# Hacking the View State

Ovidiu Diaconescu
ovidiu@ovidiudiaconescu.com
@ovidiaconescu

# Overview

HTTP - each request is independent

View State - preserves page and control values

# Storage

Hidden Field (default)

```
<input
type="hidden"
name="__VIEWSTATE"
id="__VIEWSTATE"
value="/wEPDwUKMw9kFgICAw9..">
```

Cache / Session

Database

# Malicious URL

Intercept

Decode

Insert the malicious script

Encode

http://example.com/index.aspx?__VIEWSTATE=%2fw...

# DEMO

# Prevention Methods

web.config

viewStateEncryptionMode

- (default) Auto | Always | Never

enableViewstateMac Message Authentication Code

- MachineKey server specific
- Performance Hit

# DEMO 2

# Q & A