



OWASP

Open Web Application
Security Project

Burp Suite - Teil 1

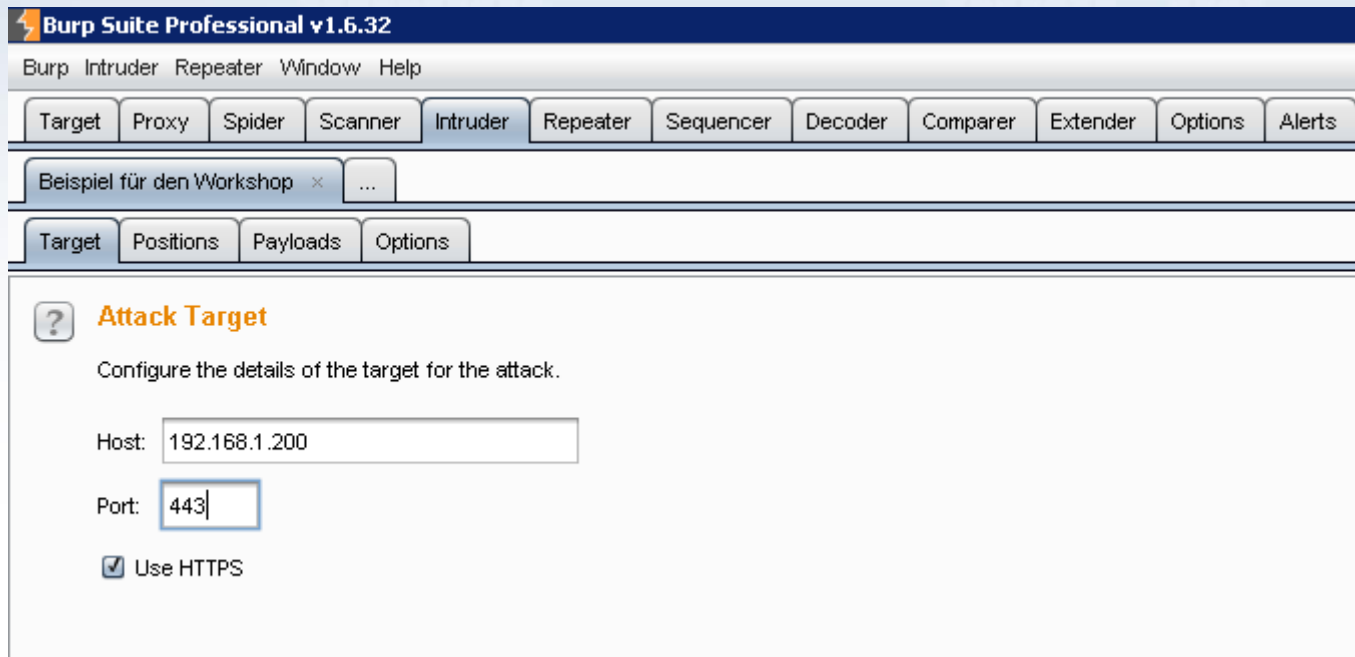
Der Intruder

Überblick

- Was ist / wie funktioniert der Intruder?
 - ! Nur die wichtigsten Schalter / Funktionen (RTFM 😊)
- Wie und wofür benutzt der Simon den Intruder?
 - Hands on bzw. Demo
- Anregung zur Diskussion
 - Wofür nutzt Ihr den Intruder (noch)?

Was ist der Intruder

- Attack-Werkzeug innerhalb der Burp Suite
- Erlaubt das Fuzzing von Parametern in HTTP-Requests



The screenshot displays the Burp Suite Professional v1.6.32 interface. The main menu includes 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below the menu is a toolbar with buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Options', and 'Alerts'. A tab titled 'Beispiel für den Workshop' is active. The 'Intruder' sub-menu is open, showing 'Target', 'Positions', 'Payloads', and 'Options' tabs. The 'Attack Target' configuration window is visible, containing a help icon, the title 'Attack Target', and the instruction 'Configure the details of the target for the attack.' The 'Host' field is set to '192.168.1.200' and the 'Port' field is set to '443'. The 'Use HTTPS' checkbox is checked.

Wie funktioniert der Intruder

- Festlegen eines Ziels
 - Am Einfachsten: Senden eines Requests zum Intruder

2	https://192.168.1.200/	
3	https://192.168.1.200/	https://192.168.1.200/
4	https://192.168.1.200/	Add to scope
5	https://192.168.1.200/	Spider from here
6	https://192.168.1.200/	Do an active scan
7	https://192.168.1.200/	Do a passive scan
8	https://192.168.1.200/	Send to Intruder
9	https://192.168.1.200/	Send to Repeater
10	https://192.168.1.200/	Send to Repeater

- Festlegen der Injektionspunkte
 - Mit „\$“ kennzeichnet man Beginn und Ende

Burp Suite Professional v1.6.32 - Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Beispiel für den Workshop

Target Positions Payloads Options

? Payload Positions Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /?bla=$blubb$ HTTP/1.1
Host: 192.168.1.200
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

Add \$ Clear \$ Auto \$ Refresh

Wie funktioniert der Intruder

- Festlegen der Attackemethode
 - Sniper: nur eine Payload-Liste. Alle Injektionspunkte (Injp) werden einzeln attackiert.
 - Je Injektionspunkt und Payload 1 Request.
 - 2 Injektionspunkte und 4 Payloads ergeben $2*4=8$ Requests
 - Battering Ram: Wie Sniper, es werden aber alle Injp gleichzeitig attackiert.
 - → Je Payload ein Request, alle Injp haben dieselbe Payload je Request
 - 2 Injektionspunkte und 4 Payloads ergeben 4 Requests
 - Pitchfork: Je Injp ein Payload-Set. Wie Battering Ram, jedoch mit einzelnen (Max 20) Injp.
 - Cluster-Bomb: Max 20 Injp und Payload-Sets Iteriert alle möglichen Kombinationen.

Wie funktioniert der Intruder

- Festlegen der Payloads
 - Typ bzw. Herkunft
 - Eigene Listen (auch aus Dateien), Vordefinierte interne (Fuzzing-)Listen, Ersetzen von Characters, Eigene Iteratoren / Nummern,¹
 - Regeln, um Payloads zu verarbeiten, bevor sie in den Injp eingesetzt werden
 - Z. B. Hinzufügen von Präfix, Suffix, Match and Replace, encoding, decoding, Aufrufen von Burp Extensions, ... und viel mehr!²
 - URL-Encoding einzelner Zeichen
 -

1 https://portswigger.net/burp/help/intruder_payloads.html

2 https://portswigger.net/burp/help/intruder_payloads_processing.html

Wie funktioniert der Intruder

- Festlegen von Optionen
 - Geschwindigkeit / Parallelisierung von Anfragen
 - Verarbeitung der Ergebnisse
 - Grep Match: Markieren der Ergebnisse in der Übersicht
 - Festlegen von Schlagwörtern, die in der Antwort vorkommen
 - Grep Extract: Extraktion von Inhalten aus den Antworten
 - Festlegen einer Position mittels String/Regex
 - Folgen von Redirections

Wie funktioniert der Intruder



Quelle: <https://memegenerator.net/instance/30704534>

Wie und wofür benutzt der Simon den Intruder

- Fuzzing encodierter Parameter
 - App nimmt nur bestimmte Payloads oder Content entgegen.
- Bau von „Proof of Concepts“
 - Passwort-Vergessen-Funktionen
 - Erstellen von Benutzerlisten
 - ID-Basierte Skripte
 - Z. B. das Iterieren von Downloads

Wie und wofür benutzt der Simon den Intruder

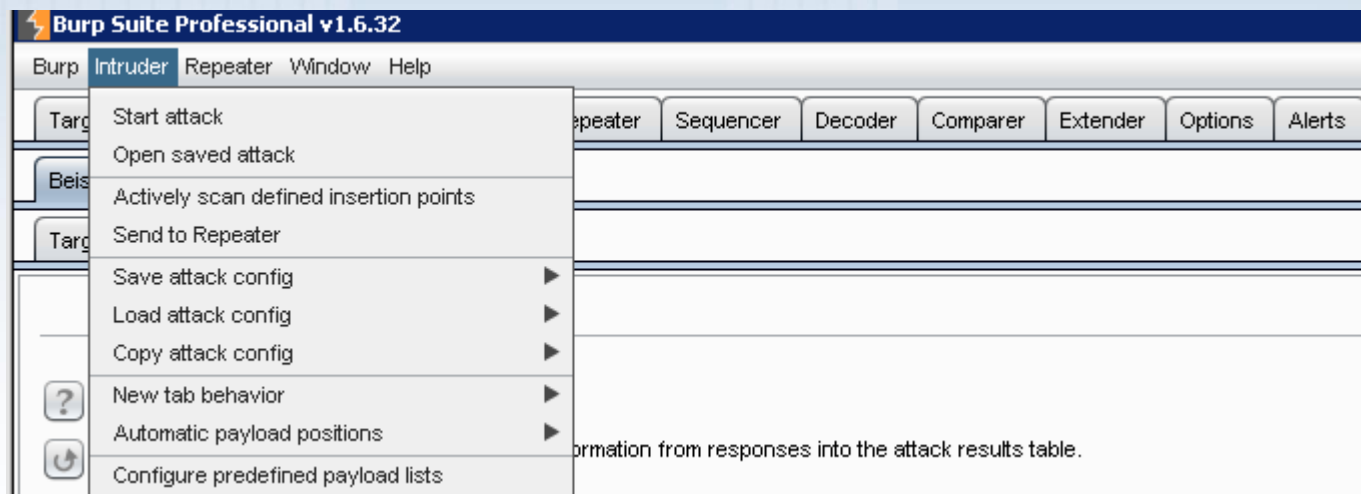
- Erraten von Benutzernamen / E-Mail-Adressen
 - Gültige E-Mail-Adressen herausfinden in veraltetem Joomla CMS
 - Demo mit OWASP Broken Web App VM aus dem OWASP [Vulnerable Web Applications Directory Project](#)

Wie und wofür benutzt der Simon den Intruder

- Demo

Wie und wofür benutzt der Simon den Intruder

- Selektives Scanning
 - „Actively Scan defined insertion Points“.



Wofür nutzt Ihr den Intruder noch?

- Was gibt's noch für Anwendungsfälle?



OWASP

Open Web Application
Security Project

Ende

Danke für die Aufmerksamkeit

Vielleicht gibt's bei einem der nächsten
Stammtische in Stuttgart den 2. Teil... 😊