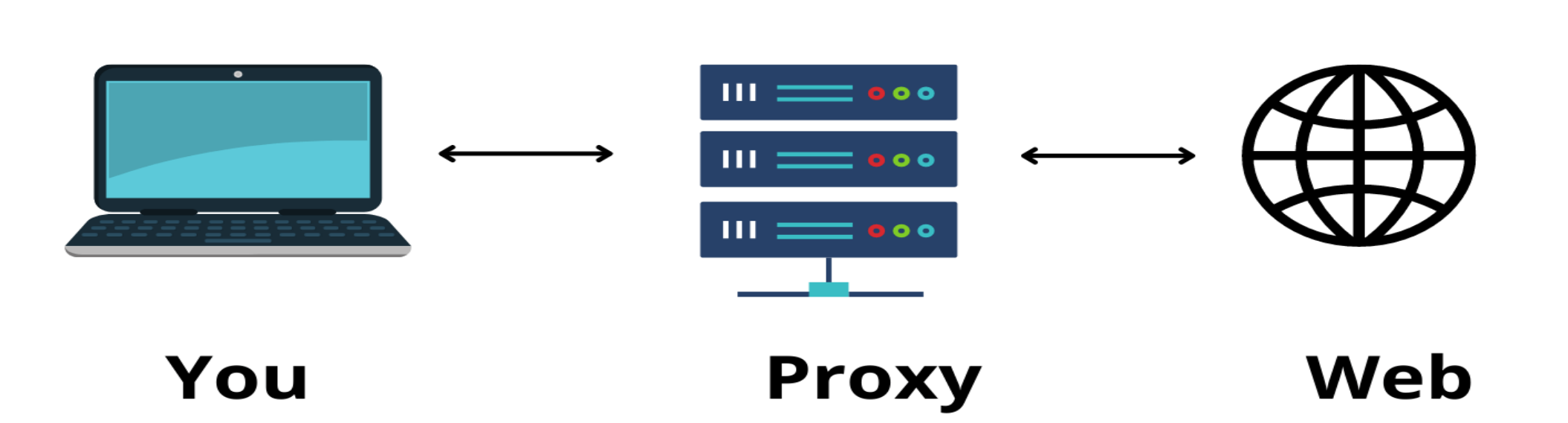
Introduction to Burp Suite

Team Members

- 1703310201375 (Afroza Sultana Riya)
- 1703310201410 (Tanjibul Hasan Rafi)
- 1703310201411 (Sabrina Yesmin)
- 1703310201421 (Pallabi Rudra)
- 1703310201423 (Mehedi Hasan Ovi)

What is Burp Suite?

✓Burp Suite is an integrated platform/graphical tool for performing security testing of web applications.



✓The tool is written in java and developed by PortSwigger.

Burp-Suite Dashboard

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Tasks

New scan | New live task

Filter: Running Paused Finished | Live task Scan Intruder attack

Search...

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

Event log

Filter: Critical Error Info Debug

Search...

Time	Type	Source	Message
12:52:09 4 Jun 2022	Info	Suite	This version of Burp Suite was released over three months ago. Please consider updating
12:52:06 4 Jun 2022	Info	Proxy	Proxy service started on 127.0.0.1:8080

Time to level up? Catch more bugs with Burp Suite Pro — Find out more

Issue activity [Pro version only]

Filter: High Medium Low Info | Certain Firm Tentative

Search...

Issue type	Host	Path	Insertion p
Suspicious input transformation (reflected)	http://insecure-bank.c...	/url-shorten	input paramete
SMTP header injection	http://insecure-websit...	/contact-us	from parameter
Serialized object in HTTP message	http://insecure-bank.c...	/blog	
Cross-site scripting (DOM-based)	https://insecure-bank....	/	
XML external entity injection	https://vulnerable-we...	/product/stock	request body
External service interaction (HTTP)	https://insecure-websi...	/product	Referer HTTP he
Web cache poisoning	http://insecure-bank.c...	/contact-us	
Server-side template injection	http://insecure-bank.c...	/user-homepage	input paramete
SQL injection	https://vulnerable-we...	/	TrackingId cook
OS command injection	https://insecure-websi...	/feedback/submit	subject parame

Advisory

Memory: 89.9MB Disk: 32KB

Burp-Suite Modules

- Target
- Proxy
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender
- Spider
- Scanner

Target Module

- ✓ The Target tool gives you an overview of your target application's content and functionality, and lets you drive key parts of your testing workflow.
- ✓ The key steps that are typically involved in using the Target tab are described below.

Target Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://polyfill.archive.org
- https://push.services.mozilla.com
- https://services.addons.mozilla.org
- https://shavar.services.mozilla.com
- http://www.google.com
- https://www.google.com
  - &ec=GAZAmgQ
  - /
  - advanced_search
  - async
  - client_204
  - complete
  - finance
  - gen_204
  - history
  - images
  - intl
  - js
  - log
  - manifest
  - preferences
  - search
  - search
  - services
  - setprefs
  - tia
  - tools
  - url
  - webhp
  - widget
  - wizrpcui
  - xjs
- https://www.gstatic.com
- https://www.wikipedia.org
- http://www.youtube.com
- https://www.youtube.com

Host	Method	URL	Params	Stat...	Length	MIME type	Title	Comment	Time reques...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.bn.W...	✓	200	2472	script			03:29:55 5 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.bn.W...	✓	200	28438	script			03:29:55 5 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.bn.W...	✓	200	262404	script			03:29:55 5 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...		200	845141	script			10:44:27 7 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	28438	script			10:44:28 7 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	178598	script			10:44:28 7 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...		200	891401	script			11:05:30 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	2460	script			11:13:10 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	350907	script			11:05:32 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	21567	script			11:05:32 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	337543	script			11:13:10 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	14513	script			11:13:09 6 J...
https://www.google.c...	GET	/xjs/_/js/k=xjs.s.en_G...	✓	200	182981	script			11:05:31 6 J...

Request

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host: www.google.com
3 Cookie: NID=
511=fPibK85MXFDbmmB20yss4pYxeESDAEzIvqm5R98c2yThhg
o8tXcojSRtapOHS1qx273qIi0fNzJQAyBRzi_016y1wTYI91BE
BeOR7aLA4tXMStPjn5XLij4ADFQualhkgLJ_h-l6E7A3WUQzFL
MmhJqsIhvvo_ah0xliom2xExap2FtmyWQppm-b2zv39NVh7TEv
Xc4K-Dw; ANID=
AHWqTUkiFl_HfDi2XHVKJttiw34xeQIvd7dnLliIxh1_QjxEuS
DrHnmQBkfD_49T; 1P_JAR=2022-06-06-15; AEC=
AakniGPjpKf7Qbtg4haaE41iqKp3zQ03x-KCnhgCm6I5leaQHt
xKbkbelXQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept:
```

Search... 0 matches

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 07 Jun 2022 14:43:48 GMT
3 Expires: -1
4 Cache-Control: private, max-age=0
5 Content-Type: text/html; charset=UTF-8
6 Strict-Transport-Security: max-age=31536000
7 Server: gws
8 Content-Length: 117643
9 X-Xss-Protection: 0
10 X-Frame-Options: SAMEORIGIN
11 Set-Cookie: 1P_JAR=2022-06-07-14; expires=Thu,
07-Jul-2022 14:43:48 GMT; path=/;
domain=.google.com; Secure; SameSite=none
12 Set-Cookie: AEC=; expires=Mon, 01-Jan-1990
00:00:00 GMT; path=/; domain=www.google.com
```

Search... 0 matches

INSPECTOR

- Request Attributes
- Request Cookies (4)
- Request Headers (14)
- Response Headers (15)

Target Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Use advanced scope control

Include in scope

Add
Edit
Remove
Paste URL
Load ...

Enabled	Prefix

Exclude from scope

Add
Edit
Remove
Paste URL
Load ...

Enabled	Prefix

Target Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope 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 request smuggling	High	0x00200140
Web cache poisoning	High	0x00200180
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310
Cross-site scripting (reflected DOM-based)	High	0x00200311
Cross-site scripting (stored DOM-based)	High	0x00200312

Cross-site scripting (stored)

Description

Stored cross-site scripting vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content.

The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.

Methods for introducing malicious content include any function where request parameters or headers are processed and stored by the application, and any out-of-band channel whereby data can be introduced into the application's processing space (for example, email messages sent over SMTP that are ultimately rendered within a web mail application).

Stored cross-site scripting flaws are typically more serious than reflected vulnerabilities because they do not require a separate delivery mechanism in order to reach target users, and are not hindered by web browsers' XSS filters. Depending on the affected page, ordinary users may be exploited during normal use of the application. In some situations this can be used to create web application worms that spread exponentially and ultimately exploit all active users.

Note that automated detection of stored cross-site scripting vulnerabilities cannot reliably determine whether attacks that are persisted within the application can be accessed by any other user, only by authenticated users, or only by the attacker themselves. You should review the functionality in which the vulnerability appears to determine whether the application's behavior can feasibly be used to compromise other application users.

Remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

Proxy Module

- ✓ Burp Proxy lies at the heart of Burp's user-driven workflow.
- ✓ It operates as a web proxy server between the browser and target applications, and lets you intercept, inspect, and modify the raw traffic passing in both directions.

Proxy Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex \n

```
1 GET /DVWA/vulnerabilities/brute/ HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; security=impossible
9 Upgrade-Insecure-Requests: 1
10
11
```

INSPECTOR

Search... 0 matches

Proxy Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on

Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/brute/ HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
4 Accept: text/html,application/xhtml+xml,application/
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; securi
9 Upgrade-Insecure-Requests: 1
10
11
```

- Scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
  - Response to this request
- Convert selection
- URL-encode as you type
- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V
- Message editor documentation
- Proxy interception documentation

INSPECTOR

Search... 0 matches

Proxy Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Response from http://127.0.0.1:80/DVWA/vulnerabilities/brute/

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2022 15:03:03 GMT
Server: Apache/2.4.51 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4298
Connection: close
Content-Type: text/html;charset=utf-8


<!DOCTYPE html>

<html lang="en-GB">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*
    </title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

    <link rel="icon" type="\image/ico" href="../../favicon.ico" />

    <script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
    </script>

  </head>

  <body class="home">
```

Search... 0 matches

INSPECTOR

Intruder Module

- ✓ Burp Intruder is a tool for automating customized attacks against web applications.
- ✓ It is extremely powerful and configurable, and can be used to perform a huge range of tasks, from simple brute-force guessing of web directories through to active exploitation of complex blind SQL injection vulnerabilities.

Intruder Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Target Positions Payloads Resource Pool 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

```
1  POST /DVWA/vulnerabilities/brute/ HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 83
9  Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
12 Cookie: PHPSESSID=§heaiaarlq3jplppsghjqda5okq§; security=§impossible§
13 Upgrade-Insecure-Requests: 1
14
15 username=§admin§&password=§123§&Login=§Login§&user_token=§d3cccdbef4bc98411776b1d3d6635703§
```

Add § Clear § Auto § Refresh

Search... 0 matches Clear

6 payload positions Length: 655

Intruder Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Target Positions Payloads Resource Pool 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

Deduplicate

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Repeater Module

- ✓ Burp Repeater is a tool for manually manipulating and reissuing individual HTTP requests and analyzing the application's responses.
- ✓ Its biggest use is to combine with other Burp Suite tools. You can browse the records from the target site map, from Burp Proxy, or send a request from the Burp Intruder attack result to the Repeater, and manually adjust the request to fine-tune the detection or attack on the vulnerability.

Repeater Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × ...

Send Cancel < > Target: http://127.0.0.1 HTTP

Request

Pretty Raw Hex \n

```
1  POST /DVWA/vulnerabilities/brute/ HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 83
9  Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
12 Cookie: PHPSESSID=heaiaar1q3jp1ppsghjqda5okq; security=impossible
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=123&Login=Login&user_token=
   2782ebef21ad810da6d84b6d5e0edc0f
```

Search... 0 matches

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 200 OK
2  Date: Thu, 09 Jun 2022 13:27:49 GMT
3  Server: Apache/2.4.51 (Debian)
4  Expires: Tue, 23 Jun 2009 12:00:00 GMT
5  Cache-Control: no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 4503
9  Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html>
14
15 <html lang="en-GB">
16
17   <head>
18     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
20     <title>
         Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA)
         v1.10 *Development*
       </title>
21
22     <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
23
24     <link rel="icon" type="\image/ico" href="../../favicon.ico" />
25
26     <script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
```

Search... 0 matches

INSPECTOR

- Request Attributes
- Query Parameters (0)
- Body Parameters (4)
- Request Cookies (2)
- Request Headers (12)
- Response Headers (9)

Sequencer Module

- ✓ Burp Sequencer is a tool for analyzing the quality of randomness in a sample of data items.
- ✓ You can use it to test an application's session tokens or other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.

Sequencer Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex \n

```
1  POST /DVWA/vulnerabilities/weak_id/ HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 0
9  Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/vulnerabilities/weak_id/
12 Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; security=impossible
13 Upgrade-Insecure-Requests: 1
14
15
```

INSPECTOR

Search... 0 matches

Sequencer Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on

Comment this item HTTP/1

Pretty Raw Hex

```
1  POST /DVWA/vulnerabilities/weak_id/ HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:
4  Accept: text/html,application/xhtml+xml,applica
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencodec
8  Content-Length: 0
9  Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/vulnerabilities/
12 Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; s
13 Upgrade-Insecure-Requests: 1
14
15
```

- Scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V
- Message editor documentation
- Proxy interception documentation

INSPECTOR

Search... 0 matches

Sequencer Module

Burp Suite Comm

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer

Live capture Manual load Analysis options

Select Live Capture Request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options be

Remove

Clear

#	Host	Request
1	http://127.0.0.1	POST /DVWA/vulnerabilities/weak_id/ HT...

Start live capture

Token Location Within Response

Select the location in the response where the token appears.

Cookie: dvwaSession=7abfd86ebfba948021d9 ...

Form field:

Custom location: Configure

Live Capture Options

These settings control the engine used for making HTTP requests and harvesting tokens when performing the live captu

Number of threads: 5

Burp Sequencer [live capture #1: http://127.0.0.1]

Live capture (5561 tokens)

Pause Copy tokens Auto analyze (next: 6000) Requests: 5561

Stop Save tokens Analyze now Errors: 0

Summary Character-level analysis Bit-level analysis Analysis Options

Sequencer Module

~/Downloads/tokens.txt - Mousepad

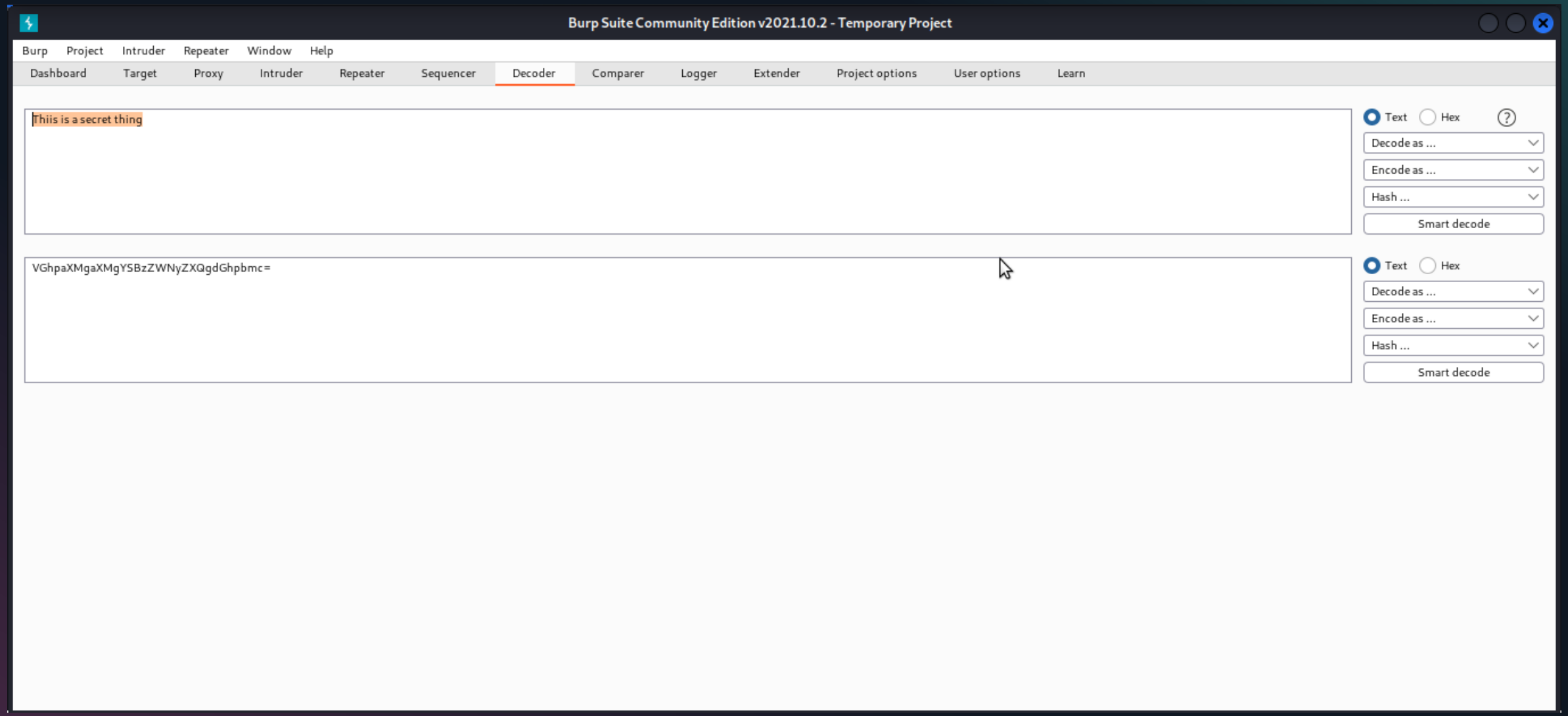
File Edit Search View Document Help

```
1 f6f24e45c002d961efced93e5af0a5deb6d53f82
2 3c458380e16ad4190458cea272df0f841c197532
3 8b1be5c6dc9374ac43468f1bcb5d16902e9e53e7
4 ecc0c52c7bf1fe058392abda996406eecafb171e
5 2d5772023eed523946c1dacfebd6f3770ef75ce5
6 7ef5061ad8b8356c1b90f2f3954b37f1c317cfb1
7 6e1f5428a8fe85b42cf68549eb14e972de156430
8 5077e9cd49a3647fc3fc4a63178a3cd56e4c9f9e
9 e0362e0a345e5353110f7592baef6ef5f97d7e6f
10 a6a9c727f29b6041b1f4368e14ce3fb591327b2c
11 f89aafeba2999bb9677c4646518f7b904e9bf8d1
12 36b76063f2cc74ca480d9a5c385d3ad19f0c5ba8
13 471c83d74a4beaa47f2f6fa7fab0d7726b35fe78
14 bb827832873e539ce1377e510fd47442bc1bf3ee
15 e4abebd8cb122e946569a98395c103b8c8a47210
16 fe80a239a989356a0f8aebd900dd935cc749eb2e
17 d1173b81866dd61aae744d2b3ec1285766faba51
18 148fd4392c3e67478f76b1b2d8d090a0a8a175ff
19 cc642d5cf814ea39728ecf4244335f925c83317e
20 d0fa0aebf890bec6c82f99cf105617bb713e86fd
21 11e60504284e1c9075d38e740b228cac71e3d033
22 9a8bda9b05d3f556c2ecc32fa0d3d7e60c67fce4
23 b302998aaeaa5117c6adbbd18d2f3638041771d9
24 2488dd7584679dfb69d93d647c9351f94ac7c897
25 82f2145de74d0a77aa550a0262563a63fd2c7616
26 df9ce26a729f85086192e24ea93da2cf86110f43
27 9b66eafb3da9a44f787934fd938cb21cf0fd0741
28 111eac66220bc10109ce0339aa706642dc2a866f
29 608341d36320f1df282ce64a4801461ffd2c1a5e
```

Decoder Module

- ✓ Burp Decoder is a simple tool for transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms.
- ✓ It is capable of intelligently recognizing several encoding formats using heuristic techniques.

Decoder Module



Comparer Module

- ✓ Comparer is simply a tool to compare to HTTP requests or responses.
- ✓ Comparer is useful when you want to see how different values for parameters and headers enable subtle changes in the responses that you receive.

Comparer Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

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
1	4794	HTTP/1.1 200 OKDate: Thu, 09 Jun 2022 15:12:37 GMTServer: Apache/2.4.51 (Debian)Expires: Tue, 23 Jun 2009 12:00:00 GMT...
2	302	HTTP/1.1 302 FoundDate: Thu, 09 Jun 2022 15:12:41 GMTServer: Apache/2.4.51 (Debian)Expires: Thu, 19 Nov 1981 08:52:00 ...

Paste
Load
Remove
Clear

Select item 2:

#	Length	Data
1	4794	HTTP/1.1 200 OKDate: Thu, 09 Jun 2022 15:12:37 GMTServer: Apache/2.4.51 (Debian)Expires: Tue, 23 Jun 2009 12:00:00 GMT...
2	302	HTTP/1.1 302 FoundDate: Thu, 09 Jun 2022 15:12:41 GMTServer: Apache/2.4.51 (Debian)Expires: Thu, 19 Nov 1981 08:52:00 ...

Compare ...
Words
Bytes

Comparer Module

Word compare of #1 and #2 (15 differences)

Length: 4,794 — Text / Hex

```
HTTP/1.1 200 OK
Date: Thu, 09 Jun 2022 15:12:37 GMT
Server: Apache/2.4.51 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4503
Connection: close
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

                <link rel="icon" type="\image/ico" href="../../favicon.ico" />

                <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>

        </head>

        <body class="home">
                <div id="container">

                        <div id="header">

                                <img src="../../dvwa/images/logo.png" alt="Damn Vulnerable Web Applicat

                        </div>

                        <div id="main_menu">
```

Length: 302 — Text / Hex

```
HTTP/1.1 302 Found
Date: Thu, 09 Jun 2022 15:12:41 GMT
Server: Apache/2.4.51 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 2
Connection: close
Content-Type: text/html; charset=UTF-8
```

Key: Modified Deleted Added

Sync views

Extender Module

- ✓ Burp Extender lets you use Burp extensions, to extend Burp's functionality using your own or third-party code.
- ✓ You can load and manage extensions, view details about installed extensions, install extensions from the BApp Store, view the current Burp Extender API, and configure options for how extensions are handled.

Extender Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Extensions BApp Store APIs Options

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Search...

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier				23 Jan 2017	
403 Bypasser				26 Jan 2022	Requires Burp S...
5GC API Parser				23 Sep 2021	
Active Scan++				25 Mar 2021	Requires Burp S...
Add & Track Custom Issues				25 Feb 2022	Requires Burp S...
Add Custom Header				08 Jul 2020	
Additional CSRF Checks				14 Dec 2018	
Additional Scanner Checks				21 Dec 2018	Requires Burp S...
Adhoc Payload Processors				31 Jan 2022	
AES Killer, decrypt AES tr...				13 May 2021	
AES Payloads				04 Feb 2022	Requires Burp S...
Anonymous Cloud, Confi...				11 Feb 2021	Requires Burp S...
Anti-CSRF Token From R...				28 Feb 2020	
Asset Discovery				12 Sep 2019	Requires Burp S...
Attack Surface Detector				16 Dec 2021	
Auth Analyzer				27 Apr 2022	
Authentication Token Ob...				04 Feb 2022	
AuthMatrix				15 Oct 2021	
Authz				01 Jul 2014	
Auto-Drop Requests				10 Feb 2022	
AutoRepeater				10 Feb 2022	
Autorize				01 Oct 2021	
Autowasp				10 Feb 2022	Requires Burp S...
AWS Security Checks				18 Jan 2018	Requires Burp S...
AWS Signer				19 Apr 2022	
AWS Sigv4				16 Feb 2022	
Backslash Powered Scanner				18 Oct 2021	Requires Burp S...
Batch Scan Report Genera...				04 Feb 2022	Requires Burp S...
BeanStack - Stack-trace F...				04 Feb 2022	Requires Burp S...

Refresh list | Manual install ...

.NET Beautifier

This extension beautifies .NET requests to make the body parameters more human readable. Built-in parameters like __VIEWSTATE have their values masked. Form field names have the auto-generated part of their name removed.

Requests are only beautified in contexts where they can be edited, such as the Proxy intercept view.

For example, a .NET request with the following body:

```
__VIEWSTATE=%2oiAIHfiohsdoigjKLASgjghajklgjSDGsjdglSDJg9SDJGsdgjSGJDDSasdfja9sdjfasdfja0sdfja ... [1000 lines later] ...
&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24FrmLogin%24TxtUsername_intern
al=username&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24FrmLogin%24TxtPass
word_internal=password&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24BtnLogi n=Login
```

will be displayed like this:

```
__VIEWSTATE=<snipped out for sanity>&TxtUsername_internal=username&TxtPassword_internal=password&BtnLogin=Login
```

This is done without compromising the integrity of the underlying message so you can edit parameter values and the request will be correctly reconstructed. You can also send the beautified messages to other Burp tools, and they will be handled correctly.

Author: Nadeem Douba

Version: 0.3

Source: https://github.com/portswigger/dotnet-beautifier

Updated: 23 Jan 2017

Rating: Submit rating

Popularity:

Install

Spider Module

- ✓ Burp Spider is a tool for automatically crawling web applications.
- ✓ While it is generally preferable to map applications manually, you can use Burp Spider to partially automate this process for very large applications, or when you are short of time.

Spider Module

burp suite free edition v1.4.01

burp intruder repeater window about

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

control options

spider running

To begin spidering, browse to the target application, then select one or more nodes in the target site map, and choose "spider from here".

requests made:	184
bytes transferred:	4,100,926
requests queued:	0
forms queued:	16

spider scope

use suite scope [defined in target tab]

use custom scope

submit form

Burp Spider needs your guidance to submit a login form. Please choose the value of each form field which should be used when submitting the form. You can control how Burp handles forms in the Spider options tab.

action URL: http://localhost/mutillidae/index.php?page=login.php
method: POST

type	name	value
text	username	admin
submit		login-php-submit-button=Login
password	password	p

submit form ignore form

burp suite free edition v... submit form 9:31 PM

Spider Module

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://127.0.0.1
- https://aus5.mozilla.org
- https://classify-client.services.mozilla.com
- https://content-signature-2.cdn.mozilla.net
- https://firefox.settings.services.mozilla.com
- https://normandy.cdn.mozilla.net
- https://push.services.mozilla.com
- https://r1---sn-vg5obxcq-jb2l.gvt1.com
- https://redirector.gvt1.com
- https://services.addons.mozilla.org
- https://shavar.services.mozilla.com
- https://www.google.com
  - &ec=GAZAmgQ
  - /
    - pccc%3D1&sig=0_AcjyCeqr3J1hRE9MZ1
  - advanced_search
  - history
    - optout
    - privacyadvisor
  - images
    - branding
  - intl
  - manifest
  - preferences
  - search
  - services
    - /
  - setprefs
  - widget
    - app
  - wizrpcui
  - xjs

Host	Method	URL	Params	Stat...	Length	MIME type	Title	Comment	Time reques...
https://www.google.c...	GET	/		200	118898	HTML	Google		11:40:12 9 J...
https://www.google.c...	GET	/&ec=GAZAmgQ							
https://www.google.c...	GET	/?pccc%3D1&sig=0_A...	✓						
https://www.google.c...	GET	/advanced_search							
https://www.google.c...	GET	/advanced_search?hl=...	✓						
https://www.google.c...	GET	/history/optout							
https://www.google.c...	GET	/history/optout?hl=en...	✓						
https://www.google.c...	GET	/history/privacyadviso...							
https://www.google.c...	GET	/history/privacyadviso...	✓						
https://www.google.c...	GET	/images/branding/goo...							
https://www.google.c...	GET	/images/branding/goo...							
https://www.google.c...	GET	/images/branding/goo...							
https://www.google.c...	GET	/intl/en_bd/ads/							
https://www.google.c...	GET	/intl/en_bd/ads/?subid...	✓						
https://www.google.c...	GET	/manifest							
https://www.google.c...	GET	/manifest?pwa=webhp	✓						
https://www.google.c...	GET	/preferences							
https://www.google.c...	GET	/preferences?hl=en-B...	✓						
https://www.google.c...	GET	/search							
https://www.google.c...	GET	/services/							
https://www.google.c...	GET	/services/?subid=ww-...	✓						

Request

Pretty Raw Hex \n

```
1 GET / HTTP/2
2 Host: www.google.com
3 Cookie: NID=
511=aaS0-SCjzn8Nw4rheMr_NYRndydFBYxco8AtjBiLi7fYXu
K3TKHKvoZjRqhiscQfsDdmU5n_40_uuxFMW6ffVK3xsQ8iq_83
ScEQgl7PWbdfvBvsJ9MGHbnKlLIRctvcNck5VxvsPfv9qLfJRE
i03htuoHy1h86FhUsichBma_k8u-il03DnC6Zij_-CHOOYLit-
```

Search... 0 matches

Response

Pretty Raw Hex Render \n

```
1 HTTP/2 200 OK
2 Date: Thu, 09 Jun 2022 15:40:12 GMT
3 Expires: -1
4 Cache-Control: private, max-age=0
5 Content-Type: text/html; charset=UTF-8
6 Strict-Transport-Security: max-age=31536000
7 Server: gws
```

Search... 0 matches

INSPECTOR

- Request Attributes
- Request Cookies (4)
- Request Headers (15)
- Response Headers (15)

Scanner Module

- ✓ Burp Scanner is a tool for performing automated scans of web sites, to discover content and audit for vulnerabilities.

Scanner Module

Burp Suite Professional v1.7.29 - Temporary Project - licensed to Tutorialspoint Pvt Ltd [single user license]

Burp Intruder Repeater Window Help

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

Issue activity | Scan queue | Live scanning | Issue definitions | Options

#	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confi
1	15:42:17 21 Nov 2017	Issue found	Unencrypted communications	http://detectportal.firefox...	/		Low	Certa
2	15:44:49 21 Nov 2017	Issue found	Frameable response (potential Clickjacking)	http://192.168.0.157	/mutillidae/		Information	Firm
3	15:44:49 21 Nov 2017	Issue found	Cookie without HttpOnly flag set	http://192.168.0.157	/mutillidae/		Low	Firm
4	15:44:49 21 Nov 2017	Issue found	Path-relative style sheet import	http://192.168.0.157	/mutillidae/		Information	Tenta
5	15:44:49 21 Nov 2017	Issue found	HTML does not specify charset	http://192.168.0.157	/mutillidae/		Information	Certa

Advisory | Request | Response

HTML does not specify charset

Issue: **HTML does not specify charset**
Severity: **Information**
Confidence: **Certain**
Host: **http://192.168.0.157**
Path: **/mutillidae/**

Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

Scanner Module

Burp Suite Professional v1.7.29 - Temporary Project - licensed to Tutorialspoint Pvt Ltd [single user license]

Burp Intruder Repeater Window Help

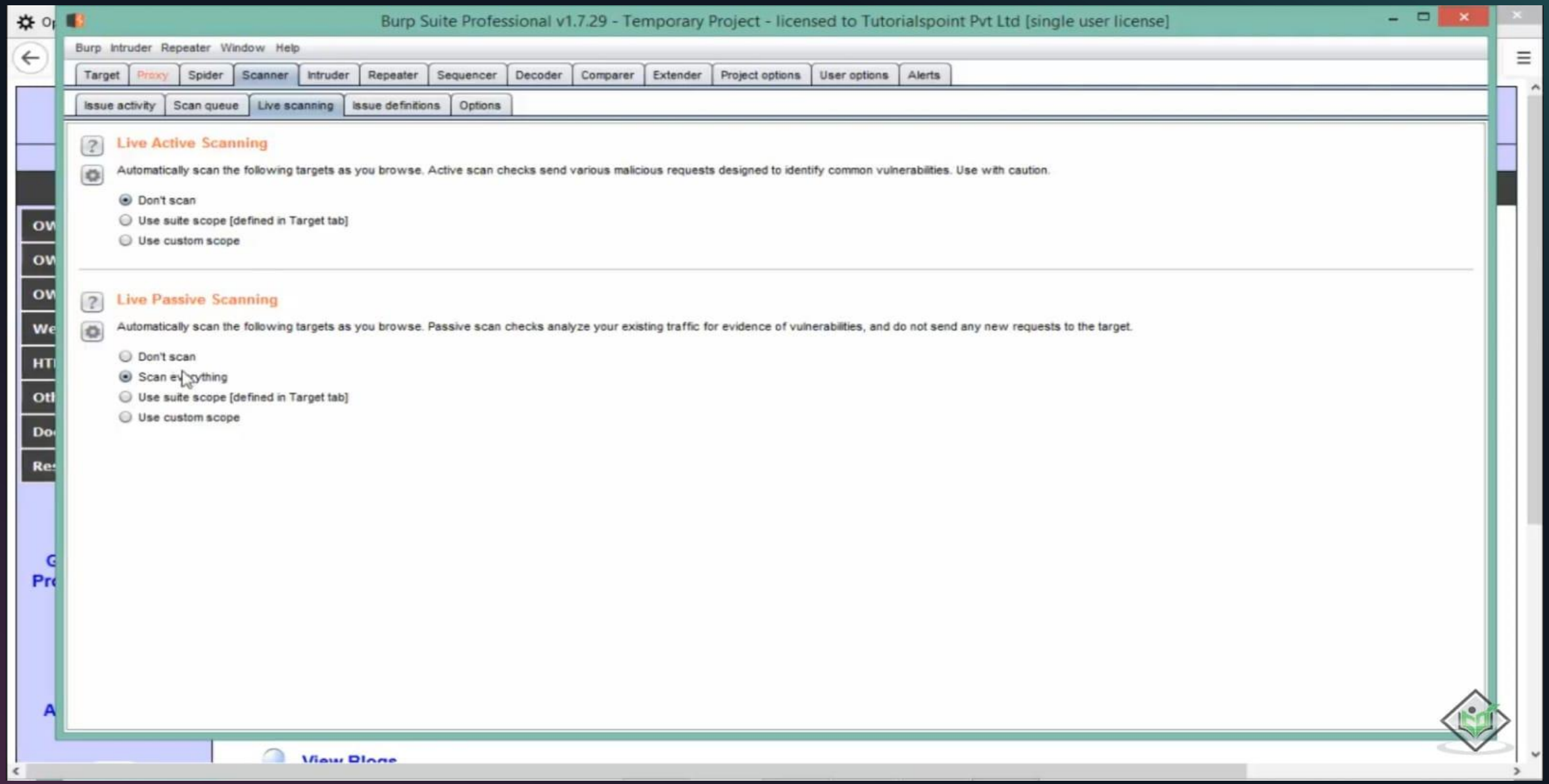
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Issue activity | Scan queue | Live scanning | Issue definitions | Options

#	Host	URL	Status	Issues	Requests	Errors	Insertion points	Start time	End time
1	https://192.168.0.157	/mutillidae/	0% complete	1	8		8	15:48:56 21 Nov 2017	
2	https://192.168.0.157	/mutillidae/	0% complete	2	8		9	15:48:56 21 Nov 2017	
3	https://192.168.0.157	/mutillidae/	0% complete	2	8		9	15:48:56 21 Nov 2017	
4	https://192.168.0.157	/mutillidae/	0% complete	2	8		9	15:48:56 21 Nov 2017	
5	https://192.168.0.157	/mutillidae/ajax/	33% complete	3	199		8	15:48:56 21 Nov 2017	
6	https://192.168.0.157	/mutillidae/ajax/	30% complete	3	[illegible]		9	15:48:56 21 Nov 2017	
7	https://192.168.0.157	/mutillidae/ajax/lookup-pen-test-tool.php	0% complete		8		9	15:48:56 21 Nov 2017	
8	https://192.168.0.157	/mutillidae/ajax/test/	33% complete	3	205		8	15:48:56 21 Nov 2017	
9	https://192.168.0.157	/mutillidae/ajax/test/	30% complete	3	203		9	15:48:56 21 Nov 2017	
10	https://192.168.0.157	/mutillidae/ajax/test/testoutput/	33% complete	8	210		8	15:48:56 21 Nov 2017	
11	https://192.168.0.157	/mutillidae/ajax/test/testoutput/	waiting						
12	https://192.168.0.157	/mutillidae/ajax/test/testoutput/ESAPI_logging_file_test	waiting						
13	https://192.168.0.157	/mutillidae/capture-data.php	waiting						
14	https://192.168.0.157	/mutillidae/documentation/	waiting						
15	https://192.168.0.157	/mutillidae/documentation/	waiting						
16	https://192.168.0.157	/mutillidae/documentation/Mutillidae-Test-Scripts.txt	waiting						
17	https://192.168.0.157	/mutillidae/documentation/change-log.html	waiting						
18	https://192.168.0.157	/mutillidae/documentation/how-to-access-Mutillidae-ov...	waiting						
19	https://192.168.0.157	/mutillidae/documentation/mutillidae-demo.txt	waiting						
20	https://192.168.0.157	/mutillidae/documentation/mutillidae-installation-on-xam...	waiting						
21	https://192.168.0.157	/mutillidae/documentation/vulnerabilities.php	waiting						
22	https://192.168.0.157	/mutillidae/framer.html	waiting						
23	https://192.168.0.157	/mutillidae/images/	waiting						
24	https://192.168.0.157	/mutillidae/images/	waiting						
25	https://192.168.0.157	/mutillidae/images/Hints.html	waiting						
26	https://192.168.0.157	/mutillidae/images/Hints_files/	waiting						
27	https://192.168.0.157	/mutillidae/images/Hints_files/	waiting						
28	https://192.168.0.157	/mutillidae/images/gritter/	waiting						
29	https://192.168.0.157	/mutillidae/images/gritter/	waiting						
30	https://192.168.0.157	/mutillidae/images/gritter/Thumbs.db	waiting						
31	https://192.168.0.157	/mutillidae/includes/	waiting						
32	https://192.168.0.157	/mutillidae/includes/	waiting						
33	https://192.168.0.157	/mutillidae/includes/anti-framing-protection.inc	waiting						
34	https://192.168.0.157	/mutillidae/includes/back-button.inc	waiting						

Running (10 active threads)

Scanner Module



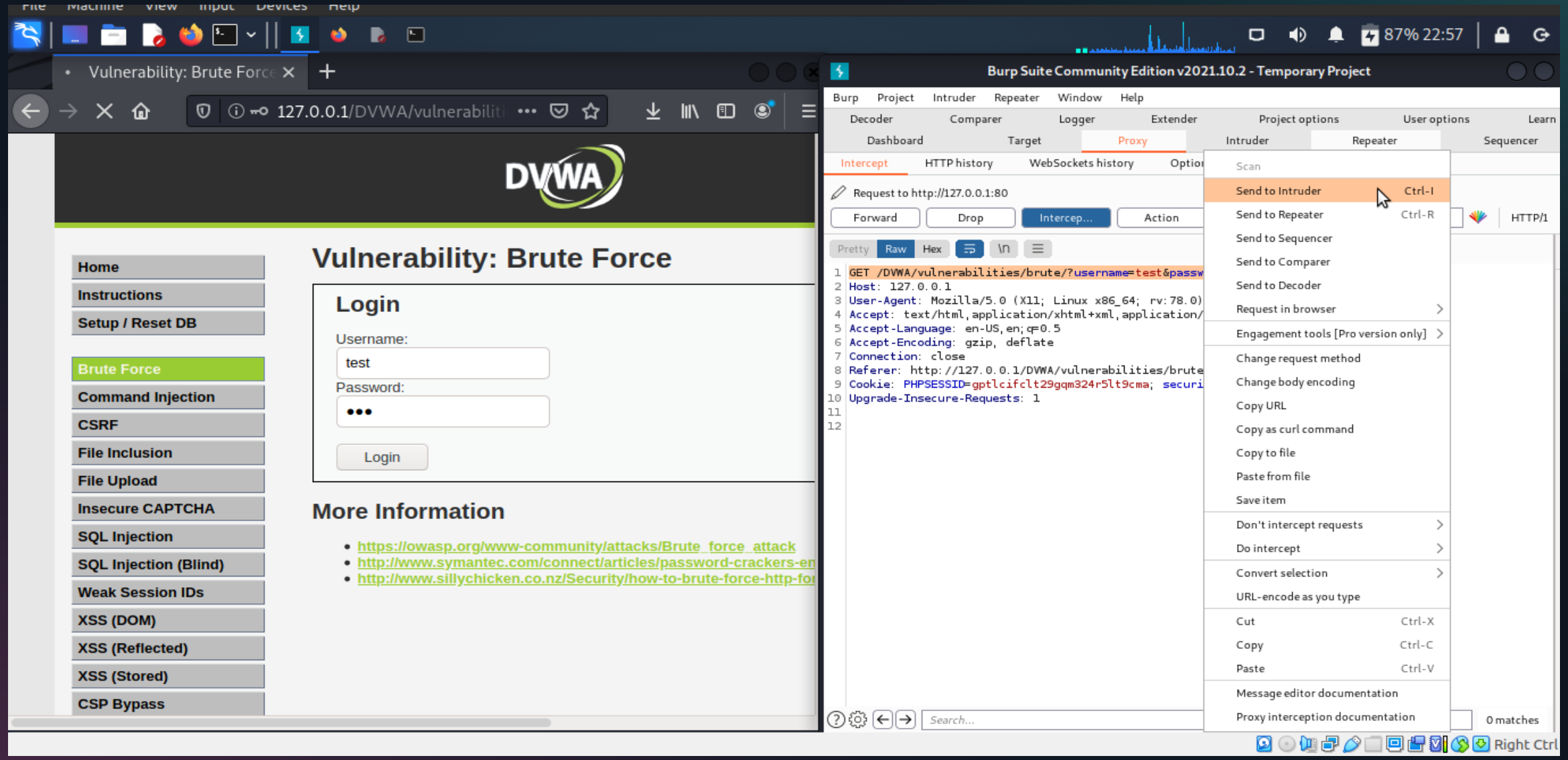
Finding web vulnerabilities using burp suite

- Brute Force
- Sql Injection
- XSS
- Csrf

Brute Force

- ✓Brute force attacks crack data by trying every possible combination, like a thief breaking into a safe by trying all the numbers on the lock.

Brute Force


Vulnerability: Brute Force
127.0.0.1/DVWA/vulnerabilit
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Vulnerability: Brute Force
Login
Username:
test
Password:
Login
More Information
https://owasp.org/www-community/attacks/Brute_force_attack
http://www.symantec.com/connect/articles/password-crackers-en
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-for
Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history
Request to http://127.0.0.1:80
Forward Drop Intercep... Action
Pretty Raw Hex
GET /DVWA/vulnerabilities/brute/?username=test&passw
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/DVWA/vulnerabilities/brute
Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; securi
Upgrade-Insecure-Requests: 1
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl-X
Copy Ctrl-C
Paste Ctrl-V
Message editor documentation
Proxy interception documentation
0 matches
Right Ctrl

Brute Force

File Machine View Input Devices Help

87% 22:57

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × 3 × 4 × ...

Target Positions Payloads Resource Pool 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

```
1  GET /DVWA/vulnerabilities/brute/?username=§test§&password=§123§&Login=§Login§ HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
9  Cookie: PHPSESSID=§gptlcifclt29gqm324r5lt9cma§; security=§low§
10 Upgrade-Insecure-Requests: 1
11
12
```

Add §

Clear §

Clear all payload markers

Refresh

Search...

0 matches

Clear

5 payload positions

Length: 506

Right Ctrl

Brute Force

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

4 × 6 × 7 × ...

Target Positions Payloads Resource Pool 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: Cluster bomb

```
1  GET /DVWA/vulnerabilities/brute/?username=§test§&password=§123§&Login=Login HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; security=low
9  Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Add § Clear § Auto § Refresh

Search... 0 matches Clear

2 payload positions Length: 471

Right Ctrl

Brute Force

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × 3 × 4 × ...

Target Positions Payloads Resource Pool 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

- Simple list
- Runtime file
- Custom iterator
- Character substitution
- Case modification
- Recursive grep
- Illegal Unicode
- Character blocks
- Numbers
- Dates
- Brute forcer
- Null payloads
- Character frobber
- Bit flipper
- Username generator

Payload Opt

This payload ty e list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicat

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Right Ctrl

Brute Force

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × 3 × 4 × ...

Target Positions Payloads Resource Pool 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: 8

Payload type: Simple list Request count: 14,568

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

username
admin
administrator
root
test

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Right Ctrl

Brute Force

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer

1 × 2 × 3 × 4 × ...

Target Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the at

Payload set: 2 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
Deduplicate

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is us

Add

Start attack

Look In: metasploit

adobe_top100_pass.txt	ipmi_passwords.txt	rservices_from_users.txt
av-update-urls.txt	ipmi_users.txt	sap_common.txt
av_hips_executables.txt	joomla.txt	sap_default.txt
burnett_top_1024.txt	keyboard-patterns.txt	sap_icm_paths.txt
burnett_top_500.txt	lync_subdomains.txt	scada_default_userpass.txt
can_flood_frames.txt	malicious_urls.txt	sensitive_files.txt
cms400net_default_userpass.txt	mirai_pass.txt	sensitive_files_win.txt
common_roots.txt	mirai_user.txt	sid.txt
dangerzone_a.txt	mirai_user_pass.txt	snmp_default_pass.txt
dangerzone_b.txt	multi_vendor_cctv_dvr_pass.txt	telerik_ui_asp_net_ajax_versions.txt
db2_default_pass.txt	multi_vendor_cctv_dvr_users.txt	telnet_cdata_ftth_backdoor_userpass.txt
db2_default_user.txt	named_pipes.txt	tftp.txt
db2_default_userpass.txt	namelist.txt	tomcat_mgr_default_pass.txt
default_pass_for_services_unhash.txt	oracle_default_hashes.txt	tomcat_mgr_default_userpass.txt
default_userpass_for_services_unhash.txt	oracle_default_passwords.csv	tomcat_mgr_default_users.txt
default_users_for_services_unhash.txt	oracle_default_userpass.txt	unix_passwords.txt
dlink_telnet_backdoor_userpass.txt	password.lst	unix_users.txt
hci_oracle_passwords.csv	piata_ssh_userpass.txt	vnc_passwords.txt
http_default_pass.txt	postgres_default_pass.txt	vxworks_collide_20.txt
http_default_userpass.txt	postgres_default_user.txt	vxworks_common_20.txt
http_default_users.txt	postgres_default_userpass.txt	wp-exploitable-plugins.txt
http_owa_common.txt	root_userpass.txt	wp-exploitable-themes.txt
idrac_default_pass.txt	routers_userpass.txt	wp-plugins.txt
idrac_default_user.txt	rpc_names.txt	wp-themes.txt

File Name: default_userpass_for_services_unhash.txt

Files of Type: All files

Open Cancel

Right Ctrl

Brute Force

6. Intruder attack of 127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
4	test	123	200			4534	
5	root	admin	200			4534	
6	admin	admin	200			4534	
7	administrator	admin	200			4534	
8	test	admin	200			4534	
9	root	password	200			4534	
10	admin	password	200			4577	
11	administrator	password	200			4534	
12	test	password	200			4534	
13	root	pass	200			4534	
14	admin	pass	200			4534	
15	administrator	pass	200			4534	
16	test	pass	200			4534	

Request Response

Pretty Raw Hex Render

Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)

Password:

Login

Welcome to the password protected area admin

More Information

Finished

Right Ctrl

Sql Injection

- ✓SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.
- ✓This information may include any number of items, including sensitive company data, user lists or private customer details.

Sql Injection

exploits.sql

```sql
SELECT ? FROM ? WHERE ? LIKE '%hammer%';


SELECT ? FROM ? WHERE ? LIKE '%'%';
```

Sql Injection

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Op

Comment this item HTTP/1

Pretty Raw Hex \n

```
1  GET /DVWA/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 F
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/w
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://127.0.0.1/DVWA/vulnerabilities/sqli/
9  Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

- Scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type
- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V
- Message editor documentation
- Proxy interception documentation

INSPECTOR

Search... 0 matches

Right Ctrl

Sql Injection

File Machine View Input Devices Help

88% 13:51

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

14 × 15 × ...

Target Positions Payloads Resource Pool 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: 125

Payload type: Simple list Request count: 125

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

```
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
```

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Right Ctrl

Sql Injection

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Dec

14 × 15 × ...

Target Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack t

Payload set: 1 Payload count: 125

Payload type: Simple list Request count: 125

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

```
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
```

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Start attack

7. Intruder attack of 127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4399	
1	'	200			465	
2	"	200			4339	
3	#	200			4339	
4	-	200			4339	
5	--	200			4339	
6	'%20--	200			463	
7	--';	200			463	
8	'%20;	200			463	
9	=%20'	200			467	
10	=%20;	200			4339	
11	=%20--	200			4339	
12	\x23	200			4339	

Request Response

Pretty Raw Hex Render \n

```
80            </p>
81
82          </form>
83          <pre>
              ID: 2<br />
              First name: Gordon<br />
              Surname: Brown
            </pre>
84        </div>
85
86        <h2>
            More Information
```

Search... 0 matches

58 of 125

Right Ctrl

Sql Injection

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer

14 × 15 × ...

Target Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack t

Payload set: 1 Payload count: 125

Payload type: Simple list Request count: 125

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

```
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
```

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Start attack

7. Intruder attack of 127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
6	'%20--	200			463	
7	--';	200			463	
8	'%20;	200			463	
19	admin'--	200			463	
26	' or 0=0 --	200			463	
32	' or 1=1--	200			463	
34	' or '1'='1'--	200			463	
41	' or a=a--	200			463	
47	hi' or 1=1 --	200			463	
1	'	200			465	
9	=%20'	200			467	
20	<>"'%;)(&+	200			468	
18	'or%20select *	200			471	

Request Response

Pretty Raw Hex Render \n

```
5  Cache-Control: no-store, no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 162
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <pre>
   You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the
   right syntax to use near ''' at line 1
   </pre>
```

Search... 0 matches

67 of 125

Right Ctrl

XSS (cross-site scripting)

- ✓ Cross-site Scripting (XSS) is a security vulnerability usually found in websites and/or web applications that accept user input.
- ✓ Examples of these include search engines, login forms, message boards and comment boxes.
- ✓ Cybercriminals exploit this vulnerability by inputting strings of executable malicious code into these functions.
- ✓ This injects the malicious code into the targeted website's content, making it a part of the website and thus allowing it to affect victims who may visit or view that website.

XSS (cross-site scripting)

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

- [ ] Remove <object> tags
- [ ] Convert HTTPS links to HTTP
- [ ] Remove secure flag from cookies

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Pro

Add | Edit | Remove | Up | Down

Enabled	Item	Match	Replace
	Request header	^If-Modified-Since.*$	
	Request header	^If-None-Match.*$	
	Request header	^Referer.*$	
	Request header	^Accept-Encoding.*$	
	Response header	^Set-Cookie.*$	
	Request header	^Host: foo.example.org$	Host: bar.example.org
	Request header		Origin: foo.example.org
	Response header	^Strict\-Transport\-Sec...	
	Response header		X-XSS-Protection: 0

Add match/replace rule

Specify the details of the match/replace rule.

Type: Request param value

Match: xss

Replace: "><script>alert(1)</script>

Comment:

- [ ] Regex match

OK Cancel

TLS Pass Through

These settings are used to specify destination web servers for which Burp will directly pass through TLS connections. No details about requests or responses made via these connections will be available in the Proxy intercept view or history.

Add | Edit | Remove | Paste URL | Load ...

Enabled	Host / IP range	Port

Right Ctrl

Csrf (Cross-site request forgery)

- ✓ Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

Csrf (Cross-site request forgery)

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Send Cancel

Target: http://127.0.0.1 HTTP/1

Request

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/csrf/?password_new=pass&password_conf=pass&Change=Change
  HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/csrf/
9 Cookie: PHPSESSID=gptlcifclt29gqm324r5lt9cma; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

Search... 0 matches

Response

Pretty Raw Hex Render

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)

Vulnerability: Cross Site

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Password Changed.

Note: Browsers are starting to default to setting the
some types of CSRF attacks. When they have com
expected.

INSPECTOR

Selection (78)

SELECTED TEXT

/DVWA/vulnerabilities/csrf/?password_new=pass&password_conf=pass&Change=Change

DECODED FROM: Select

Cancel Apply changes

Request Attributes

Query Parameters (3)

Body Parameters (0)

Request Cookies (2)

Request Headers (9)

Response Headers (9)

Done

5,662 bytes | 98 millis

Right Ctrl

More with Burp Suite…

Information Gathering

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host | Method | URL | Params | Stat... | Length | MIME type | Title | Comment | Time reques...

Request (Pretty / Raw / Hex)

```
1  GET /model3 HTTP/2
2  Host: www.tesla.com
3  Cookie: ak_bmsc=
   962C46528506C7448EE142A05CC3FFF1~000000000000000000000000
   000000~YAAQFmU+F0SFyDuBAQAAraAwSRCFo/VF21RwAkajGkFEWvTP+P
   dxvzFqnMQ/Err0CI6b45I3cn9SuIeFMNxHAguS+bFe1y0xjErI8OfAL0B
   C9zv1Tn7xP4Mp2TYWqtJwl5IwltGl717Xdqgd9roiAz7YE20KbJ+Fk0DN
   eSMWUxaSBhR5sswvGHEF6FuhxaXXMXXSujWFxGH2AE2Y0gdlp2ukelksP
   PJhL2Be329AgBfaCelFc2yYxQN7c003AL/7Ew2L94rdndnUpI4NbwwBEd
   7ddSn8fXisIgolvMnAGXcWQWpadBZLqGzoV8sWKdSoepu+LmJB9zsW6c0
   mk5n0i3N5G6uUyIhBVbsj2RRqXm70oazvcHospUJeCs/Ebvn6+unC8Y/W
   XIynhw==; _ga=GA1.1.748732855.1654790337; _gid=
   GA1.2.1654227542.1654790337; bm_sv=
   B64D69B3F7636F826F34A434572BE2F9~YAAQJmU+F+iagzuBAQAAxjsy
   SRCUvzlrPjvY8NZ81i62jg+kTc/R5QL66uBOWgpCVRxdzgY0FE/s2Putz
   /fRe1RRTTGsX2pgACNYZfoUWym6ONR7MCkAbs6knb/RjQwJ7nplVMISww
   udJqiLkBFF5P5eIa0Sxs/bjvhFII6BGgSZPLsp4Eomb0ddrdZzIwC99vt
   8bDUgY03+c5vDBcdkCjCuJqoLLildS0rxLR669deRhNgEofuziUKBwB4Y
   szs=~1; _ga_KFP8T9JWYJ=GS1.1.1654790439.1.0.1654790439.0
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
5  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,ima
   ge/webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Referer: https://www.tesla.com/
9  Upgrade-Insecure-Requests: 1
10 Te: trailers
11
```

Search... 0 matches

Response (Pretty / Raw / Hex / Render)

```
1  HTTP/2 200 OK
2  Content-Type: text/html; charset=UTF-8
3  X-Drupal-Dynamic-Cache: MISS
4  X-Ua-Compatible: IE=edge
5  Content-Language: en
6  Permissions-Policy: interest-cohort=()
7  Last-Modified: Thu, 09 Jun 2022 04:40:21 GMT
8  Etag: "1654749621"
9  X-Generator: Drupal 9 (https://www.drupal.org)
10 X-Drupal-Cache: HIT
11 Cache-Control: max-age=10
12 X-Tzla-Edge-Hostname-Vcl: drupal8-prod
13 X-Tzla-Edge-Backend-Fetch-If-Stale: false
14 X-Tzla-Edge-Was-304: false
15 X-Tzla-Edge-Age: 60.000
16 X-Tzla-Edge-Grace: 0.000
17 X-Tzla-Edge-Backend-Retry: 0
18 X-Tzla-Edge-Backend-Conn-Time: 0.000
19 X-Tzla-Edge-Backend-Ttfb: 0.000
20 X-Tzla-Edge-Backend-Reason: OK
21 X-Tzla-Edge-Backend-Status: 200
22 X-Varnish: 887354518 887185598
23 X-Frame-Options: SAMEORIGIN
24 X-Content-Type-Options: nosniff
25 X-Tzla-Edge-Cache-Hit: Hit
26 X-Tzla-Edge-Ttl: 23.448
27 X-Tzla-Edge-Grace-Backend-Unhealthy: 0.000
28 X-Tzla-Edge-Backend-Stream: false
29 X-Tzla-Edge-Client-Restarts: 0
30 X-Tzla-Edge-Client-Req-Ttl: -1.000
```

Search... 0 matches

INSPECTOR

Selection (46)

SELECTED TEXT

X-Generator: Drupal 9 (https://www.drupal.org)

Request Attributes

Request Headers (9)

Response Headers (40)

Right Ctrl

More with Burp Suite…

Url Encoding

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User

1 ...

Send | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
GET /vulnerabilities/sqli/?id=1' OR 1=1 #&Submit=Submit HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; L
Firefox/72.0
Accept: text/html,application/xhtml+xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost/vulnerabiliti
Cookie: PHPSESSID=8m0od4kevghff8lgrqfpd
Upgrade-Insecure-Requests: 1
```

- Scan [Pro version only]
- Send to Intruder — Ctrl+I
- Send to Repeater — Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Show response in browser
- Request in browser ►
- Engagement tools [Pro version only] ►
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Save entire history
- Paste URL as request
- Add to site map
- Convert selection ► → URL ►, HTML ►, Base64 ►, Construct string ►
- URL-encode as you type
- Cut — Ctrl+X
- Copy — Ctrl+C
- Paste — Ctrl+V
- Message editor documentation
- Burp Repeater documentation

Response

Raw | Heade

```
HTTP/1.1 400
Date: Wed, 22
Server: Apach
Content-Lengt
Connection: c
Content-Type:

<!DOCTYPE HTM
<html><head>
<title>400 Ba
</head><body>
<h1>Bad Reque
<p>Your brows
</p>
<hr>
<address>Apac
</body></html
```

? < + > Type a search term 0 matches

? < +

Done

Thank You