

STRING OF ILLUSIONS



The background is a dark red gradient. It features abstract geometric patterns consisting of thin white lines forming various polygons and star-like shapes. Small, bright pinkish-red dots are placed at some of the vertices of these geometric figures. One dot is in the upper left, and a cluster of three dots is in the lower right.

ID -UN

The background is a dark red gradient with abstract geometric patterns. Thin white lines connect small dots, forming a network-like structure. One dot is visible in the upper left, and a cluster of dots is in the lower right.

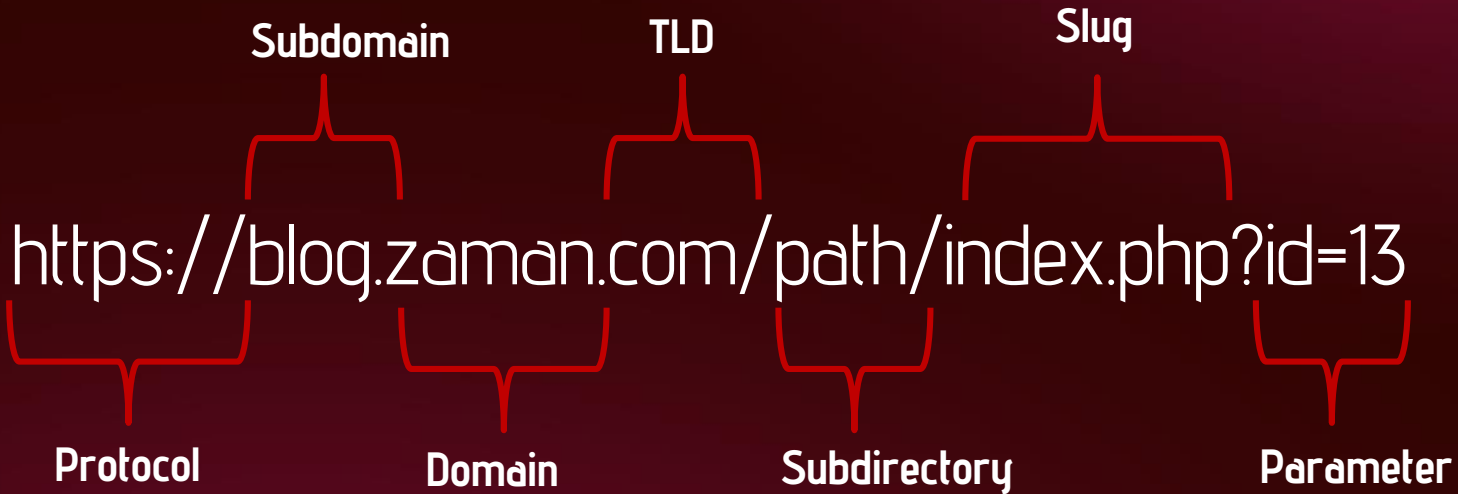
ALMAS ZAMAN

An Information Security Researcher
and Adjunct Assistant Professor

OBJECTIVE

- **Concept** Development
- Structure of a **URL**, **Character Encoding**, **DNS**
- Use of non-ASCII **TLD** in Bangladesh
- **Vulnerability** of Character Encoding Standards (Homograph)
- **Advanced Homograph** or Illusion
- Method of generate a **Advanced Homograph Illusion** URL
- **Vectors**
- **Remedies**

STRUCTURE OF A URL



CHARACTER ENCODING STANDARDS

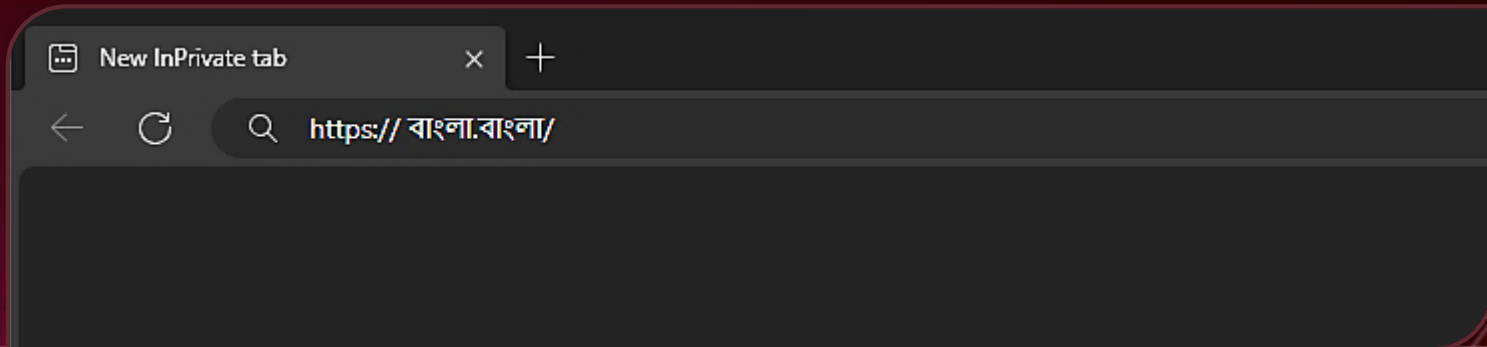
- **ASCII:** Basic Latin characters and symbols, fully compatible with UTF-8.
- **UTF-8:** Widely used, supports diverse languages, variable-length encoding.
- **UTF-16:** Uses 16 bits per character, common in programming.
- **UTF-32:** Fixed 32 bits per character, simplifies text processing.
- **ISO 8859:** Series of standards for specific languages.

	Code Point	UTF-8 Binary
A	-	01000001
ব	U+09AC	11100000 10100110 10101100

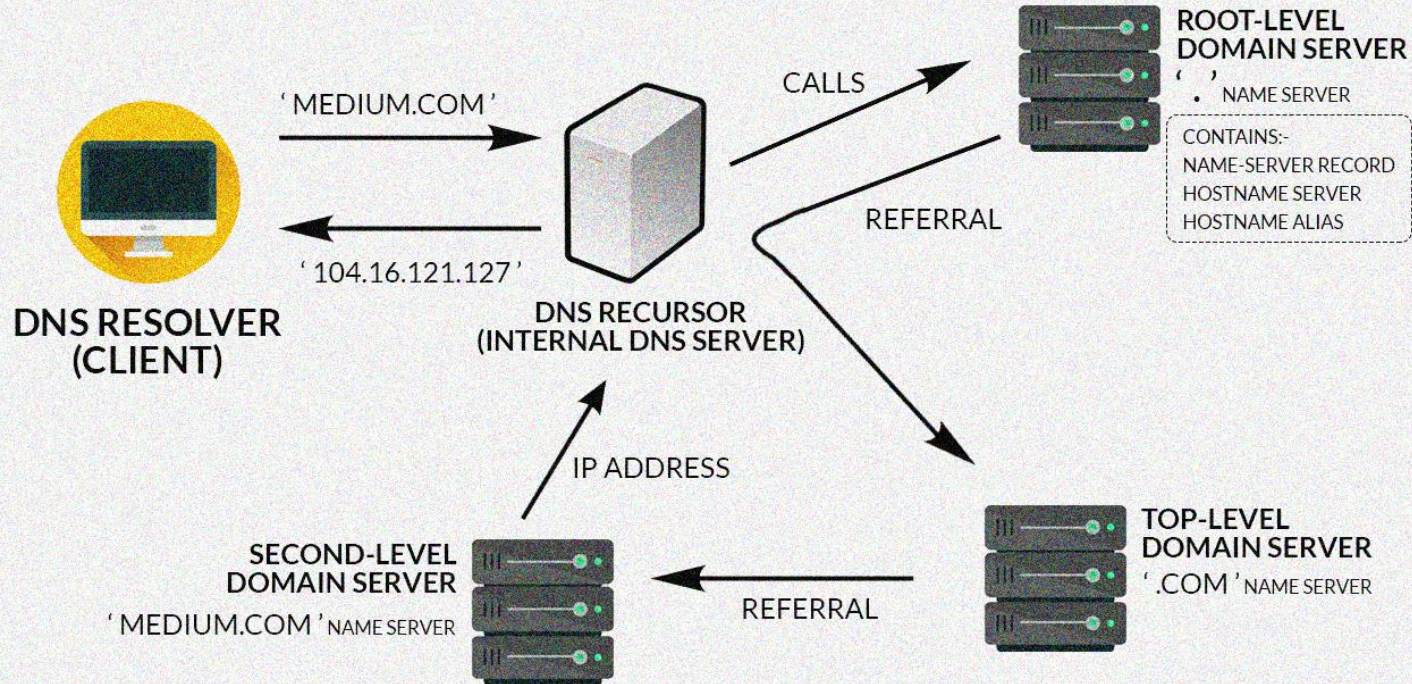
USE OF NON-ASCII (UNICODE) TLD IN BANGLADESH

[https:// বাংলা.বাংলা](https://বাংলা.বাংলা)

The first domain name registered with the **.বাংলা** (Dot Bangla) top-level domain (TLD) was **'বাংলা.বাংলা'** This domain was registered on **October 27, 2016**



HOW A URL WORKS? (DNS CONTEXT)



VULNERABILITY OF CHARACTER ENCODING STANDERS

Homograph or Homoglyph attack

Domain	Homograph Domain	Codepoint
theteamphoenix.org	thêteamphoenix.org	‘ê’ U+00EA
tapkori.com	tapkori.com	‘i’ U+13A5

BUT! CAN YOU FIND ANY DIFFERENCES?

- <https://www.facebook.com/paGe.uCo.AUtoS>
- <https://www.facebook.com/paGe.uCo.AUtoS>

ADVANCED HOMOGRAPH OR ILLUSION

Use of **DIVISION SLASH** or **FRACTION SLASH**

- <https://www.facebook.com/paGe.uCo.AUtoS>
- <https://www.facebook.com/paGe.uCo.AUtoS>

Font: Barlow Condensed SemiBold	Font: Arial	Codepoint
/	/	U+002F
/	/	U+2215

ANALYSIS

Subdomain TLD

<https://www.facebook.com/paGe.uCo.AUtoS>



Genuine

<https://www.facebook.com/paGe.uCo.AUtoS>



Fake or Malicious

Domain and Subdomain

TLD

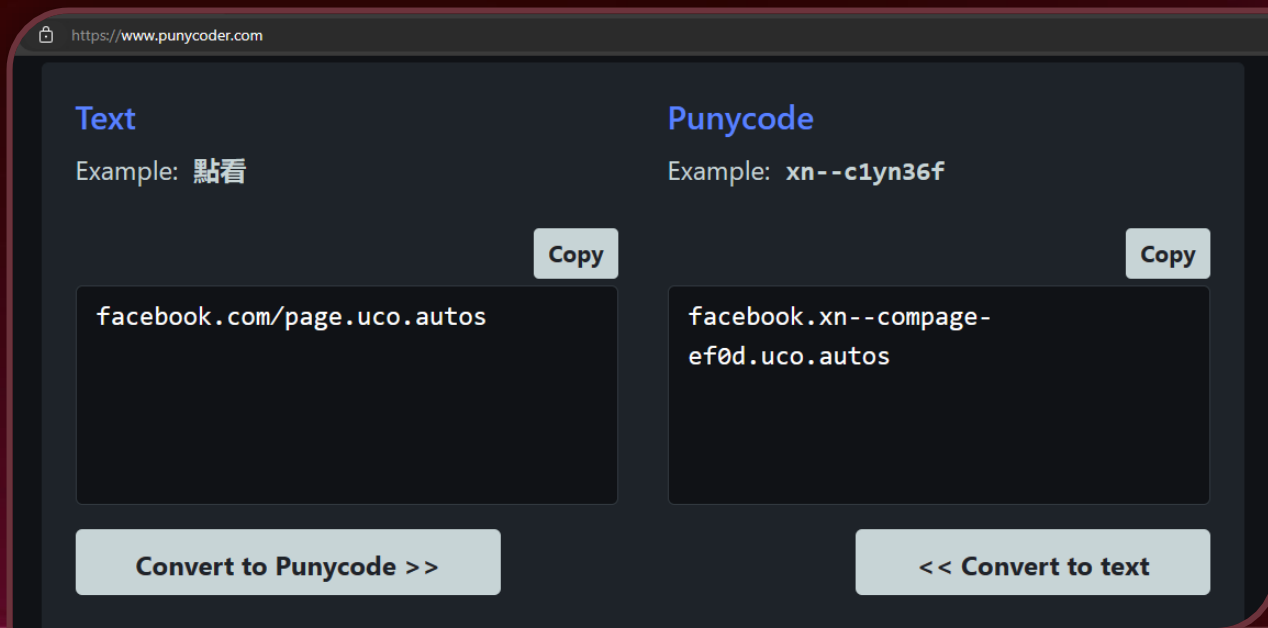
METHODOLOGY (PUNYCODE)

Domain names with non-ASCII characters would not be compatible with the existing **Domain Name System (DNS)** infrastructure, which primarily supports ASCII characters. **Punycode** provides a way to represent non-ASCII characters in a format that can be resolved by DNS servers.


non-ASCII Character	Punycode Encoding
https:// বাংলা.বাংলা/	https://xn--54b7fta0cc.xn--54b7fta0cc/

METHODOLOGY (PUNYCODE)




non-ASCII Character	Punycode Encoding
<code>https://www.facebook.com/paGe.uCo.AUtoS</code>	<code>https://facebook.xn--compa- ef0d.uco.autos</code>



METHODOLOGY (PUNYCODE)



Search Tools (/)




Domains

[← List Domains](#)


Use this interface to manage your domains. For more information, read the [documentation](#).

Create a New Domain

Domain 

Enter the domain that you would like to create:

facebook.xn--compage-ef0d.uco.autos

Document Root (File System Location) 

If the document root is shared then the created domain will serve the same content as "uco.autos". **This setting is permanent.**

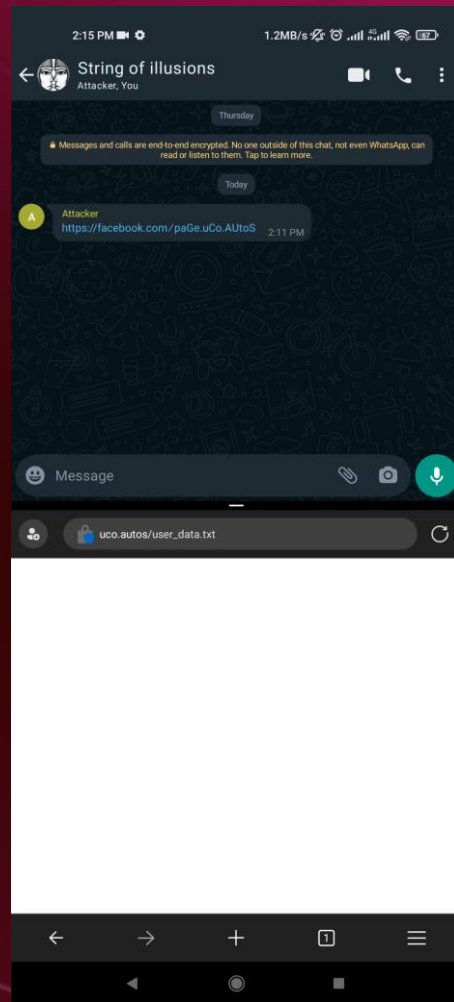
☒ Share document root (/home/ucoautos/public_html) with "uco.autos".

Submit

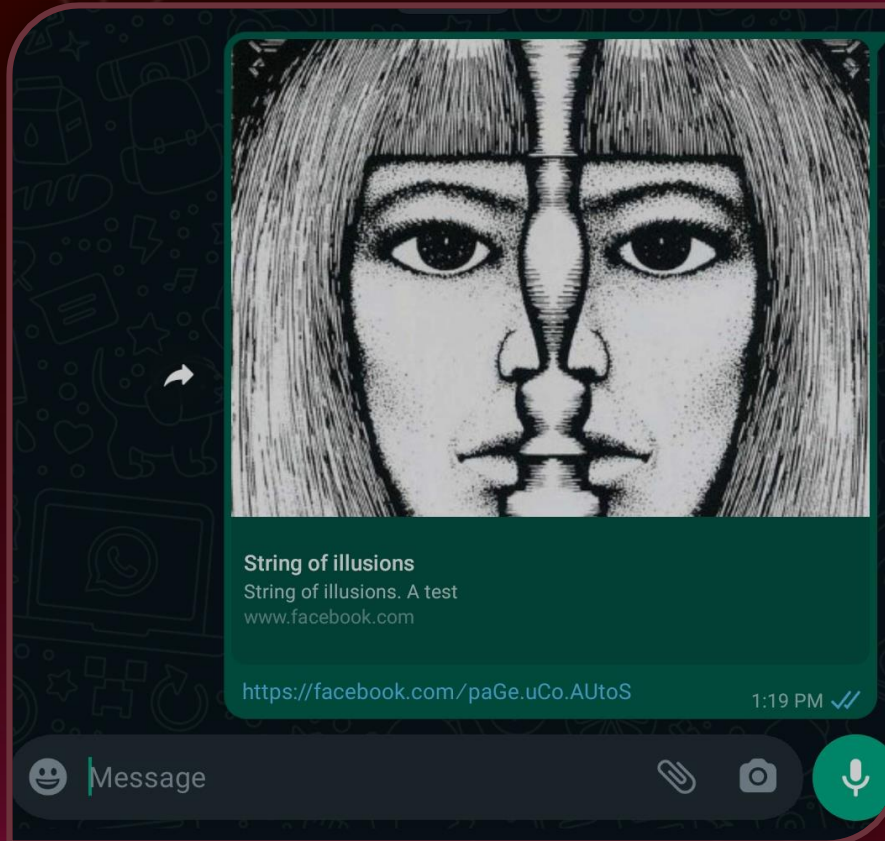
Submit And Create Another

[← Return To Domains](#)

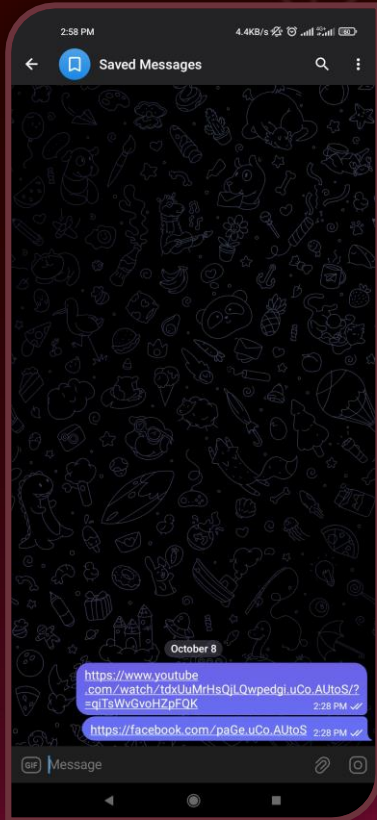
VECTORS (WHATSAPP)



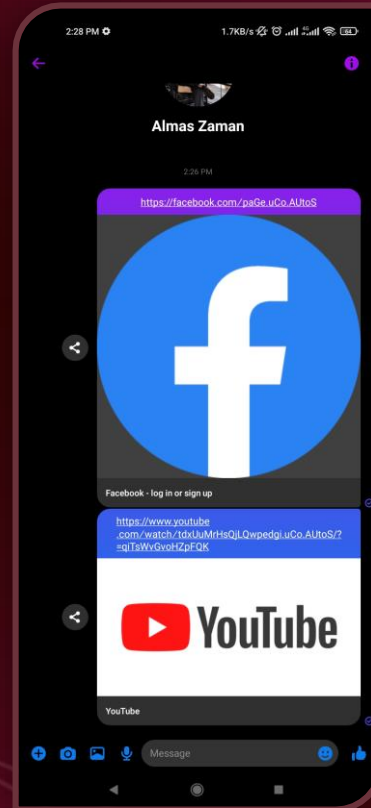
THUMBNAIL WHATSAPP



VECTORS



Telegram



Messenger

HOW IT CAN BE USED

Red Team can use is as

- Advanced **Phishing** Attack
- IP **Logger**

1337 can use is as

- Browser **SBX** (One click)

REMEDIES

- Use **custom font** in smartphone
 - Decoder the URL in **punycode decoder** if suspected
- ...and most important

Think Before You Click

QUESTION?

>NC -LVP 133?

