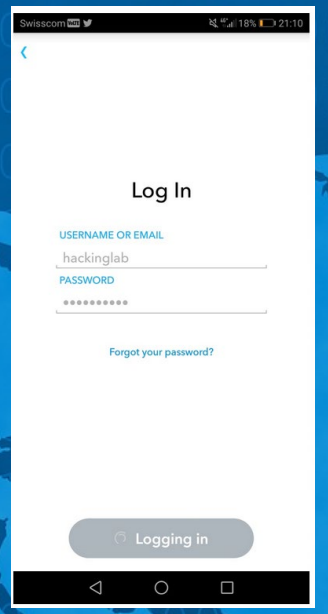
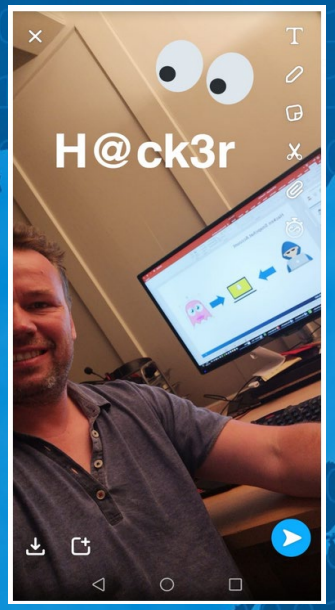
DIREKTE ATTACKEN


Snap
Chat
H@ck3r


H@ck3r
Snap
Chat
Hacking Server
Hacking des Handy oder des PC eines Benutzers

Benutzername
Passwort





Hier ist Dein
Passwort
gespeichert

Default Passwords

https://github.com/scadastrangelove/SCADAPASS

G18 | http://www.router-defaults.com/Router/BinTec--x1200-ip-password-username

	A	B	C	D	E	F
1	#SCADA StrangeLove Default/Hardcoded Passwords List					
2	#Find more at http://www.scada.sl					
3	#Please contact us at scadastrangelove@gmail.com and @scadasl					

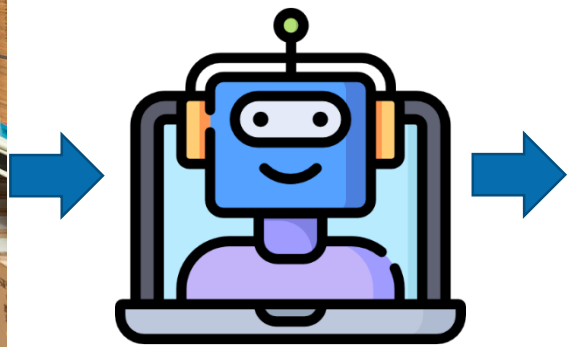
siemens	Simatic S7-300 (pre-2009 versions)	Hardcoded password:, Basisk:Basisk			
siemens	Scalance	admin:admin, user:user			
siemens	Scalance (x 200, W788-1PRO, W788-2PF	Admin:admin, User:user, for FTP access:			
siemens	SyncoTM living Web server OZW772 V2	Administrator:Password			
siemens	Siemens WinCC 7.x	winccd:winccpass, wincce:winccpass, DI			
siemens	Ruggedcom RMC30	admin:admin			
siemens	RuggedSwitch, RS8000 / RS1600 / RS900	admin			

19	BinTec Elmeg	any routers	(##unknown - means not known or any ch		Router	
20	BinTec Elmeg	BinTec R230aw	admin:funkwerk		Router	
21	BinTec Elmeg	bintec W2002T-n,	admin:funkwerk, admin:admin		WLAN Access Point f	
22	Contemporary Control Systems	BASRT-B	admin:admin	80/tcp	Router	http
23	Datasensor	UR5i/UR5i SL	root:root	80/tcp	Router	http
24	Digi	DC-ME-01T-S	root:dbps		Networki	http
25	Digi	Digi Connect SP, Digi Connect Wi-SP, Di	root:dbps	80/tcp	Network I	http
26	Digi	Digi Connect ES 4/8 SB with Switch, Digi	root:dbps	80/tcp	Concentra	http

Wie kann sich der Snapchat Server schützen?

Ein Hacker Tool versucht alle Benutzernamen und Passwortkombinationen

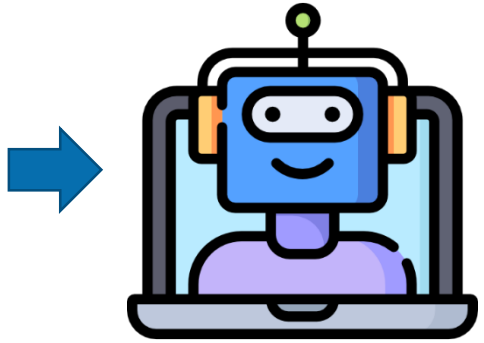
Wörterbuch Attacke



Brute Force Attacke

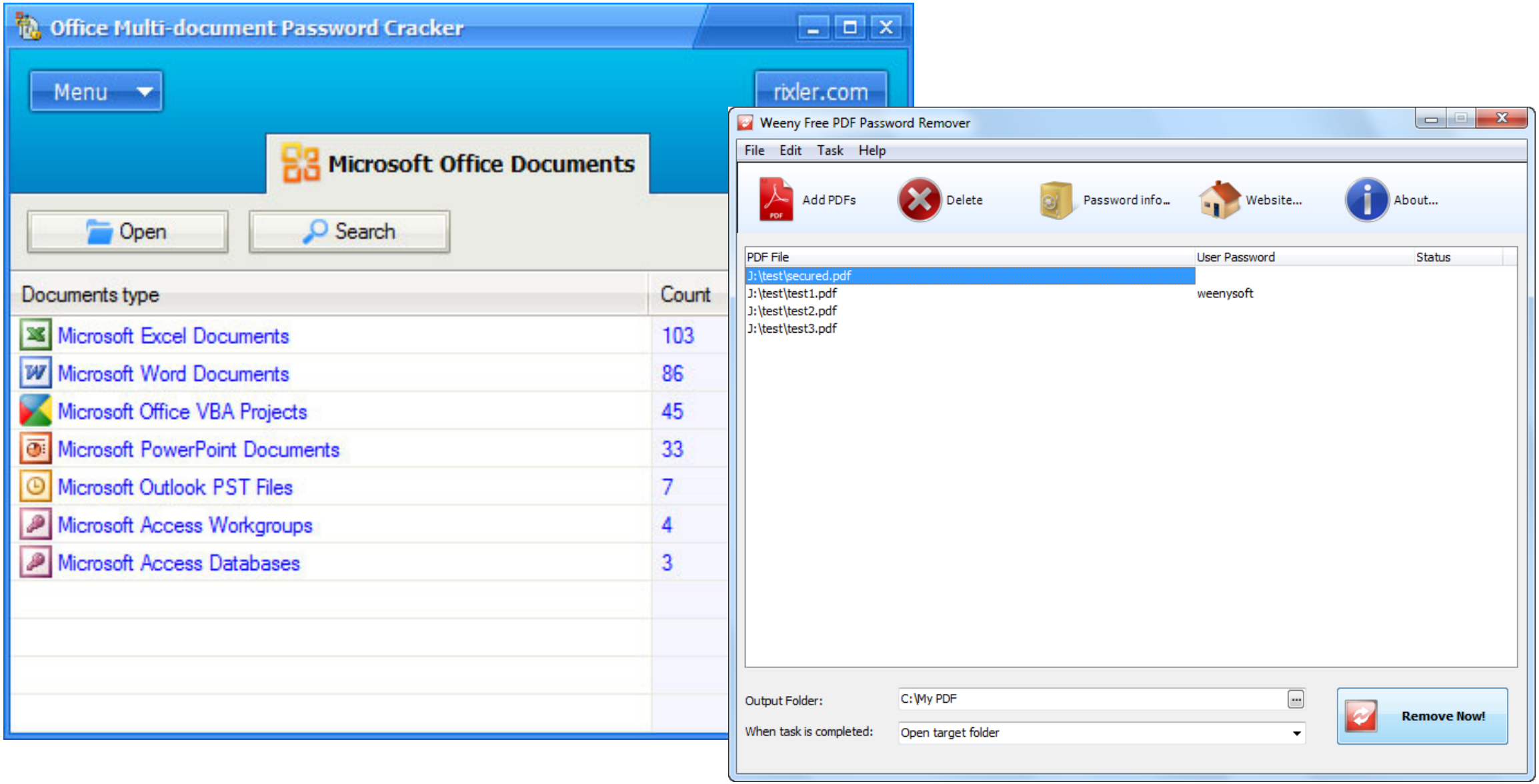
A-Z, a-z, 0-9, ;.:-_$!?

6-10 Zeichen lang



Beispiel: iCloud Angriff am 31. August 2014

Brute Force Angriffe auf Passwort-geschützte Files

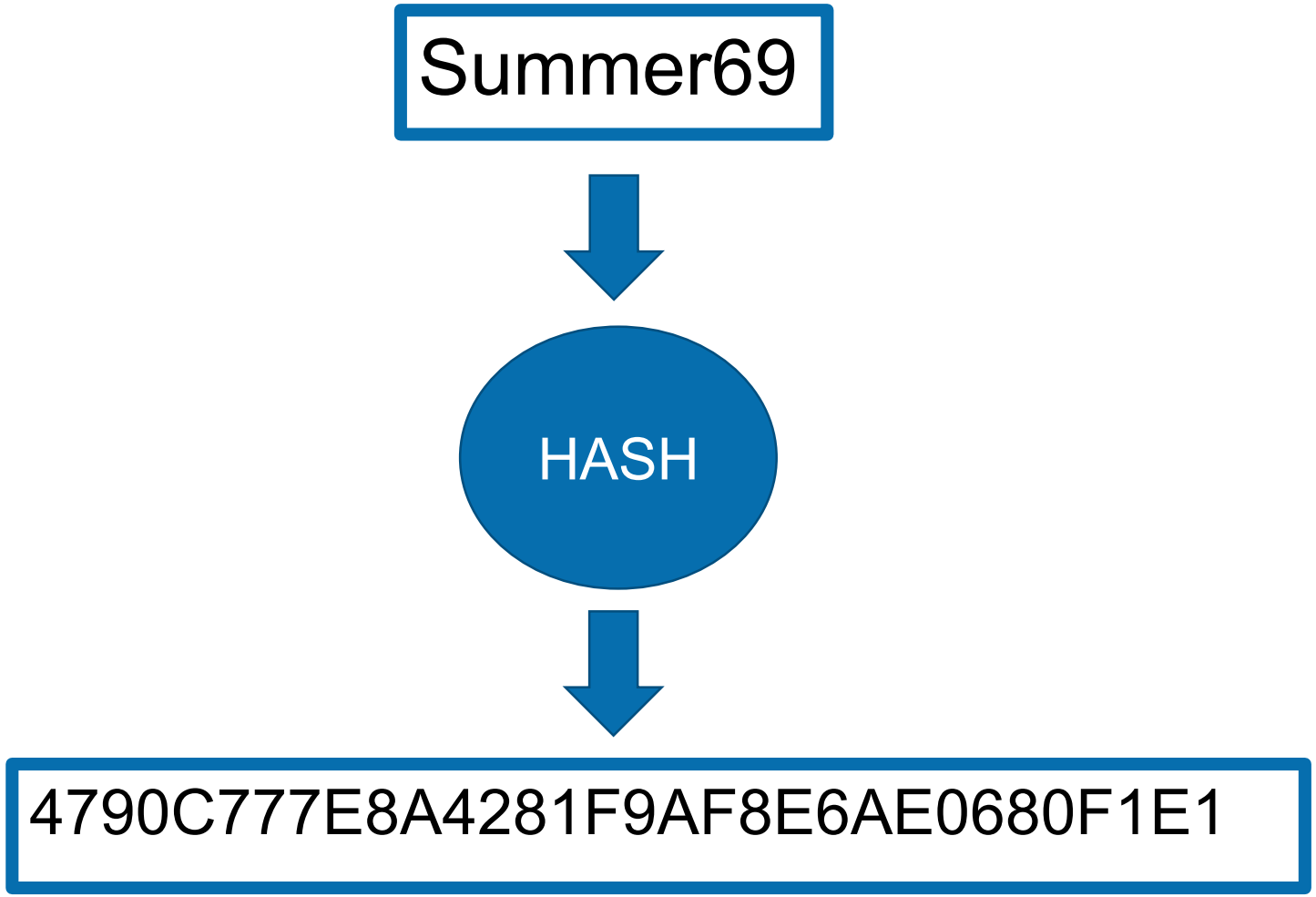


Benutzername	Passwort
Amelie	super.duper
Amrei	gugus.blabla
Antonia	I.love.you
Ariane	Zürich.rockt
Charlotte	CoolerTyp
Daniela	JustinB
Emmanuelle	Warum.warum
Flurina	LOListcool
Friederike	SnapMeIfYouCan
Jenny-Lee	ManInBlack
Leanne	Tarzan
Lilly	Sorglos
Louisa	Ottawa
Luisa	E12344
Lynn	TomJerry
Mina	Knalltüte
Nancy	CuperReagan
Noëmi	WhyYou
Sara	Katakombe
Sarah	Traumschiff
Silvy	SATW.WTAS
Edith	Summer69

Wie kann sich der Snapchat Server schützen?

Ein Hacker findet eine Sicherheitslücke im Snapchat Server und kann auf alle Passwörter zugreifen

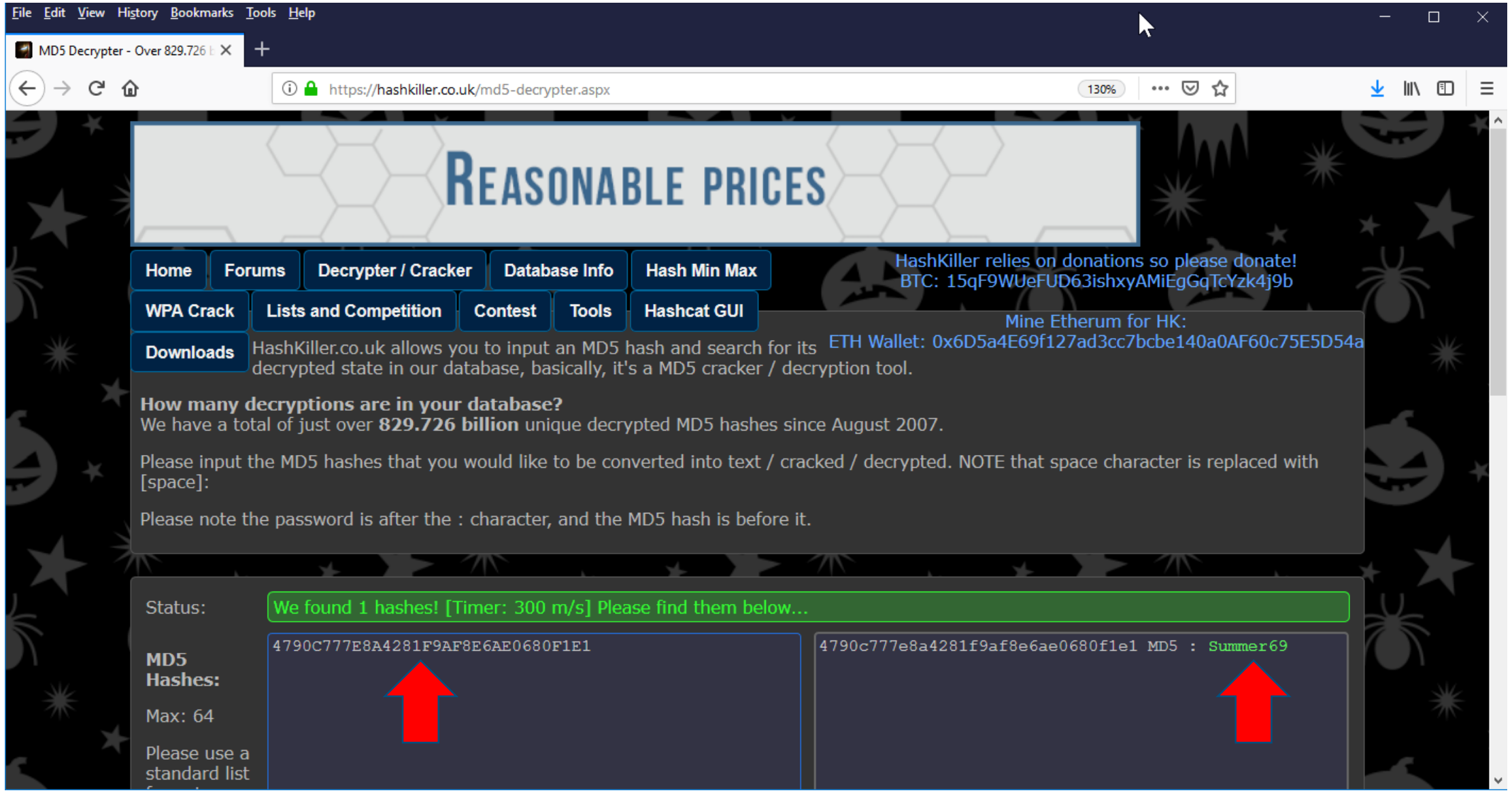
Kryptografische Einwegfunktion – Hash Funktion



Benutzername	Passwort Hash
Amelie	A0337491D534C454B0FFC189A16C5B68
Amrei	46F82E1044FB484CF7B8D6A20940E7E4
Antonia	B3A94D0953B0C235E252184418D7CC9A
Ariane	5F7CDFBB90BAECE317B464DAB7A4C137
Charlotte	FF805A2B2E90AB8611225018D44BF289
Daniela	242EA2AF70D3CCA14F28B22FFDC4D6F0
Emmanuelle	2590B9230225A7B4B073A2F3378D4563
Flurina	8DF09C418A115B5BA31151AE00FB540C
Friederike	438EDEC0D099C59B97E848908653703A
Jenny-Lee	5F8332B873790798969087ED722DB487
Leanne	4DE848360ED53B999421A6024CE41516
Lilly	46F281CB06C1530AE8692D20AF836F8D
Louisa	AEEE33366B173305B90377ED63C1084A
Luisa	408956C5A776196BD0BA578ECC6F9E97
Lynn	933E1F4B9EB0720C27FAE08D41294D5A
Mina	1AD9D64D109BF16108387B52FF1AD0AC
Nancy	D7E0EAA746A35898FDC50986A53A1A14
Noëmi	4B4C8261D3850EAE0F114FB582CE1263
Sara	252020B288D5BEDE8F124102E34AC97E
Sarah	3B43745CCAF1AF61D50F4DDEF59B1BEF
Silvy	DDEACCF090EB084B457395E2CC882EAD
Edith	4790C777E8A4281F9AF8E6AE0680F1E1

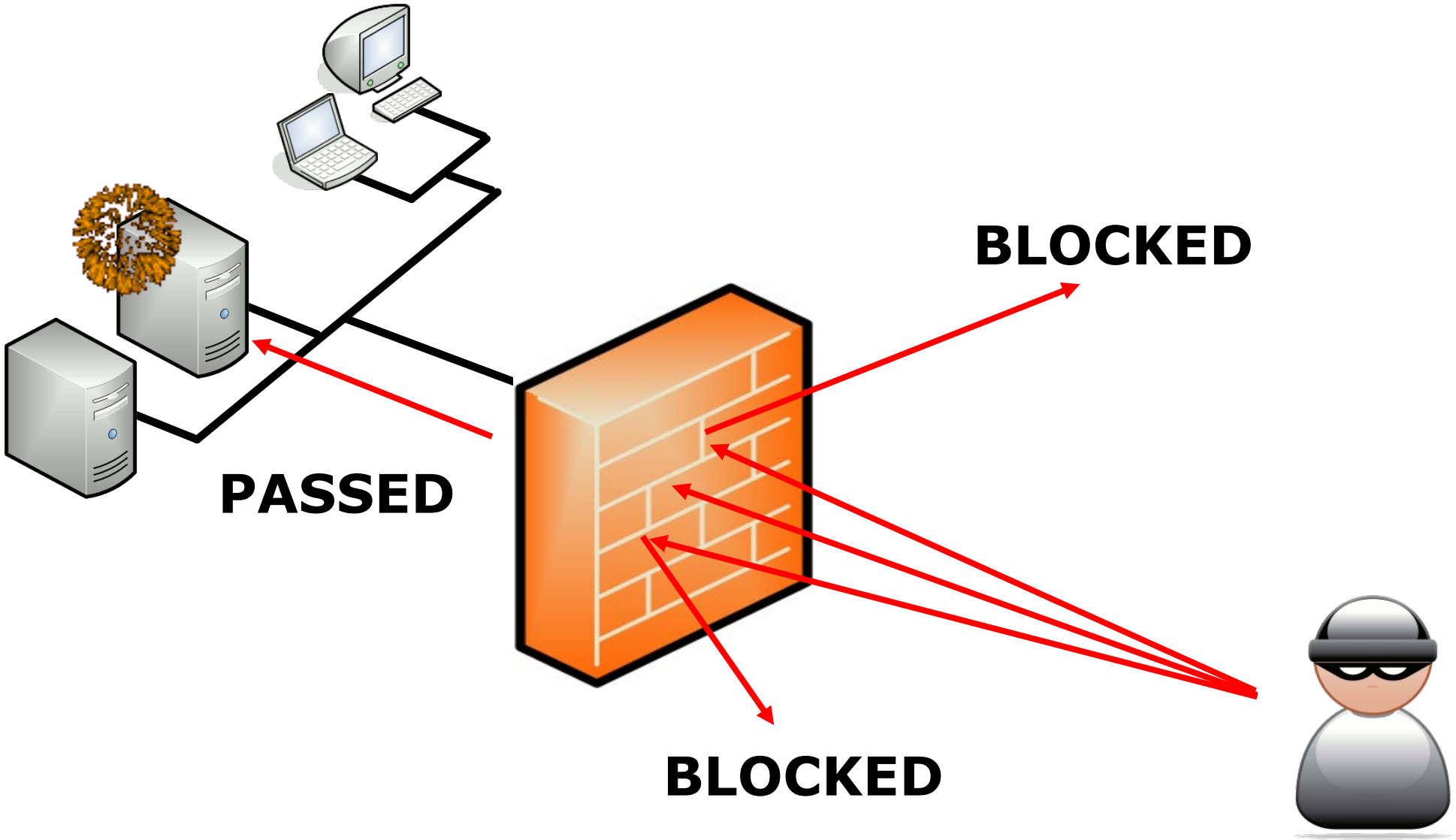
Ein Hacker findet eine Sicherheitslücke im Snapchat Server und kann auf alle Hashes zugreifen

https://hashkiller.co.uk/md5-decrypter.aspx



Ein Hacker findet eine Sicherheitslücke im Server und kann Daten auslesen

Hacker 1x1: Server Exploit



Was waren die letzten 5 Folien für Schwachstellen?

Schwachstelle im Monitoring, Überwachung	Forensic Readiness, Fraud Detection
Schwachstelle in der Anwendung	Sichere Programmierung, Schulung Entwickler
Schwachstellen bei eingesetzten Bibliotheken (Libraries)	Patching, Updating von Libraries, Bibliotheken
Schlecht konfigurierte Anwendung (z.B. SSL/TLS)	Hardening (muss man selbst machen)
Schwachstelle des Application Services (Web, DNS, FTP, SSH)	Patching (Hersteller)
Schwachstelle auf TCP/IP (Netzwerk Ebene)	Firewall & Patching OS (Produkt) durch Hersteller

Schwachstellen in Anwendungen: OWASP TOP 10 / 2010

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Schwachstellen in Anwendungen: OWASP TOP 10 / 2013

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Schwachstellen in Anwendungen: OWASP TOP 10 / 2017

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

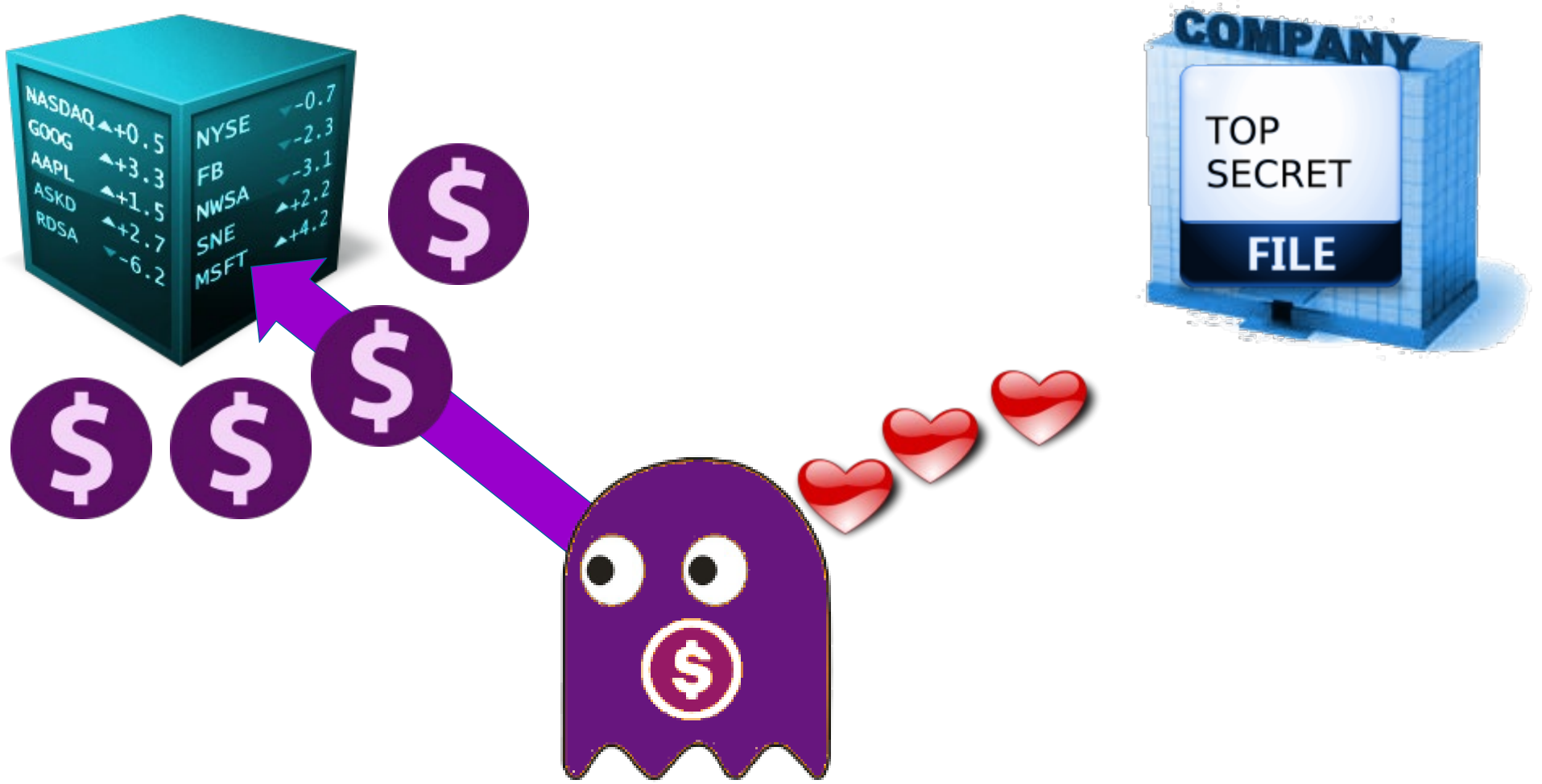
A1 «SQL Injection»

siehe separate Folien (umfassend)

A7 «XSS Cross Site Scripting»

siehe separate Folien (umfassend)

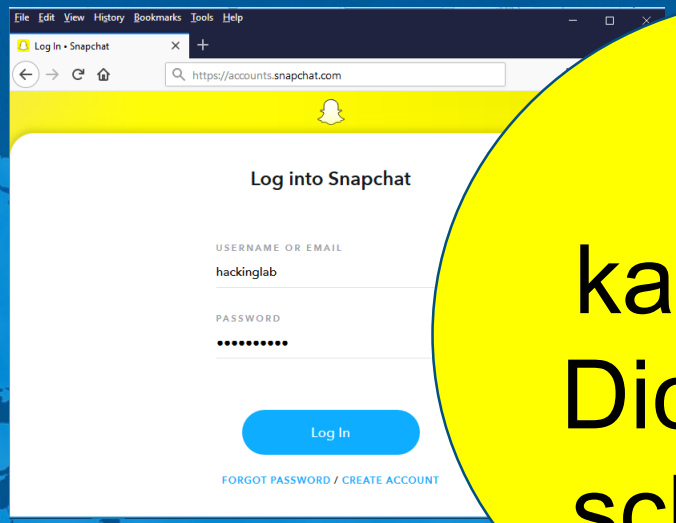
Vertrauliche Daten von kompromittierten Servern



SQL Injection

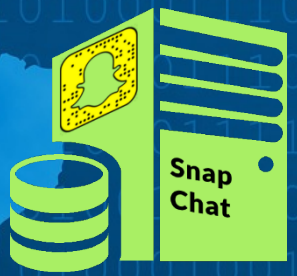
Phishing Angriff

Benutzername
Passwort



Wie kannst Du Dich davor schützen?

Benutzername
Passwort



Der Hacker erstellt eine Seite, die genau gleich aussieht wie das Original

«Phishing»

siehe separate Folien (umfassend)


SECURITY