

XYZ Corporation Vulnerability Assessment & Penetration Testing (VAPT) Report

SAMPLE DELIVERABLE — FOR DEMONSTRATION PURPOSES ONLY



Prepared For	XYZ Corporation
Prepared By	Vaptora Security Services
Report Reference	VAP-2026-0731-XYZ
Assessment Dates	07 – 21 July 2026
Report Date	5-Aug-26
Classification	Confidential — Sample Report



Document Control

Revision History

Version	Date	Author	Description
1.0	22 Jul 2026	Vaptora Security Services	Initial draft for internal QA review
1.1	28 Jul 2026	Vaptora Security Services	Findings validated; remediation guidance added
2.0	05 Aug 2026	Vaptora Security Services	Final sample report for public distribution

Distribution List

Name / Role	Organization	Purpose
Lead Penetration Tester	Vaptora Security Services	Report author
Engagement Manager	Vaptora Security Services	Quality review & sign-off
Chief Information Security Officer	XYZ Corporation	Primary recipient

Classification

This document is classified CONFIDENTIAL. All content, including the organization name, personnel, domains, and technical findings, is entirely fictitious and created solely to demonstrate Vaptora's reporting format and quality. It does not describe any real assessment, system, or vulnerability.

Table of Contents

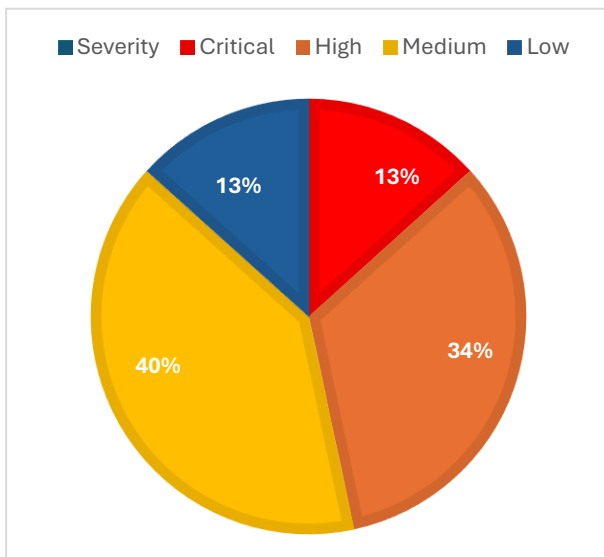
1.Executive Summary	4
1.1 Assessment Scope	5
1.2 Methodology	6
1.3 Tools Used	6
1.4 Risk Rating Methodology (CVSS v3.1)	7
1.5 Identified Findings and Risk Levels	8
2. Vulnerabilities	9
F-01 — SQL Injection – Authentication Bypass	9
F-02 — Unrestricted File Upload leading to Remote Code Execution	10
F-03 — Broken Access Control – Insecure Direct Object Reference (IDOR)	11
F-04 — Server-Side Request Forgery (SSRF).....	12
F-05 — Stored Cross-Site Scripting (XSS).....	13
F-06 — Privilege Escalation via Role Parameter Tampering	14
F-07 — Weak Authentication – Missing Account Lockout / Brute-Force Protection.....	15
F-08 — Reflected Cross-Site Scripting (XSS)	16
F-09 — Cross-Site Request Forgery (CSRF).....	17
F-10 — Sensitive Data Exposure via Verbose Error Messages	18
F-11 — Security Misconfiguration – Directory Listing Enabled	19
F-12 — Session Management Weaknesses (No Session Expiry)	20
F-13 — Use of Outdated and Vulnerable Components.....	21
F-14 — Open Redirect	22
F-15 — Missing Security Headers.....	23
3. Remediation Recommendations.....	24
Strategic Recommendations	24
Conclusion	25

1.Executive Summary

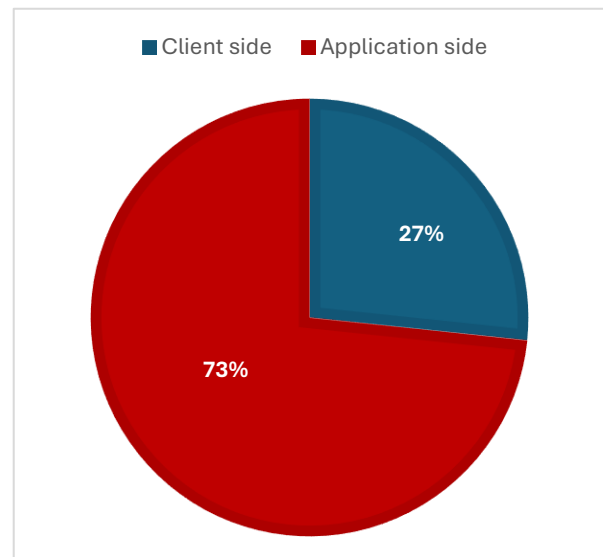
Vaptora Security Services performed a black-box and gray-box Web Application Penetration Test of XYZ Corporation's customer-facing portal and supporting API between 07 and 21 July 2026. The objective was to identify exploitable security weaknesses across the application's authentication, authorization, input-handling, and configuration layers before they could be leveraged by a malicious actor.

Testing identified a total of 15 findings spanning Critical, High, Medium, and Low severity. Two Critical-severity issues — a SQL injection flaw enabling authentication bypass and an unrestricted file-upload vulnerability enabling remote code execution — present an immediate and severe risk to the confidentiality, integrity, and availability of the platform and should be remediated as a priority.

Findings by severity



Affected Components



Key Recommendations

- Remediate both Critical findings (F-01, F-02) within 7 days; consider taking the affected upload feature offline until fixed.
- Address all High-severity findings within 30 days, prioritizing access-control and authentication weaknesses.
- Establish parameterized-query and output-encoding standards as part of the secure software development lifecycle (SSDLC).
- Introduce routine dependency scanning and a patch-management cadence to prevent recurrence of outdated-component issues.
- Conduct a retest following remediation to validate fixes before the next production release.

1.1 Assessment Scope

Inscope

Asset	Description
portal.xyzcorp.com	Customer-facing web application (authenticated + unauthenticated areas)
api.xyzcorp.com	REST API backing the web and mobile clients
Admin Console	Internal administrative interface (gray-box, low-privilege account supplied)

Out of Scope

- Physical security testing of client premises
- Denial-of-Service (DoS/DDoS) testing
- Third-party services not owned or operated by XYZ Corporation
- Social engineering of client personnel

Testing Type

Gray-box assessment combining unauthenticated reconnaissance with authenticated testing using two low-privilege test accounts provided by XYZ Corporation.

1.2 Methodology

The assessment followed a structured methodology aligned with the OWASP Testing Guide (v4.2), the OWASP Application Security Verification Standard (ASVS), the Penetration Testing Execution Standard (PTES), and NIST SP 800-115.

Phases

- **Planning & Reconnaissance** — scope confirmation, passive/active information gathering, technology fingerprinting
- **Vulnerability Discovery** — automated scanning combined with manual analysis of business logic
- **Exploitation** — controlled, non-destructive validation of identified weaknesses
- **Post-Exploitation** — impact analysis and, where safe, demonstration of chained attack paths
- **Reporting** — consolidation of findings, risk rating, and remediation guidance

1.3 Tools Used

Tool	Purpose
Burp Suite Professional	Web proxy, manual request manipulation, active/passive scanning
OWASP ZAP	Automated vulnerability scanning and fuzzing
Nmap	Network and service discovery
SQLmap	SQL injection detection and validation
Nikto	Web server misconfiguration scanning
Nessus	Infrastructure vulnerability scanning
Gobuster	Directory / endpoint enumeration
testssl.sh	TLS/SSL configuration review
Postman	API request crafting and testing

1.4 Risk Rating Methodology (CVSS v3.1)

Each finding is scored using the Common Vulnerability Scoring System version 3.1 (CVSS v3.1), an industry-standard framework maintained by FIRST.org for rating the severity of security vulnerabilities. The base score (0.0 – 10.0) reflects exploitability and impact, and is mapped to a qualitative severity rating as follows:

Severity	CVSS Score Range	Description
Critical	9.0 – 10.0	Immediate risk of full system or data compromise; exploit is typically trivial.
High	7.0 – 8.9	Significant risk requiring prompt remediation; exploitation likely with moderate effort.
Medium	4.0 – 6.9	Moderate risk; exploitation may require specific conditions or user interaction.
Low	0.1 – 3.9	Limited risk; exploitation has minimal impact or requires significant effort.
Informational	0.0	No direct risk; observation provided for best-practice hardening.

1.5 Identified Findings and Risk Levels

The table below lists all 15 findings identified during the engagement, ordered by severity (Critical first).

#	Findings	Severity	CVSS	Status
F-01	SQL Injection – Authentication Bypass	Critical	9.8	Open
F-02	Unrestricted File Upload leading to Remote Code Execution	Critical	9.8	Open
F-03	Broken Access Control – Insecure Direct Object Reference (IDOR)	High	8.1	Open
F-04	Server-Side Request Forgery (SSRF)	High	8.6	Open
F-05	Stored Cross-Site Scripting (XSS)	High	8.2	Open
F-06	Privilege Escalation via Role Parameter Tampering	High	8.8	Open
F-07	Weak Authentication – Missing Account Lockout / Brute-Force Protection	High	7.5	Open
F-08	Reflected Cross-Site Scripting (XSS)	Medium	6.1	Open
F-09	Cross-Site Request Forgery (CSRF)	Medium	6.5	Open
F-10	Sensitive Data Exposure via Verbose Error Messages	Medium	5.3	Open
F-11	Security Misconfiguration – Directory Listing Enabled	Medium	5.3	Open
F-12	Session Management Weaknesses (No Session Expiry)	Medium	6.5	Open
F-13	Use of Outdated and Vulnerable Components	Medium	5.9	Open
F-14	Open Redirect	Low	4.3	Open
F-15	Missing Security Headers	Low	3.1	Open

2. Vulnerabilities

F-01 — SQL Injection – Authentication Bypass

Severity	Critical
CVSS Score	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE ID	CWE-89
OWASP Top 10 Mapping	A03:2021 – Injection
Status	Open
Affected Assets	https://portal.xyzcorp.com/login (username parameter)
Description	The login form on the customer portal fails to sanitize the "username" parameter before using it in a backend SQL query. An attacker can inject SQL syntax to bypass authentication or extract arbitrary data from the underlying database.
Impact	Full compromise of the application database, including customer records, credentials, and payment metadata. Authentication can be bypassed entirely, allowing account takeover for any user, including administrators.
Remediation	Use parameterized queries / prepared statements for all database access. Apply strict input validation, enforce least-privilege database accounts, and enable a Web Application Firewall (WAF) rule set for SQL injection as a compensating control.
Reference	OWASP: SQL Injection Prevention Cheat Sheet; CWE-89

Evidence:

F-02 — Unrestricted File Upload leading to Remote Code Execution

Severity	Critical
CVSS Score	9.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE ID	CWE-434
OWASP Top 10 Mapping	A04:2021 – Insecure Design
Status	Open
Affected Assets	https://portal.xyzcorp.com/account/documents/upload
Description	The document-upload feature accepts files of any type/extension and stores them in a web-accessible directory without content validation, allowing upload of executable server-side scripts.
Impact	An authenticated attacker can upload a web shell and achieve remote code execution on the application server, leading to full host compromise and lateral movement into internal systems.
Remediation	Restrict uploads to an allow-list of file types, validate file content (magic bytes, not extension), store uploads outside the web root, disable script execution in the upload directory, and enforce file-size limits with antivirus/malware scanning.
Reference	OWASP: File Upload Cheat Sheet; CWE-434

Evidence:

F-03 — Broken Access Control – Insecure Direct Object Reference (IDOR)

Severity	High
CVSS Score	8.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N)
CWE ID	CWE-639
OWASP Top 10 Mapping	A01:2021 – Broken Access Control
Status	Open
Affected Assets	https://api.xyzcorp.com/v1/invoices/{invoiceId}
Description	The invoice API returns records based solely on a sequential, client-supplied "invoiceId" without verifying that the requesting user owns the resource, allowing enumeration of other customers' invoices.
Impact	Unauthorized disclosure of other customers' billing data, names, and addresses; systematic enumeration could expose the entire customer base.
Remediation	Enforce server-side object-level authorization checks on every request, use indirect/non-sequential reference identifiers (UUIDs), and log access-denied attempts for monitoring.
Reference	OWASP Top 10: A01:2021; CWE-639

Evidence:

F-04 — Server-Side Request Forgery (SSRF)

Severity	High
CVSS Score	8.6 (AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N)
CWE ID	CWE-918
OWASP Top 10 Mapping	A10:2021 – Server-Side Request Forgery
Status	Open
Affected Assets	https://api.xyzcorp.com/v1/integrations/webhook-test
Description	The webhook-test utility fetches a user-supplied URL server-side without restricting destination hosts, allowing requests to internal-only endpoints and cloud metadata services.
Impact	An attacker can pivot the application server into the internal network, reach cloud instance-metadata endpoints, and potentially retrieve temporary cloud credentials or access internal management interfaces.
Remediation	Validate and allow-list destination hosts/IP ranges, block requests to link-local and private address ranges, and disable redirect-following for outbound requests initiated on behalf of users.
Reference	OWASP: SSRF Prevention Cheat Sheet; CWE-918

Evidence:

F-05 — Stored Cross-Site Scripting (XSS)

Severity	High
CVSS Score	8.2 (AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:N)
CWE ID	CWE-79
OWASP Top 10 Mapping	A03:2021 – Injection
Status	Open
Affected Assets	https://portal.xyzcorp.com/support/tickets (message field)
Description	User-supplied text in the support-ticket "message" field is stored and later rendered to support agents without output encoding, allowing persistent script injection.
Impact	An attacker can hijack support-agent sessions, perform actions on their behalf (including access to elevated back-office tooling), or deliver malware to internal staff.
Remediation	Apply context-aware output encoding on render, implement a strict Content-Security-Policy, and sanitize rich-text input using an allow-list HTML sanitizer.
Reference	OWASP: XSS Prevention Cheat Sheet; CWE-79

Evidence:

F-06 — Privilege Escalation via Role Parameter Tampering

Severity	High
CVSS Score	8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)
CWE ID	CWE-269
OWASP Top 10 Mapping	A01:2021 – Broken Access Control
Status	Open
Affected Assets	https://api.xyzcorp.com/v1/users/{userId}/profile
Description	The profile-update endpoint accepts a "role" field from the client and applies it without server-side authorization checks, allowing a standard user to elevate their own account to administrator.
Impact	Complete loss of the application's authorization model; a low-privilege user can obtain full administrative control over the platform.
Remediation	Never trust role/permission fields from the client; derive privilege exclusively from server-side session state, and require a secondary approval workflow for any privilege change.
Reference	OWASP Top 10: A01:2021; CWE-269

Evidence:

F-07 — Weak Authentication – Missing Account Lockout / Brute-Force Protection

Severity	High
CVSS Score	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE ID	CWE-307
OWASP Top 10 Mapping	A07:2021 – Identification and Authentication Failures
Status	Open
Affected Assets	https://portal.xyzcorp.com/login
Description	The login endpoint does not enforce account lockout, rate limiting, or CAPTCHA after repeated failed attempts, allowing unlimited password-guessing attempts against any account.
Impact	An attacker can perform automated credential-stuffing or brute-force attacks to compromise user accounts, particularly where weak or reused passwords are in use.
Remediation	Implement progressive account lockout or rate limiting after a small number of failed attempts, add CAPTCHA challenges, and monitor/alert on anomalous authentication patterns.
Reference	OWASP: Credential Stuffing Prevention Cheat Sheet; CWE-307

Evidence:

F-08 — Reflected Cross-Site Scripting (XSS)

Severity	Medium
CVSS Score	6.1 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CWE ID	CWE-79
OWASP Top 10 Mapping	A03:2021 – Injection
Status	Open
Affected Assets	https://portal.xyzcorp.com/search?q=
Description	The search results page reflects the "q" query parameter directly into the HTML response without encoding, allowing script injection via a crafted link.
Impact	An attacker can craft a malicious link that executes JavaScript in a victim's browser session, enabling session-token theft or phishing within a trusted domain.
Remediation	Encode all reflected user input for the output context (HTML, attribute, JS) and deploy a Content-Security-Policy to reduce impact of any missed encoding.
Reference	OWASP: XSS Prevention Cheat Sheet; CWE-79

Evidence:

F-09 — Cross-Site Request Forgery (CSRF)

Severity	Medium
CVSS Score	6.5 (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)
CWE ID	CWE-352
OWASP Top 10 Mapping	A01:2021 – Broken Access Control
Status	Open
Affected Assets	https://portal.xyzcorp.com/account/email/change
Description	The email-change form does not include an anti-CSRF token and relies solely on session cookies, allowing a malicious site to submit the request on a victim's behalf.
Impact	An attacker can change a victim's registered email address and subsequently trigger a password reset, resulting in full account takeover.
Remediation	Implement per-session, per-request anti-CSRF tokens on all state-changing requests and set session cookies with the SameSite=Strict/Lax attribute.
Reference	OWASP: CSRF Prevention Cheat Sheet; CWE-352

Evidence:

F-10 — Sensitive Data Exposure via Verbose Error Messages

Severity	Medium
CVSS Score	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE ID	CWE-209
OWASP Top 10 Mapping	A02:2021 – Cryptographic Failures
Status	Open
Affected Assets	https://api.xyzcorp.com/v1/* (unhandled exception responses)
Description	Unhandled application exceptions return full stack traces, internal file paths, and database driver details to the client instead of a generic error message.
Impact	Disclosure of internal architecture and technology stack details that materially aid an attacker in planning further, more targeted attacks.
Remediation	Return generic, non-descriptive error messages to clients, log detailed errors server-side only, and disable framework debug/verbose-error modes in production.
Reference	OWASP Top 10: A02:2021; CWE-209

Evidence:

F-11 — Security Misconfiguration – Directory Listing Enabled

Severity	Medium
CVSS Score	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE ID	CWE-548
OWASP Top 10 Mapping	A05:2021 – Security Misconfiguration
Status	Open
Affected Assets	https://portal.xyzcorp.com/assets/uploads/
Description	Directory browsing is enabled on the web server, exposing the full file listing of an uploads directory that is not intended to be publicly indexable.
Impact	Disclosure of file names and structure may expose sensitive documents or provide reconnaissance data that assists further attacks.
Remediation	Disable directory listing at the web-server configuration level and apply the principle of least exposure to all static-content directories.
Reference	OWASP: Testing for Directory Listing; CWE-548

Evidence:

F-12 — Session Management Weaknesses (No Session Expiry)

Severity	Medium
CVSS Score	6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CWE ID	CWE-613
OWASP Top 10 Mapping	A07:2021 – Identification and Authentication Failures
Status	Open
Affected Assets	https://portal.xyzcorp.com/ (session cookie)
Description	Session tokens remain valid indefinitely after issuance and are not invalidated on logout, allowing captured session cookies to be reused long after the user's session should have ended.
Impact	A stolen or leaked session token grants an attacker indefinite access to the victim's account, significantly widening the window of exposure for any session-hijacking attack.
Remediation	Enforce both idle and absolute session timeouts, invalidate session tokens server-side on logout, and rotate session identifiers after authentication.
Reference	OWASP: Session Management Cheat Sheet; CWE-613

Evidence:

F-13 — Use of Outdated and Vulnerable Components

Severity	Medium
CVSS Score	5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)
CWE ID	CWE-1104
OWASP Top 10 Mapping	A06:2021 – Vulnerable and Outdated Components
Status	Open
Affected Assets	Web application server – front-end and back-end framework libraries
Description	Several front-end and back-end libraries in use are multiple major versions behind current releases and have publicly disclosed vulnerabilities with available patches.
Impact	Exposure to known, publicly documented exploits that could be used to compromise confidentiality, integrity, or availability of the application without requiring novel research.
Remediation	Establish a routine dependency-patching process, integrate software composition analysis (SCA) into the CI/CD pipeline, and remove unused/unmaintained libraries.
Reference	OWASP Top 10: A06:2021; CWE-1104

Evidence:

F-14 — Open Redirect

Severity	Low
CVSS Score	4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)
CWE ID	CWE-601
OWASP Top 10 Mapping	A01:2021 – Broken Access Control
Status	Open
Affected Assets	https://portal.xyzcorp.com/redirect?url=
Description	The "url" parameter on the redirect handler accepts any external destination without validation, allowing the trusted domain to be used to redirect victims to attacker-controlled sites.
Impact	Facilitates convincing phishing campaigns that abuse the organization's trusted domain to lend credibility to a malicious destination.
Remediation	Validate redirect targets against an allow-list of internal paths/domains, or display an interstitial warning page before redirecting off-site.
Reference	OWASP: Unvalidated Redirects and Forwards Cheat Sheet; CWE-601

Evidence:

F-15 — Missing Security Headers

Severity	Low
CVSS Score	3.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE ID	CWE-693
OWASP Top 10 Mapping	A05:2021 – Security Misconfiguration
Status	Open
Affected Assets	https://portal.xyzcorp.com/* (all responses)
Description	Application responses do not include recommended hardening headers, including Content-Security-Policy, X-Content-Type-Options, X-Frame-Options, and Strict-Transport-Security.
Impact	Absence of these headers removes a layer of browser-enforced defense-in-depth, increasing the impact of otherwise-mitigated client-side issues such as clickjacking or MIME-sniffing attacks.
Remediation	Configure the web server / application framework to send the recommended security headers on every response, and validate configuration with an automated header-scanning tool.
Reference	OWASP Secure Headers Project; CWE-693

Evidence:

3. Remediation Recommendations

Findings should be remediated in priority order based on severity. The following timeframes are recommended as industry best practice in the industry:

Priority	Timeframe	Related Findings
Critical	Immediate (≤ 7 days)	F-01, F-02
High	≤ 30 days	F-03, F-04, F-05, F-06, F-07
Medium	≤ 90 days	F-08, F-09, F-10, F-11, F-12, F-13
Low	Next scheduled release cycle	F-14, F-15

Strategic Recommendations

- Adopt secure coding standards (e.g., OWASP ASVS) and enforce them via mandatory code review.
- Integrate SAST/DAST and software composition analysis (SCA) into the CI/CD pipeline.
- Implement centralized, server-side authorization checks rather than relying on client-side controls.
- Conduct periodic penetration testing (at minimum annually, or after significant releases).
- Provide secure-development training to engineering teams, focused on the OWASP Top 10.

Conclusion

The assessment of XYZ Corporation's web application identified a total of 15 findings, including 2 Critical- and 5 High-severity issues that pose a significant risk if left unaddressed. The presence of an authentication-bypassing SQL injection flaw and an unrestricted file upload vulnerability indicates that foundational input-validation and access-control controls require immediate strengthening.

Vaptora recommends remediating all Critical and High findings on the timeline set out in this report, followed by a full retest to validate the effectiveness of applied fixes. Adopting the strategic recommendations in this report will materially reduce the organization's overall attack surface and improve long-term security posture.



Disclaimer

This report is a SAMPLE deliverable created by Vaptora Security Services for demonstration purposes only. The organization name "XYZ Corporation", all domains, endpoints, personnel, dates, and findings described herein are entirely fictitious and do not represent any real assessment, system, individual, or organization, living or otherwise. Any resemblance to an actual entity is purely coincidental.

This document is intended solely to illustrate Vaptora's reporting methodology, structure, and quality to prospective clients. It must not be relied upon as evidence of the security posture of any real system, and must not be redistributed as an authentic assessment report.

© 2026 Vaptora Security Services. All rights reserved.