Burp Suite

Beginner CheatSheet
from
Getting Started
to
Tips for Effective Usage

By Chaos

Burp Suite Cheat Sheet

1. Getting Started

راه‌اندازی Burp

- Burpرا اجرا کرده و مرورگر را باز کنید.
- به مسیر Proxy > Intercept رفته و interception مربوط به HTTP را فعال کنید.

تنظیم Scope هدف:

- Scope هدف خود را در Target > Site map تعریف کنید.
- بر روی ورودی مورد نظر در site map راست‌کلیک کرده و Add to scope را انتخاب کنید.
- با انتخاب گزینه Yes هنگامی که از شما سؤال می‌شود، ترافیک خارج از scope را حذف کنید.

---

2. Proxy

Intercept ترافیک:

- Proxy > Intercept را فعال کنید تا درخواست‌ها ضبط شوند.
- از Forward برای ارسال درخواست استفاده کنید، یا قبل از forwarding آن را ویرایش کنید.

تاریخچه HTTP:

- تمامی ترافیک را در Proxy > HTTP history مشاهده کنید.
- برای مشاهده فقط ترافیک درون scope، از Filter > Show only in-scope items استفاده کنید.

---

3. Burp Repeater (Manual Testing)

ارسال درخواست به Repeater:

- روی یک درخواست HTTP در Proxy یا Target راست‌کلیک کرده و Send to Repeater را انتخاب کنید.

تغییر و ارسال درخواست‌ها:

- پارامترها، headers یا body درخواست را تغییر دهید.
- برای مشاهده پاسخ‌های سرور به صورت بلادرنگ، روی Send کلیک کنید.

تجزیه و تحلیل پاسخ‌ها:

- با جابجایی بین tabs در Repeater، پاسخ‌های مختلف را مقایسه کنید.

---

4. Burp Intruder (Automated Attacks)

ارسال درخواست به Intruder:

- روی یک درخواست راست‌کلیک کرده و Send to Intruder را انتخاب کنید.

انواع Attack:

- Sniper: تست یک متغیر در هر زمان.
- Battering Ram: استفاده از یک payload یکسان در چندین موقعیت.
- Pitchfork: استفاده از چندین payload، هر کدام برای یک موقعیت خاص.
- Cluster Bomb: ترکیب payloadها با چندین متغیر.

Payloadها:

- موقعیت‌های payload را انتخاب کرده و نوع payloadها را تنظیم کنید: simple lists، brute-force اعداد یا dictionaries سفارشی.

اجرای Attack:

- برای اجرای brute force یا تست چندین payload به صورت همزمان، روی Start Attack کلیک کنید.

5. Burp Scanner (Vulnerability Scanning)

راه‌اندازی یک Scan:

- به Dashboard > New Scan رفته و URL هدف را وارد کنید.
- بین اسکن‌های Lightweight (سریع) و Thorough (جامع) انتخاب کنید.

پیکربندی Scan:

- گزینه‌های اسکن را تنظیم کنید: cookies، authentication، login sequences و غیره.
- می‌توانید اسکن را به ترافیک درون scope محدود کنید یا تنظیم صحیح scope.

مشاهده نتایج Scan:

- به Dashboard > Issues بروید تا آسیب‌پذیری‌های یافت شده را مشاهده کنید.
- روی هر issue کلیک کنید تا راهنمایی‌های رفع آن را ببینید.

6. Burp Collaborator (Out-of-Band Testing)

پیکربندی Burp Collaborator:

- Collaborator را در مسیر Project options > Misc > Burp Collaborator client فعال کنید.

تست برای OAST:

- Burp Collaborator با ایجاد تعاملات خارجی با سرویس‌ها، به شما در شناسایی آسیب‌پذیری‌های Out-Of-Band مانند DNS lookups یا درخواست‌های asynchronous HTTP کمک می‌کند.

7. Burp Sequencer (Session Analysis)

ضبط Tokens:

- به Sequencer > Live Capture رفته و session tokens را ضبط کنید.
- tokens را برای بررسی میزان randomness آنالیز کنید تا امنیت ارزیابی شود.

آنالیز Manual:

- می‌توانید session tokens را از HTTP history یا یک لیست manual import کرده و randomness آن را ارزیابی کنید.

8. Extender (Extend BurpSuite with Plugins)

بارگذاری Extensions:

- از تب Extender برای بارگذاری قابلیت‌های اضافی از طریق BApp Store استفاده کنید.
- همچنین می‌توانید با استفاده از Burp Extender API، extensions مورد نظر خود را بنویسید.

Extensions محبوب:

- Logger++: قابلیت logging پیشرفته را اضافه می‌کند.
- JWT۴B: JWTs را برای تست authentication مدیریت می‌کند.
- Autorize: تست‌های authorization را به صورت خودکار انجام می‌دهد.

9. Burp Decoder (Encode/Decode Data)

Encoding/Decoding دستی:

- به تب Decoder رفته، داده را paste کنید و متدهای encoding (Base۶۴, URL encoding و غیره) را انتخاب کنید.

رمزگشایی هوشمند:

- از Smart Decode استفاده کنید تا Burp به صورت خودکار ورودی را شناسایی و decode کند.

10. Burp Comparer (Compare Responses)

مقایسه درخواست‌ها و پاسخ‌ها:

- آیتم‌ها را به Comparer ارسال کنید (راست‌کلیک > Send to Comparer).
- آن‌ها را به صورت خط به خط یا به صورت کلی مقایسه کنید که برای تشخیص تفاوت‌های ظریف در رفتار عالی است.

11. Target (Site Mapping & Analysis)

نقشه سایت (Site Map):

- از طریق Target > Site map ساختار سایت را مرور کنید.
- فایل‌ها یا پوشه‌های خاص را برای تحلیل بیشتر هایلایت کنید.

گزینه‌های فیلتر (Filter Options):

- ترافیک در Site Map را فیلتر کنید تا انواع خاصی از درخواست‌ها (مانند JavaScript، تصاویر) را شامل یا حذف کند.

12. Tips for Effective Usage

همکاری بین ابزارها (Collaborate Across Tools):

چندین ابزار Burp را برای تست مؤثر ترکیب کنید. به عنوان مثال، یک درخواست را از Proxy به Intruder یا Repeater ارسال کنید، پاسخ‌ها را تحلیل کرده و سپس تست‌ها را تکرار کنید.

اتوماتیک کردن وظایف رایج (Automate Common Tasks):

- از Macros در Burp برای اتوماتیک کردن اقدامات تکراری مانند login sequences استفاده کنید.

استفاده از Burp Extensions:

- extensions مربوط به Burp Suite (مانند Retire.js برای تشخیص کتابخانه‌های JavaScript منسوخ) را برای گسترش قابلیت‌ها بررسی کنید.

ذخیره/خروجی یافته‌ها (Save/Export Findings):

- session خود را از طریق Project > Save As ذخیره کنید.
- می‌توانید یافته‌ها (مانند issues یا HTTP history) را برای مستندسازی یا تحلیل بیشتر export کنید.

میانبرهای رایج (Common Shortcuts):

- CTRL+Shift+R: ارسال درخواست به Repeater
- CTRL+Shift+I: ارسال درخواست به Intruder
- CTRL+Shift+S: شروع یک scan
- CTRL+Shift+C: ارسال درخواست به Comparer
- CTRL+E: Encode/Decode یک درخواست