



# Rational tehnički gablec - Otvaranje CROZ testnog centra

## **(ne)sigurnost?**

Neven Biruški, [nbiruski@croz.net](mailto:nbiruski@croz.net)

*Ilustracije:*

*Dražen Spalatin, [dspalatin@croz.net](mailto:dspalatin@croz.net)*

*Filip Herceg, [fherceg@croz.net](mailto:fherceg@croz.net)*




# CROZ





## (de)Motivacijski citat




"When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like. But in all my experience, I have never been in any accident ... or any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort."



**CROZ**



## (de)Motivacijski citat



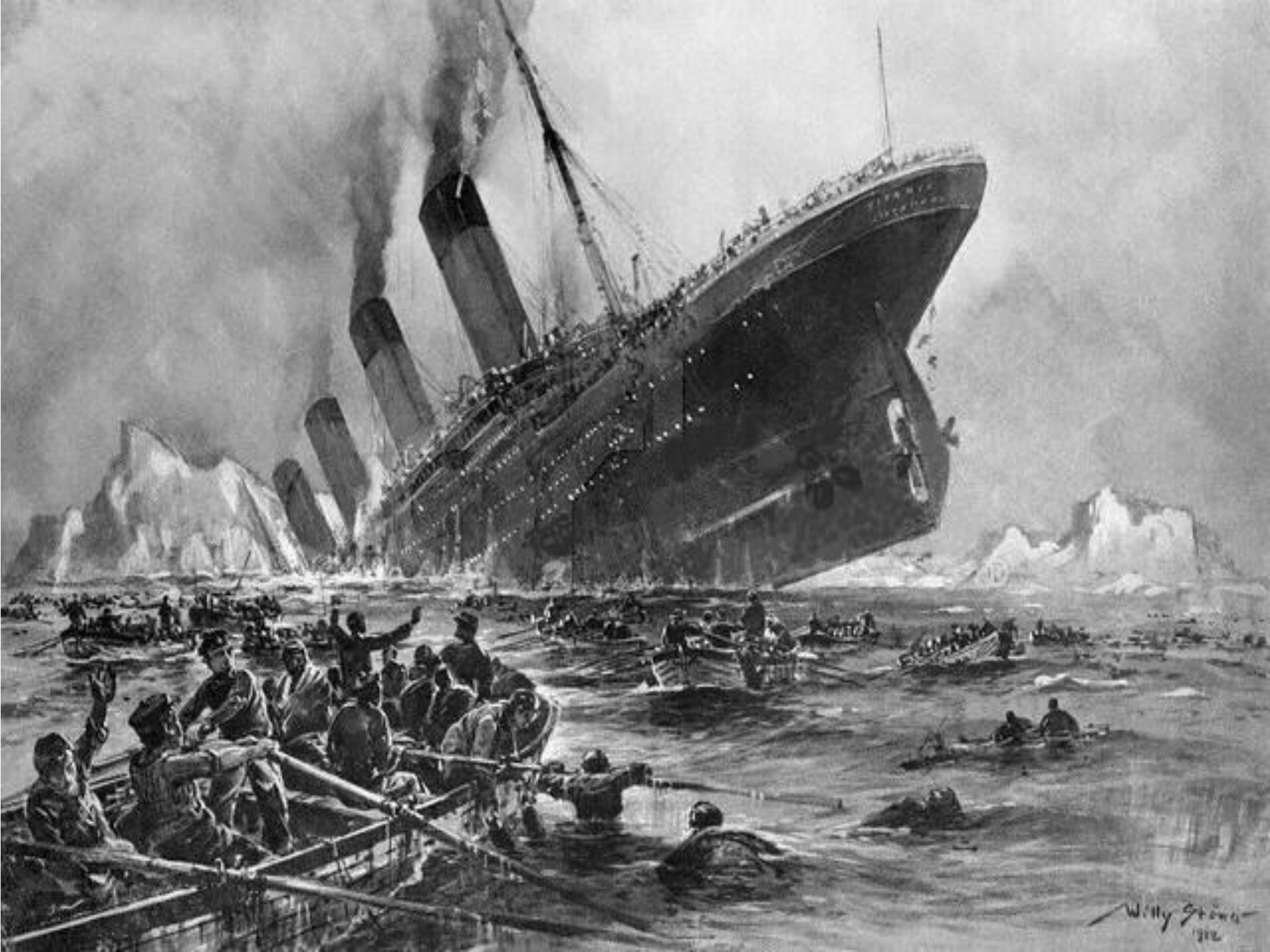
"When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like. But in all my experience, I have never been in any accident ... or any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort."

**Captain Edward John Smith**

**1850-1912**



**CROZ**

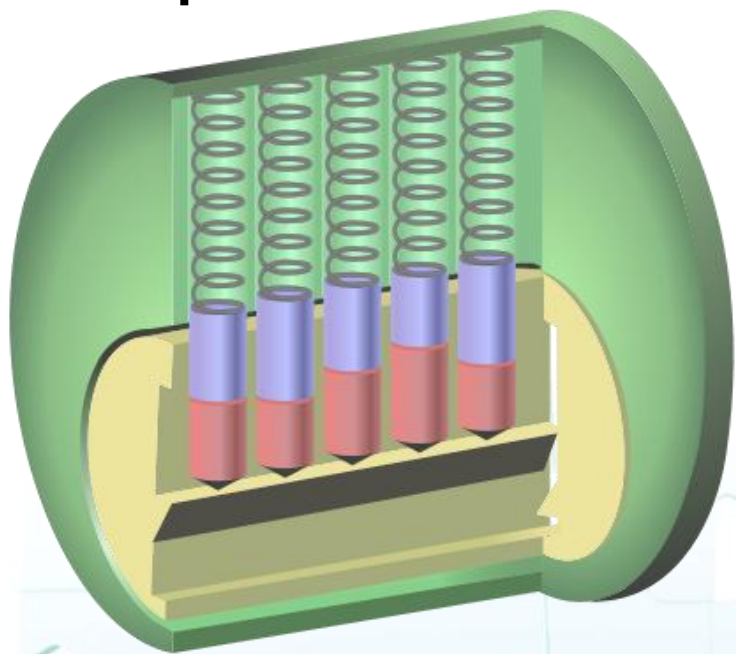


Willy Stöckert  
1916

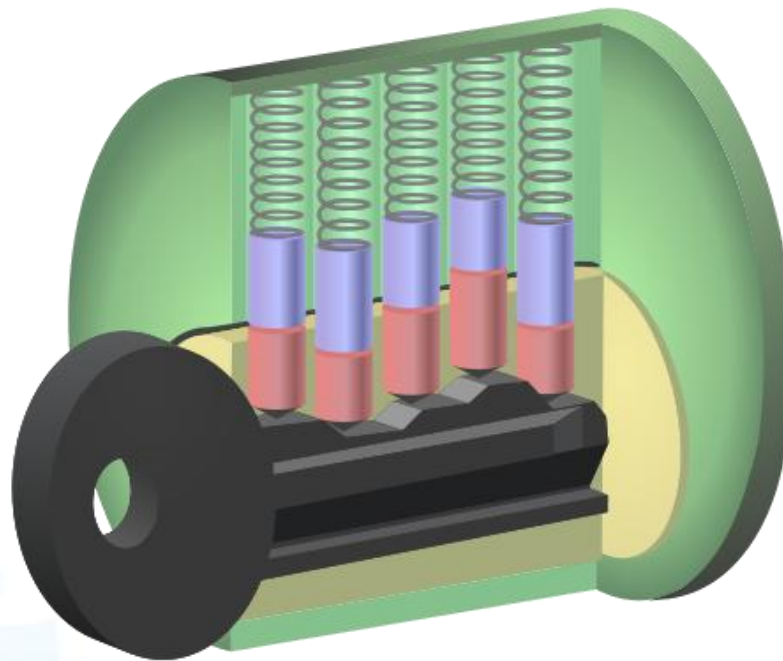
**Osjećate li se sigurni?**



● ● ● | Klasična brava



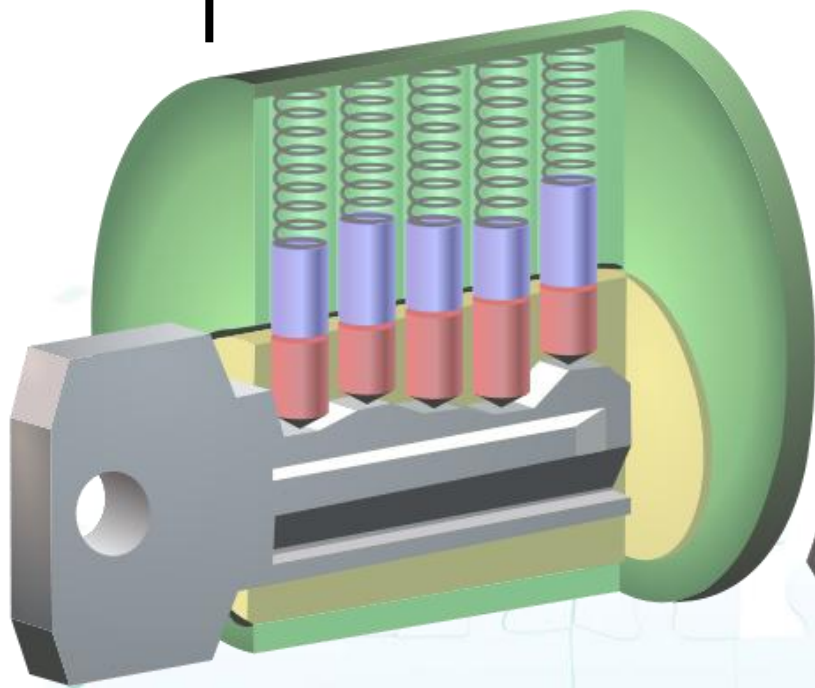
**Brava bez ključa**



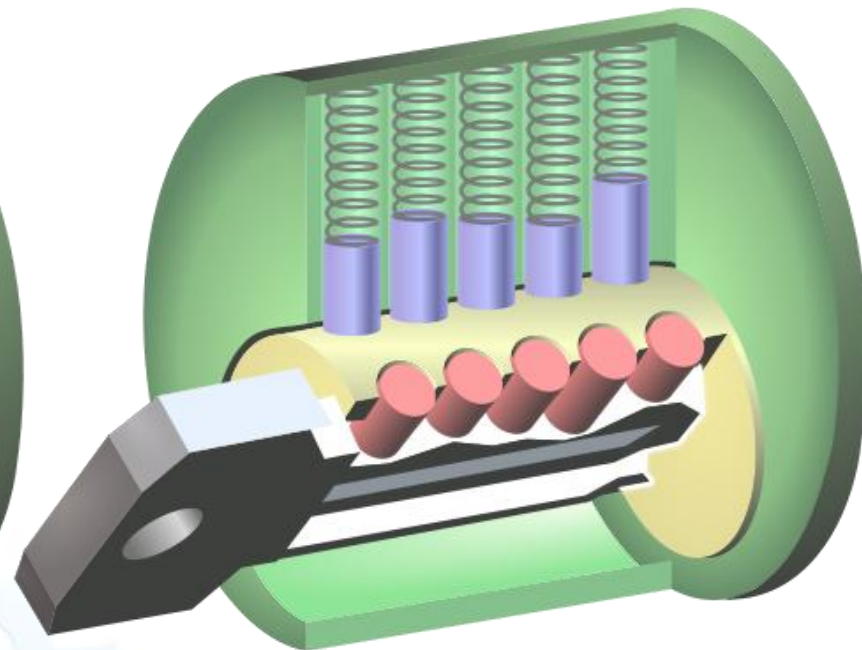
**Brava s pogrešnim ključem**

**CROZ**

● ● ● | **Otvorena brava**



**Brava s  
odgovarajućim  
ključem**



**Otključana brava**

**CROZ**

# Bump key film

**CROZ**





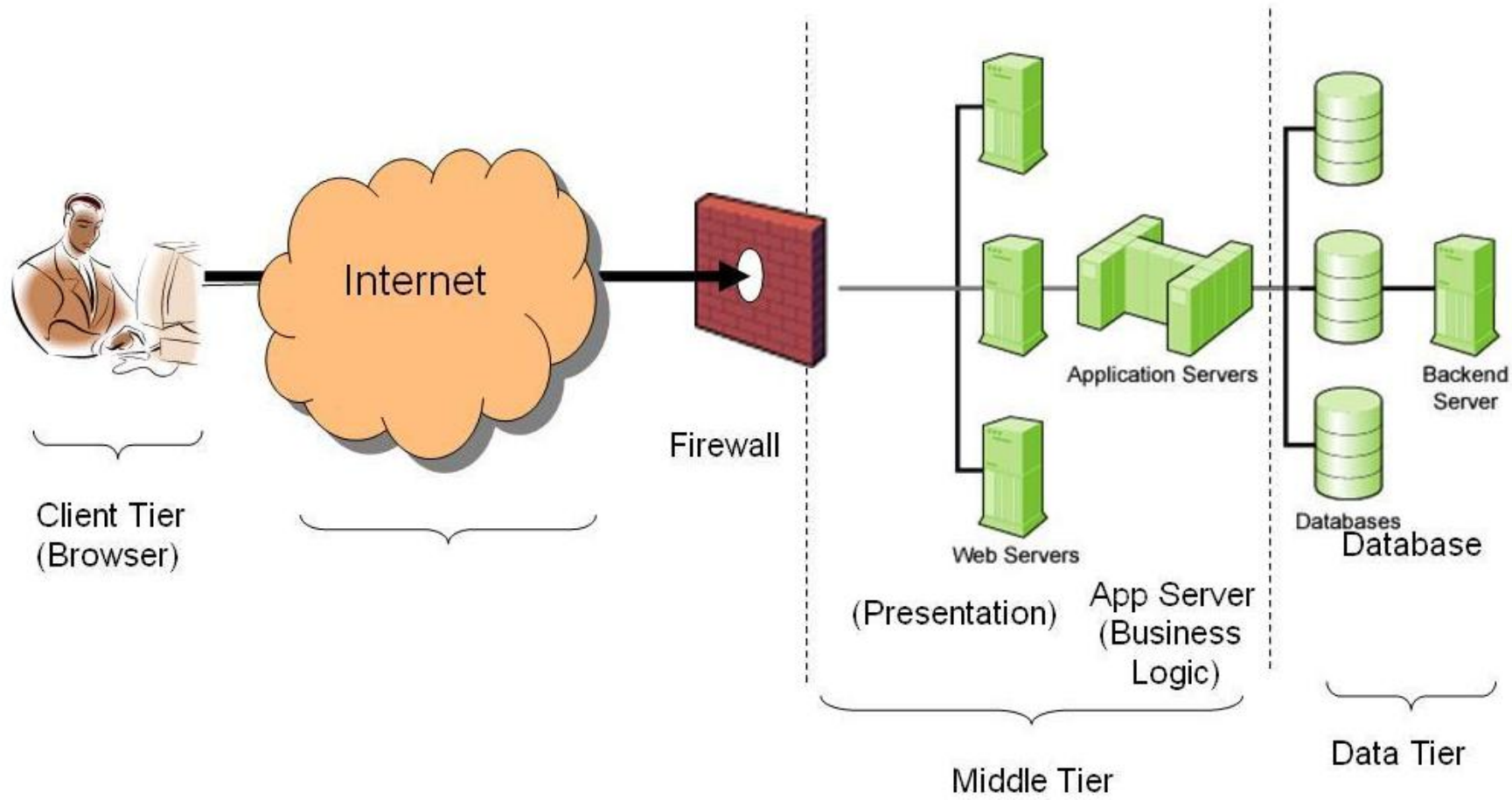
**To know your enemy you  
must become your enemy.**

**Keep your friends close  
and your enemy even  
closer.**

*Sun Tzu, The Art of War*

**CROZ**

# Pregled arhitekture web aplikacija



# Zašto sigurnost web aplikacija mora imati visoki prioritet?

Web aplikacije su prioritet hakerima:

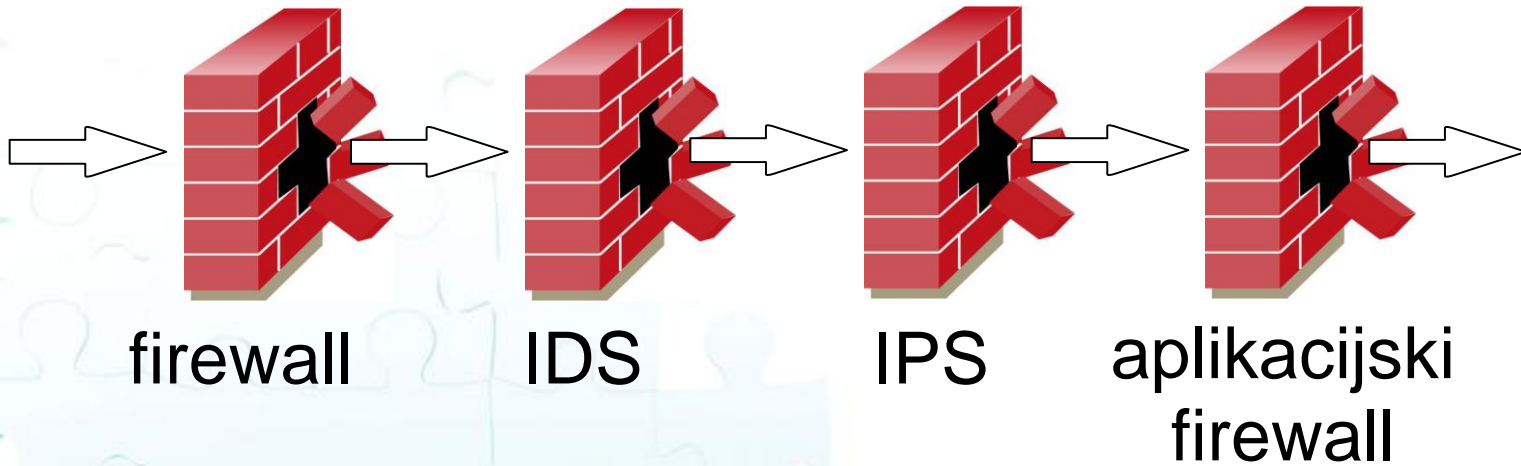
- 75% napada je usmjereno prema aplikacijskom sloju (Gartner)
- XSS i SQL injekcija drže prvo i drugo mjesto na popisu prijavljenih ranjivosti (Mitre)

Većina stranica su ranjive:

- 90% stranica je ranjivo na napade prema aplikacijskom sloju (Watchfire)
- 78% lako zlouporabljivih ranjivosti se odnose na web aplikacije (Symantec)
- 80% organizacija će u periodu od 2006. do 2010. doživjeti sigurnosni incident vezan uz sigurnost web aplikacija (Gartner)

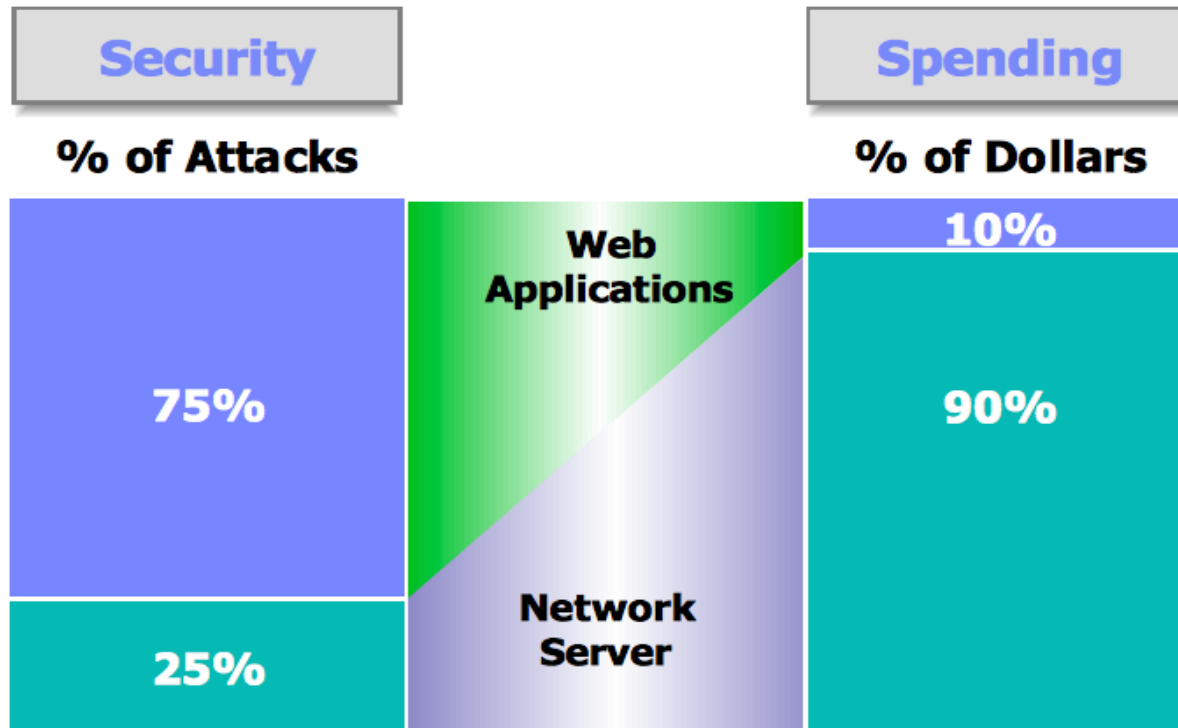
**CROZ**

● ● ● | ...pa imamo zaštitu!



**CROZ**

# Neproporcionalni troškovi za sigurnost



**75%** of All Attacks on Information Security Are Directed to the Web Application Layer

Gartner

# Programeri - zadnja linija obrane



- Kratki rokovi
- Neznanje
- Nedostatak suradnje
- Koga uopće brine sigurnost?

**CROZ**

**Vaše trenutno stanje sigurnosti**



# IBM Rational AppScan

- Detekcija sigurnosnih propusta web aplikacija
- Preporuke za sistemce
- Preporuke za programere
- Izvještaji za management
- Detekcija i otklanjanje sigurnosnih propusta u toku razvoja aplikacija
- Sukladnost standardima

Spoznajte vlastite slabosti prije nego ih netko drugi spozna umjesto Vas!

**CROZ**

# Appscan Vas napada

- "cross-site scripting"
- "HTTP response splitting"
- "parameter tampering"
- manipulacija skrivenim poljima
- backdoor/debug opcije
- "stealth commanding"
- "forceful browsing"
- buffer overflow napadi
- trovanje cookie-a
- pogreške u postavkama
- poznate ranjivosti
- HTTP napadi
- SQL injekcije
- simulacija sumnjivog sadržaja
- XML/SOAP testovi
- "spoof" sadržaja
- Lightweight Directory Access Protocol (LDAP) injekcija
- XPath injekcija
- fiksacija sesije
- ...

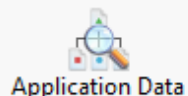
**CROZ**

# Kontinuirani proces

- Ne postoji "čudotvorni lijek"
- Zajednička borba
- Sigurnost pri izradi
- Periodičke provjere



View



- My Application (53)
  - http://demo.testfire.net/ (53)
    - / (3)
      - cgi.exe (1)
      - comment.aspx (2)
      - default.aspx
      - disclaimer.htm
      - feedback.aspx (1)
      - search.aspx (1)
      - servererror.aspx
      - subscribe.aspx (3)
      - subscribe.swf
      - survey\_questions.aspx
    - admin (1)
    - bank (40)
    - images (1)

Scan is Incomplete [More Information](#)

Arranged By: Severity Highest on top  
 53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

Advisory Fix Recommendation Request/Response

Variant: 1 of 2 **Test** Original [Properties](#)

Show in Browser Report False Positive Manual Test Delete Variant Set as Non-vulnerable

```
POST /bank/account.aspx HTTP/1.0
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter
Content-Length: 35
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.testfire.net/bank/main.aspx
```

**listAccounts=0%2B0%2B1001160141%2B0**

```
HTTP/1.1 200 OK
Content-Length: 11744
Connection: close
Date: Thu, 05 Apr 2007 15:03:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
```

Variant Details Screenshot

ID: 9294

**Difference:**

The following changes were applied to the original request:

- Set parameter **listAccounts's** value to **'0%2B0%2B1001160141%2B0'**

**Reasoning:**

This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting test requests show that requests

Enter additional comments for this variant.

View

- Security Issues
- Remediation Tasks
- Application Data

My Application (53)

- http://demo.testfire.net/ (53)
  - / (3)
    - cgi.exe (1)
    - comment.aspx (2)
    - default.aspx
    - disclaimer.htm
    - feedback.aspx (1)
    - search.aspx (1)
    - servererror.aspx
    - subscribe.aspx (3)
    - subscribe.swf
    - survey\_questions.aspx
  - admin (1)
  - bank (40)
  - images (1)

Scan is Incomplete [More Information](#)

- Arranged By: Severity Highest on top
- 53 Security Issues (368 variants) for 'My Application'
- Blind SQL Injection (4)
    - http://demo.testfire.net/bank/account.aspx (1)
    - http://demo.testfire.net/bank/login.aspx (2)
    - http://demo.testfire.net/bank/transaction.aspx (1)
  - Cross-Site Scripting (5)
  - Format String Remote Command Execution (1)
  - HTTP Response Splitting (1)
  - SQL Injection (6)
  - XPath Injection (1)
  - Cookie Poisoning SQL Injection (1)

Advisory Fix Recommendation Request/Response

## Blind SQL Injection

### Fix Recommendation

**General**

There are several issues whose remediation lies in sanitizing user input. By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:

- [1] | (pipe sign)
- [2] & (ampersand sign)
- [3] ; (semicolon sign)

# Primjer izvještaja

## Detailed Findings

Vulnerable URL: <http://fake/fake.aspx>

Total of 2 findings in this URL

### [1 of 2] Cross site scripting

Severity: **High**

Advisory & Fix Recommendation: [See Appendix 1](#)

Vulnerable URL: <http://fake/fake.aspx> (parameter = fake)

Remediation:

**Sanitize user input**

#### Variant 1 of 4 [ID=2416]

This test variant was constructed from the original request by applying the following change(s):

- Set parameter 'uid's value to '>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph10rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/Login.aspx
```

#### Variant 2 of 4 [ID=2418]

This test variant was constructed from the original request by applying the following change(s):

- Set parameter 'uid's value to '>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph10rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/Login.aspx
```

# Što dalje?



- Zatražite besplatno demo testiranje Vaše aplikacije
  - [security@croz.net](mailto:security@croz.net)
- Provedite penetracijsko testiranje i spoznajte vlastite slabosti
  - [www.croz.net/security](http://www.croz.net/security)

**CROZ**