CS 455 – Computer Security Fundamentals

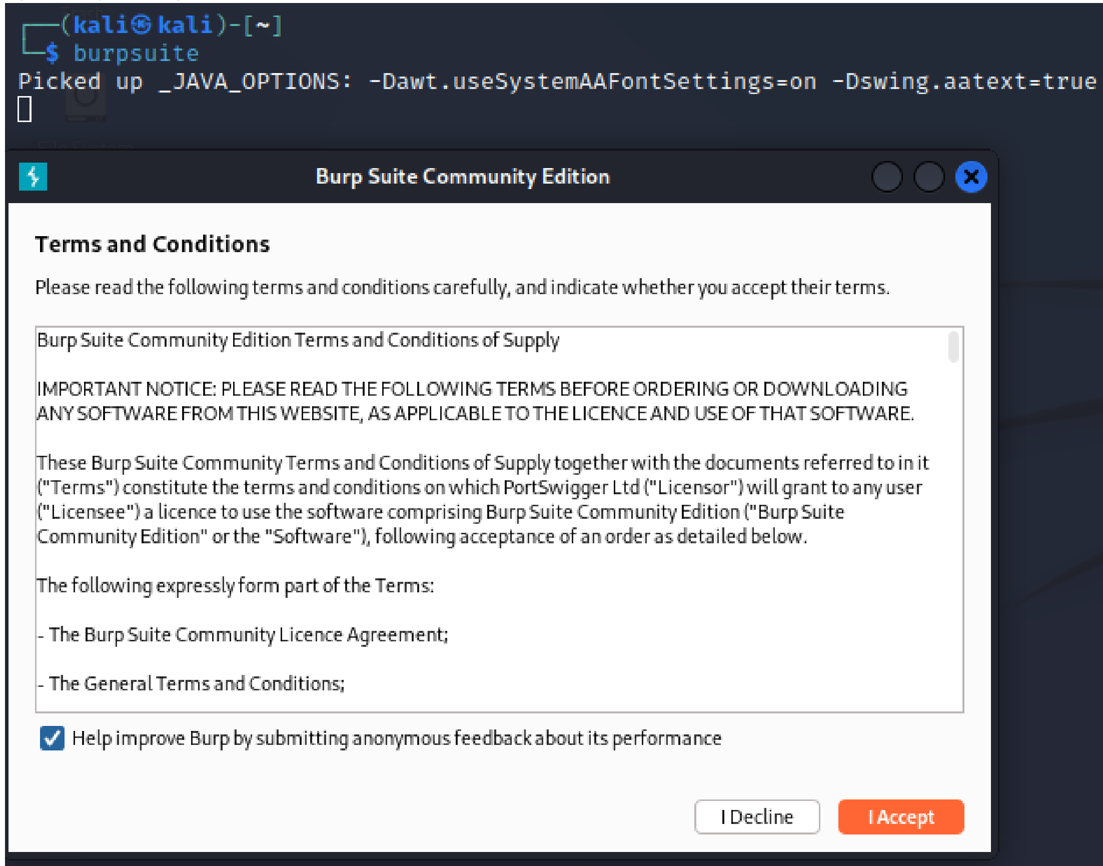
Dr. Chen-Yeou (Charles) Yu

System and Networks Security

- **Web application vulnerability**
  - Burp Suite
    - It is powerful.
    - Little bit too detail (complicated)
    - It can perform brute force attack!
    - “**Brute Force Attack**”

Web application vulnerability

- The first time of the launch, type the “burpsuite” in the command line and followed by an [Enter], there is a Java popup
- Click the OK to continue and check the box to accept the terms
- If you have messages about JRE issues, you will need to fix that first



```
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

Burp Suite Community Edition

Terms and Conditions

Please read the following terms and conditions carefully, and indicate whether you accept their terms.

Burp Suite Community Edition Terms and Conditions of Supply

IMPORTANT NOTICE: PLEASE READ THE FOLLOWING TERMS BEFORE ORDERING OR DOWNLOADING ANY SOFTWARE FROM THIS WEBSITE, AS APPLICABLE TO THE LICENCE AND USE OF THAT SOFTWARE.

These Burp Suite Community Terms and Conditions of Supply together with the documents referred to in it ("Terms") constitute the terms and conditions on which PortSwigger Ltd ("Licensor") will grant to any user ("Licensee") a licence to use the software comprising Burp Suite Community Edition ("Burp Suite Community Edition" or the "Software"), following acceptance of an order as detailed below.

The following expressly form part of the Terms:

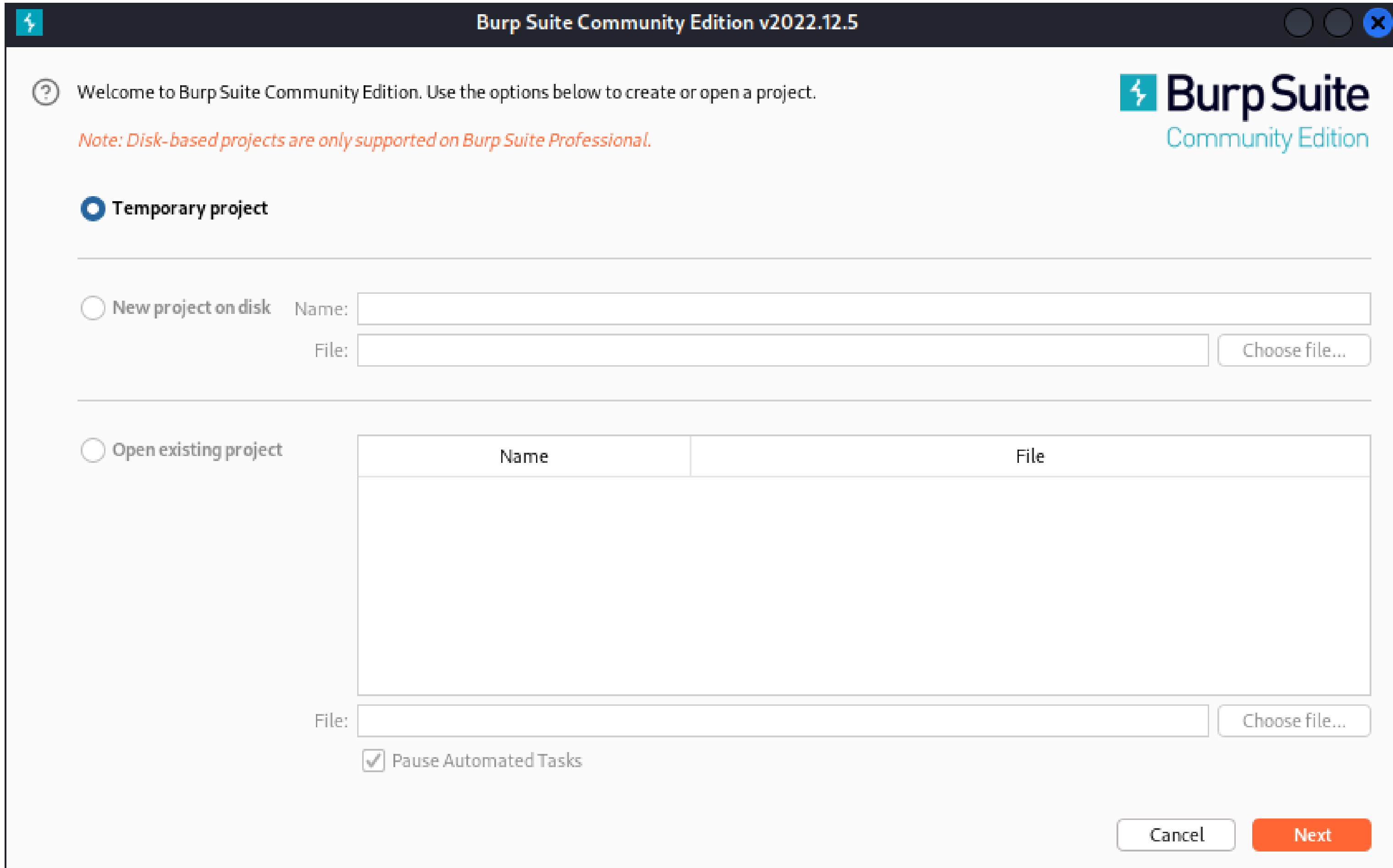
- The Burp Suite Community Licence Agreement;

- The General Terms and Conditions;

☑ Help improve Burp by submitting anonymous feedback about its performance

Web application vulnerability

- We can just go ahead the launch the temporary project.



Burp Suite Community Edition v2022.12.5

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk Name:

File:

○ Open existing project

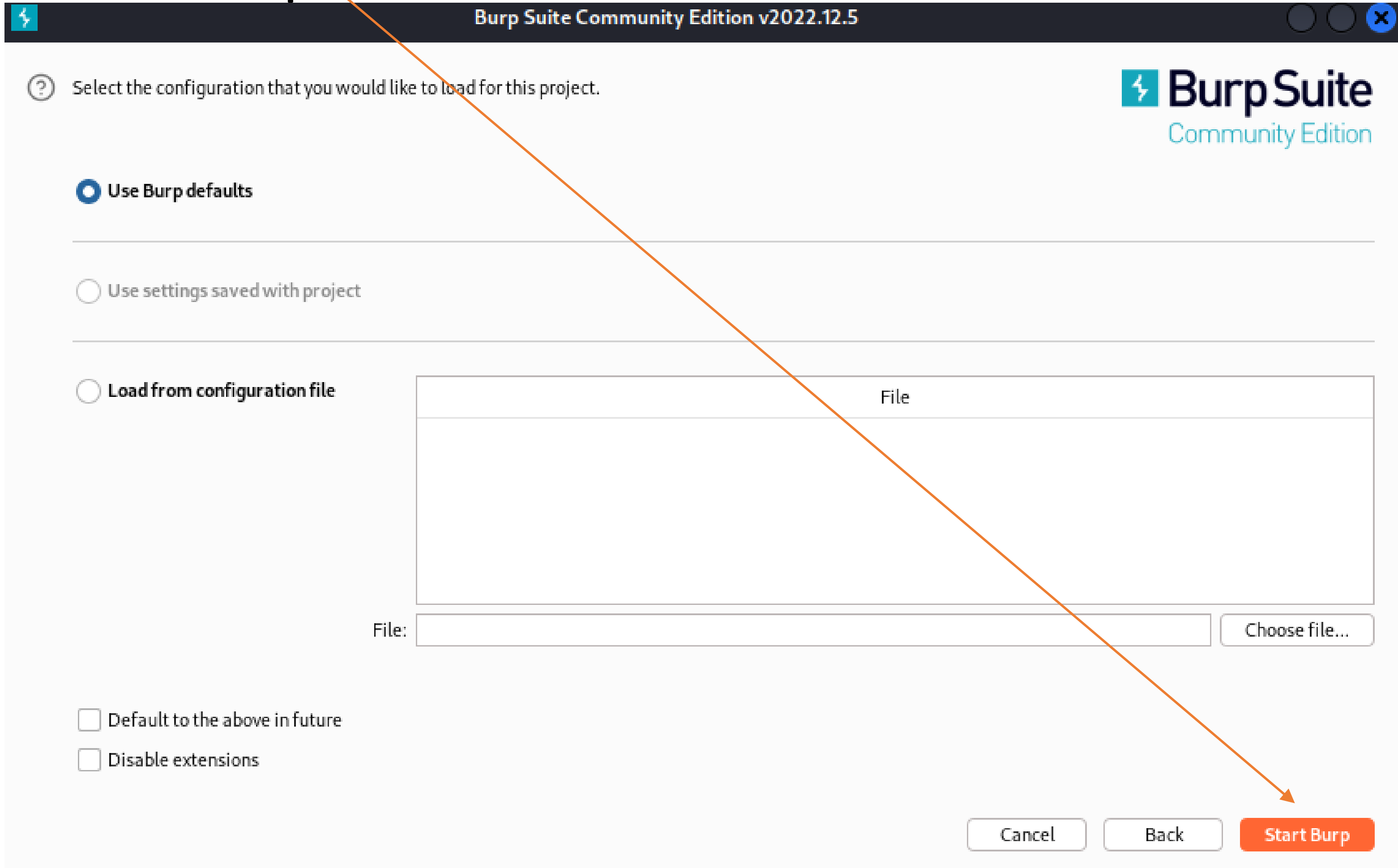
Name	File

File:

☑ Pause Automated Tasks

Web application vulnerability

- Use the Burp defaults and Start Burp



Burp Suite Community Edition v2022.12.5

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

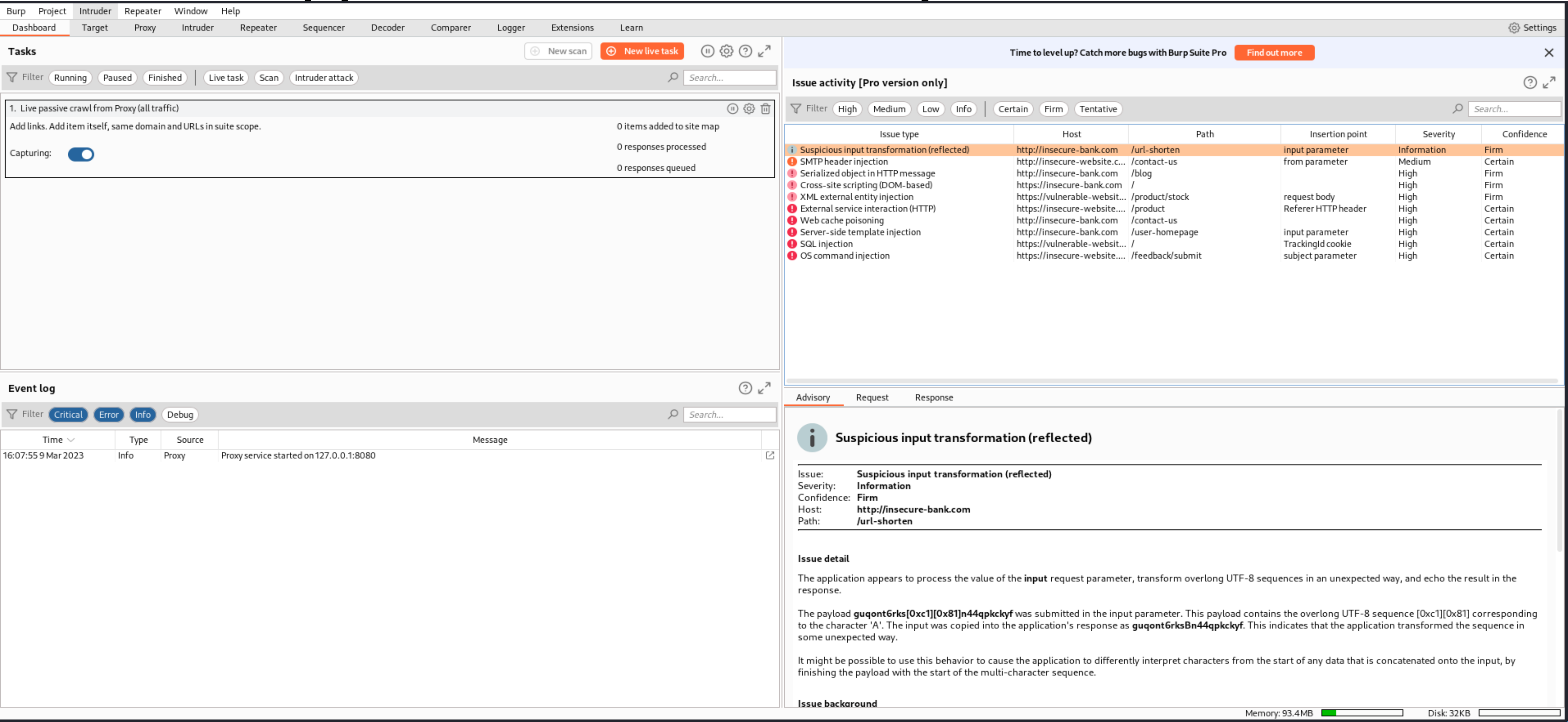
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

Web application vulnerability



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

Time	Type	Source	Message
16:07:55 9 Mar 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Issue type	Host	Path	Insertion point	Severity	Confidence
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten	input parameter	Information	Firm
SMTP header injection	http://insecure-website.c...	/contact-us	from parameter	Medium	Certain
Serialized object in HTTP message	http://insecure-bank.com	/blog		High	Firm
Cross-site scripting (DOM-based)	https://insecure-bank.com	/		High	Firm
XML external entity injection	https://vulnerable-websit...	/product/stock	request body	High	Firm
External service interaction (HTTP)	https://insecure-website....	/product	Referer HTTP header	High	Certain
Web cache poisoning	http://insecure-bank.com	/contact-us		High	Certain
Server-side template injection	http://insecure-bank.com	/user-homepage	input parameter	High	Certain
SQL injection	https://vulnerable-websit...	/	TrackingId cookie	High	Certain
OS command injection	https://insecure-website....	/feedback/submit	subject parameter	High	Certain

Suspicious input transformation (reflected)

Issue:	**Suspicious input transformation (reflected)**
Severity:	**Information**
Confidence:	**Firm**
Host:	**http://insecure-bank.com**
Path:	**/url-shorten**

Issue detail

The application appears to process the value of the **input** request parameter, transform overlong UTF-8 sequences in an unexpected way, and echo the result in the response.

The payload **guqont6rks[0xc1][0x81]n44qpkckyf** was submitted in the input parameter. This payload contains the overlong UTF-8 sequence [0xc1][0x81] corresponding to the character 'A'. The input was copied into the application's response as **guqont6rksBn44qpkckyf**. This indicates that the application transformed the sequence in some unexpected way.

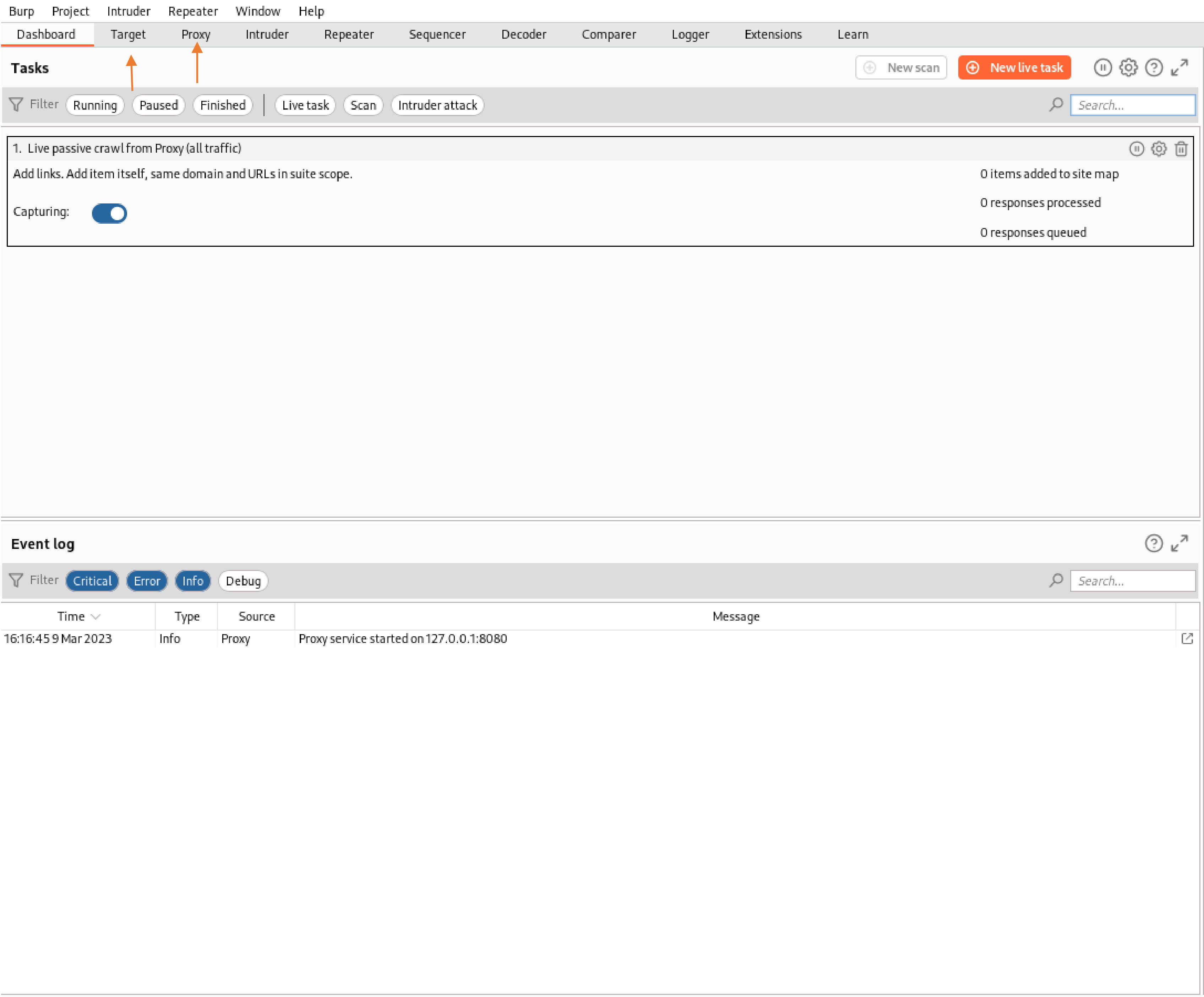
It might be possible to use this behavior to cause the application to differently interpret characters from the start of any data that is concatenated onto the input, by finishing the payload with the start of the multi-character sequence.

Issue background

Memory: 93.4MB Disk: 32KB

Web application vulnerability

- So basically, there are 2 major Panes
- We will focus primarily on the 2 tabs: Target and Proxy
- Proxy will be introduced in the part of brute force hacking



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

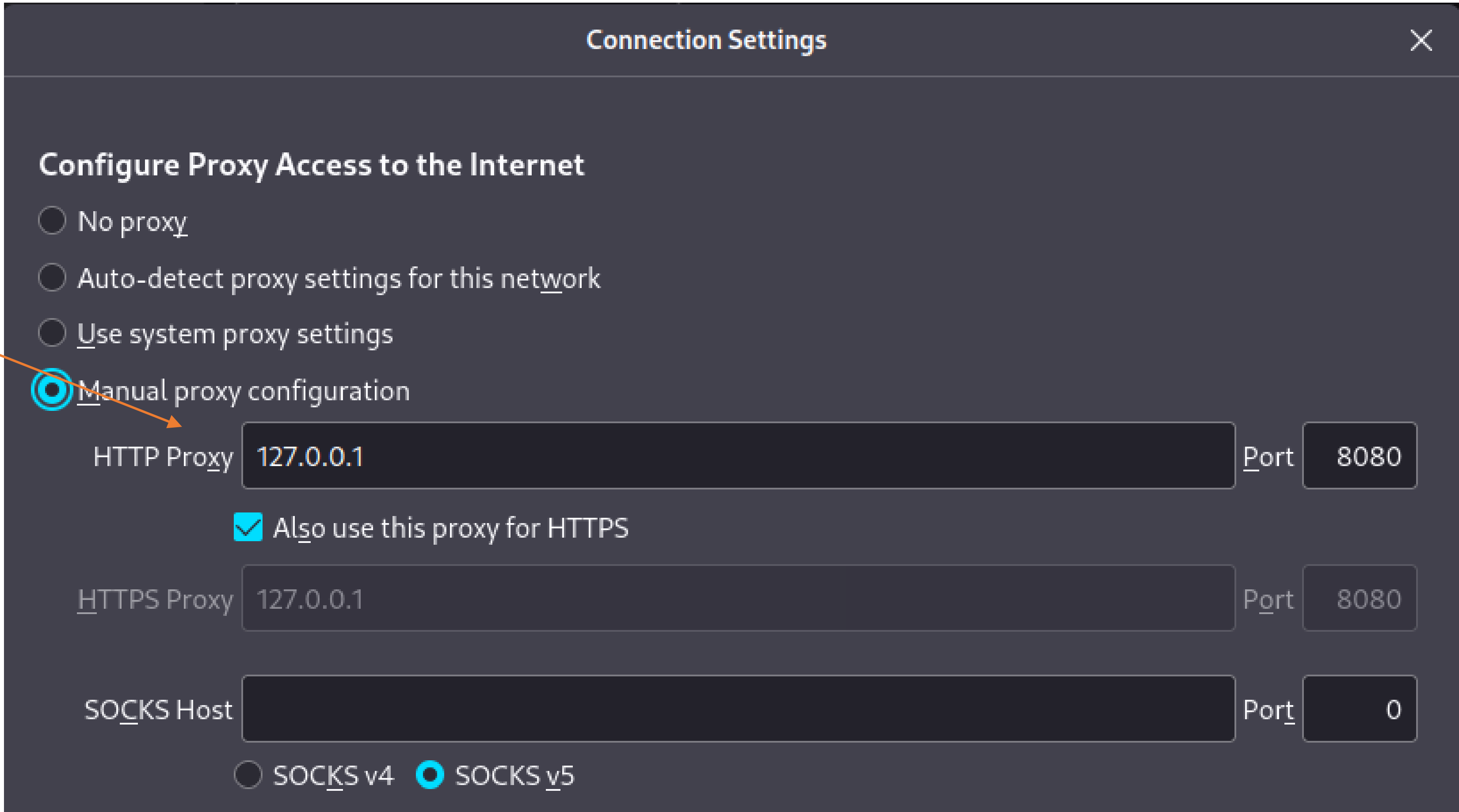
Time	Type	Source	Message
16:16:45 9 Mar 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Web application vulnerability

- Burp Suite functions as a proxy to capture the traffic (over the network)
- Before we can start capturing traffic, we need to setup burp suite to be our interception proxy in terms of web browser
- So, the first job is to setup our interception
- We choose Firefox browser to enable our proxy.
  - Firefox is built in our Kali

Web application vulnerability

- Here’s the configuration in Firefox, basically we use Burp Suite to interact with ourselves
- Settings → General →Network Settings, click the “Settings”
- Input the following
- Exit the FireFox (new setup will be saved automatically)



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

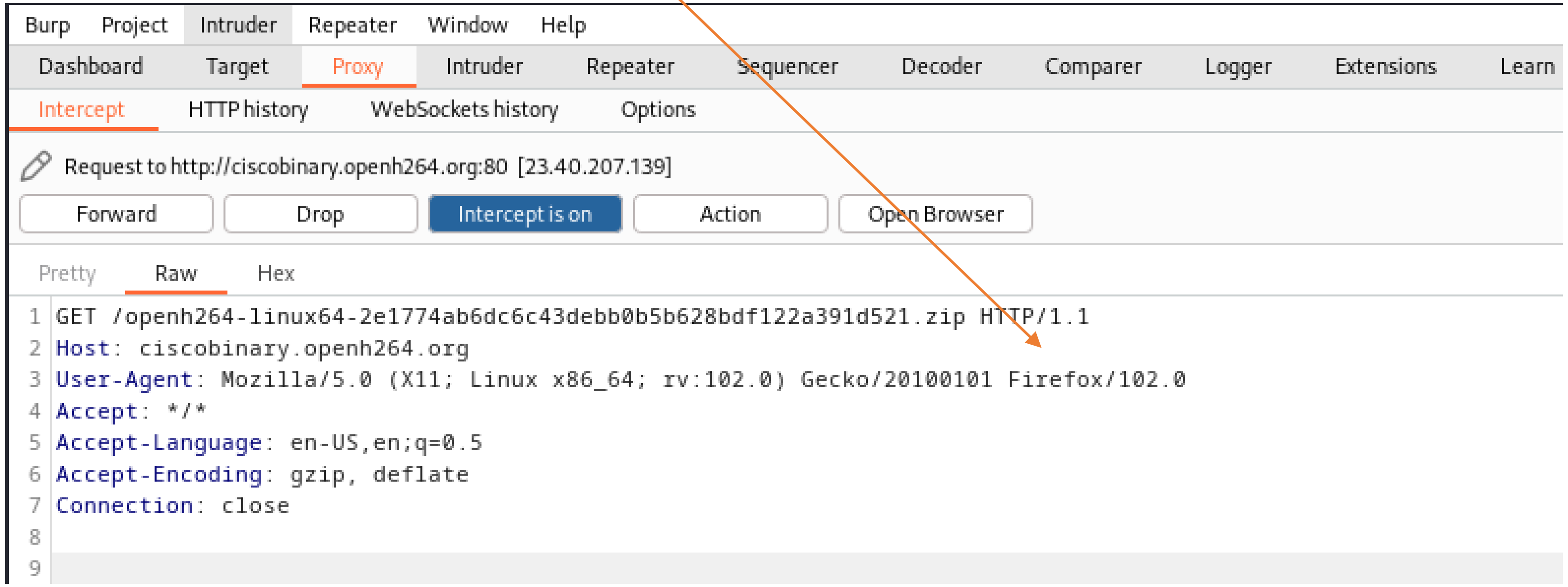
○ SOCKS v4 ● SOCKS v5

Web application vulnerability

- One thing you need to be careful.
  - You will need to start the “Burp Suite” first
  - Then, go back to the Firefox to “change the settings”
  - If you reverse the order, the Burp Suite doesn’t start its logging

Web application vulnerability

- Go back to the Burp Suite → Click the Proxy tab → Enable the "Interception" → After a while, it will detect the changes we have made in the Firefox browser (Interception is working now!)



Request to http://ciscobinary.openh264.org:80 [23.40.207.139]

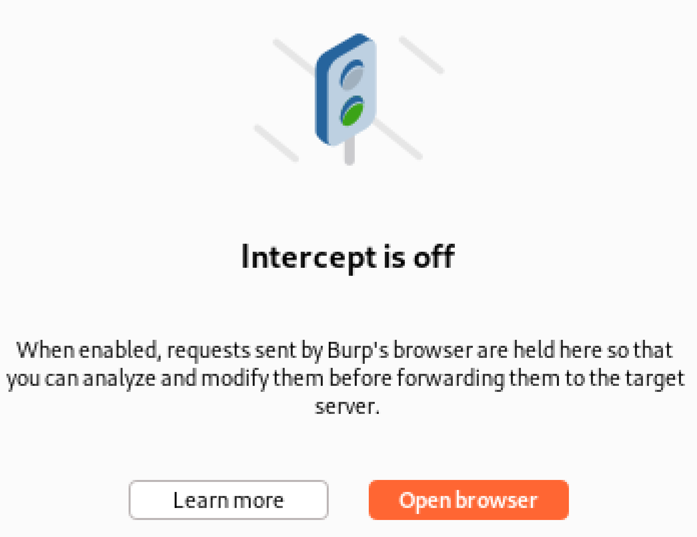
```
GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1
Host: ciscobinary.openh264.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close


```

Web application vulnerability

- Now, we quickly “turn off the” Interception of the proxy, and click the tab of “Target”
- In the beginning, there is nothing in the Target.
- What if we go back to the Firefox and type

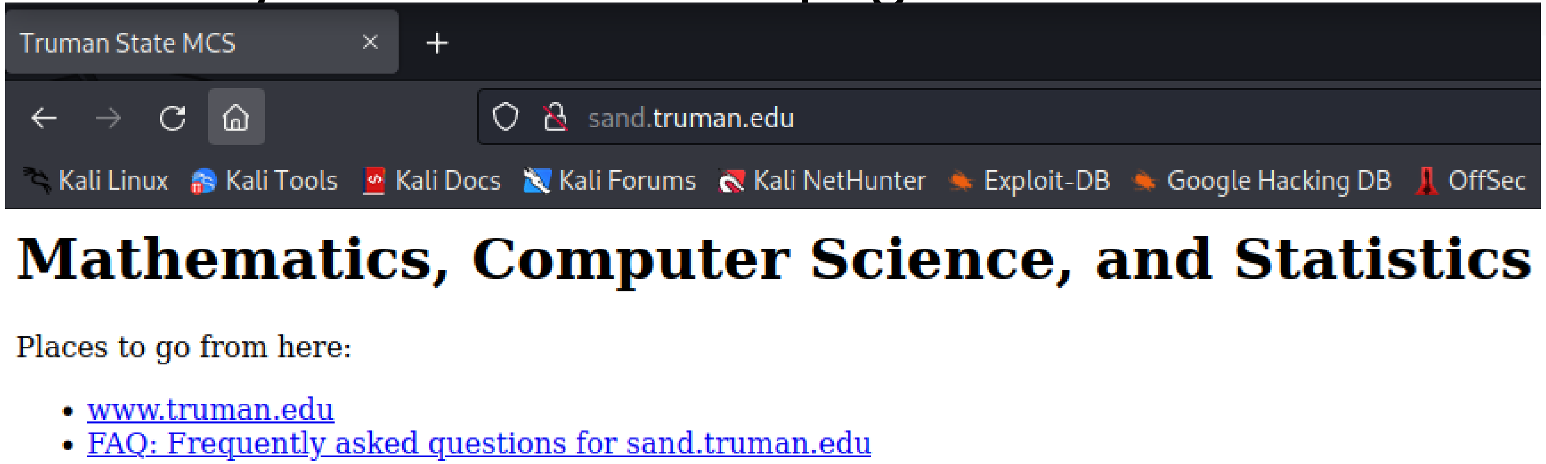
“sand.truman.edu”?

- It is actually this kind of web page in the Firefox



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.



Mathematics, Computer Science, and Statistics

Places to go from here:

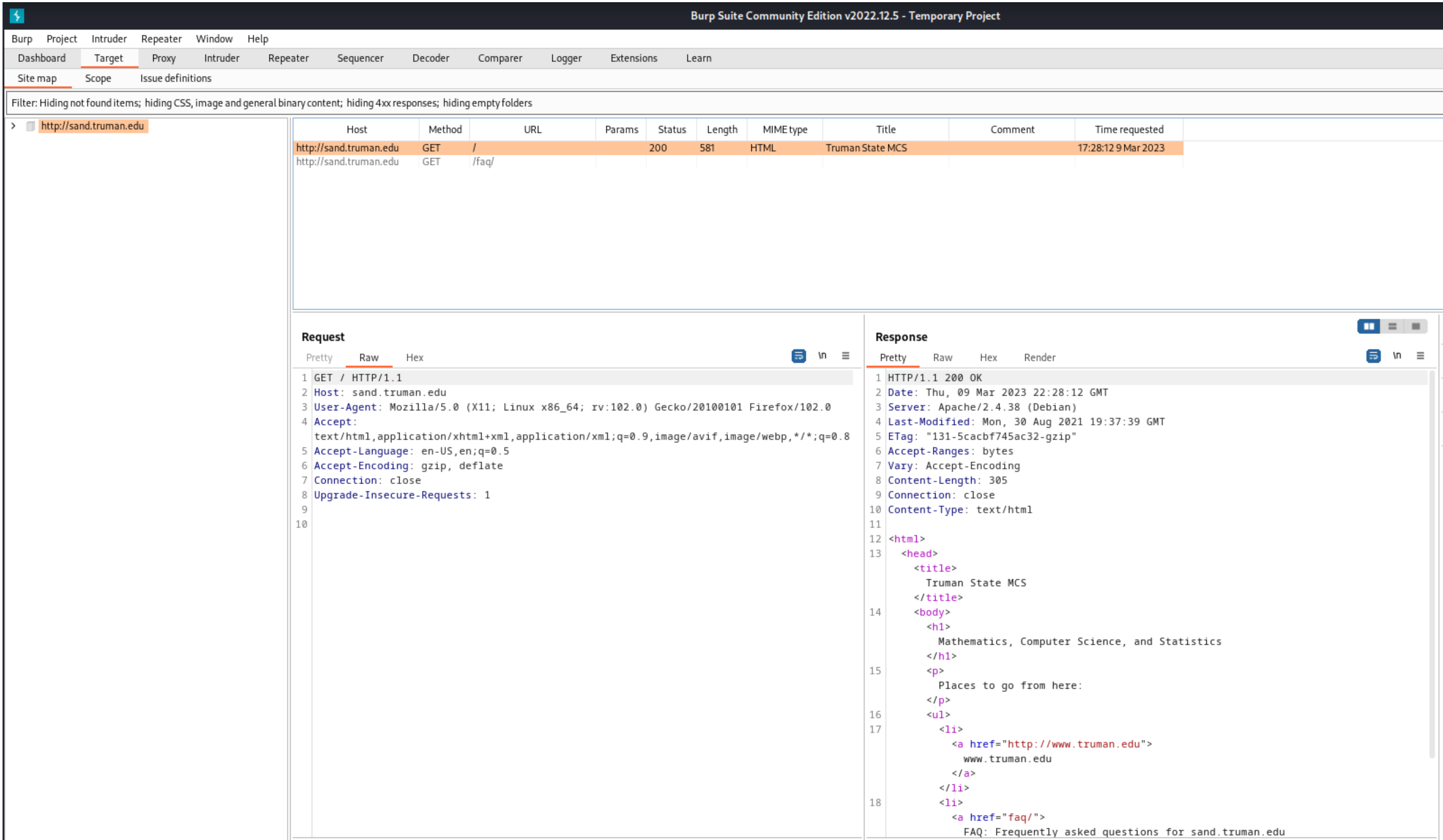
- www.truman.edu
- FAQ: Frequently asked questions for sand.truman.edu

Web application vulnerability

- But?

In the Burp Suite?

Lots of info.!



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

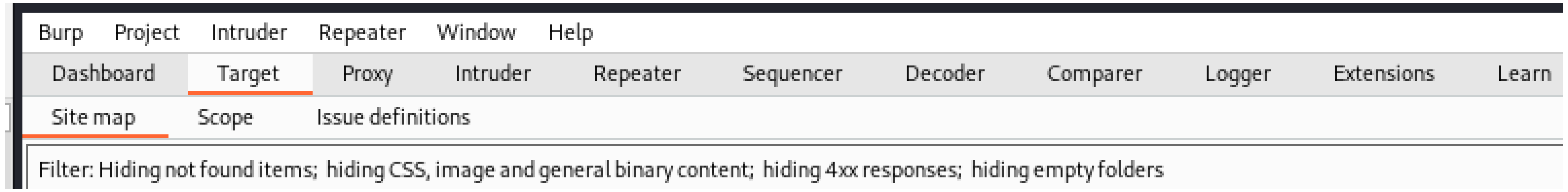
Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://sand.truman.edu	GET	/		200	581	HTML	Truman State MCS		17:28:12 9 Mar 2023
http://sand.truman.edu	GET	/faq/							

```
GET / HTTP/1.1
Host: sand.truman.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

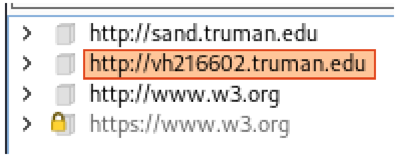
```
HTTP/1.1 200 OK
Date: Thu, 09 Mar 2023 22:28:12 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Mon, 30 Aug 2021 19:37:39 GMT
ETag: "131-5cacbf745ac32-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 305
Connection: close
Content-Type: text/html

<html>
  <head>
    <title>
      Truman State MCS
    </title>
    <body>
      <h1>
        Mathematics, Computer Science, and Statistics
      </h1>
      <p>
        Places to go from here:
      </p>
      <ul>
        <li>
          <a href="http://www.truman.edu">
            www.truman.edu
          </a>
        </li>
        <li>
          <a href="faq/">
            FAQ: Frequently asked questions for sand.truman.edu
```

Web application vulnerability

- The one on our LHS is actually called site map
- Go to the Firefox and type the address in the URL
- Go back to see the Burp Suite and see if there is anything changes?
- The one, vh216602 is Dr. Alan’s apache folder structure

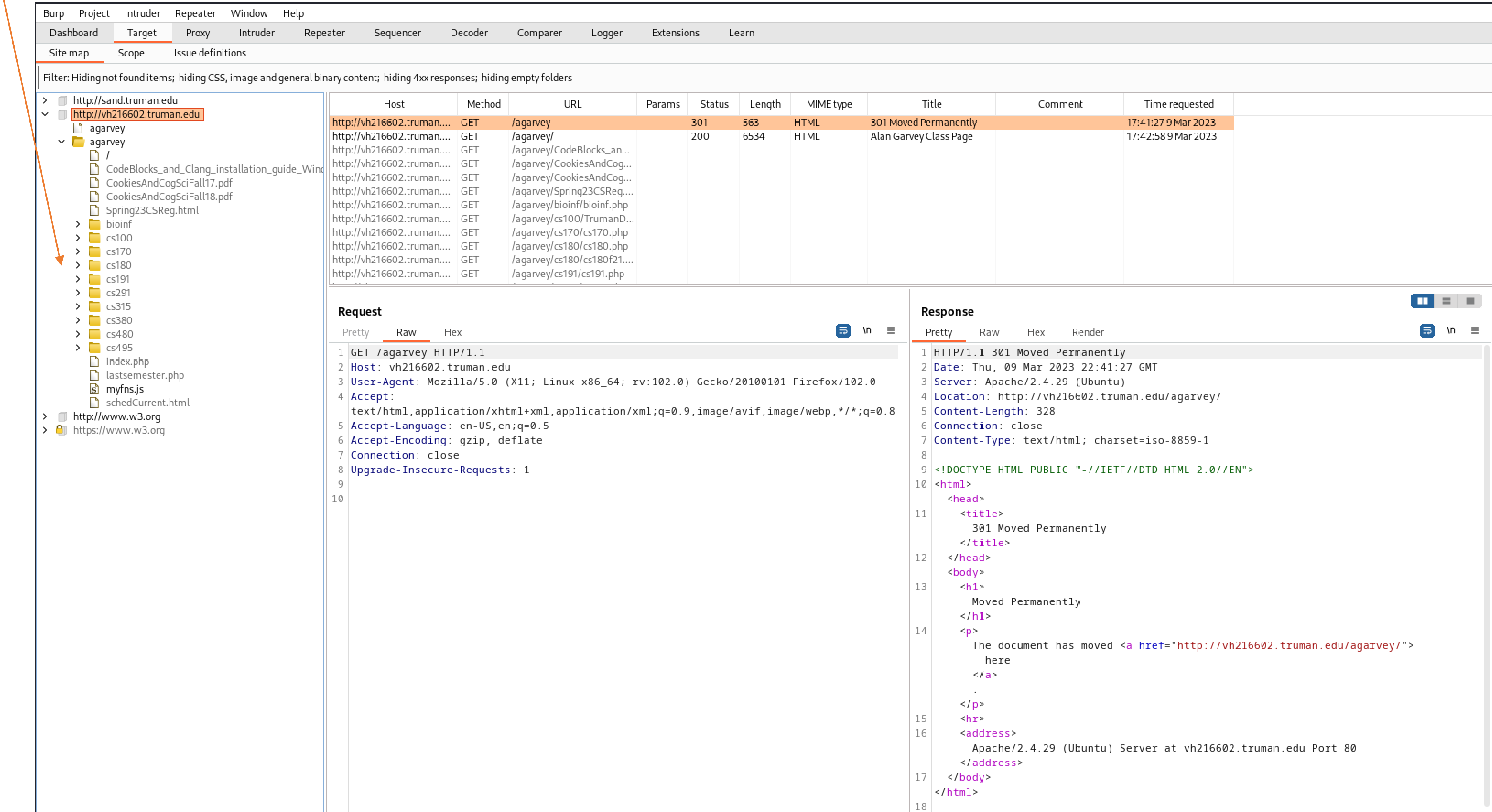


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders



http://sand.truman.edu
http://vh216602.truman.edu
http://www.w3.org
https://www.w3.org

Wow! He teaches lots of classes!



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

```
> http://sand.truman.edu
v http://vh216602.truman.edu
    agarvey
  v agarvey
      /
      CodeBlocks_and_Clang_installation_guide_Wind
      CookiesAndCogSciFall17.pdf
      CookiesAndCogSciFall18.pdf
      Spring23CSReg.html
    > bioinf
    > cs100
    > cs170
    > cs180
    > cs191
    > cs291
    > cs315
    > cs380
    > cs480
    > cs495
      index.php
      lastsemester.php
      myfns.js
      schedCurrent.html
> http://www.w3.org
> https://www.w3.org
```

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://vh216602.truman....	GET	/agarvey		301	563	HTML	301 Moved Permanently		17:41:27 9 Mar 2023
http://vh216602.truman....	GET	/agarvey/		200	6534	HTML	Alan Garvey Class Page		17:42:58 9 Mar 2023
http://vh216602.truman....	GET	/agarvey/CodeBlocks_an...							
http://vh216602.truman....	GET	/agarvey/CookiesAndCog...							
http://vh216602.truman....	GET	/agarvey/CookiesAndCog...							
http://vh216602.truman....	GET	/agarvey/Spring23CSReg....							
http://vh216602.truman....	GET	/agarvey/bioinf/bioinf.php							
http://vh216602.truman....	GET	/agarvey/cs100/TrumanD...							
http://vh216602.truman....	GET	/agarvey/cs170/cs170.php							
http://vh216602.truman....	GET	/agarvey/cs180/cs180.php							
http://vh216602.truman....	GET	/agarvey/cs180/cs180f21....							
http://vh216602.truman....	GET	/agarvey/cs191/cs191.php							

Request

```
GET /agarvey HTTP/1.1
Host: vh216602.truman.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 09 Mar 2023 22:41:27 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: http://vh216602.truman.edu/agarvey/
Content-Length: 328
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      301 Moved Permanently
    </title>
  </head>
  <body>
    <h1>
      Moved Permanently
    </h1>
    <p>
      The document has moved <a href="http://vh216602.truman.edu/agarvey/">
        here
      </a>
      .
    </p>
    <hr>
    <address>
      Apache/2.4.29 (Ubuntu) Server at vh216602.truman.edu Port 80
    </address>
  </body>
</html>
```

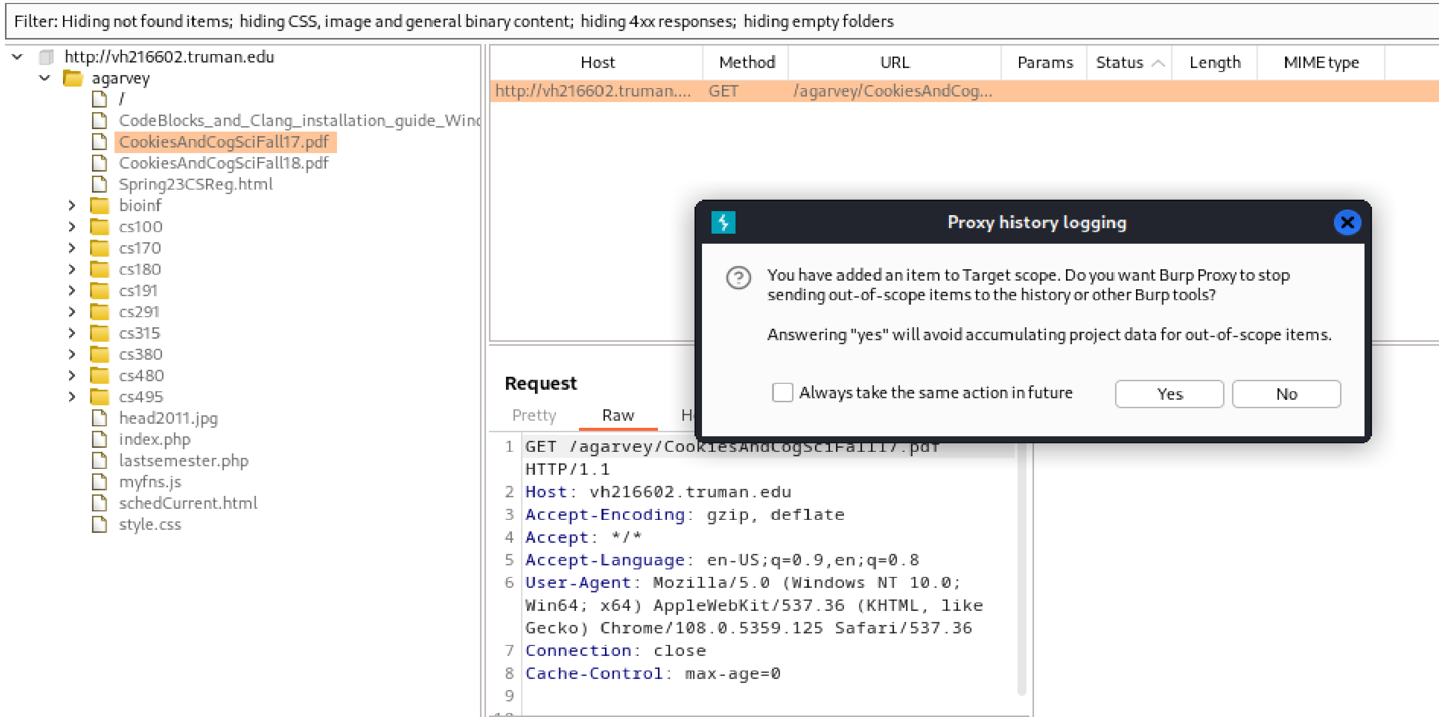
Web application vulnerability

- If you were to browse multiple web sites, they would start showing up on the left pane
  - You can see I had visited our “sand” server and Dr. Alan’s server
- There is one more thing, in order to focus on our attention to the target, for example, Dr. Alan’s server. You will need to add this “host” to a thing, called “**scope**”
  - The scope is used for filtering. Or you can say it can help us getting “concentrated”
  - After a setup of the “**scope**”, in this example, **no matter how we visit other websites, there is just one record**! Dr. Alan’s server
  - How to do that?

Web application vulnerability

- Right click the http://vh216602.Truman.edu, and select "Add to scope"
- Just click "Yes". This is just a asking if you don't like to see the "out-of-scope" traffic? Are you sure of that?
- We will only be collecting

data on this web server



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

http://vh216602.truman.edu
agarvey
/
CodeBlocks_and_Clang_installation_guide_Wind
CookiesAndCogSciFall17.pdf
CookiesAndCogSciFall18.pdf
Spring23CSReg.html
bioinf
cs100
cs170
cs180
cs191
cs291
cs315
cs380
cs480
cs495
head2011.jpg
index.php
lastsemester.php
myfns.js
schedCurrent.html
style.css

Host	Method	URL	Params	Status	Length	MIME type
http://vh216602.truman....	GET	/agarvey/CookiesAndCog...				

Proxy history logging

You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

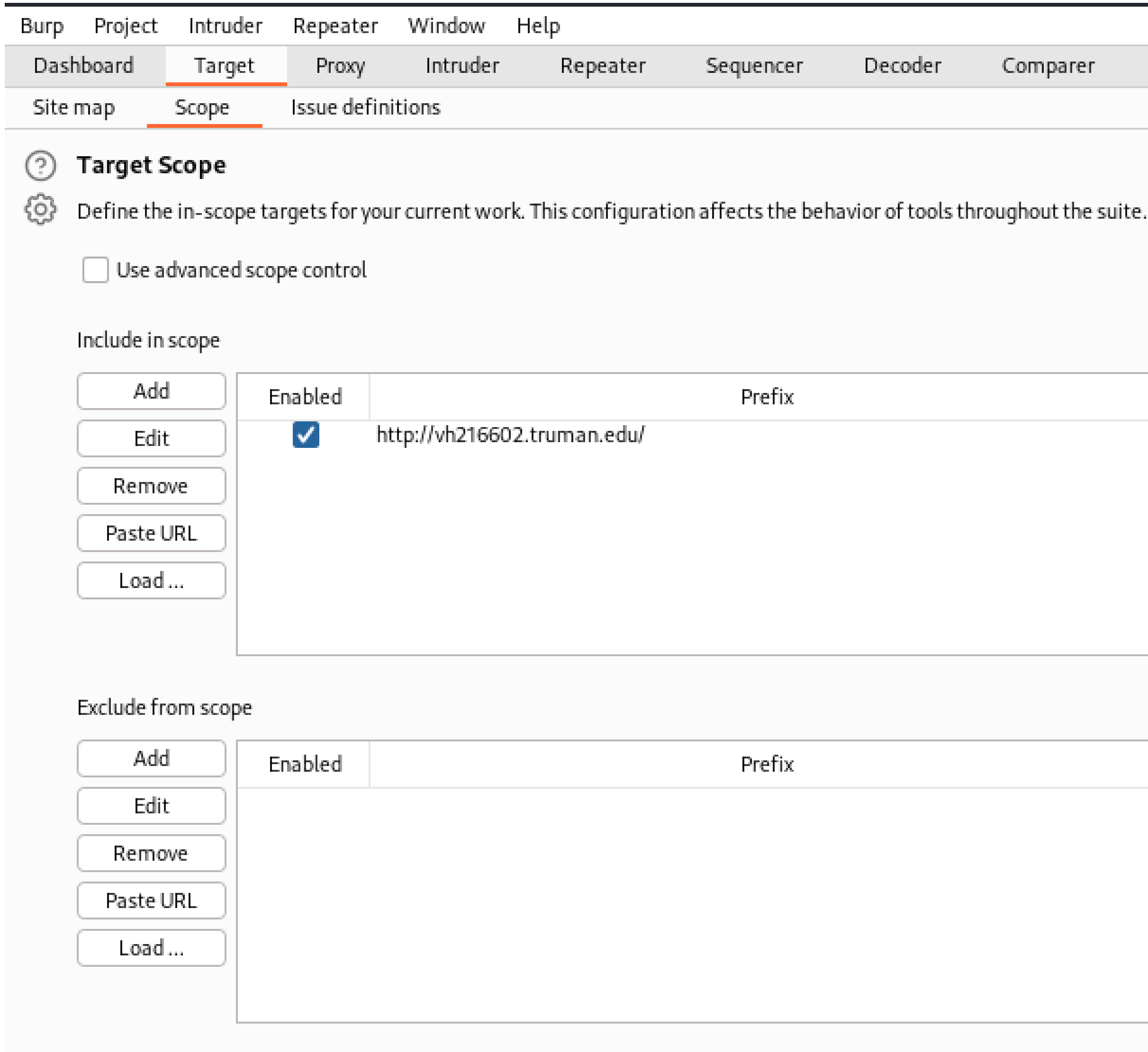
Answering "yes" will avoid accumulating project data for out-of-scope items.

□ Always take the same action in future

```
GET /agarvey/CookiesAndCogSciFall17.pdf
HTTP/1.1
Host: vh216602.truman.edu
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.5359.125 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Web application vulnerability

- Click the “**Scope**” tab under the “**Target**” and you will see that host has been added to the “Include in scope”
- So, this will filter the info. in the “site map”
- But it will not filter the intercept mode of the Proxy unless you specify it to.
- Click [Proxy] tab → [Options]



Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite.

☐ Use advanced scope control

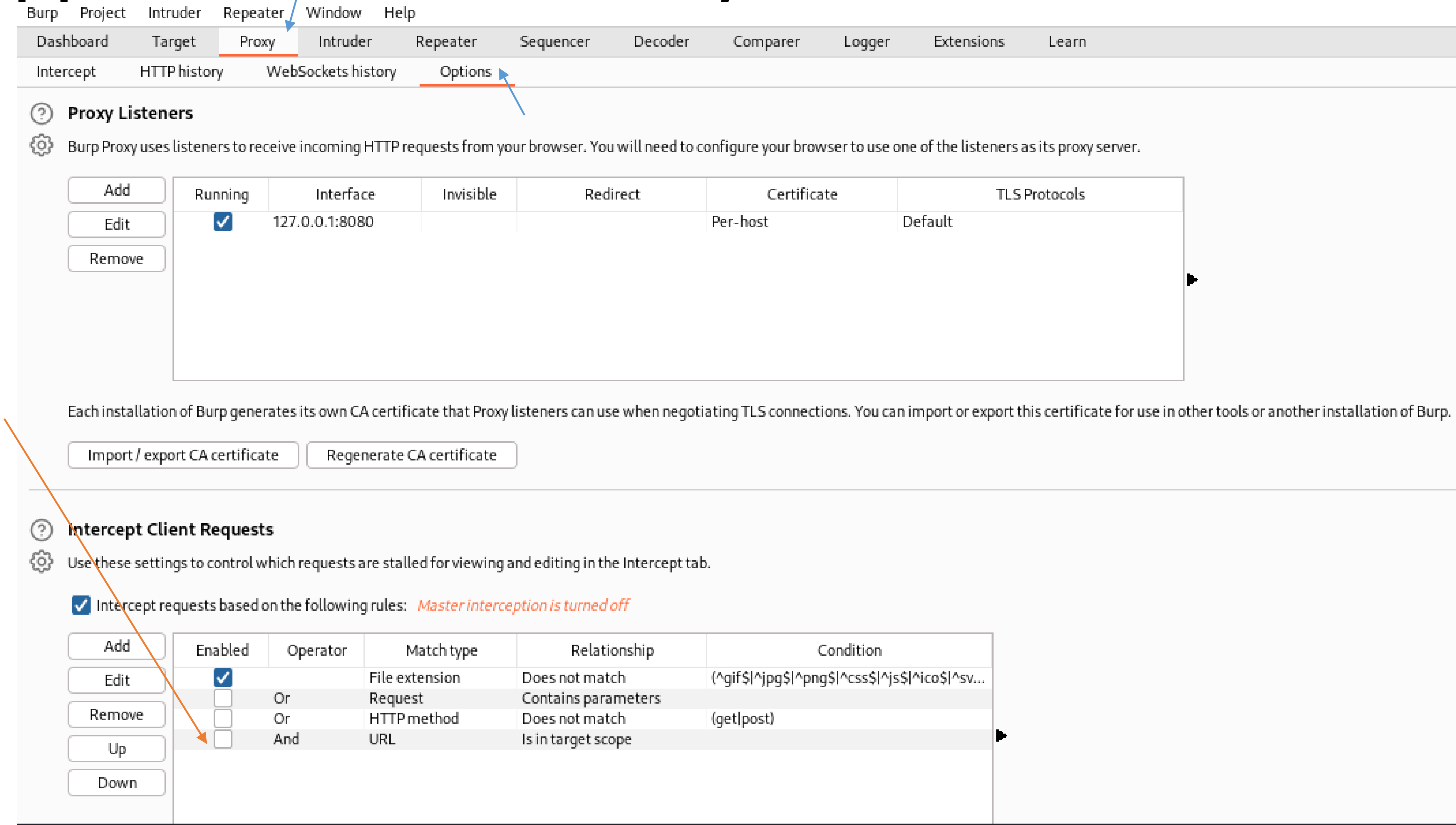
Include in scope

Enabled	Prefix
☑	http://vh216602.truman.edu/

Exclude from scope

Enabled	Prefix

Web application vulnerability



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|^sv...
☐	Or	Request	Contains parameters	
☐	Or	HTTP method	Does not match	(get|post)
☐	And	URL	Is in target scope	

We still like to see this one get checked

Web application vulnerability

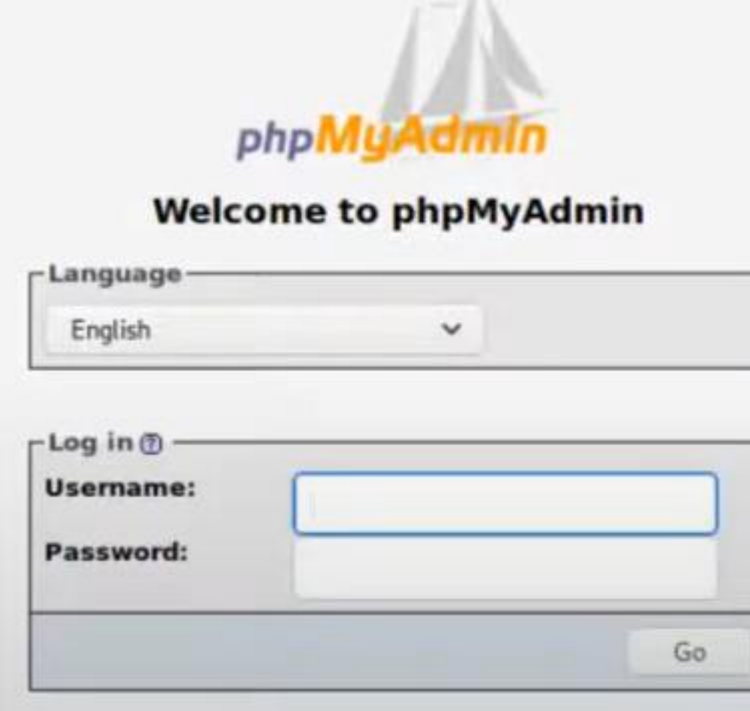
- So, that means, under the “Intercept Client Requests” section, I want to add one more intercept rule by adding “And” “URL is in target scope”
- This is the setup of the target which we want to “focus on” ^_^
  - We are not collecting info. from totally different website
- If you use the browser to click something, some links in the website, the “sitemap” grows.
  - It can explore somewhere, you never know ^_^
  - Now, I’m showing you something which is really, really fun. [Demo]

Web application vulnerability

- Brute Force Attack!
  - The following might involve hacking activities. I'm just briefly describe that
    - Like I said, if you can find out this web server is using "phpMyAdmin", you need to smile or to smirk ☺
    - This one is vulnerable
    - If you try to use default phpMyAdmin user name and password

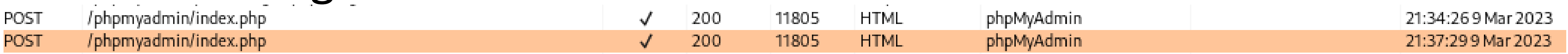
    to login, (root, password) you might got login error.

    But sometimes, you can get it if you are still lucky enough…
    - Mostly, you will get a quick refuse-to-login, not a big deal!
      - We still get something
      - Check your Burp Suite!

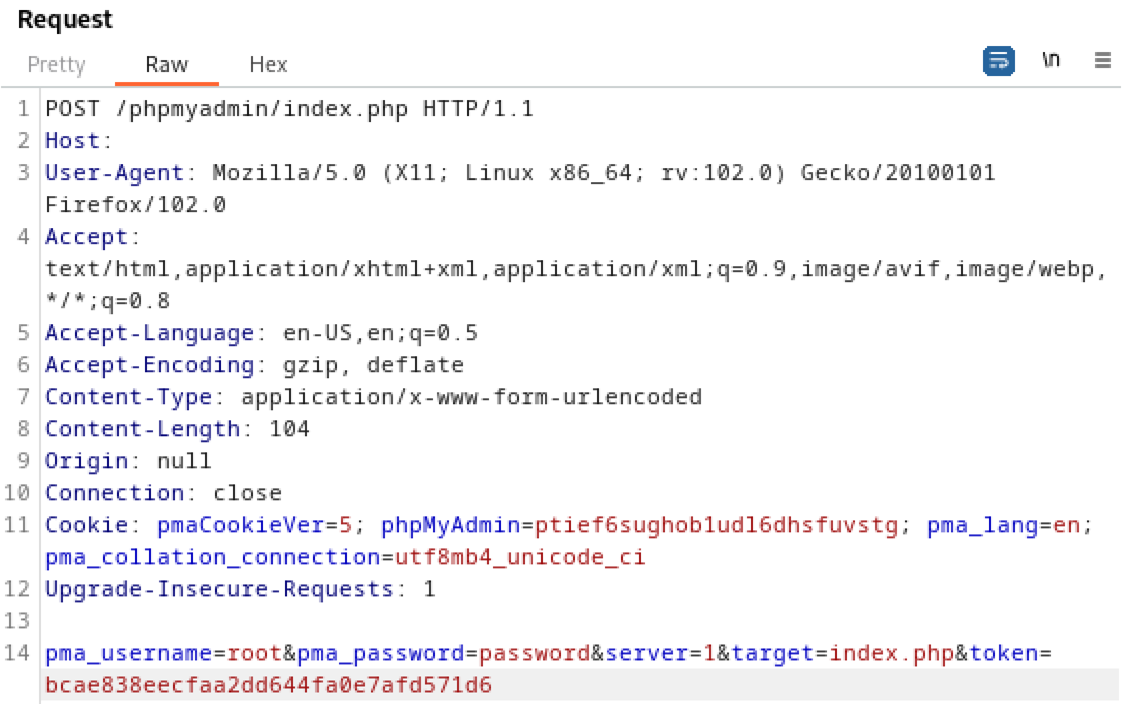


Web application vulnerability

- In the Target / Sitemap, if you can find a record like this, for this time of “fail-to-login”:



POST	/phpmyadmin/index.php	✓	200	11805	HTML	phpMyAdmin	21:34:26 9 Mar 2023
POST	/phpmyadmin/index.php	✓	200	11805	HTML	phpMyAdmin	21:37:29 9 Mar 2023



```
POST /phpmyadmin/index.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: null
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=ptief6sughob1udl6dhsfuvstg; pma_lang=en;
pma_collation_connection=utf8mb4_unicode_ci
Upgrade-Insecure-Requests: 1

pma_username=root&pma_password=password&server=1&target=index.php&token=
bcae838eecfaa2dd644fa0e7afd571d6
```

There are still something valuables. For example, some of parameters.

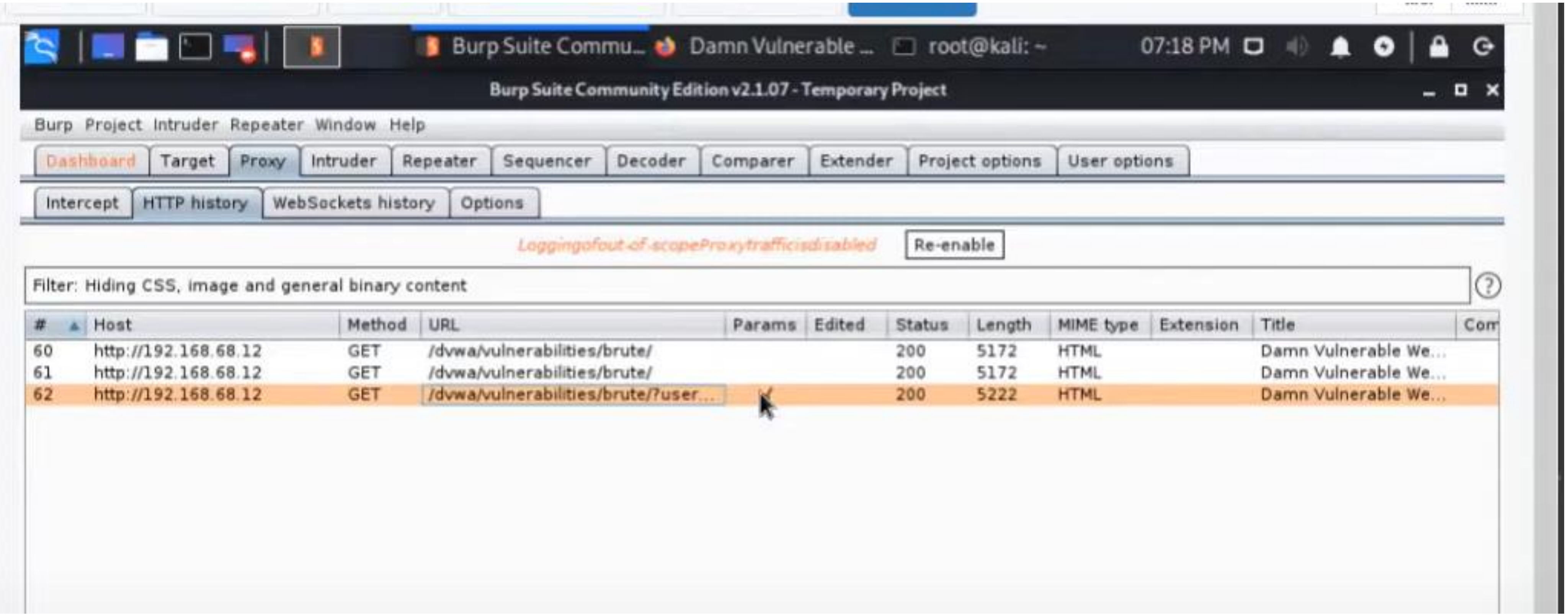
I removed the Host name

Some parameters, for example, pma_username, pma_password, target are giving us information.

Web application vulnerability

- If you go to the [Proxy] tab → [Httphistory], you will see the similar screen for a list of http history
- You can clean up the history if it is needed → What to purify your current observation
- What we can do in a request is: **right click the request → [Send to Intruder]**
- I had removed all the "sensitive" host names

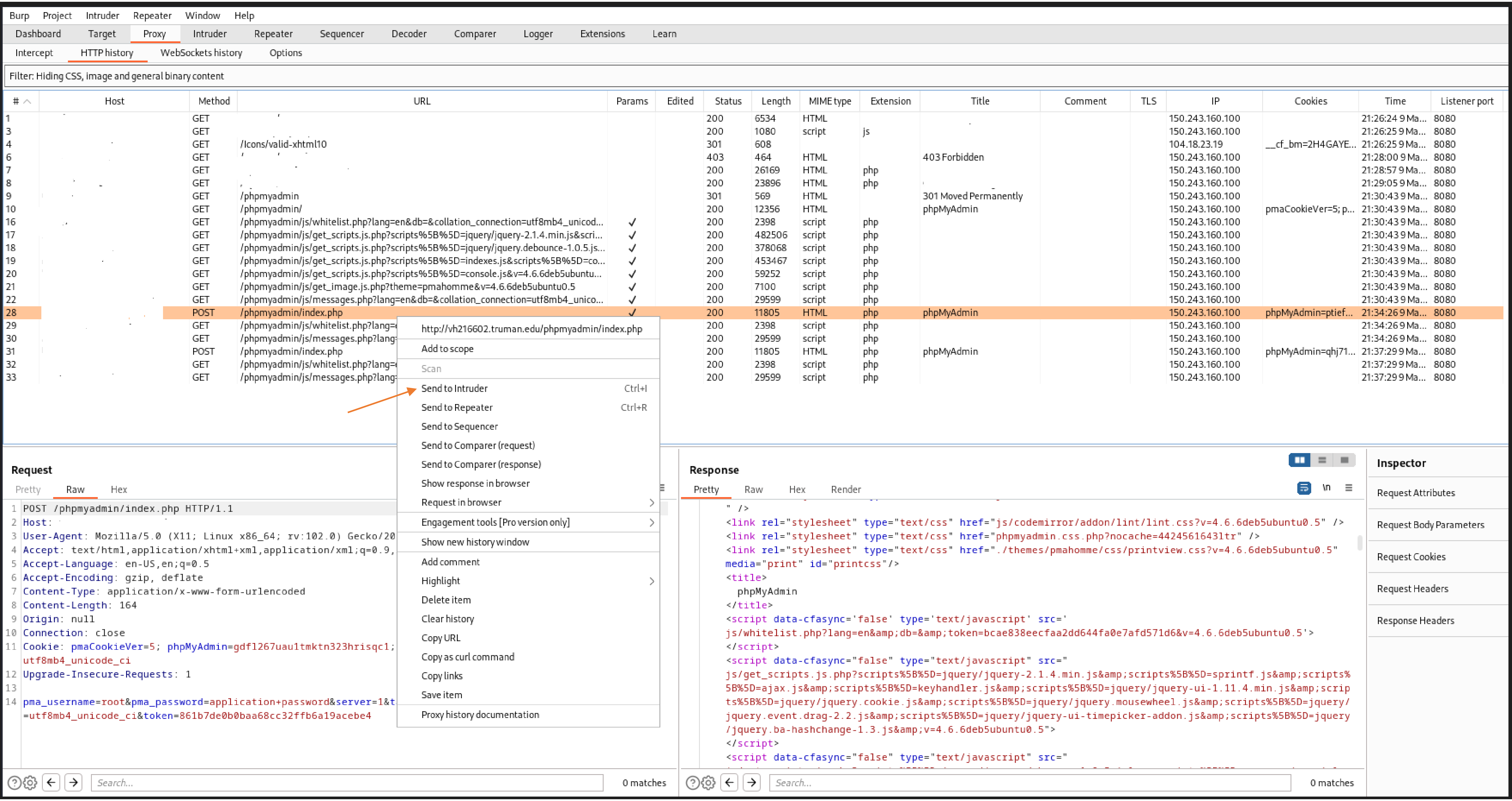
Web application vulnerability



Loggingofout-of-scopeProxytrafficisdisabled

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Com
60	http://192.168.68.12	GET	/dvwa/vulnerabilities/brute/			200	5172	HTML		Damn Vulnerable We...	
61	http://192.168.68.12	GET	/dvwa/vulnerabilities/brute/			200	5172	HTML		Damn Vulnerable We...	
62	http://192.168.68.12	GET	/dvwa/vulnerabilities/brute/?user...	✓		200	5222	HTML		Damn Vulnerable We...	



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1		GET				200	6534	HTML					150.243.160.100		21:26:24 9 Ma...	8080
3		GET				200	1080	script	js				150.243.160.100		21:26:25 9 Ma...	8080
4		GET	/Icons/valid-xhtml10			301	608						104.18.23.19	__cf_bm=2H4GAYE...	21:26:25 9 Ma...	8080
6		GET				403	464	HTML		403 Forbidden			150.243.160.100		21:28:00 9 Ma...	8080
7		GET				200	26169	HTML	php				150.243.160.100		21:28:57 9 Ma...	8080
8		GET				200	23896	HTML	php				150.243.160.100		21:29:05 9 Ma...	8080
9		GET	/phpmyadmin			301	569	HTML		301 Moved Permanently			150.243.160.100		21:30:43 9 Ma...	8080
10		GET	/phpmyadmin/			200	12356	HTML		phpMyAdmin			150.243.160.100	pmaCookieVer=5; p...	21:30:43 9 Ma...	8080
16		GET	/phpmyadmin/js/whitelist.php?lang=en&db=&collation_connection=utf8mb4_unicod...	✓		200	2398	script	php				150.243.160.100		21:30:43 9 Ma...	8080
17		GET	/phpmyadmin/js/get_scripts.js.php?scripts%5B%5D=jquery/jquery-2.1.4.min.js&scri...	✓		200	482506	script	php				150.243.160.100		21:30:43 9 Ma...	8080
18		GET	/phpmyadmin/js/get_scripts.js.php?scripts%5B%5D=jquery/jquery.debounce-1.0.5.js...	✓		200	378068	script	php				150.243.160.100		21:30:43 9 Ma...	8080
19		GET	/phpmyadmin/js/get_scripts.js.php?scripts%5B%5D=indexes.js&scripts%5B%5D=co...	✓		200	453467	script	php				150.243.160.100		21:30:43 9 Ma...	8080
20		GET	/phpmyadmin/js/get_scripts.js.php?scripts%5B%5D=console.js&v=4.6.6deb5ubuntu...	✓		200	59252	script	php				150.243.160.100		21:30:43 9 Ma...	8080
21		GET	/phpmyadmin/js/get_image.js.php?theme=pmahomme&v=4.6.6deb5ubuntu0.5	✓		200	7100	script	php				150.243.160.100		21:30:43 9 Ma...	8080
22		GET	/phpmyadmin/js/messages.php?lang=en&db=&collation_connection=utf8mb4_unico...	✓		200	29599	script	php				150.243.160.100		21:30:43 9 Ma...	8080
28		POST	/phpmyadmin/index.php	✓		200	11805	HTML	php	phpMyAdmin			150.243.160.100	phpMyAdmin=ptief...	21:34:26 9 Ma...	8080
29		GET	/phpmyadmin/js/whitelist.php?lang=			200	2398	script	php				150.243.160.100		21:34:26 9 Ma...	8080
30		GET	/phpmyadmin/js/messages.php?lang=			200	29599	script	php				150.243.160.100		21:34:26 9 Ma...	8080
31		POST	/phpmyadmin/index.php			200	11805	HTML	php	phpMyAdmin			150.243.160.100	phpMyAdmin=qhj71...	21:37:29 9 Ma...	8080
32		GET	/phpmyadmin/js/whitelist.php?lang=			200	2398	script	php				150.243.160.100		21:37:29 9 Ma...	8080
33		GET	/phpmyadmin/js/messages.php?lang=			200	29599	script	php				150.243.160.100		21:37:29 9 Ma...	8080

Request

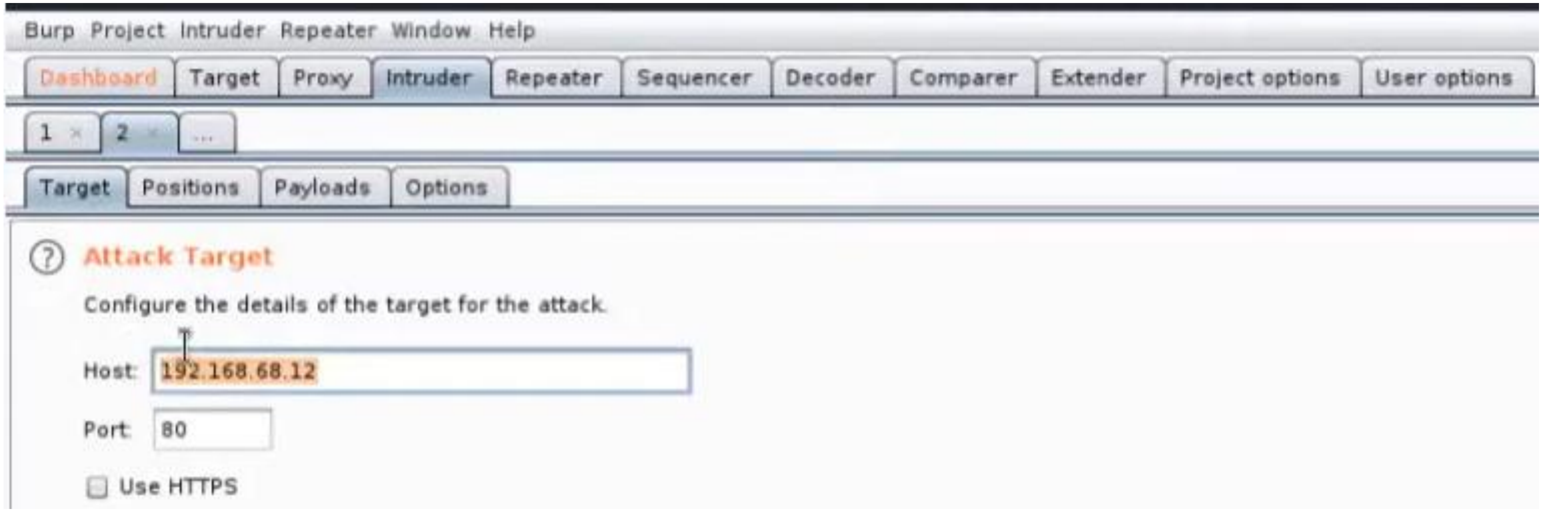
```
POST /phpmyadmin/index.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 164
Origin: null
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=gdfl267uau1tmktn323hrisqc1;
utf8mb4_unicode_ci
Upgrade-Insecure-Requests: 1

pma_username=root&pma_password=application+password&server=1&t
=utf8mb4_unicode_ci&token=861b7de0b0baa68cc32ffb6a19acebe4
```

Response

```
" />
<link rel="stylesheet" type="text/css" href="js/codemirror/addon/lint/lint.css?v=4.6.6deb5ubuntu0.5" />
<link rel="stylesheet" type="text/css" href="phpmyadmin.css.php?nocache=4424561643ltr" />
<link rel="stylesheet" type="text/css" href="./themes/pmahomme/css/printview.css?v=4.6.6deb5ubuntu0.5"
media="print" id="printcss"/>
<title>
  phpMyAdmin
</title>
<script data-cfasync='false' type='text/javascript' src='
js/whitelist.php?lang=en&amp;db=&amp;token=bcae838eecfaa2dd644fa0e7afd571d6&v=4.6.6deb5ubuntu0.5'>
</script>
<script data-cfasync="false" type="text/javascript" src="
js/get_scripts.js.php?scripts%5B%5D=jquery/jquery-2.1.4.min.js&amp;scripts%5B%5D=sprintf.js&amp;scripts%
5B%5D=ajax.js&amp;scripts%5B%5D=keyhandler.js&amp;scripts%5B%5D=jquery/jquery-ui-1.11.4.min.js&amp;scrip
ts%5B%5D=jquery/jquery.cookie.js&amp;scripts%5B%5D=jquery/jquery.mousewheel.js&amp;scripts%5B%5D=jquery/
jquery.event.drag-2.2.js&amp;scripts%5B%5D=jquery/jquery-ui-timepicker-addon.js&amp;scripts%5B%5D=jquery
/jquery.ba-hashchange-1.3.js&amp;v=4.6.6deb5ubuntu0.5">
</script>
<script data-cfasync="false" type="text/javascript" src="
```

Web application vulnerability

- We do have some other types of functions: Repeater, Sequencer, Decoder,…
- Since we have sent it to intruder, the target will be auto-populated.
- I cannot show you the detail, but here is the example.



Attack Target

Configure the details of the target for the attack.

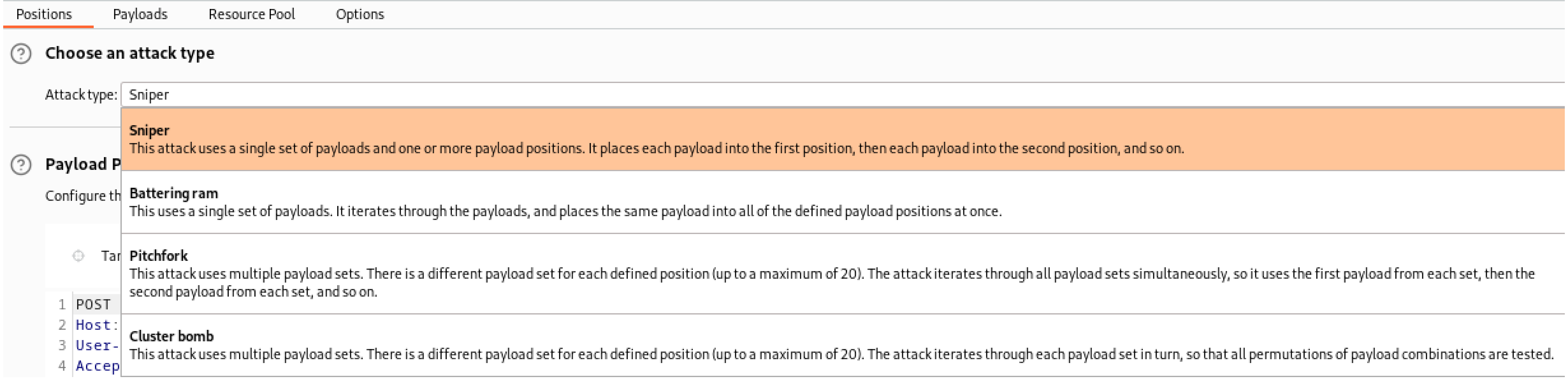
Host: 192.168.68.12

Port: 80

□ Use HTTPS

Web application vulnerability

- Now, switch to the [Intruder] → [Positions] tab, there is an option called Attack Type. 4 different types here
- Each of the type are saying how the **payload** is **used** or is **set**.
    - I'm not the expert of this, but you can try to ask Google
    - **Cluster bomb** is very useful for brute force attacks



Choose an attack type

Attack type: Sniper

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

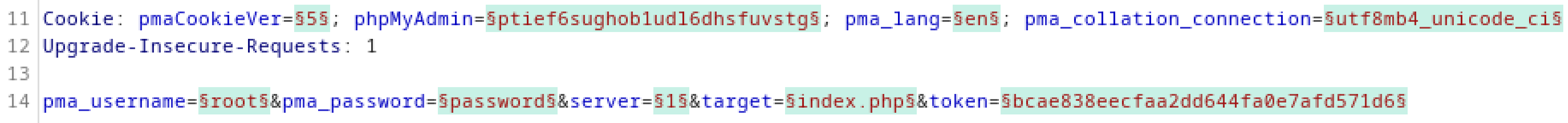
Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

```
POST
Host:
User-
Accep
```

Web application vulnerability

- The payloads are automatically marked

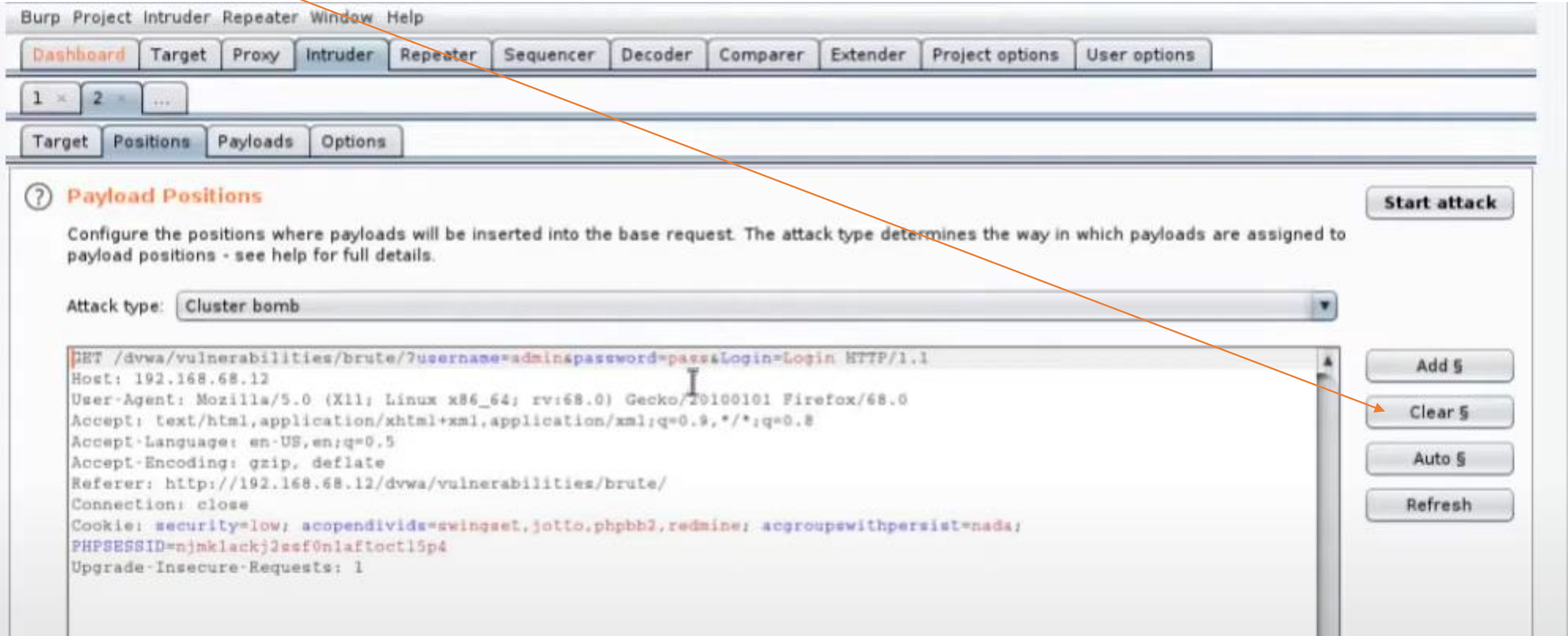


```
Cookie: pmaCookieVer=§5§; phpMyAdmin=§ptief6sughob1udl6dhsfuvstg§; pma_lang=§en§; pma_collation_connection=§utf8mb4_unicode_ci§
Upgrade-Insecure-Requests: 1

pma_username=§root§&pma_password=§password§&server=§1§&target=§index.php§&token=§bcae838eecfaa2dd644fa0e7afd571d6§
```

- Our “simulated” attack target is 192.168.68.12 ☺

Web application vulnerability

- Let’s go clear payloads that is automatically set on payload positions



Payload Positions

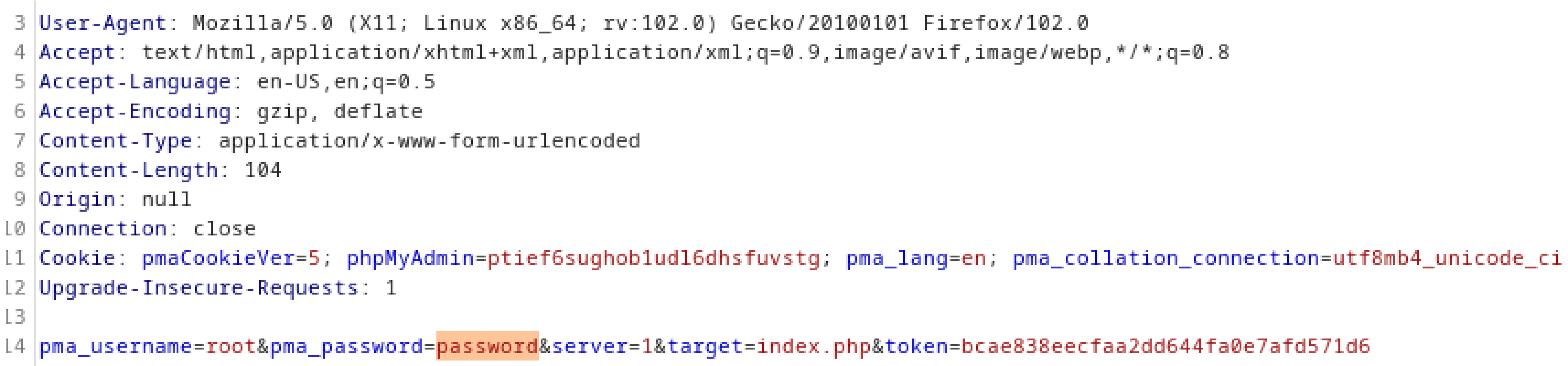
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=pass&Login=Login HTTP/1.1
Host: 192.168.68.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://192.168.68.12/dvwa/vulnerabilities/brute/
Connection: close
Cookie: security=low; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
PHPSESSID=njmklackj2ssf0n1aftoct15p4
Upgrade-Insecure-Requests: 1
```

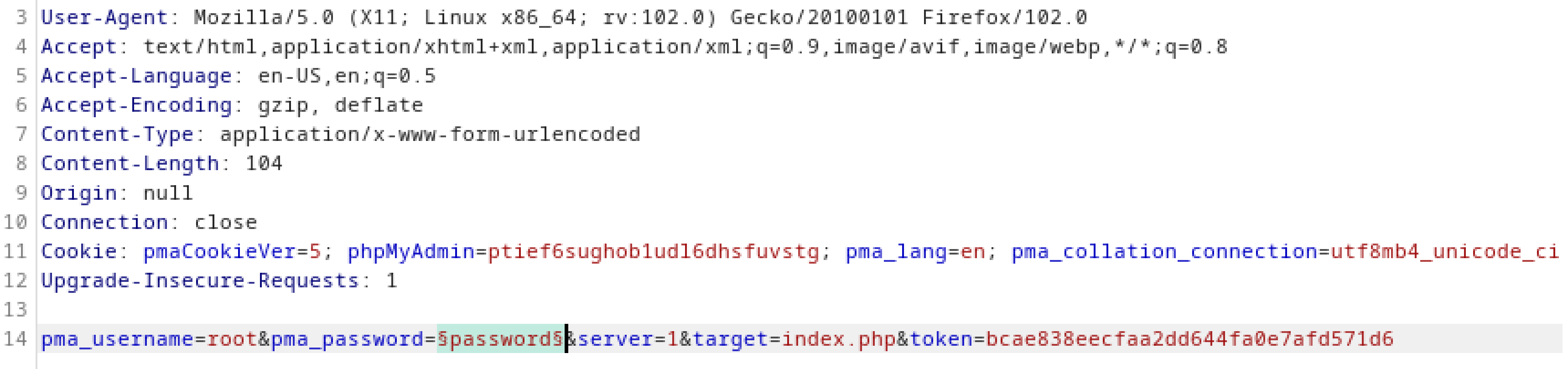
Web application vulnerability

- Double click the “password” and click the [Add $]



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: null
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=ptief6sughob1udl6dhsfuvstg; pma_lang=en; pma_collation_connection=utf8mb4_unicode_ci
Upgrade-Insecure-Requests: 1

pma_username=root&pma_password=password&server=1&target=index.php&token=bcae838eecfaa2dd644fa0e7afd571d6
```

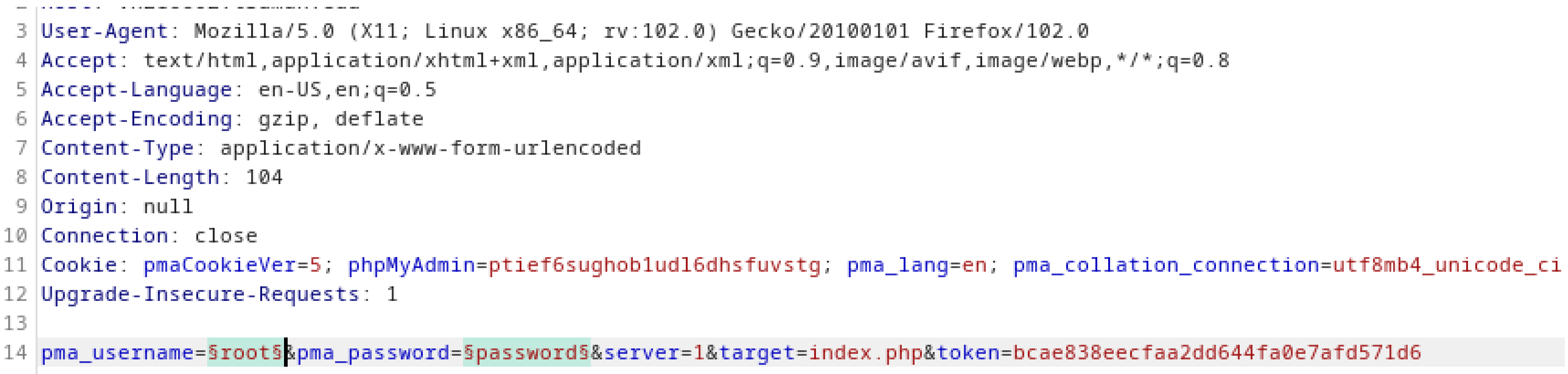
- It will be…



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: null
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=ptief6sughob1udl6dhsfuvstg; pma_lang=en; pma_collation_connection=utf8mb4_unicode_ci
Upgrade-Insecure-Requests: 1

pma_username=root&pma_password=§password§&server=1&target=index.php&token=bcae838eecfaa2dd644fa0e7afd571d6
```

Web application vulnerability

- Do the same thing for “root”.

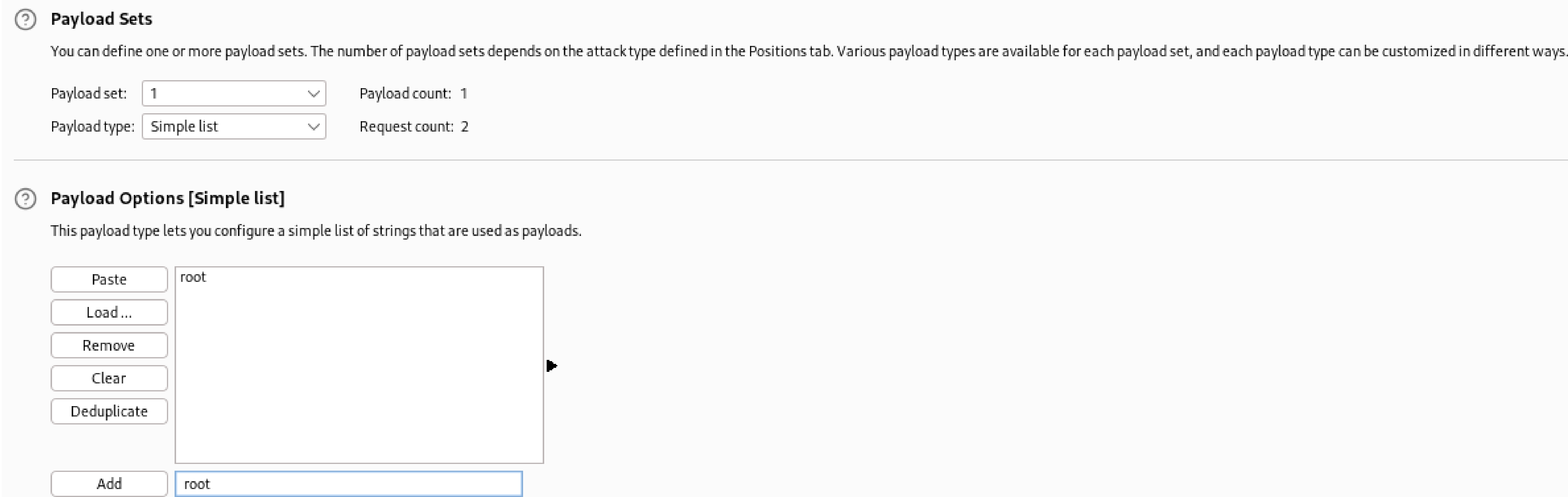


```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: null
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=ptief6sughob1udl6dhsfuvstg; pma_lang=en; pma_collation_connection=utf8mb4_unicode_ci
Upgrade-Insecure-Requests: 1

pma_username=§root§&pma_password=§password§&server=1&target=index.php&token=bcae838eecfaa2dd644fa0e7afd571d6
```

- So, we just basically set 2 payload positions.
- We click the [Payloads] tab
- (Now, we are still sticking on “Cluster bomb” algorithm)

Web application vulnerability

- The 1st one will be a “root”, then [Add] it
- Or if you know someone’s user name. (smile)



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 available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1

Payload type: Simple list Request count: 2

Payload Options [Simple list]

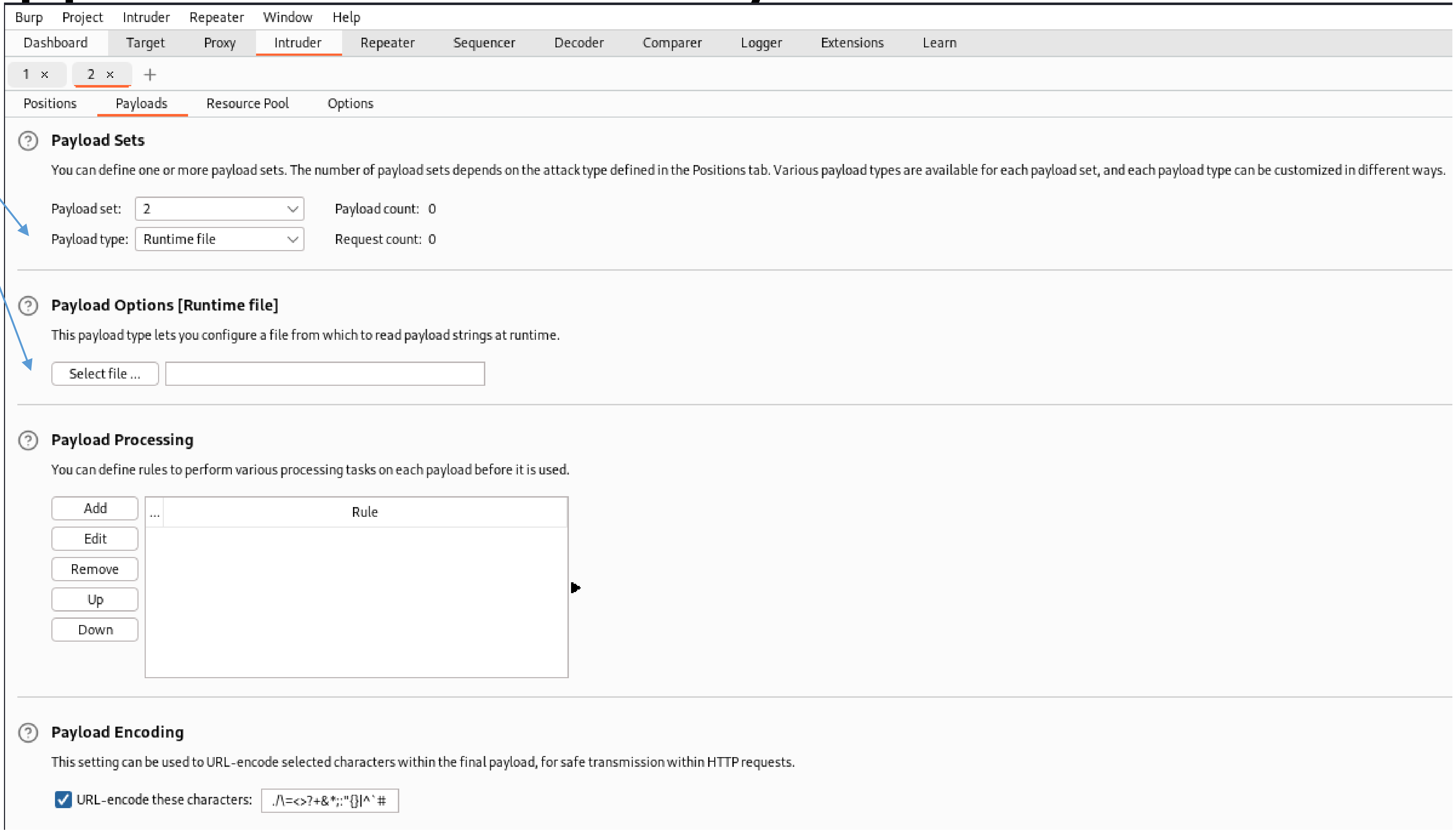
This payload type lets you configure a simple list of strings that are used as payloads.

root

Add: root

Web application vulnerability

The 2nd payload set, we use the “Runtime file” in this time



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
1 × 2 × +
Positions Payloads Resource Pool Options

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 available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 0

Payload type: Runtime file Request count: 0

Payload Options [Runtime file]

This payload type lets you configure a file from which to read payload strings at runtime.

Payload Processing

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

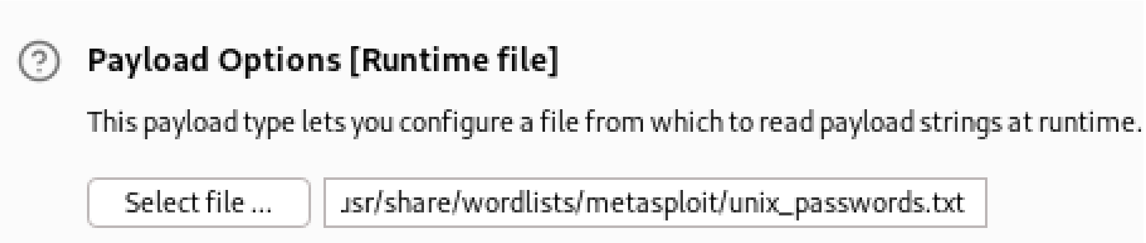
Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Web application vulnerability

- Choose the following file as our 2nd parameter, the password
    - /usr/share/wordlists/metasploit/unix_passwords.txt
- This is basically a text file filled with words. We can say it is a "dictionary"



Payload Options [Runtime file]

This payload type lets you configure a file from which to read payload strings at runtime.

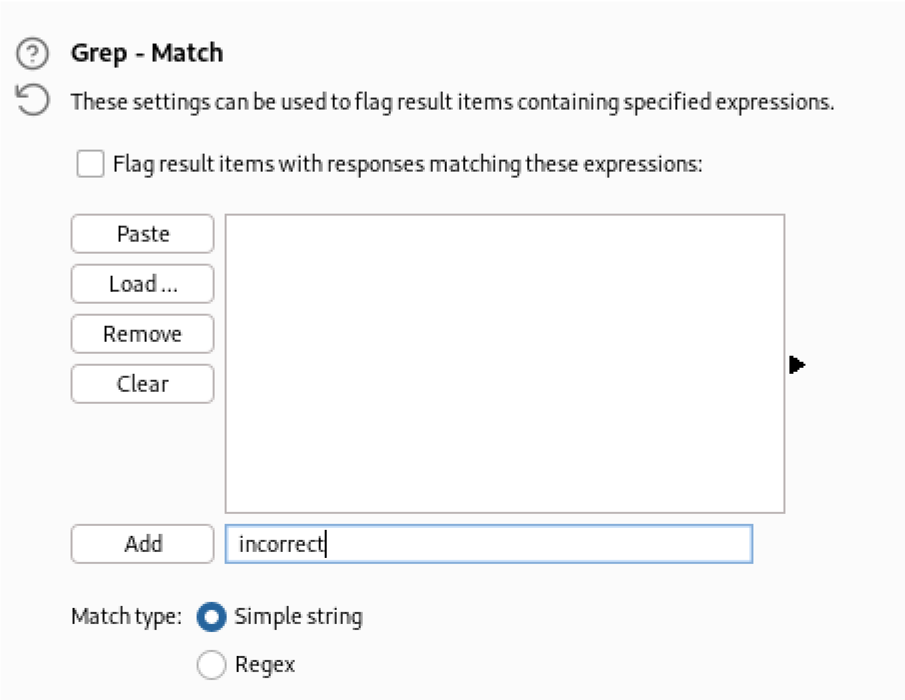
ɹsr/share/wordlists/metasploit/unix_passwords.txt

- Now, we click the [options] tab and scroll down to the "Grab-Match" section

Web application vulnerability

Let’s go ahead to clear the current list

And just put something like “Incorrect”
You will see why we to do this?
It is helpful in the outputs



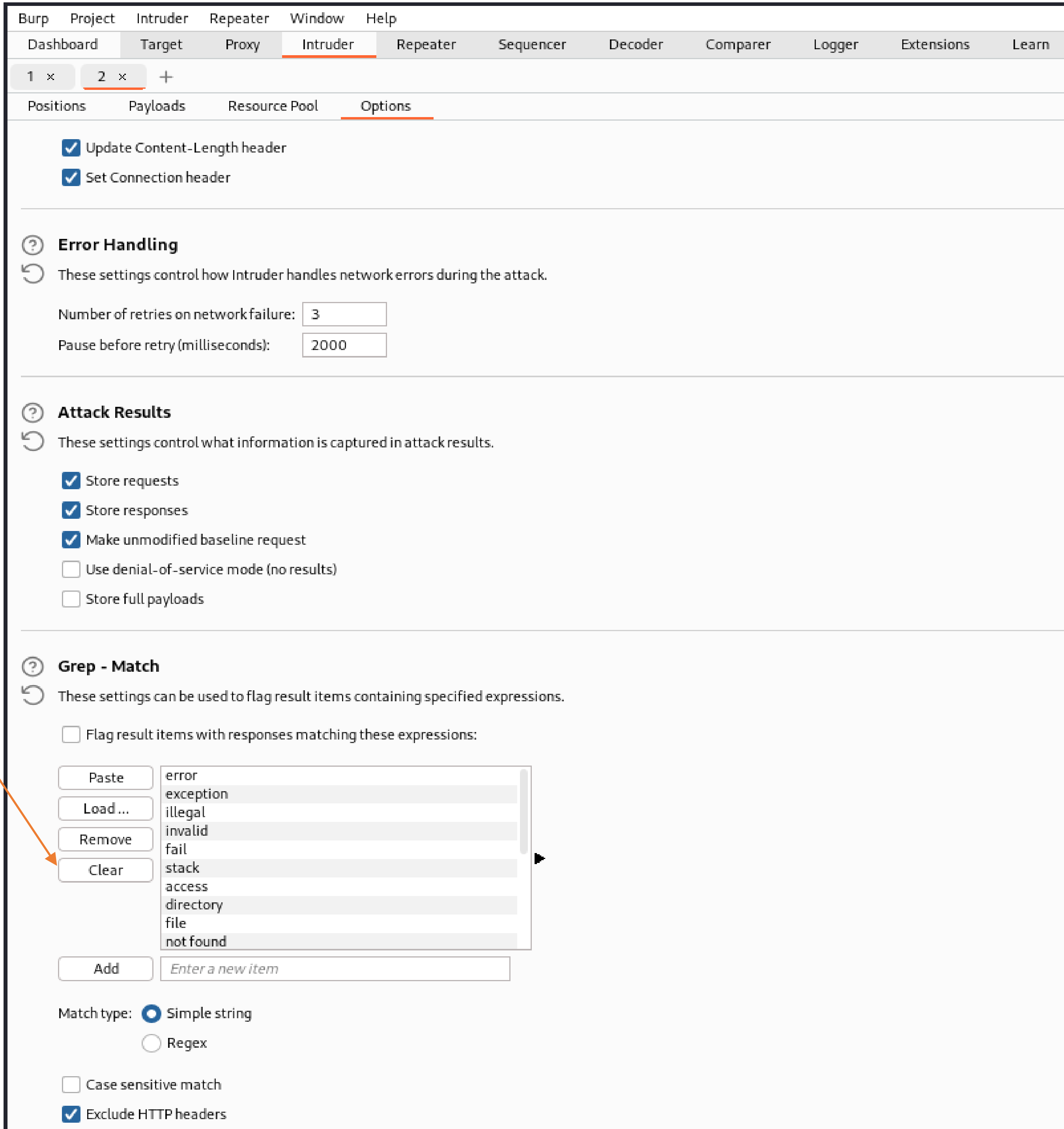
Grep - Match

These settings can be used to flag result items containing specified expressions.

☐ Flag result items with responses matching these expressions:

incorrect

Match type: ● Simple string
○ Regex



☑ Update Content-Length header
☑ Set Connection header

Error Handling

These settings control how Intruder handles network errors during the attack.

Number of retries on network failure: 3
Pause before retry (milliseconds): 2000

Attack Results

These settings control what information is captured in attack results.

☑ Store requests
☑ Store responses
☑ Make unmodified baseline request
☐ Use denial-of-service mode (no results)
☐ Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions.

☐ Flag result items with responses matching these expressions:

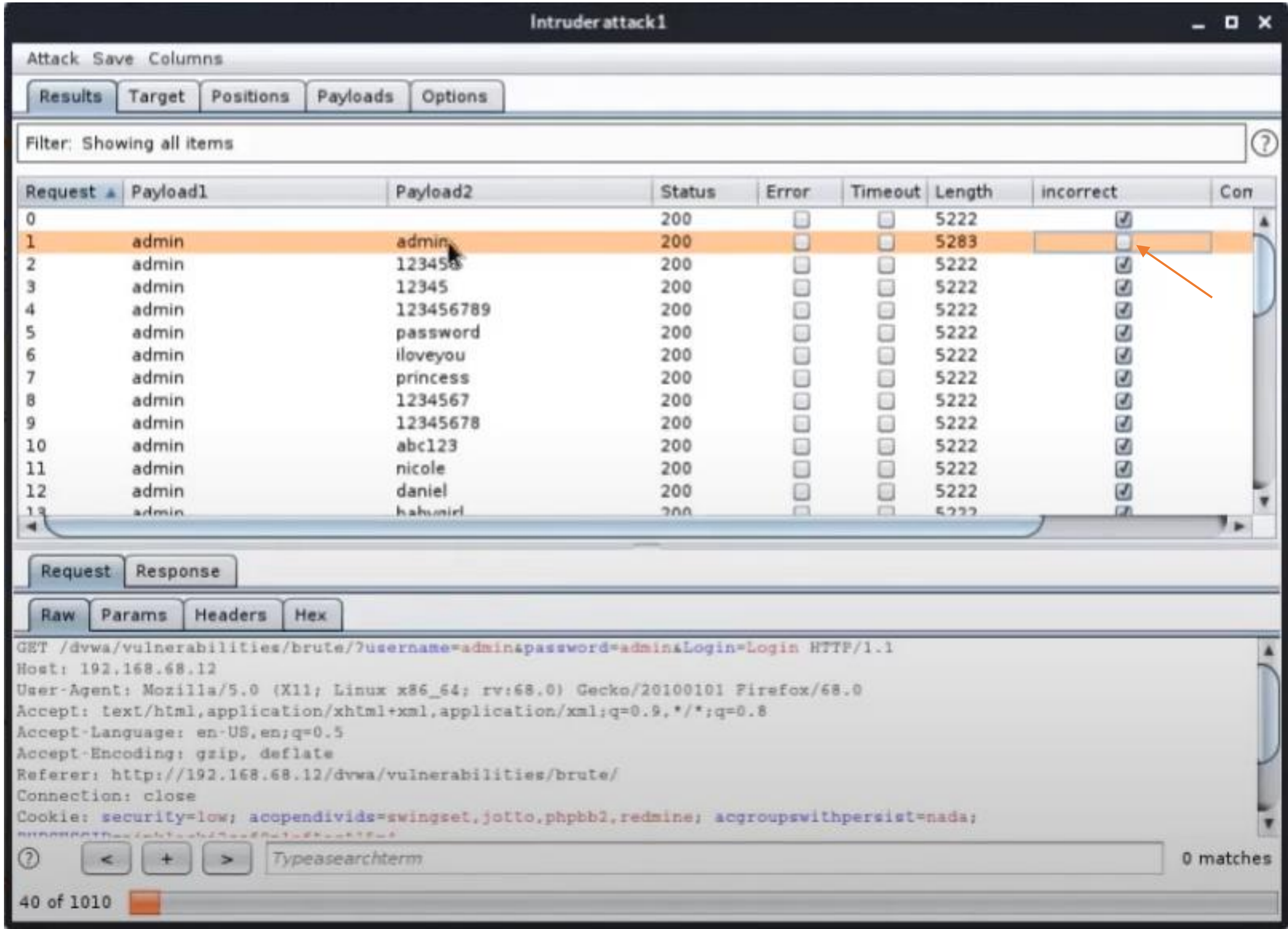
error
exception
illegal
invalid
fail
stack
access
directory
file
not found

Match type: ● Simple string
○ Regex

☐ Case sensitive match
☑ Exclude HTTP headers

Web application vulnerability

- Get out of the options tab, no matter where we are. It is easily see the button "Start attack"
- One it starts, it will bring up a small window like this.
- In this example, its user name is admin, not our "root"
- But for the password, it is trying everything from the file



Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	incorrect	Con
0			200	☐	☐	5222	☑	
1	admin	admin	200	☐	☐	5283	☐	
2	admin	123456	200	☐	☐	5222	☑	
3	admin	12345	200	☐	☐	5222	☑	
4	admin	123456789	200	☐	☐	5222	☑	
5	admin	password	200	☐	☐	5222	☑	
6	admin	iloveyou	200	☐	☐	5222	☑	
7	admin	princess	200	☐	☐	5222	☑	
8	admin	1234567	200	☐	☐	5222	☑	
9	admin	12345678	200	☐	☐	5222	☑	
10	admin	abc123	200	☐	☐	5222	☑	
11	admin	nicole	200	☐	☐	5222	☑	
12	admin	daniel	200	☐	☐	5222	☑	
13	admin	babygirl	200	☐	☐	5222	☑	

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: 192.168.68.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://192.168.68.12/dvwa/vulnerabilities/brute/
Connection: close
Cookie: security=low; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
```

Web application vulnerability

- Oh wow! There is a match. The user name and password are both “admin” --- not a very smart combination
- There are totally 1010 words in the dictionary for password, by the way.
- You can see the progress bar