

bueroX Web Security Testprotokoll

Sicherheitsprüfung für bueroX Web / UniGUI / NexusDB

Produkt	bueroX Web
Hersteller	Markus Gall
Vertrieb / Inverkehrbringer	GFK Autonomous Systems UG (haftungsbeschränkt)
Version / Build	
Testdatum	
Prüfer	
Testumgebung	
Gesamtergebnis	☐ bestanden ☐ bestanden mit Abweichungen ☐ nicht bestanden

1. Zweck und Geltungsbereich

Dieses Protokoll dokumentiert die sicherheitsrelevante Prüfung von bueroX Web. Es dient als reproduzierbarer Nachweis für interne Freigaben, CRA-Nachweisführung und externe Sicherheitsprüfungen. Geprüft werden insbesondere Authentifizierung, Session-Schutz, Autorisierung, Dokumentzugriff, Upload/Download, Transportverschlüsselung, NexusDB-Zugriff und Sicherheitsprotokollierung.

2. Voraussetzungen

- Freigegebener bueroX-Web-Build ist in der Testumgebung installiert.
- UniGUI-Webserver ist gestartet und SSL/TLS ist aktiv.
- NexusDB-Server ist erreichbar; Zugriff erfolgt über den vorgesehenen TCP/IP-Port.
- Mindestens zwei Testbenutzer mit unterschiedlichen Zugriffsgruppen sind vorhanden.
- Mindestens ein Dokument ist Benutzer A freigegeben und Benutzer B nicht freigegeben.
- Testdateien für Upload und Download sind vorhanden.
- Zugriff auf die NexusDB-Logdaten ist für den Prüfer möglich.

3. Bewertung

Bewertung je Testfall: BESTANDEN = Sollverhalten vollständig erfüllt; ABWEICHUNG = Sollverhalten teilweise erfüllt, Maßnahme erforderlich; NICHT BESTANDEN = sicherheitsrelevante Schutzfunktion nicht wirksam. Jeder Testfall erhält einen Nachweis, z. B. Screenshot, Logeintrag, Testdatei oder Protokollreferenz.

4. Authentifizierung und Benutzerkonten

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-AUTH-001	Anmeldung mit gültigem Benutzer / Passwort	Anmeldung nur mit gültigen Zugangsdaten möglich.	☐ B ☐ A ☐ NB		
WEB-AUTH-002	Falsches Passwort	Anmeldung wird abgewiesen; sicherheitsrelevanter Vorgang wird nachvollziehbar behandelt.	☐ B ☐ A ☐ NB		
WEB-AUTH-003	Nicht berechtigter	Nicht	☐ B		

GFK Autonomous Systems

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
	Benutzer	freigegebene Programmteile sind nicht verfügbar.	☐ A ☐ NB		
WEB-AUTH-004	Zugriffsgruppe	Beim Login wird die Oberfläche entsprechend der Benutzergruppe aufgebaut.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

5. Session-Sicherheit

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-SES-001	Session-ID-Bindung	Aktive Sitzung ist dem authentifizierten Benutzer und der Session-ID zugeordnet.	☐ B ☐ A ☐ NB		
WEB-SES-002	TCP/IP-Kontext	Session-Kontext berücksichtigt den vorgesehenen TCP/IP-Verbindungskont ext.	☐ B ☐ A ☐ NB		
WEB-SES-003	Geräte-ID, falls vorhanden	Geräte-ID wird in die Sessionbindung einbezogen, sofern verfügbar.	☐ B ☐ A ☐ NB		
WEB-SES-004	Zweiter Login von anderem Gerät	Zweiter Login desselben Benutzers wird während aktiver Session verweigert.	☐ B ☐ A ☐ NB		
WEB-SES-005	Übernahme fremder Session	Manipulierte oder übernommene Session darf keinen gültigen Zugriff ermöglichen.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

6. Menü-, Masken- und Funktionsautorisierung

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-AUTHZ-001	Menüaufbau nach Login	Nur für die Zugriffsgruppe freigegebene Menüpunkte werden erzeugt.	☐ B ☐ A ☐ NB		
WEB-AUTHZ-002	Nicht berechtigter Menüpunkt	Nicht autorisierte Menüpunkte sind nicht aufrufbar.	☐ B ☐ A ☐ NB		

GFK Autonomous Systems

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-AUTHZ-003	DOM-/HTML-Prüfung	Nicht autorisierte Funktionen werden nicht als versteckte HTML-/DOM-Elemente an den Browser übertragen.	☐ B ☐ A ☐ NB		
WEB-AUTHZ-004	Fachmethoden-Zuordnung	Menüeintrag öffnet nur die zugeordnete Fachmethode / Maske / Datenbereich.	☐ B ☐ A ☐ NB		
WEB-AUTHZ-005	Rechtestufen	Unsichtbar, sichtbar, Korrektur/Bearbeitung, Drucken und Vollzugriff wirken entsprechend der Konfiguration.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

7. Dokumentzugriff und IDOR-Schutz

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-DOC-001	Dokumenten-ID vorhanden	Dokumenten-ID allein ermöglicht keinen Zugriff ohne Benutzerfreigabe.	☐ B ☐ A ☐ NB		
WEB-DOC-002	Freigegebenes Dokument	Freigegebenes Dokument ist für den berechtigten Benutzer zugänglich.	☐ B ☐ A ☐ NB		
WEB-DOC-003	Fremdes Dokument	Dokument ohne Benutzerfreigabe wird verweigert.	☐ B ☐ A ☐ NB		
WEB-DOC-004	Manipulierte Dokumenten-ID	Durchprobieren oder Ändern der Dokumenten-ID führt nicht zu fremdem Dokumentzugriff.	☐ B ☐ A ☐ NB		
WEB-DOC-005	Direkter Dateipfad	Direkter Zugriff auf physischen Datei-/Cache-Pfad ist nicht möglich.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

8. Upload, Download und temporärer Cache

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-FILE-001	Upload in temporären Cache	Upload wird zunächst ausschließlich im temporären Cache gespeichert.	☐ B ☐ A ☐ NB		
WEB-FILE-002	Zufallsdateiname	Temporäre Datei erhält einen zufälligen, nicht aus dem Originalnamen ableitbaren Dateinamen.	☐ B ☐ A ☐ NB		
WEB-FILE-003	Zeitfenster	Temporärer Zugriff ist zeitlich begrenzt.	☐ B ☐ A ☐ NB		
WEB-FILE-004	Automatische Löschung	Cache-Datei wird nach Ablauf des Zeitfensters serverseitig gelöscht.	☐ B ☐ A ☐ NB		
WEB-FILE-005	Download-Limit pro Session	Ungewöhnlich hohe Download-Aktivität wird begrenzt oder gesperrt.	☐ B ☐ A ☐ NB		
WEB-FILE-006	Upload-Limit pro Session	Ungewöhnlich hohe Upload-Aktivität wird begrenzt oder gesperrt.	☐ B ☐ A ☐ NB		
WEB-FILE-007	Nutzerbezogener Durchschnitt	Algorithmus berücksichtigt das typische Upload-/Download-Verhalten des Benutzers.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

9. Transport- und Serverkommunikation

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-NET-001	HTTPS/TLS beim Start	Webserver startet mit aktivem SSL/TLS; Browserzugriff erfolgt verschlüsselt.	☐ B ☐ A ☐ NB		
WEB-NET-002	Definierter Web-Port	Webzugriff erfolgt nur über den vorgesehenen TCP/IP-Port.	☐ B ☐ A ☐ NB		
WEB-NET-003	Browser zu NexusDB	Browser besitzt keinen direkten Zugriff auf NexusDB.	☐ B ☐ A ☐ NB		
WEB-NET-004	UniGUI zu	UniGUI-	☐ B		

GFK Autonomous Systems

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
	NexusDB	Webserver verbindet sich über den vorgesehenen NexusDB-TCP/IP-Port.	☐ A ☐ NB		
WEB-NET-005	NexusDB Transportverschlüsselung	Transport zwischen Webserver und NexusDB ist entsprechend der Freigabekonfiguration verschlüsselt.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

10. NexusDB und Logging

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-DB-001	Rollen / Datenbankrechte	NexusDB-Rollen verhindern unberechtigten Datenbankzugriff.	☐ B ☐ A ☐ NB		
WEB-DB-002	Verschlüsselte Tabellen	Als geschützt definierte Tabellen werden entsprechend der Freigabekonfiguration verschlüsselt betrieben.	☐ B ☐ A ☐ NB		
WEB-LOG-001	Session-/ Transfer-Logging	Sicherheitsrelevante Session- und Transferereignisse werden in der NexusDB-Datenbankumgebung protokolliert.	☐ B ☐ A ☐ NB		
WEB-LOG-002	Sperrereignisse	Ausgelöste Upload-/Download-Begrenzungen oder Sperren sind nachvollziehbar protokolliert.	☐ B ☐ A ☐ NB		
WEB-LOG-003	Nachvollziehbarkeit	Logeinträge enthalten ausreichenden Benutzer-, Session- und Zeitbezug für eine spätere Prüfung.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

11. Manipulations- und Negativtests

Test-ID	Prüfung	Sollverhalten	Ergebnis	Nachweis	Bemerkung / Maßnahme
WEB-NEG-001	URL-/Parametermanipulation	Manipulierte Parameter führen nicht zu unberechtigtem Zugriff.	☐ B ☐ A ☐ NB		
WEB-NEG-002	Direkter Maskenaufruf	Nicht autorisierte Masken können nicht durch direkten Aufruf erzwungen werden.	☐ B ☐ A ☐ NB		
WEB-NEG-003	Druck-/Korrekturrechte	Nicht freigegebene Korrektur- oder Druckaktionen werden verhindert.	☐ B ☐ A ☐ NB		
WEB-NEG-004	Fehlerbehandlung	Fehlermeldungen geben keine unnötigen internen Pfade, Zugangsdaten oder sensiblen Systemdetails preis.	☐ B ☐ A ☐ NB		

Legende: B = bestanden, A = Abweichung, NB = nicht bestanden.

12. Ergebniszusammenfassung

Anzahl Testfälle	_____
Bestanden	_____
Abweichungen	_____
Nicht bestanden	_____
Kritische Findings	_____
Freigabeempfehlung	☐ freigeben ☐ mit Auflagen freigeben ☐ nicht freigeben

13. Abweichungen und Maßnahmen

Finding-ID	Test-ID	Beschreibung	Schweregrad	Maßnahme / Fix-Version	Status

14. Freigabe

Prüfer / Datum: _____

Technische Freigabe / Datum: _____

Security-Verantwortlicher / Datum: _____

GFK Autonomous Systems

Hinweis: Dieses Protokoll dokumentiert einen versionsbezogenen Sicherheitstest. Bei sicherheitsrelevanten Änderungen, Änderungen an Basismasken, Session-/Dateilogik, Kommunikationswegen oder zentralen Komponenten ist eine erneute bzw. gezielte Regression der betroffenen Testfälle durchzuführen.