Demo Audit

SCHWACHSTELLENBERICHT

09.01.2023

VERSIONEN

Version	Date	Author	Description
1.0	01/09/2023	Matthias Hoffmann	Initiale Version

INHALTSVERZEICHNIS

ALLGEMEINE INFORMATIONEN

SCOPE

PentestMy.Network hat uns zur Durchführung eines „undefined“ beauftragt, der die folgenden Bereiche abdeckt:

- 10.10.11.0/24
- *.example.org

ORGANISATION

Der Zeitraum des Tests wurde zwischen dem 02.01.2023 und 05.01.2023 festgelegt.

KONTAKTPERSONEN

Name	E-Mail-Adresse	Position	Telefonnummer
Matthias Hoffmann	info@pentestmy.network	Penetration Tester	0151 / 401 89391
Hans Mustermann	Hans.mustermann@example.org	CEO	

ZUSAMMENFASSUNG

Hier könnte die Zusammenfassung des Penetration Tests stehen.

ÜBERSICHT DER SCHWACHSTELLEN

Folgende Schwachstellen oder Fehlkonfigurationen wurden gefunden:

Risiko	ID	Schwachstelle	Betroffener Bereich
High	IDX-002	Denial of Service durch fehlendes Rate Limiting	https://demo.example.org
High	IDX-005	Hardcoded Passwörter und / oder Benutzernamen	https://demo.example.org
Medium	IDX-001	Cross Site Scripting (XSS)	https://demo.example.org
Medium	IDX-003	Insecure Direct Object References (IDOR)	https://demo.example.org

TECHNISCHE DETAILS

DENIAL OF SERVICE DURCH FEHLENDES RATE LIMITING

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.5**
CVSSV3 KRITERIEN	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**None**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**High**
BETROFFENER BEREICH	https://demo.example.org			
BESCHREIBUNG	Aufgrund fehlenden Limitieren von HTTP-Request, die von einer einzelnen IP stammen, kann der Webserver keine weitere Anfragen bearbeiten.			
BEOBACHTUNG				
TEST DETAILS	 Image 1 – image.png			
VERMEIDUNG / BEHEBUNG	Setzen von maximalen HTTP Requests pro Sekunde für einzelne IPs mit anschließender Drosselung.			
REFERENZEN	https://www.cloudflare.com/de-de/learning/bots/what-is-rate-limiting/#:~:text=Eine%20Rate%2DLimiting%2DL%C3%B6sung%20misst,Anfragen%20innerhalb%20eines%20bestimmten%20Zeitrahmens.			

HARDCODED PASSWÖRTER UND / ODER BENUTZERNAMEN

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.5**
CVSSV3 KRITERIEN	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**None**
BETROFFENER BEREICH	https://demo.example.org			
BESCHREIBUNG	Es wurde eine Reihe von Diensten identifiziert, die ein fest codiertes Passwort verwenden. Das Risiko dieses Problems besteht darin, dass sich ein Angreifer mit einem Konto mit einem fest codierten Passwort anmelden könnte.			
BEOBACHTUNG				
TEST DETAILS Unter https://demo.example.org/data/server/config.json waren hinterlegte Zugangsdaten öffentlich einsehbar.				

Image 2 – image.png

VERMEIDUNG / BEHEBUNG	
REFERENZEN	

CROSS SITE SCRIPTING (XSS)

CVSS SEVERITY	Medium		CVSSV3 SCORE	6.5
CVSSV3 KRITERIEN	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**Low**
	Required Privileges :	**None**	Integrity :	**Low**
	User Interaction :	**None**	Availability :	**None**
BETROFFENER BEREICH	https://demo.example.org			
BESCHREIBUNG	Der OWASP-Leitfaden [1] enthält folgende Beschreibung für Cross-Site Scripting: Cross-Site Scripting (XSS)-Angriffe sind eine Art von Injektion, bei der bösartige Skripte in ansonsten gutartige und vertrauenswürdige Websites eingeschleust werden. XSS-Angriffe treten auf, wenn ein Angreifer eine Webanwendung nutzt, um bösartigen Code, in der Regel in Form eines browserseitigen Skripts, an einen anderen Endbenutzer zu senden. Schwachstellen, die diese Angriffe ermöglichen, sind weit verbreitet und treten überall dort auf, wo eine Webanwendung Eingaben eines Benutzers innerhalb der von ihr erzeugten Ausgabe verwendet, ohne sie zu validieren oder zu kodieren. Ein Angreifer kann XSS nutzen, um ein bösartiges Skript an einen ahnungslosen Benutzer zu senden. Der Browser des Endbenutzers hat keine Möglichkeit zu erkennen, dass das Skript nicht vertrauenswürdig ist, und führt das Skript aus. Da er davon ausgeht, dass das Skript von einer vertrauenswürdigen Quelle stammt, kann das bösartige Skript auf Cookies, Sitzungs-Token oder andere vertrauliche Informationen zugreifen, die vom Browser gespeichert und mit dieser Website verwendet werden. Diese Skripte können sogar den Inhalt der HTML-Seite umschreiben.			
BEOBACHTUNG				

TEST DETAILS

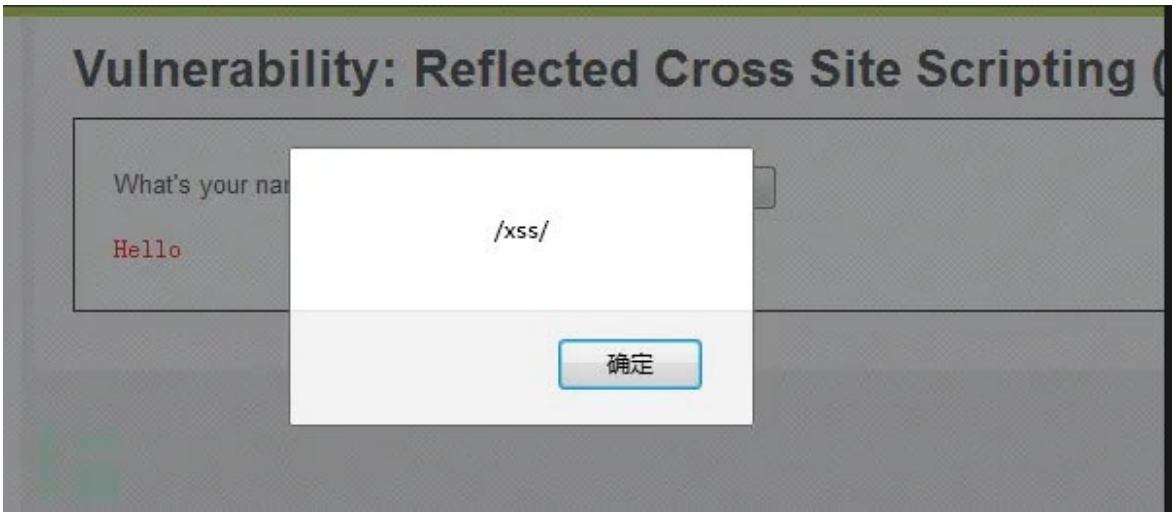

Image 3 – image.png

Payload: `><script>alert(/xss/)</script>`

Der Input von "What´s your name" wird nicht validiert und es ist ein "reflected cross site scripting" möglich.	
VERMEIDUNG / BEHEBUNG	Zur Behebung von XSS-Schwachstellen wird Folgendes empfohlen: • Niemals Benutzereingaben vertrauen • Fügen Sie niemals nicht vertrauenswürdige Daten ein, außer an zulässigen Stellen • HTML-Escape vor dem Einfügen von nicht vertrauenswürdigen Daten in den Inhalt von HTML-Elementen • Verwenden Sie Whitelists anstelle von Blacklists zum Filtern von Eingaben.
REFERENZEN	https://owasp.org/www-community/attacks/xss/

INSECURE DIRECT OBJECT REFERENCES (IDOR)

CVSS SEVERITY	**Medium**		**CVSSV3 SCORE**	**6.5**
CVSSV3 KRITERIEN	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**None**
BETROFFENER BEREICH	https://demo.example.org			
BESCHREIBUNG	Der OWASP-Leitfaden [1] gibt die folgende Beschreibung für Insecure Direct Object Reference: Anwendungen verwenden häufig den tatsächlichen Namen oder Schlüssel eines Objekts, wenn sie Webseiten generieren. Die Anwendungen überprüfen nicht immer, ob der Benutzer für das Zielobjekt autorisiert ist. Dies führt zu einer unsicheren direkten Objektreferenz. Tester können Parameterwerte leicht manipulieren, um solche Fehler zu erkennen, und eine Codeanalyse zeigt schnell, ob die Autorisierung ordnungsgemäß überprüft wird.			
BEOBACHTUNG				
TEST DETAILS Beim Zugriff auf https://demo.example.org/customer/id/XY kann durch IDOR auf Ressourcen anderer Kunden zugegriffen werden.				
VERMEIDUNG / BEHEBUNG	Verwenden Sie indirekte Objektverweise pro Benutzer oder Sitzung. Dies hindert Angreifer daran, direkt auf nicht autorisierte Ressourcen zuzugreifen. Anstatt den Datenbankschlüssel der Ressource zu verwenden, könnte beispielsweise eine Dropdown-Liste mit sechs für den aktuellen Benutzer autorisierten Ressourcen die Zahlen 1 bis 6 verwenden, um anzuzeigen, welchen Wert der Benutzer ausgewählt hat. Die Anwendung muss den indirekten Verweis pro Benutzer auf den tatsächlichen Datenbankschlüssel auf dem Server zurückführen. Zugriff prüfen! Jede Verwendung eines direkten Objektverweises aus einer nicht vertrauenswürdigen Quelle muss eine Zugriffskontrollprüfung beinhalten, um sicherzustellen, dass der Benutzer für das angeforderte Objekt berechtigt ist.			
REFERENZEN	https://owasp.org/Top10/A01_2021-Broken_Access_Control/			