as a standard technical measure. The two can differ: CVSS rates the weakness itself, while the risk rating reflects your data and systems. The risk rating sets the order of the findings and the priorities in the remediation roadmap.

Likelihood	Meaning
High	Can be exploited remotely without credentials, or with an account anyone can create; little skill or effort is needed.
Medium	Needs a valid account, specific knowledge, user interaction or some effort.
Low	Needs privileged or local access, unusual conditions, or other weaknesses to be exploited first.

Business impact	Meaning
High	Exposure or change of sensitive data or of personal data at scale, control of critical systems or administrator accounts, or serious financial, legal or reputational harm.
Medium	Limited exposure of personal or internal data, control of an ordinary user's account or part of a system, or disruption of a non-critical service.
Low	Minor information disclosure, or a weakness that makes other attacks easier without direct harm.

Business impact / Likelihood	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Informational	Low	Medium

CVSS base score	Rating
9.0 to 10.0	Critical
7.0 to 8.9	High
4.0 to 6.9	Medium
0.1 to 3.9	Low
0.0	None

Informational findings have no direct security impact, for example a missing hardening measure, and their CVSS score is 0.0.

Critical findings are reported to your escalation contact within 24 hours of confirmation, before this report. By default, a finding is critical if its risk rating is Critical or its CVSS base score is 9.0 or higher; the Statement of Work may set another threshold.

Appendix B. Testing timeline

Date	Activity
10 September 2026	Kick-off meeting
13 September 2026	Testing started
13 September 2026, 13:15	Critical finding TH-01 reported to escalation contact
15 September 2026	Testing ended
20 September 2026	Report delivered
22 September 2026	Readout session
25 October 2026	Retest
27 October 2026	Report version 1.1 and closure letter delivered

Appendix C. Test coverage

Area (OWASP WSTG)	Tested	Findings
Information gathering (WSTG-INFO)	Yes	None
Configuration and deployment (WSTG-CONF)	Yes	TH-07
Identity management (WSTG-IDNT)	Yes	None
Authentication (WSTG-ATHN)	Yes	TH-02, TH-03
Authorisation (WSTG-ATHZ)	Yes	TH-01, TH-05
Session management (WSTG-SESS)	Yes	TH-06
Input validation (WSTG-INPV)	Yes	TH-04
Error handling (WSTG-ERRH)	Yes	None
Cryptography (WSTG-CRYP)	Yes	None
Business logic (WSTG-BUSL)	Yes	None
Client side (WSTG-CLNT)	Yes	TH-04
APIs (WSTG-APIT)	Yes	None

SAMPLE