En quête de meilleurs rapports de tests d'intrusion

Introduction aux contrôles de sécurité manquants

GoSecure

À propos

Maxime Nadeau

Directeur, Piratage Éthique

- Testeur d'intrusion depuis 6 ans
- Maintenant payé pour présenter aux clients les choses que des personnes plus intelligentes que moi découvrent

Avertissement

Cette présentation est faite à partir du point de vue d'un testeur d'intrusion

L'approche présentée n'est en aucun cas parfaite. Cette dernière peut être hautement influencée par le testeur en change de l'attribution du score.

L'approche présentée n'est pas le résultat d'une importante consultation ou de le mise en place d'un comité de travail inter-compagnies

Comment nous communiquons la sévérité

GoSecure

Comment nous communiquons la sévérité

~~DREAD~~ CVSS 2 / 3 / 3.1 CWSS

Impact

Probabilité	Négligible	Mineur	modéré	Important	Sévère
Très probable	Medium	Élevé	Critique	Critique	Critique
Probable	Medium	Élevé	Élevé	Critique	Critique
Possible	Faible	Medium	Élevé	Élevé	Critique
Peu probable	Faible	Medium	Medium	Élevé	Élevé
Très peu probable	Faible	Faible	Faible	Medium	Medium

Évaluation d'une vulnérabilité

CVSS

Le Common Vulnerability Scoring System (CVSS) offre une méthodologie permettant de capturer les principales caractéristiques d'une **vulnérabilité** et de produire une valeur numérique représentant sa **sévérité**. Cette valeur numérique peut ensuite être traduite en une représentation qualitative (tel que « faible », « medium , « haute » et « critique ») afin d'aider les organisation à correctement évaluer et prioriser chaque vulnérabilité accordement à leur processus de gestion des vulnérabilités.

- Traduction Libre - Forum of Incident Response and Security Teams

Évaluation d'une vulnérabilité

CVSS

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Évaluation d'une vulnérabilité

Défis

Dans un article datant de 2018, le SEI de l'université Carnegie Mellon soulève divers défis associés à CVSS 3.1 :

- Ne permet pas de prendre en compte le contexte
    - *CVSS Struggles to Remain Viable in the Era of Cloud Native Computing* (Jack Wallen – TheNewStack, 2020)

Évaluation d'une vulnérabilité

Défis

Dans un article datant de 2018, le SEI de l'université Carnegie Mellon soulève divers défis associés à CVSS 3.1 :

- Ne permet pas de prendre en compte les conséquences matérielles ou humaines d'une vulnérabilité
    - *Collateral Damage (CDP) might be good to reintroduce, and could be tweaked/renamed to be a "Safety" (S) metric* (Garret Wassermann – CERT/CC, 2015)

Évaluation d'une vulnérabilité

Défis

Dans un article datant de 2018, le SEI de l'université Carnegie Mellon soulève divers défis associés à CVSS 3.1 :

- Problèmes associés au fonctionnement du mode d'attribution des scores
  - *The overrepresentation of High and Critical (or perhaps it's really an underrepresentation of Low) is reasonably attributable to reporter incentives** [Jacques Chester - Predictable Software, 2022]
  - *There are 47 permutations to reach 7.5, 12 to reach 7.8, 11 to reach 8.8 and 1 to reach 9.8* [Jacques Chester - Predictable Software, 2022]

* Certains CNA n'attribuent pas de CVE pour des vulnérabilités de sévérité faible ou moyenne

Évaluation d'une vulnérabilité

Défis

Lors de la présentation de nos rapports de test d'intrusion aux clients, nous avons observé un défi supplémentaire.

Utilisons l'entête HSTS à titre d'exemple :

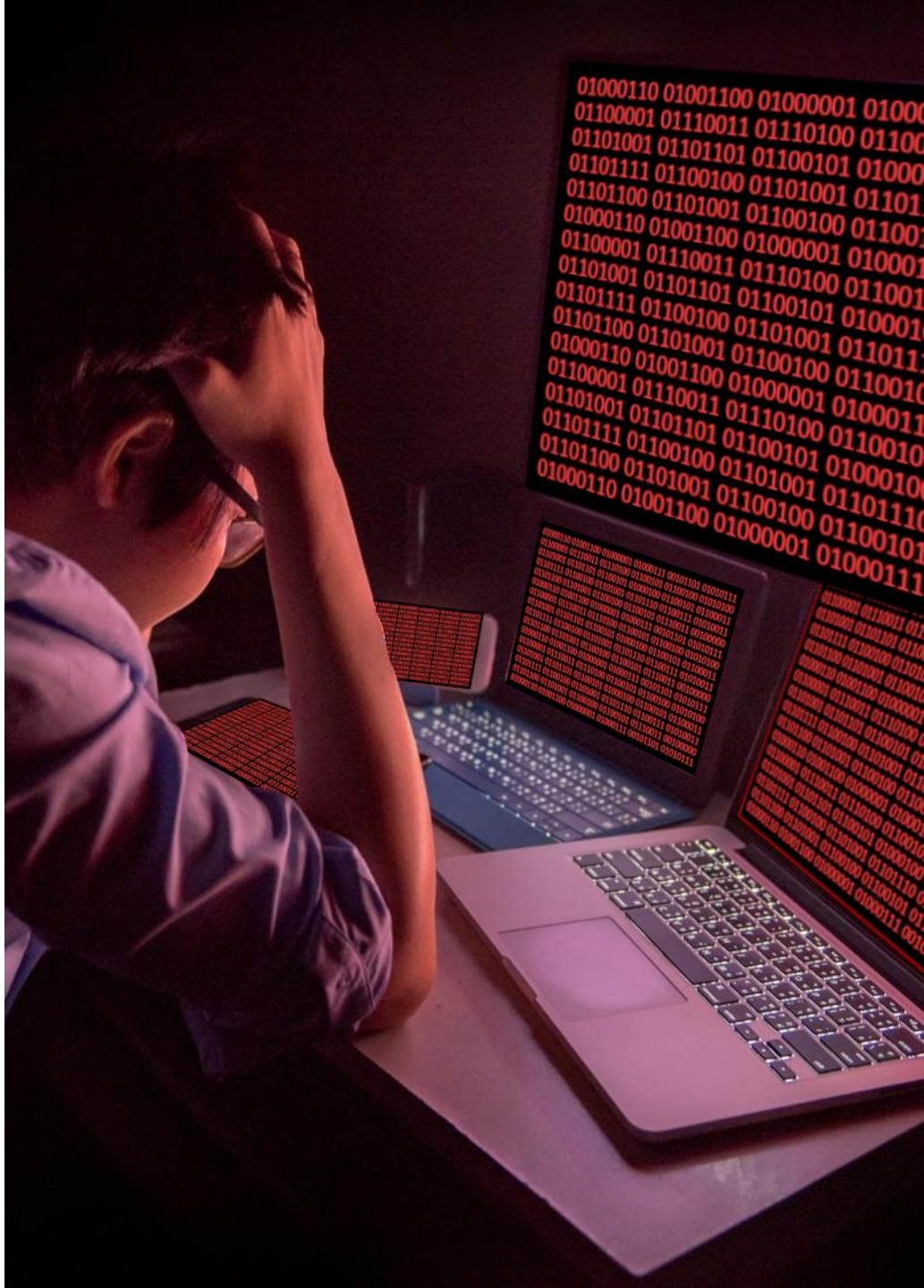
AV	AC	PR	UI	S	C	I	A	Score	Note	Note affichée	Source
-	-	-	-	-	-	-	-	-	-	Info	Tenable Nessus – Plugin 84502
N	L	N	N	U	L	L	N	6.5	Medium	Medium	Tenable Nessus – Plugins 98056 and 142960
N	H	N	N	U	H	N	N	4.8	Medium	Medium	Crash-Test Security
N	H	N	N	U	H	H	L	7.7	Élevée	Medium	Invicti
N	L	N	R	C	N	N	N	0.0	Aucun	Faible	Acunetix
N	H	N	N	U	H	H	N	7.4	Élevée	Faible	Probely
N	H	N	N	U	H	N	N	5.9	Medium	Medium	IBM CVE-2021-38978
N	L	N	N	U	L	L	N	6.5	Medium	Medium	HPE CVE-2017-5784

Évaluation d’une vulnérabilité

Défis

Nos conclusions ?

- CVSS est complexe
- CVSS n’est pas fait pour évaluer les contrôles de sécurité



Contrôles de sécurité manquants

Rapport de tests d'intrusion - année 1

Niveau de sévérité	Liste des vulnérabilités	Score CVSS
Élevée	1. Local File Inclusion (LFI)	8.5
Medium	2. Cross-Site Scripting (XSS)	6.1
Medium	3. Énumération d'utilisateurs	5.3
Medium	4. Stockage d'information sensible dans le stockage local ou stockage de session du navigateur	4.0
Faible	5. Divulgation d'information via les entêtes HTTP serveur	3.7
Info	6. Témoins de navigateur sans les attributs "HttpOnly", "Secure" et/ou "SameSite"	0.0
Info	7. Entête HTTP Strict Transport Security (HSTS) manquante	0.0
Info	8. Protection Content-Security-Policy (CSP) Inadéquate	0.0

Contrôles de sécurité manquants

Rapport de tests d'intrusion - années 2,3,4 et 5

Niveau de sévérité	Liste des vulnérabilités	Score CVSS
Faible	1. Divulgation d'information via les entêtes HTTP serveur	3.7
Info	2. Témoins de navigateur sans les attributs "HttpOnly", "Secure" et/ou "SameSite"	0.0
Info	3. Entête HTTP Strict Transport Security (HSTS) manquante	0.0
Info	4. Protection Content-Security-Policy (CSP) Inadéquate	0.0

Introduction aux “Contrôles de sécurité manquants”

GoSecure

Contrôles de sécurité manquants

Comment « vendre » la sécurité ?

Comment tracer la ligne entre une vulnérabilité et un contrôle de sécurité manquant ?

Comment communiquer un problème à divers partie prenantes ?

Comment évaluer les bénéfices de quelque chose qui n'a pas d'impact immédiat?

Contrôles de sécurité manquants

Comment « vendre » la sécurité ?

Contrôles de sécurité manquants

Comment « vendre » la sécurité ?

Contrôle d'accès au réseau (Crédit à Laurent Desaulniers)

- Mandat « Red team »
- Aucune façon de compromettre le périmètre externe
- Tentatives de phishing n'ont pas permis d'obtenir de l'exécution de code

Contrôles de sécurité manquants

Comment « vendre » la sécurité ?

Tous “informationnel”, mais le client s’est quand même fait compromettre

Niveau de sévérité	Liste des vulnérabilités	Score CVSS
Informationel	1. Absence de Network Access Control (NAC)	0.0
Informationel	2. Programme de sensibilization à la cybersécurité inadéquat	0.0
Informationel	3. Segmentation / Isolation réseau insuffisante	0.0
Informationel	4. Utilisation d’un protocole de communication RFID désuet	0.0

Niveau de sévérité	Liste des contrôles de sécurité manquants	Score CVSS
Élevé	1. Absence de Network Access Control (NAC)	-
Medium	2. Programme de sensibilization à la cybersécurité inadéquat	-
Faible	3. Segmentation / Isolation réseau insuffisante	-
Faible	4. Utilisation d’un protocole de communication RFID désuet	-

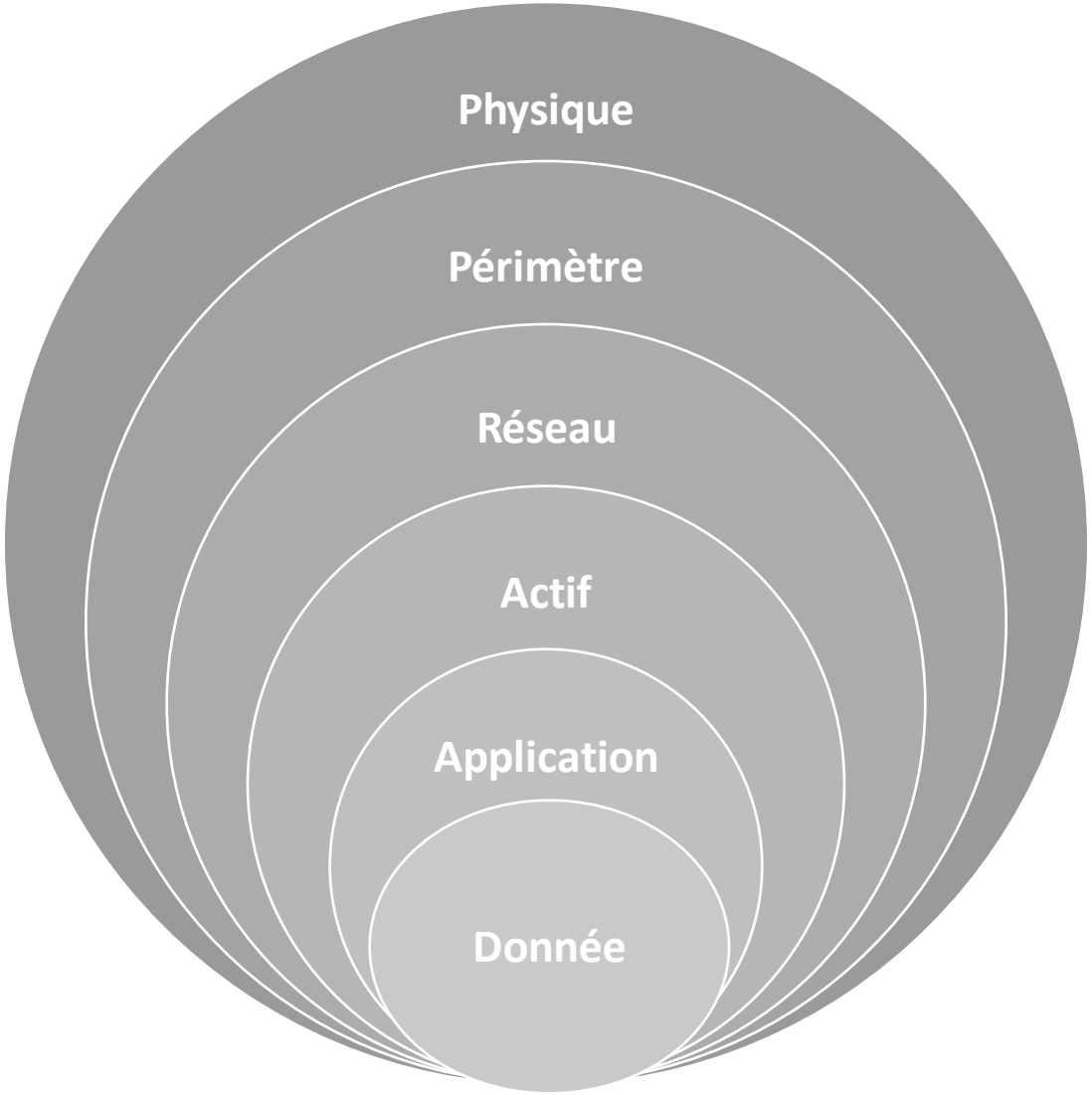
Contrôles de sécurité manquants

Comment tracer la ligne ?

- CVSS évalue déjà les vulnérabilités
- Les contrôles de sécurité manquants ne devraient pas être utilisés pour modifier un score avec lequel vous n'êtes pas en accord.
- Peut toujours être complexe à évaluer dans certains cas (Par exemple la mise en place d'une politique vs la déviation à cette politique)

Contrôles de sécurité manquants

Comment communiquer un problème à divers partie prenantes ?



Contrôles de sécurité manquants

Comment communiquer un problème à divers partie prenantes ?

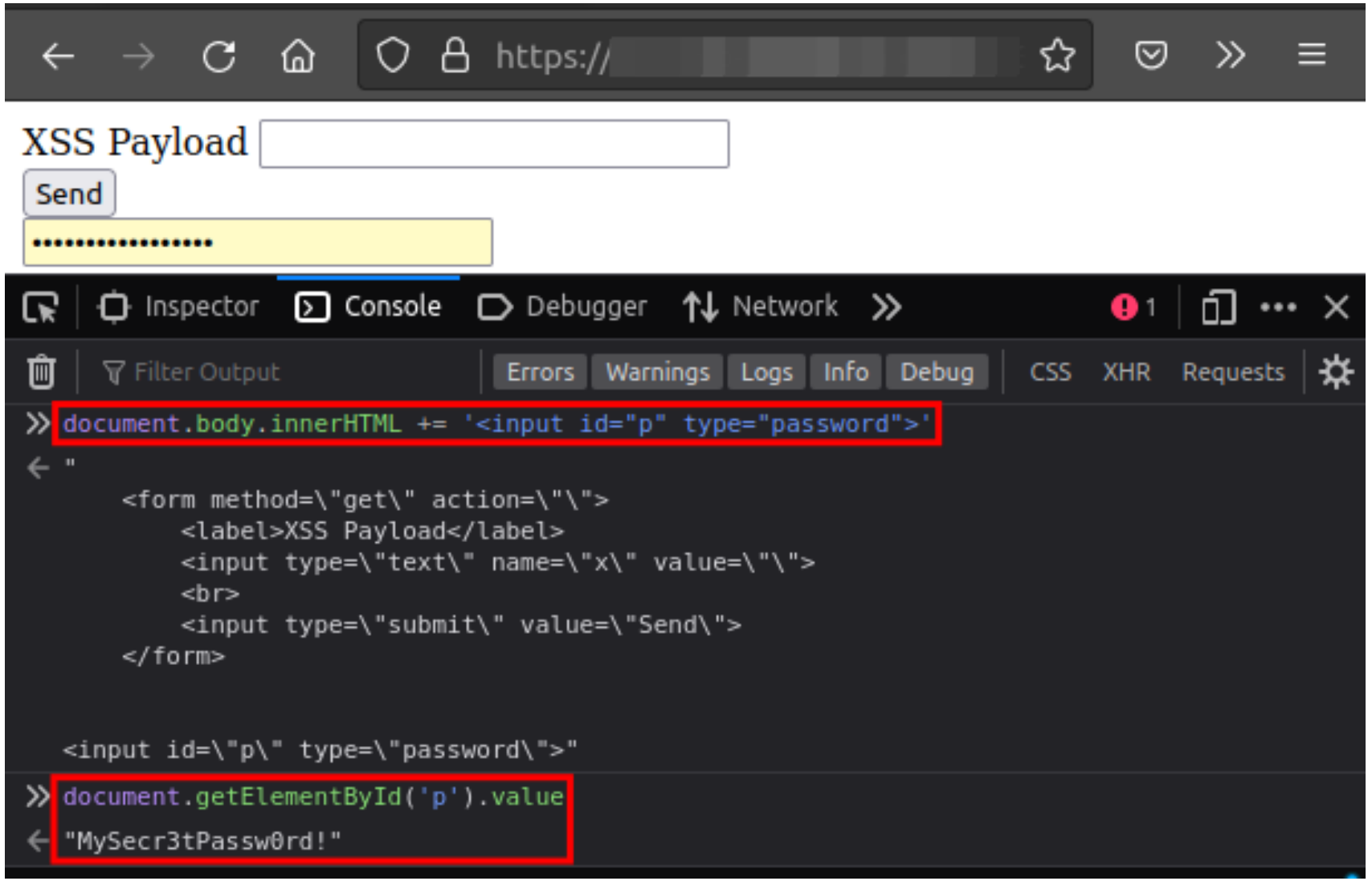
Autocompletion pour navigateurs (Crédit à Marc Olivier Bergeron)

Plusieurs des navigateurs modernes offrent un mécanisme de « voute de mots de passes » permettant de remplir automatiquement vos authentifiant.

Ce mécanisme peut souvent être exploité par des attaquant afin de voler ces authentifiant lorsqu'une vulnérabilité de type « XSS » est présente.

Contrôles de sécurité manquants

Comment communiquer un problème à divers partie prenantes ?



Contrôles de sécurité manquants

Comment communiquer un problème à divers partie prenantes ?

Mitigations

- **Développeur Web**
- **Administrateurs du serveur web**
- **Administrateurs de sécurité**
- **Architectes de sécurité**

Contrôles de sécurité manquants

Comment communiquer un problème à divers partie prenantes ?

Mitigations

- **Développeur Web**
  - Encodage / filtrage des entrées utilisateur
- **Administrateurs du serveur web**
  - Mettre en place une entête « CSP »
- **Administrateurs de sécurité**
  - Prévenir la sauvegarde d'authentifiant dans les navigateurs via politique de groupe (« GPO »)
- **Architectes de sécurité**
  - Création d'une politique servant a promouvoir l'utilisation de voutes de mots de passes et communication de cette stratégie pour encourager les utilisateurs à éviter l'utilisation de solutions inclues dans les navigateurs

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Impact Sub-Score (ISS)		
	1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]	
Impact		
	If Scope is Unchanged	6.42 × ISS
	If Scope is Changed	7.52 × (ISS - 0.029) - 3.25 × (ISS - 0.02)15
Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Impact <= 0	0
	If Scope is Unchanged	Roundup (Minimum [(Impact + Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Impact + Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

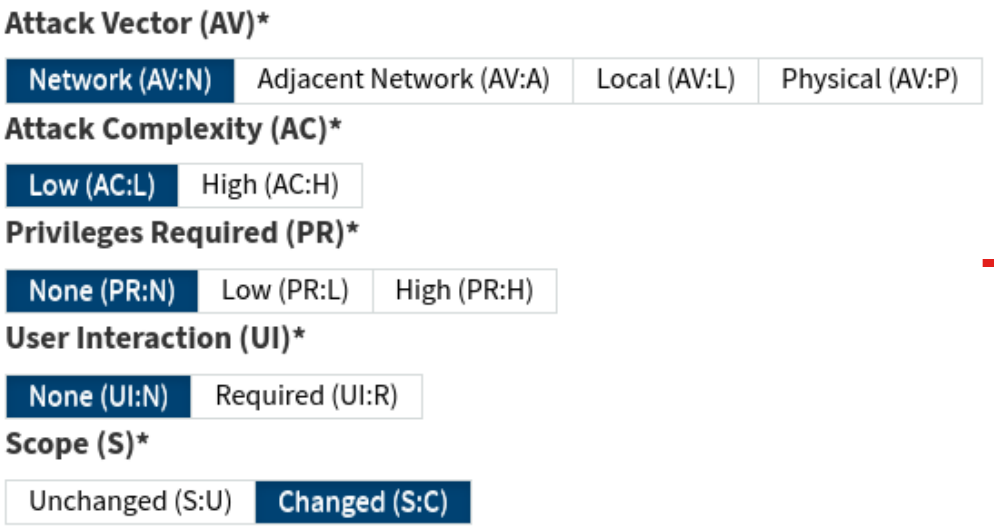
Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

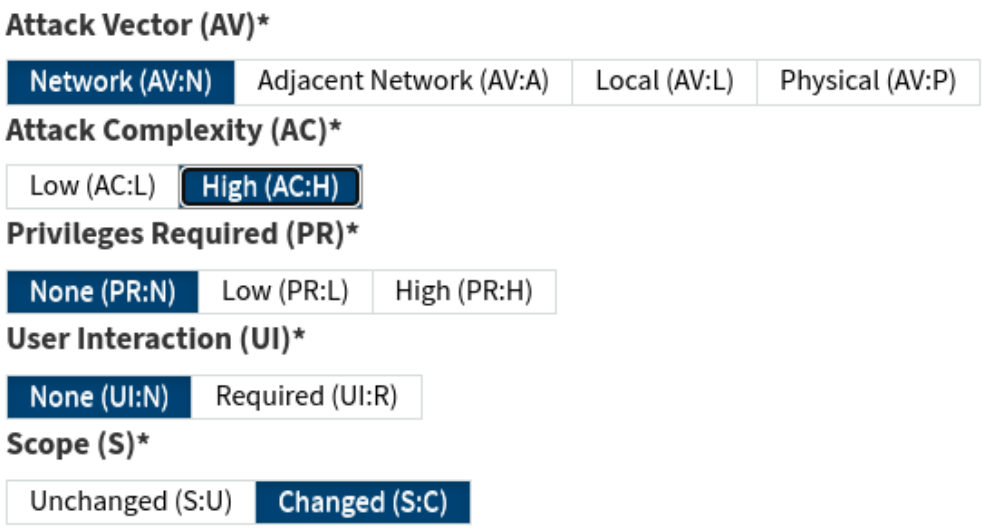
Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?



Score: 4.2



Score: 2.4

Nous avons une difference de 1.8 sur un maximum théorique possible de 4.0

Contrôles de sécurité manquants

Comment évaluer les bénéfices ?

0 → Informationnel

0.1 to 1.3 → Faible

1.3 to 2.7 → Medium

2.8 to 4.0 → Élevé

Contrôles de sécurité manquants

Niveau de sévérité	Liste des contrôles de sécurité manquants	Score CVSS
Medium	1. Entête HTTP Strict Transport Security (HSTS) manquante	-
Medium	2. Protection Content-Security-Policy (CSP) Inadéquate	-
Faible	3. Témoins de navigateur sans les attributs "HttpOnly", "Secure" et/ou "SameSite"	-
Niveau de sévérité	**Liste des vulnérabilités**	**Score CVSS**
Élevée	1. Local File Inclusion (LFI)	8.5
Medium	2. Cross-Site Scripting (XSS)	6.1
Medium	3. Énumération d'utilisateurs	5.3
Medium	4. Stockage d'information sensible dans le stockage local ou stockage de session du navigateur	4.0
Faible	5. Divulgation d'information via les entêtes HTTP serveur	3.7

Contrôles de sécurité manquants

Conclusion

La notion de contrôles de sécurité manquants est encore un travail inachevé

Une calculatrice de base utilisant la méthodologie présentée dans ces diapositives (avec les diapositives) peuvent être obtenues à l'adresse https://gosecure.github.io/missing-security-controls/

Les commentaires sont toujours les bienvenus

Questions

GoSecure