# STEK Sharing is Not Caring: **Bypassing TLS Authentication in Web Servers using Session Tickets**

**Sven Hebrok** Tim Leonhard Storm Felix Matthias Cramer
Maximilian Radoy Juraj Somorovsky

USENIX Security '25 | August 13–15, 2025

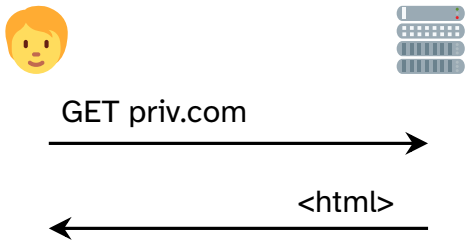
PADERBORN UNIVERSITY

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen

NERD.NRW

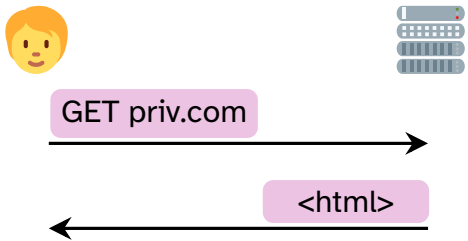
# TLS Protects Web Traffic

- Commonly used in the web



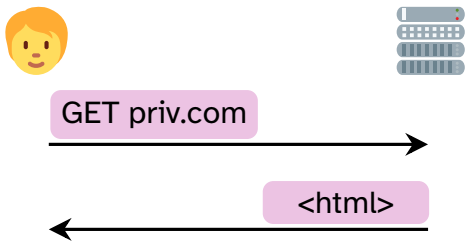
# TLS Protects Web Traffic

- Commonly used in the web
- Encrypts content



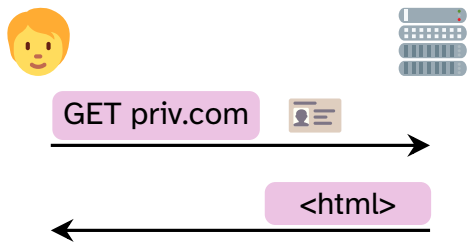
# TLS Protects Web Traffic

- Commonly used in the web
- Encrypts content
- Authenticates server



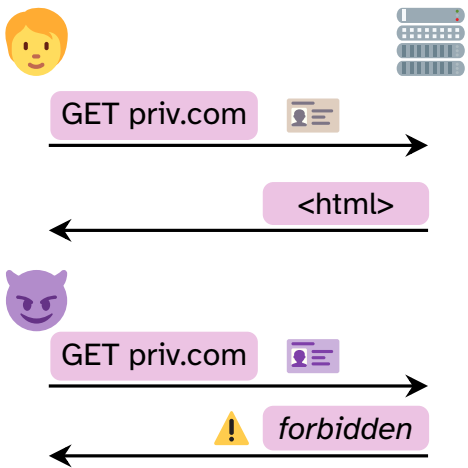
# TLS Protects Web Traffic

- Commonly used in the web
- Encrypts content
- Authenticates server
- Can authenticate client



# TLS Protects Web Traffic

- Commonly used in the web
- Encrypts content
- Authenticates server
- Can authenticate client
  - Access control



# Bypassing Client Authentication

# Bypassing Client Authentication

vHosting

pub.com

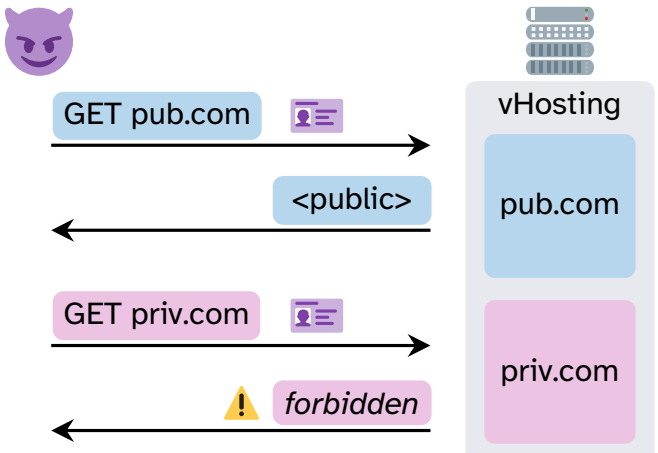
priv.com

GET priv.com

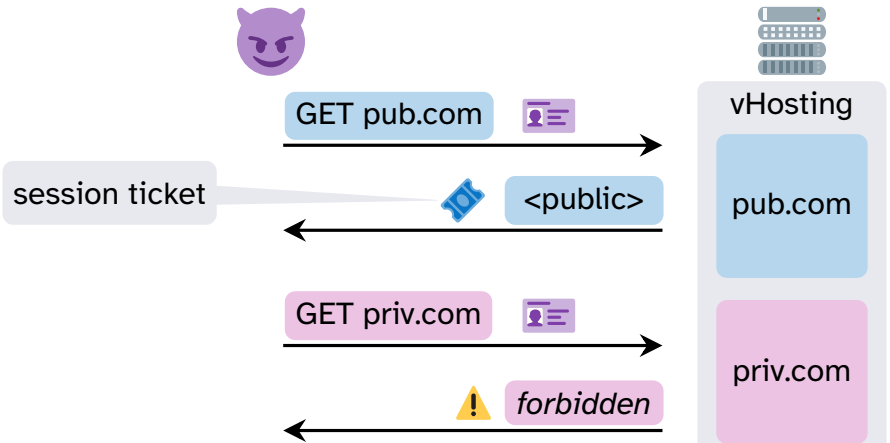


*forbidden*

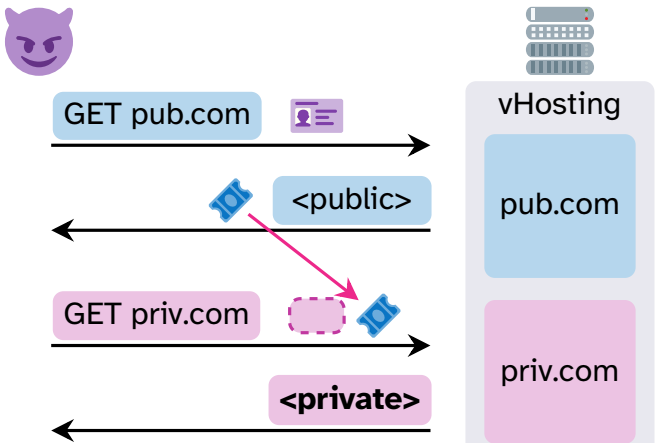
# Bypassing Client Authentication



# Bypassing Client Authentication



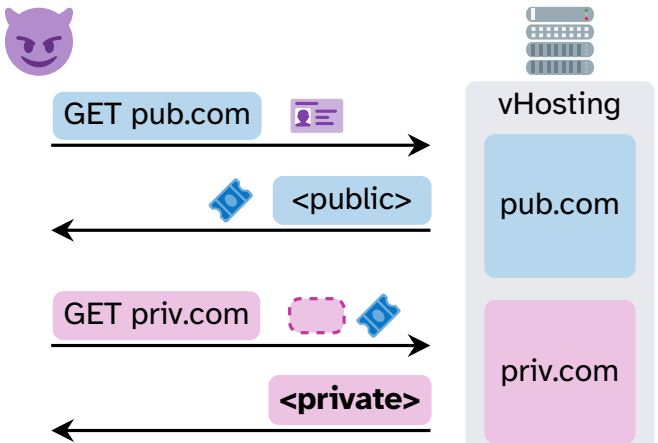
# Bypassing Client Authentication



# Bypassing Client Authentication

Automatically tested servers

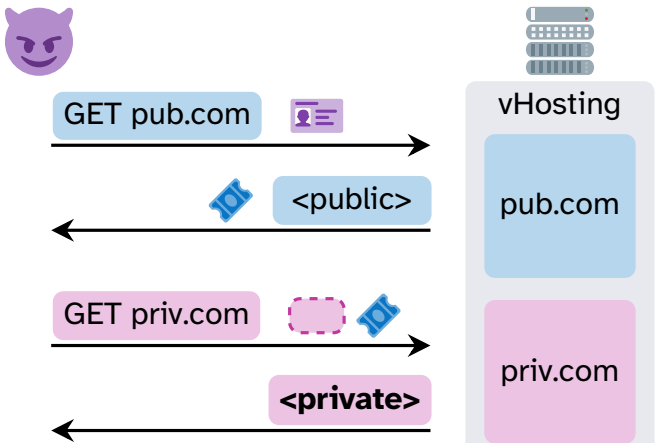
- Apache
- Caddy
- nginx
- LiteSpeed



# Bypassing Client Authentication

Automatically tested servers

- !! Apache
- !! Caddy
- !! nginx
- !! LiteSpeed



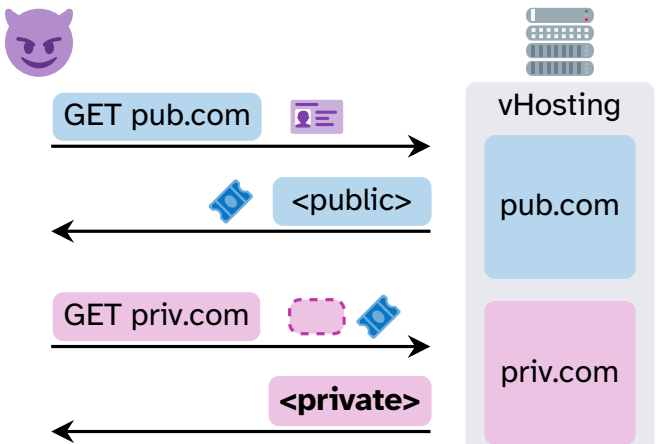
# Bypassing Client Authentication

Automatically tested servers

- !! Apache
- !! Caddy
- !! nginx
- !! LiteSpeed

Manually tested cloud providers

- Azure
- Cloudflare
- Google Cloud



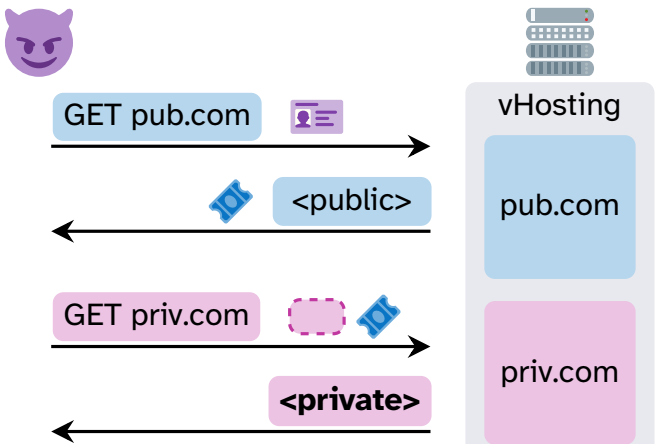
# Bypassing Client Authentication

Automatically tested servers

- !! Apache
- !! Caddy
- !! nginx
- !! LiteSpeed

Manually tested cloud providers

- Azure
- !! Cloudflare
- Google Cloud



# HTTPS is Complex

- Server authentication

# HTTPS is Complex

- Server authentication
- Client authentication

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
    - Skips authentication

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

+

- Virtual hosting

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

+

- Virtual hosting
  - Fallback/Default hosts

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

+

- Virtual hosting
  - Fallback/Default hosts
  - CDNs

# HTTPS is Complex

- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

+

- Virtual hosting
  - Fallback/Default hosts
  - CDNs
- HTTP Host header vs TLS SNI

# HTTPS is Complex

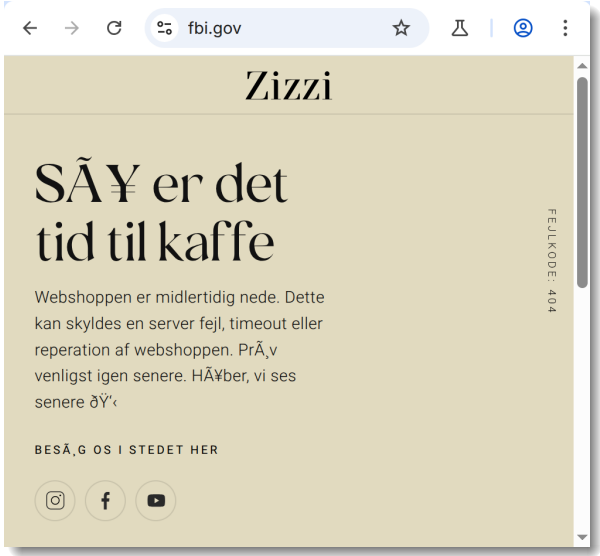
- Server authentication
- Client authentication
- Session resumption (Tickets)
  - Skips authentication
- Multiple TLS versions

+

- Virtual hosting
  - Fallback/Default hosts
  - CDNs
- HTTP Host header vs TLS SNI

= Complexity

# Visit our Poster




*STEK Sharing is Not Caring:*

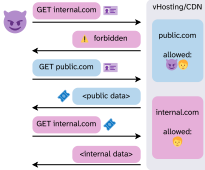
## Bypassing TLS Authentication in Web Servers using Session Tickets

*Sven Hebrok, Tim Leonhard Storm, Felix Matthias Cramer, Maximilian Radoy, Juraj Somorovsky*

- TLS session tickets accelerate connections
- Skip costly authentication step in resumption
- Virtual hosting uses a single server for multiple domains

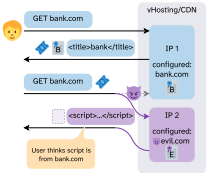
***How do session tickets affect TLS authentication guarantees?***

*Client Authentication*




Privilege Escalation / Authentication Bypass

*Server Authentication*




XSS, MitM

***Do these vulnerabilities exist in the real-world?***

| TLS SNI → / HTTP Host → | | public | | internal | | omitted | |
|---|---|---|---|---|---|---|---|
| | | public | internal | public | internal | public | internal |
| Apache | TLS 1.2 / TLS 1.3 | public | 421 | not resumed | | public | 421 internal |
| Apache (strict) | TLS 1.2 | public | 421 | not resumed | | public | 421 |
| | TLS 1.3 | | | | | 400 | 400 |
| Caddy | TLS 1.2 / TLS 1.3 | public | 421 | 421 | internal | not resumed | |
| nginx | TLS 1.2 | public | 421 | public | 421 | public | 421 |
| | TLS 1.3 | | | 421 | internal | | internal |
| nginx (strict SNI) | TLS 1.2 | public | 421 | public | 421 | public | 421 |
| | TLS 1.3 | | | 421 | internal | | internal |
| LiteSpeed | TLS 1.2 / TLS 1.3 | public | internal | not resumed | | public | internal |

Manually found affected provider: Cloudflare

Performed large-scale scan
Found 3 affected CDNs/providers:
Fastly, DDoS-Guard, Variti
Discovered routing issue in Cloudflare allowing MitM

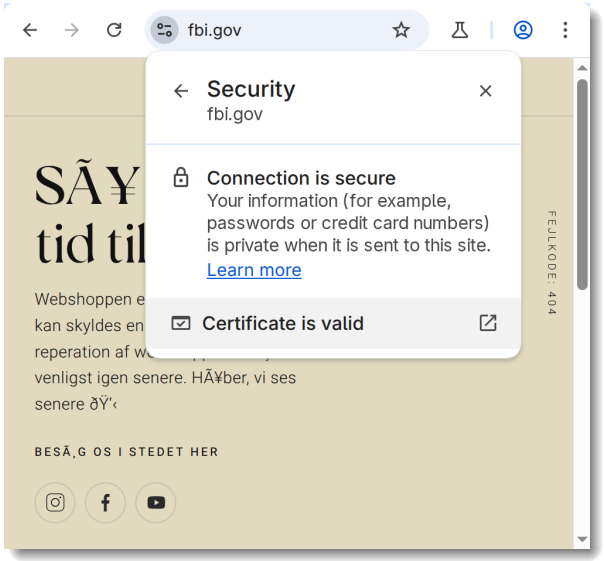
Reasons for these vulnerabilities:
- Easy to misuse APIs in TLS libraries
- Standards vague about interaction of
  - Session resumption
  - Virtual hosting (SNI, Host header)

Read the Paper

Contact us
sven.hebrok@upb.de

PADERBORN UNIVERSITY
NERD.NRW
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

# Visit our Poster




*STEK Sharing is Not Caring:*

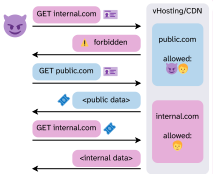
## Bypassing TLS Authentication in Web Servers using Session Tickets

*Sven Hebrok, Tim Leonhard Storm, Felix Matthias Cramer, Maximilian Radoy, Juraj Somorovsky*

- TLS session tickets accelerate connections
- Skip costly authentication step in resumption
- Virtual hosting uses a single server for multiple domains

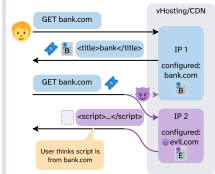
***How do session tickets affect TLS authentication guarantees?***

*Client Authentication*




Privilege Escalation / Authentication Bypass

*Server Authentication*




XSS, MitM

***Do these vulnerabilities exist in the real-world?***

| | TLS SNI → | | public | | internal | | omitted | |
|---|---|---|---|---|---|---|---|---|
| | HTTP Host → | public | internal | public | internal | public | internal |
| Apache | TLS 1.2 | public | 421 | not resumed | | public | 421 |
| | TLS 1.3 | | | | | | internal |
| Apache (strict) | TLS 1.2 | public | 421 | not resumed | | public | 421 |
| | TLS 1.3 | | | | | 400 | 400 |
| Caddy | TLS 1.2 | public | 421 | 421 | internal | not resumed | |
| | TLS 1.3 | | | | | | |
| nginx | TLS 1.2 | public | 421 | public | 421 | public | 421 |
| | TLS 1.3 | | | 421 | internal | | internal |
| nginx (strict SNI) | TLS 1.2 | public | 421 | public | 421 | public | 421 |
| | TLS 1.3 | | | 421 | internal | not resumed | |
| LiteSpeed | TLS 1.2 | public | internal | not resumed | | public | internal |
| | TLS 1.3 | | | | | | |

Manually found affected provider: Cloudflare

Performed large-scale scan
Found 3 affected CDNs/providers:
Fastly, DDoS-Guard, Variti
Discovered routing issue in Cloudflare allowing MitM

Reasons for these vulnerabilities:
- Easy to misuse APIs in TLS libraries
- Standards vague about interaction of
  - Session resumption
  - Virtual hosting (SNI, Host header)

Read the Paper

Contact us
sven.hebrok@upb.de

PADERBORN UNIVERSITY
NERD.NRW
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen