The Quest for Better Pentest Reports

Introducing Missing Security Controls

GoSecure

About me

Maxime Nadeau

Director, Ethical Hacking

- Intrusion Tester for the last 6 years
- Now paid to present to customers the awesome things more clever people than I are doing

Disclaimer

This talk is presented from the intrusion tester's point-of-view

The presented approach is in no way perfect and is still biased by tester's input

The method presented here is not the result of a multi-company commitee

How do we currently communicate severity

How do we currently communicate severity

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

Impact

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Moderate	High	Critical	Critical	Critical
Likely	Moderate	High	High	Critical	Critical
Possible	Low	Moderate	High	High	Critical
Unlikely	Low	Moderate	Moderate	High	High
Very Unlikely	Low	Low	Low	Moderate	Moderate

Vulnerability Scoring

CVSS

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a **vulnerability** and produce a numerical score reflecting its **severity**. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

- Forum of Incident Response and Security Teams

Vulnerability Scoring

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)

Vulnerability Scoring

Challenges

In a 2018 whitepaper, Carnegie Mellon University's SEI highlights the following challenges:

- Failure to account for context
    - *CVSS Struggles to Remain Viable in the Era of Cloud Native Computing* (Jack Wallen – TheNewStack, 2020)

Vulnerability Scoring

Challenges

In a 2018 whitepaper, Carnegie Mellon University's SEI highlights the following challenges:

- Failure to account for material consequences of vulnerability
    - *Collateral Damage (CDP) might be good to reintroduce, and could be tweaked/renamed to be a "Safety" (S) metric* (Garret Wassermann – CERT/CC, 2015)

Vulnerability Scoring

Challenges

In a 2018 whitepaper, Carnegie Mellon University's SEI highlights the following challenges:

- Operational scoring problems
  - *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]

* Some CNA do not attribuate CVEs to low and medium severity vulnerabilities

Vulnerability Scoring

Challenges

While presenting reports to customers, we encountered another challenge.
Lets use HSTS as an example:

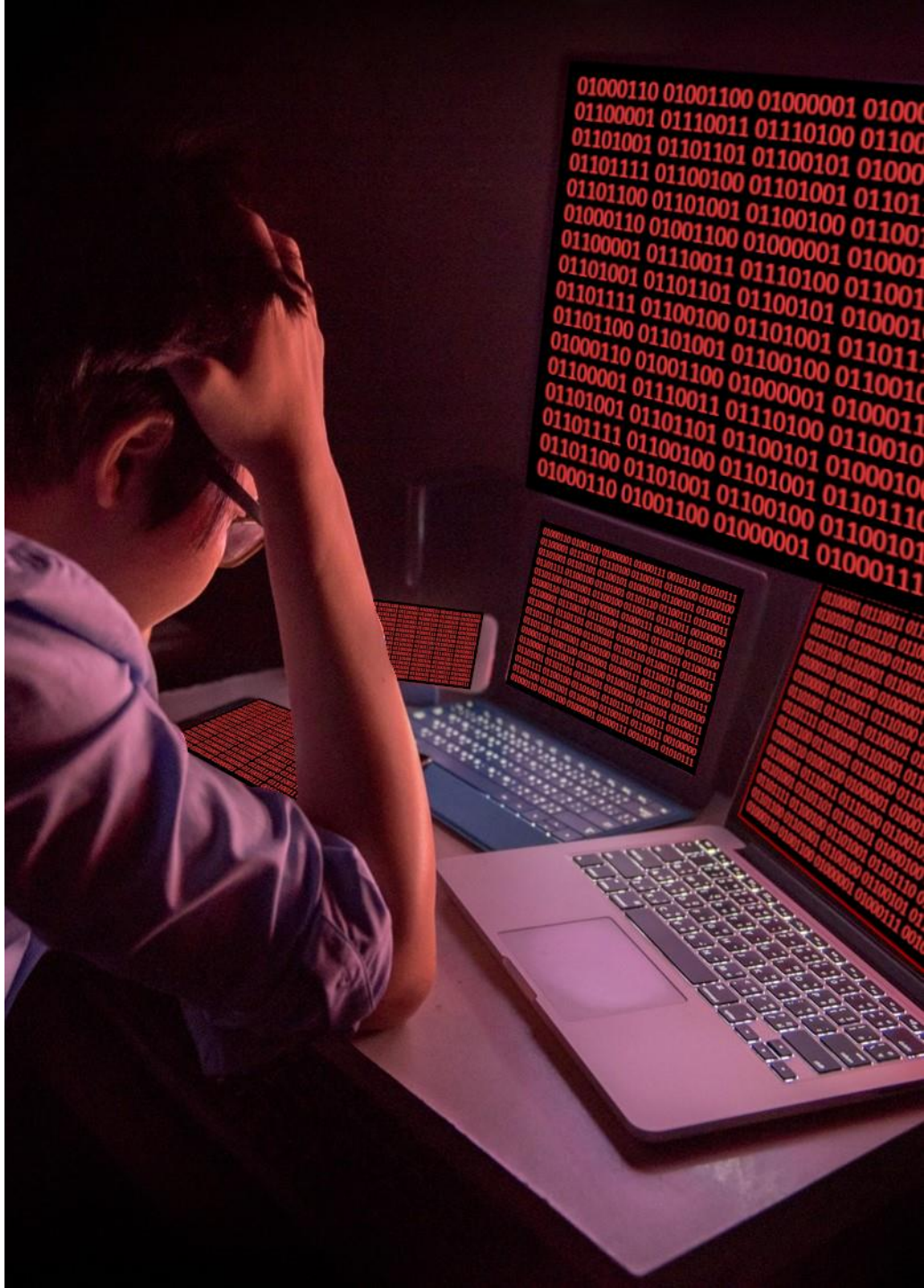
AV	AC	PR	UI	S	C	I	A	Score	Rating	Shown Rating	Source
-	-	-	-	-	-	-	-	-	-	Info	Tenable Nessus – Plugin 84502
N	L	N	N	U	L	L	N	6.5	Medium	Medium	Tenable Nessus – Plugins 98056 and 142960
N	H	N	N	U	H	N	N	4.8	Medium	Medium	Crash-Test Security
N	H	N	N	U	H	H	L	7.7	High	Medium	Invicti
N	L	N	R	C	N	N	N	0.0	None	Low	Acunetix
N	H	N	N	U	H	H	N	7.4	High	Low	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

Vulnerability Scoring

Challenges

The takeaways ?

- CVSS is hard
- CVSS is not made to evaluate security controls



Missing Security Controls

What a report may look like year 1

Severity Level	List of Findings	CVSS Score
High	1. Local File Inclusion (LFI)	8.5
Medium	2. Cross-Site Scripting (XSS)	6.1
Medium	3. User Enumeration	5.3
Medium	4. Sensitive Information in Browser's Local or Session Storage	4.0
Low	5. Information Disclosure through Server Headers	3.7
Info	6. Cookie Without the "HttpOnly", "Secure" and/or "SameSite" Flags	0.0
Info	7. Missing HTTP Strict Transport Security (HSTS)	0.0
Info	8. Inadequate Content-Security-Policy (CSP) protection	0.0

Missing Security Controls

What a report may look like year 2, 3, 4, 5, etc.

Severity Level	List of Findings	CVSS Score
Low	1. Information Disclosure through Server Headers	3.7
Info	2. Cookie Without the "HttpOnly", "Secure" and/or "SameSite" Flags	0.0
Info	3. Missing HTTP Strict Transport Security (HSTS)	0.0
Info	4. Inadequate Content-Security-Policy (CSP) protection	0.0

Introducing "Missing Security Controls"

GoSecure

Missing Security Controls

How do you "sell" safety?

Where do you trace the line between a vulnerability and a missing security control?

How do you communicate issues to the different stakeholders?

How do you evaluate the benefits of something that has no immediate impact?

Missing Security Controls

How do you "sell" safety?

Missing Security Controls

How do you "sell" safety?

Network Access Control (Credit to Laurent Desaulniers)

- Red team engagement
- No way to compromise servers via the external perimeter
- Phishing attempts did not yield code execution

Missing Security Controls

How do you "sell" safety?

All “Informational”, and yet the customer was breached

Severity Level	List of Vulnerabilities	CVSS Score
Informational	1. Missing network Access Control (NAC)	0.0
Informational	2. Inadequate Security Awareness Training Program	0.0
Informational	3. Insufficient Network Segmentation / Isolation	0.0
Informational	4. Usage of Legacy RFID Protocols	0.0

VS.

Severity Level	List of Missing Security Controls	CVSS Score
High	1. Missing network Access Control (NAC)	-
Medium	2. Inadequate Security Awareness Training Program	-
Low	3. Insufficient Network Segmentation / Isolation	-
Low	4. Usage of Legacy RFID Protocols	-

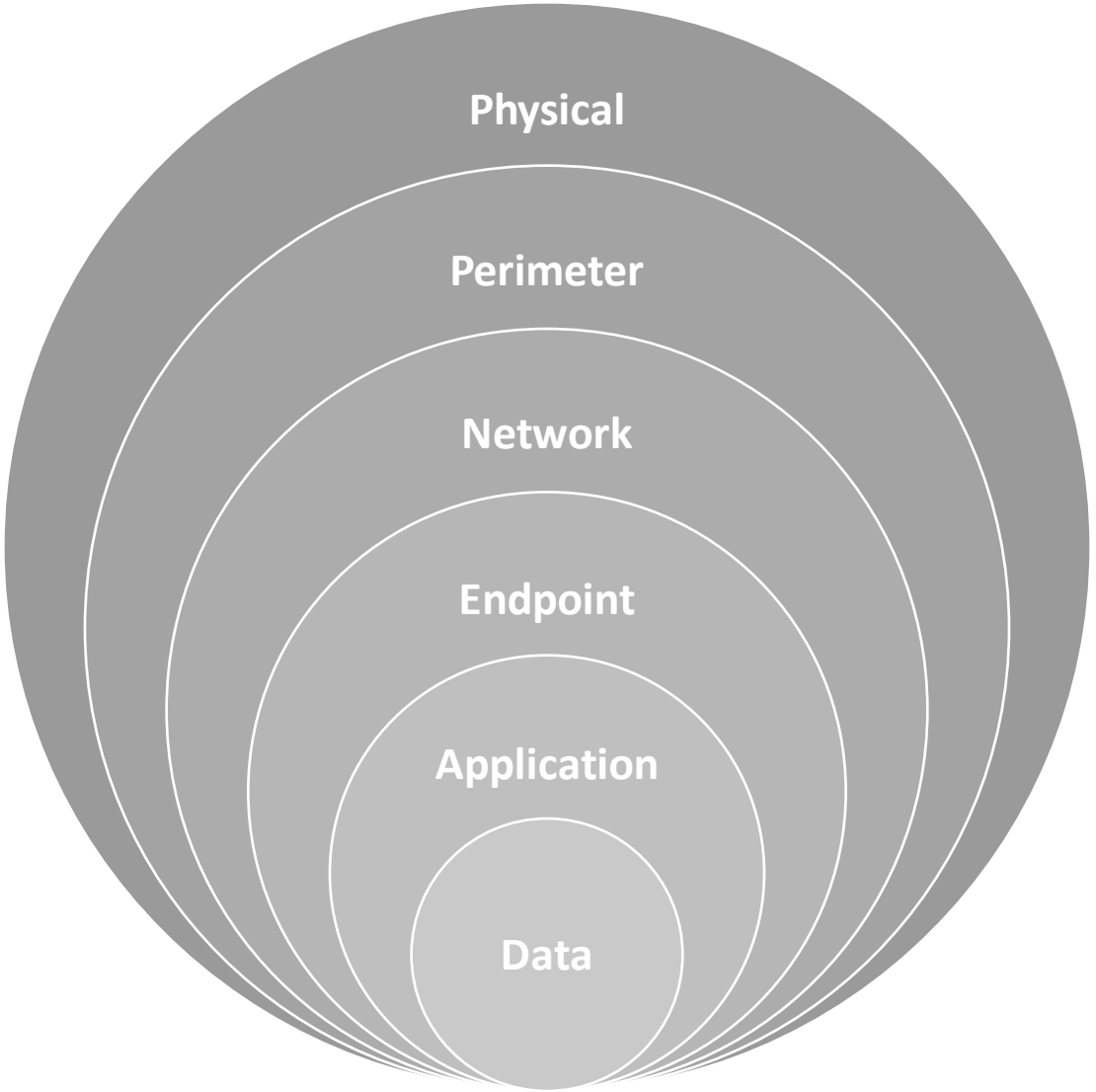
Missing Security Controls

Where do you trace the line?

- CVSS already evaluates vulnerabilities
- Missing Security Controls should only be used to cover the gaps, not to override a severity you do not agree with
- Still somewhat complex to evaluate in some cases (Policy vs. occurrence)

Missing Security Controls

How do you communicate the issues to the different stakeholders?



Missing Security Controls

How do you communicate the issues to the different stakeholders?

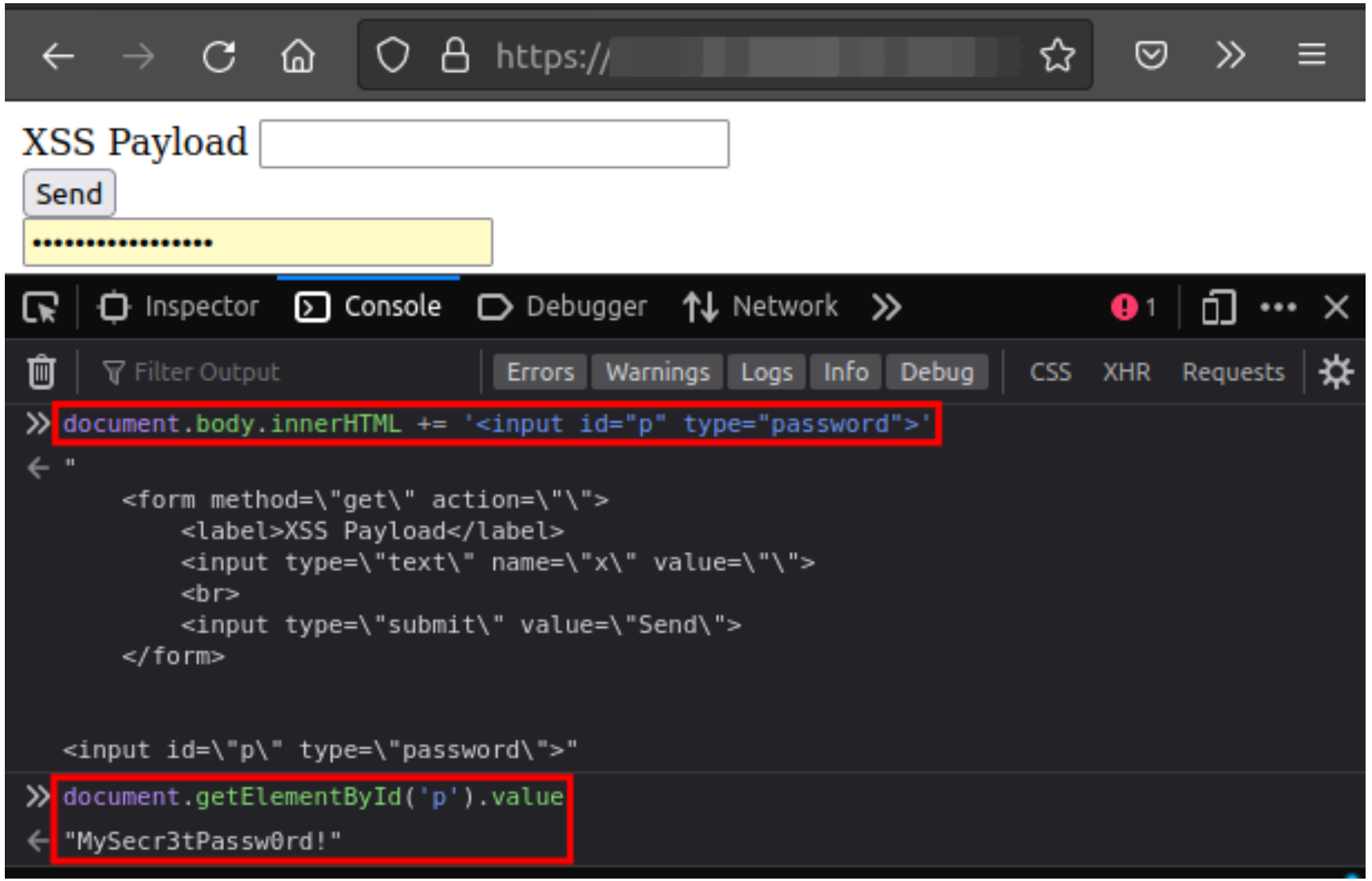
Browser's Autofill (Credit to Marc Olivier Bergeron)

Most browsers nowadays will offer some kind of "password vault" system that can autofill credentials for you.

This feature can often be abused by attackers to steal credentials when an XSS vulnerability is discovered.

Missing Security Controls

How do you communicate the issues to the different stakeholders?



Missing Security Controls

How do you communicate the issues to the different stakeholders?

Mitigations

- **Web Developer**
- **Web Server Administrators**
- **Security Administrators**
- **Security Architects**

Missing Security Controls

How do you communicate the issues to the different stakeholders?

Mitigations

- **Web Developer**
  - Encode / Filter user inputs
- **Web Server Administrators**
  - Put in place a CSP
- **Security Administrators**
  - Prevent users from saving their credentials via GPO
- **Security Architects**
  - Create a policy governing password vaults and encourage users to avoid browser-based solutions

Missing Security Controls

How do you evaluate the benefits?

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])

Missing Security Controls

How do you evaluate the benefits?

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])

Missing Security Controls

How do you evaluate the benefits?

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])

Missing Security Controls

How do you evaluate the benefits?

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])

Missing Security Controls

How do you evaluate the benefits?

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])

Missing Security Controls

How do you evaluate the benefits?

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])

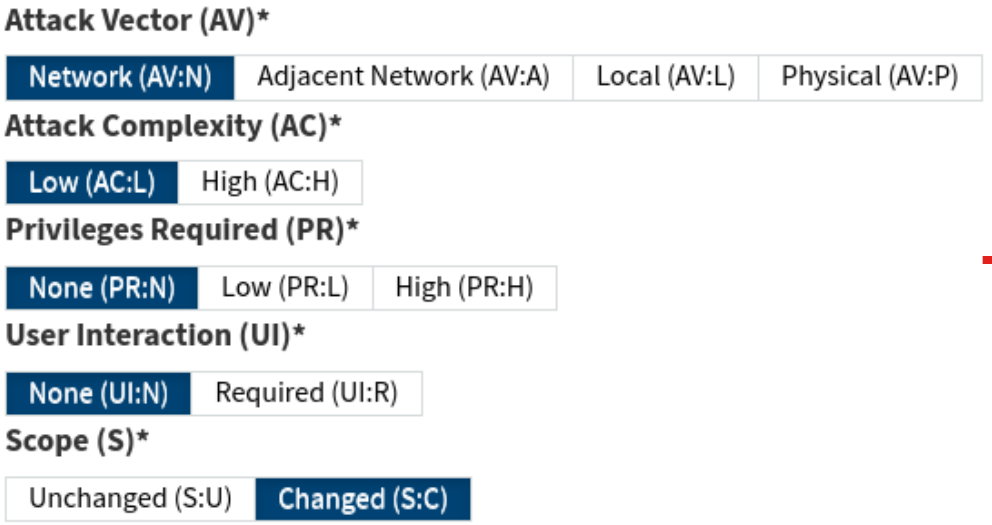
Missing Security Controls

How do you evaluate the benefits?

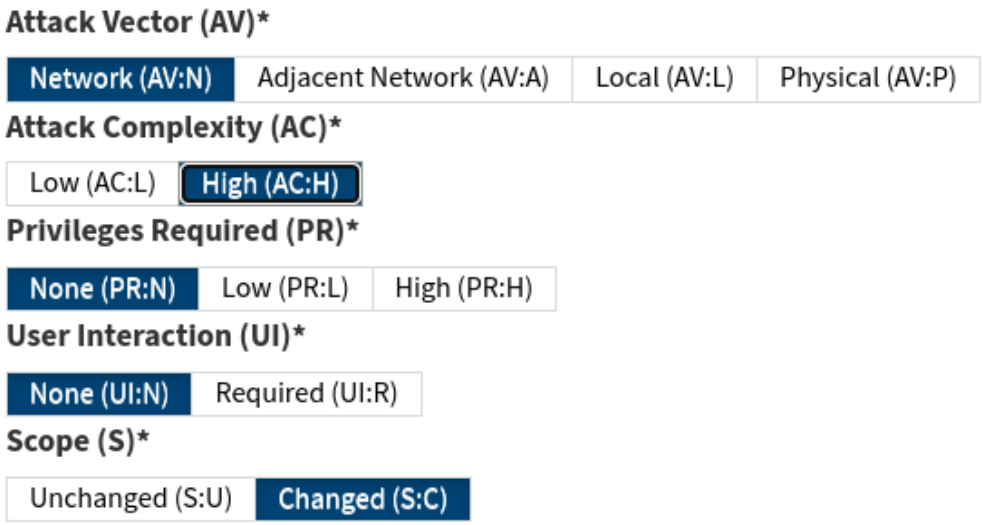
Exploitability		
	8.22 × Attack Vector × Attack Complexity × Privileges Required × User Interaction	
Base Score		
	If Scope is Unchanged	Roundup (Minimum [(Exploitability), 10])
	If Scope is Changed	Roundup (Minimum [1.08 × (Exploitability), 10])

Missing Security Controls

How do you evaluate the benefits?



Score: 4.2



Score: 2.4

We have a delta of 1.8 out of a theorical possible 4.0

Missing Security Controls

How do you evaluate the benefits?

0 → Informational

0.1 to 1.3 → Low

1.3 to 2.7 → Medium

2.8 to 4.0 → High

Missing Security Controls

Severity Level	List of Missing Security Controls	CVSS Score
Medium	1. Missing HTTP Strict Transport Security (HSTS)	-
Medium	2. Inadequate Content-Security-Policy (CSP) protection	-
Low	3. Cookie Without the "HttpOnly", "Secure" and/or "SameSite" Flags	-
Severity Level	**List of Findings**	**CVSS Score**
High	4. Local File Inclusion (LFI)	8.5
Medium	5. Cross-Site Scripting (XSS)	6.1
Medium	6. User Enumeration	5.3
Medium	7. Sensitive Information in Browser's Local or Session Storage	4.0
Low	8. Information Disclosure through Server Headers	3.7

Missing Security Controls

Conclusion

The notion of “Missing Security Controls” is still a work in progress

A basic calculator using our latest rating methodology (along with the slides for this presentation) can be found at https://gosecure.github.io/missing-security-controls/

Comments are always welcome!

Questions

GoSecure