



Ochrana webových aplikací v praxi

Ing. Ján Odzgan

Mobil: 0905767951 | E-mail: jan.odzgan@lynx.sk



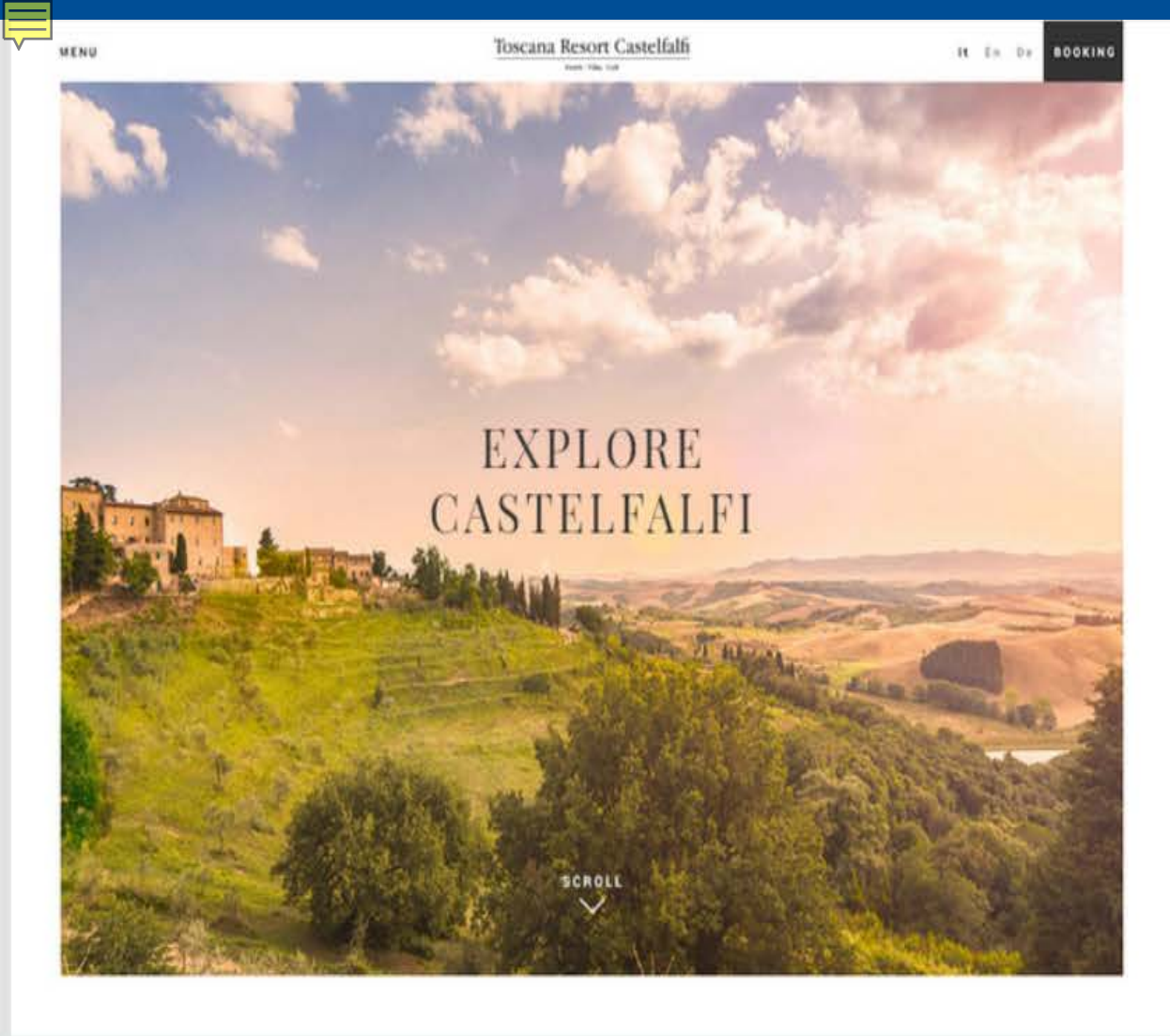
I. Prečo by som mal riešiť webovú
bezpečnosť?

II. Aké prostriedky použiť?

III. Bude mi to vôbec stačiť?



I. Prečo by som mal riešiť webovú bezpečnosť?



Toscana Resort Castelfalfi ⚡

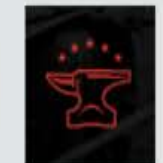
By Luca Fasoli (Italy) Salvatore Spinnato

17 ❤️



03 DAYS 04 HOURS 18 MINS 28 SECS

VOTE NOW!



54 user votes

Evaluation System [Read more](#)

Castelfalfi is an enchanting and evocative place offering hospitality and good cuisine. The website shows hotels, villas, many beautiful apartments, a prestigious golf course and excellent restaurants. All it surrounded by nature and timeless landscapes.

Business & Corporate

Hotel / Restaurant

Clean

CSS3

HTML5

Minimal

Responsive Design

Scroll





Leor

Intro

Services

References

About

Contact

We are the beasts
in web developmen

Our websites and e-shops
are your path to success.



Leor - creative agency ⚡

By Leor (Czech Republic)

21



DESIGN



USABILITY



CREATIVITY



CONTENT



AVERAGE

04 16 44 10
DAYS HOURS MINS SECS

VOTE NOW!



65 user votes

Evaluation System [Read more](#)

We create authentic and lovely websites.

Design Agencies

Web & Interactive

Animation

CSS3

HTML5

jQuery

Responsive Design

SVG







Name

Jan Odzgan

E-mail

jan.odzgan@lynx.sk

Phone

Message

I'm interested by your design. I'd want you
to create my own web site.

Kontakty

Prevádzka Košice:

Recepcia: 7.30 hod - 17.00 hod

Adresa:

Gavlovičova 9, 040 17 Košice

Telefón: +421 55 727 17 17

Fax: +421 55 728 85 55

E-mail: lynx@lynx.sk

GPS: N: 48°40'48" E: 21°16'8"



Prevádzka Bratislava:

Adresa:

Jelačičova 8, 821 08 Bratislava

Telefón: +421 2 501 065 11

Fax: +421 2 501 065 14

E-mail: lynxba@lynx.sk

GPS: N: 48°09'17" E: 17°07'44"



V TEJTO SEKCI

Kontaktné údaje

Fakturačné údaje

MOHLO BY VÁS ZAUJÍMAŤ

Výročná správa

Vízia a poslanie spoločnosti

Tlačové správy

Kariéra

Referencie

ZAUJÍMAVOSTI

Globálne riziká a ich dopady

Integrácia systémov SAP a KLIS

MIDS pre dátové centrum

Vyhľadávanie

OK

Celkovo zverejnených **1124551** zmlúv[Rozšírené vyhľadávanie](#)[Domov](#)[Zmluvy](#)[O stránke](#)[FAQ](#)[Kontakt](#)[Užívateľská zóna](#)

Dodávateľ:

Názov zmluvy:

IČO dodávateľa:

Cena v € s DPH od:

do:

Zverejnené od:

26

do:

26

Rezort:

Objednávateľ:

Číslo zmluvy:

IČO odberateľa:

Vyhľadať

Web Services

14.03.2012

V [technickej zóne](#) je k dispozícii špecifikácia pre **Web Services**.

Informácia o nasadení WS na CRZ bude zverejnená v [Novinách a oznamoch](#).



Vybrané vlastnosti web aplikácií

- jednoduchá, ale stála dostupnosť
- lacné zriadenie a prevádzka
- nutnosť klientskej interakcie a prezentácie
- identifikácia klienta
- komunikácia s partnermi a zdieľanie informácií

HACKER FOR HIRE

URL should be HACKHARHOAM3YK5Q.ONION

Hacking

- Have you been hacked?
- Do you want to find out if your website, computer or network can be or has been hacked?
- Would you like to hack into a computer, website or network?

Social Media Threats

Rent-A-Hacker

Products FAQs Register Login

Rent-A-Hacker

Experienced hacker offering his services!
(Legal) Hacking and social engineering is my business since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +- 20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Recent prices from the black market

		1BTC	213,200 EUR
N	SERVICES	BTC	EUR
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60

N	SERVICES	BTC	EUR
1	Start your own maket	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44

TYPE	KIT	BTC	EUR
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40

TYPE	EXPLOIT	BTC	EUR
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
0day	Internet Explorer <= 11	35,00	7.462,00
0day	Android WebView 0day RCE	36,50	7.781,80
0day	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40

Hrozby spojené s webovými aplikáciami

- získanie detailov o firme
- riziko poškodenia reputácie (zmena obsahu, prezentácia údajov)
- finančné poškodenie (napr. zmena fakturačných údajov)
- odcudzenie údajov v údajových štruktúrach (napr. osobné údaje, finančné údaje)
- odstránenie údajov
- zmena (nesprávnosť) údajov
- zdroj ďalších útokov (Vaše systémy sú považované za útočníkov)



Here's the Top 10 Website Defacers as of January 2016:

1. **GHoST61**: 51
2. **Kadimoun**: 39
3. **AnonCoders**: 35
4. **root-x**: 31
5. **Shor7cut**: 28
6. **Owner Dzz**: 27
7. **Toxic Phantom FROM BANGLADESH BLACK HAT HACKERS**: 27
8. **TechnicalL**: 21
9. **virus3033**: 21
10. **Yuba**: 17

List of Hacking Websites:

1. **Cybrary – Free Cyber Security Training**
URL: <http://www.cybrary.it>
2. **Hak5 – New Hacks Every Week**
URL: <https://hak5.org>
3. **Tinkernut**
URL: <http://www.tinkernut.com>
4. **Cyberpunk**
URL: <http://nowhere.net>
5. **Exploit Database**
URL: <http://www.exploit-db.com>
6. **Darknet**
URL: <http://www.darknet.org.uk>
7. **HackADay – Fresh hack everyday**
URL: <http://hackaday.com>
8. **Evil Zone – Hacking Community**
URL: <https://evilzone.org>
9. **Hack this Site**
URL: <https://www.hackthissite.org>
10. **Cellphone Hacks Forum**
URL: <http://www.cellphonehacks.com>
11. **HackSociety – Grey Hat Hacking Forrum**
URL: <http://hacksociety.net>
12. **HackForums – Hacks & Exploits**
URL: <http://www.hackforums.net>
13. **SecuriTeam – Vulnerabilities information**
URL: <http://www.securiteam.com>



95% web aplikací má nějakú chybu

Hacked!!!

78% web aplikací má zneužitelnú slabinu

The image shows a hand holding a pen, pointing at a computer screen. The screen displays a web browser window with the address bar showing "http://test.test/web.app". The main content area shows an XML document with the following structure:

```

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-
  <s:Header>
  </s:Header>
  <s:Body>
    <Message>
      <Authentication>
        <username>Admin</username>
        <password>supertajneheslo</password>
      </Authentication>
      <NewItems>
        <Item>
          <Name>SSH shell</Name>
          <Price>10 eur</Price>
        </Item>
      </NewItems>
    </Message>
  </s:Body>
</s:Envelope>
  
```

The XML document is displayed in a web browser window. The address bar shows the URL "http://test.test/web.app". The XML content is shown in a structured, color-coded format. The background of the image is a green screen with white text and binary code, suggesting a technical or programming context.

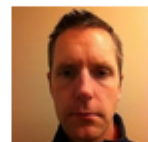
New Year, New Problems: CMS Vulnerabilities Take on 2016

BY DOUGLAS BONDERUD • JANUARY 11, 2016

Another day, another critical vulnerability. That's the life cycle of content management systems (CMS) WordPress and Drupal — just over a week into the new year, and already big problems have been found in both popular tools. As noted by [SecurityWeek](#), WordPress 4.4.1 patches a worrisome cross-site scripting (XSS) issue, while problems with the [update manager in Drupal 7 and 8](#) remain at large. Here's a rundown of 2016's first content management flaws.

Big Fix, Limited Data

According to [US-CERT](#), it's a good idea for users to patch version 4.4 of WordPress up to 4.4.1 since all earlier versions are subject to a XSS vulnerability that could give remote attackers total website control. The flaw was reported to parent company Automattic via a Philippines-based security researcher known only as Crtc4L. Obviously the problem was serious enough to warrant action since Automattic quickly rolled out its first update for version 4.4 and paid out an undisclosed sum to Crtc4L.



**Douglas
Bonderud**

Freelance Writer

A freelance writer for three years, Doug Bonderud is a Western Canadian with expertise in the fields of technology and innovation. In addition to working for the IBM Midsize...

[SEE ALL POSTS](#)

I. Prečo by som mal riešiť webovú bezpečnosť?



I. Prečo by som mal riešiť webovú bezpečnosť?

II. Aké prostriedky použiť?

III. Bude mi to vôbec stačiť?



II. Aké prostriedky použiť?

A1-Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2-Broken Authentication and Session Management**A3-Cross-Site Scripting (XSS)**

XSS flaws occur when a web application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web pages, and redirect the user to malicious sites.

A4-Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

A5-Insecure Configuration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, and defaults should be disabled. Additionally, software should be kept up to date.

A6-Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, and special precautions when exchanging data with the browser.

A7-Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

A8-Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A9-Using Components



Hrozby

- SQL Injection
 - `http://www.example.com/index.php?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1`
- Cross Site Scripting
 - `<SCRIPT type="text/javascript">`
 - `var adr = '../evil.php?cakemonster=' + escape(document.cookie);`
 - `</SCRIPT>`
- CSRF
- XPath injection
- XML poisoning
- chyby v spracovaní autentizácie a session
- nebezpečné odkazy na interné časti riešenia
- odkazy na nebezpečné externé servery

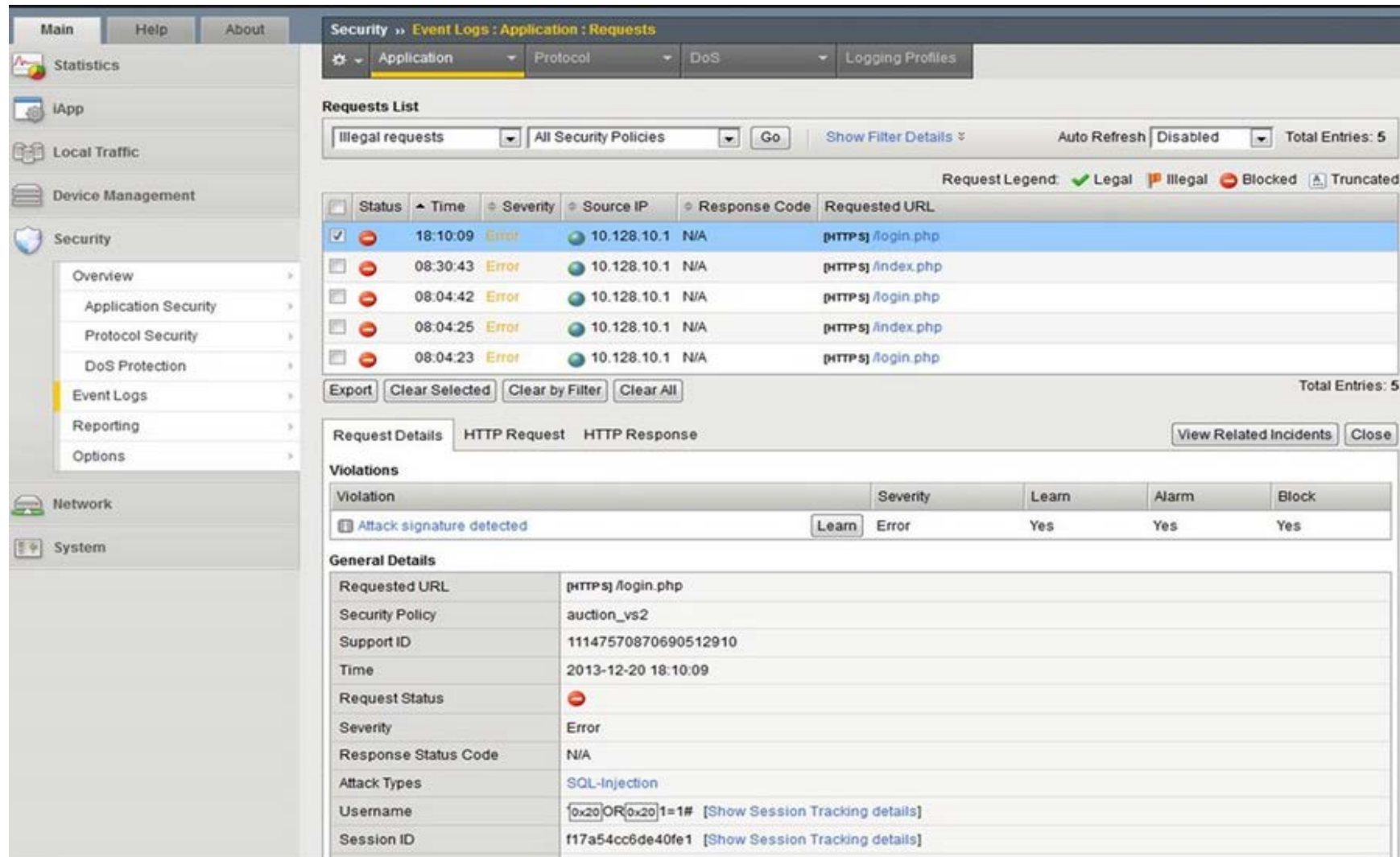
Web application firewall (WAF)

https://www.owasp.org/index.php/Web_Application_Firewall



Web application firewall (WAF)

https://www.owasp.org/index.php/Web_Application_Firewall



The screenshot displays a WAF management console with a sidebar on the left containing links to Main, Help, About, Statistics, iApp, Local Traffic, Device Management, Security, Network, and System. The Security section is expanded, showing Overview, Application Security, Protocol Security, DoS Protection, Event Logs, Reporting, and Options. The main panel is titled 'Security » Event Logs : Application : Requests' and features a 'Requests List' table. The table has columns for Status, Time, Severity, Source IP, Response Code, and Requested URL. It shows five entries, all marked as 'Error' with a red status icon. The first entry is selected, and its details are shown in the 'Request Details' section below. The 'Violations' section shows a single violation: 'Attack signature detected' with a severity of 'Error' and actions for 'Learn', 'Alarm', and 'Block' all set to 'Yes'. The 'General Details' section provides further information about the request, including the URL, security policy, support ID, time, request status, severity, response status code, attack types (SQL-Injection), username, and session ID.

Status	Time	Severity	Source IP	Response Code	Requested URL
☒	18:10:09	Error	10.128.10.1	N/A	[HTTPS] /login.php
☐	08:30:43	Error	10.128.10.1	N/A	[HTTPS] /index.php
☐	08:04:42	Error	10.128.10.1	N/A	[HTTPS] /login.php
☐	08:04:25	Error	10.128.10.1	N/A	[HTTPS] /index.php
☐	08:04:23	Error	10.128.10.1	N/A	[HTTPS] /login.php

Violation	Severity	Learn	Alarm	Block
Attack signature detected	Error	Yes	Yes	Yes

General Details	
Requested URL	[HTTPS] /login.php
Security Policy	auction_vs2
Support ID	11147570870690512910
Time	2013-12-20 18:10:09
Request Status	
Severity	Error
Response Status Code	N/A
Attack Types	SQL-Injection
Username	{0x20}OR{0x20}1=1# [Show Session Tracking details]
Session ID	f17a54cc6de40fe1 [Show Session Tracking details]



Web application firewall (WAF) – vlastnosti/výhody

- niekoľko možností implementácie, často bez nutnosti zmeny aplikácie, stačí sieťovo predradiť
- poskytuje funkcionality LB
- podporuje tzv. virtual patch (virtuálna oprava)
- poskytuje dodatočnú bezpečnostnú vrstvu pre existujúce aplikácie
 - doplnenie autentizácie, šifrovanie na úrovni protokolu, atď.
- oboznámenie sa s detailom o fungovaní chránenej aplikácie (poskytnutie ako podkladu)
- ochrana pred známymi aj neznámymi hrozbami
 - využitím signatúr (podobne ako známe systémy IPS)
 - s naučeným profilom používania aplikácie
- významná koordinácia činností pri aktualizácii webovej aplikácie



Web application firewall (WAF) – nevýhody/nedostatky

- zložitosť jazyka môže virtual patch výrazne obmedzovať
- pocit falošnej bezpečnosti
- nie je nutné opravovať aplikáciu
- ide o bezpečnostný produkt, ale rovnako môže mať chyby
- obmedzenie na podporované technológie
- false positive pri signatúrach





Web application firewall (WAF) – poznatky z praxe

- chýbajú informácie o fungovaní aplikácie
- názor, že už samotný komponent je dostatočný na realizáciu bezpečnosti web aplikácie
- nepripravenosť na prevádzku
 - personálne obsadenie
 - odborné skúsenosti
- chýbajúci budget pre zmeny samotnej web aplikácie



Service Gateway (SOA firewall)

POST web.app HTTP/1.1

HTTP/1.1 200 OK

Content-Type: application/soap+xml

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
  </s:Header>
  <s:Body>
    <Message>
      <Authentication>
        <username>Admin</username>
        <password>supertajneheslo</password>
      </Authentication>
      <NewItem>
        <Item>
          <Name>SSH shell</Name>
          <Price>10 eur</Price>
        </Item>
      </NewItem>
    </Message>
  </s:Body>
</s:Envelope>
```

GET /articles?include=author HTTP/1.1X

HTTP/1.1 200 OK

Content-Type: application/vnd.api+json

```
{
  "data": [{
    "type": "articles",
    "id": "1",
    "attributes": {
      "title": "JSON API paints my bikeshed!", "body": "The shortest article. Ever.", "created": "2015-05-22T14:56:29.000Z", "updated": "2015-05-22T14:56:28.000Z"
    },
    "relationships": {
      "author": {
        "data": {"id": "42", "type": "people"}
      }
    }
  }],
  "included": [
    {
      "type": "people",
      "id": "42", "attributes": {
        "name": "John",
        "age": 80,
        "gender": "male"
      }
    }
  ]
}
```



Service Gateway (SOA firewall)

DataPower Gateway admin @ 192.168.150.10:9090

Control Panel
Blueprint Console

Search

Multi-Protocol Gateway status: [up]

General Configuration

Multi-Protocol Gateway Name: mpg-ssltest

Summary

Type
☐ dynamic-backends
☒ static-backend

Back side settings

Default Backend URL: http://dummy

MQ Helper WebSphere JMS Helper IMSConnect Helper

User Agent settings

Configure Multi-Protocol Gateway Style Policy

Policy:
Policy Name: mpg-policy-ssltest

Rule:
Rule Name: mpg-policy-ssltest_rule_0 Rule Direction: Both Directions

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Filter Sign Verify Validate Encrypt Decrypt Transform Route GatewayScript AAA Results Advanced

ORIGIN SERVER CLIENT

Create Reusable Rule

Order	Rule Name	Direction	Actions
1	mpg-policy-ssltest_rule_0	Both Direction	delete rule

mpg-fsh-https-7777 (HTTPS Front Side Handler)
mpg-fsh-https-7775 (HTTPS Front Side Handler)
mpg-fsh-https-7776 (HTTPS Front Side Handler)
mpg-fsh-https-7778 (HTTPS Front Side Handler)

+ ... Add



Service Gateway (SOA firewall) – vlastnosti/výhody

- podporuje tzv. virtual patch (virtuálna oprava)
- dokáže "odbremeniť" cieľovú platformu na spracovanie vybraných vstupov (transformácie)
- poskytuje dodatočnú bezpečnostnú vrstvu pre existujúce aplikácie
 - doplnenie autentizácie, šifrovanie na úrovni protokolu alebo samotnej správy (SOAP)
- identifikuje hrozby pre XML štruktúry
- zabezpečí oboznámenie sa s detailom o fungovaní chránenej aplikácie
- významná koordinácia činností pri aktualizácii webovej aplikácie (niekto to môže vnímať ako nevýhodu)



Service Gateway (SOA firewall) – nevýhody/nedostatky

- znalosť jazyka, ktorým sa realizuje virtual patch a transformácie
- menšia prehľadnosť pri ladení
- obmedzenie na podporované technológie
- false positive pri SQLi



Service Gateway (SOA firewall) – poznatky z praxe

- chýbajú informácie o fungovaní aplikácie
- nevyužívanie možností samotnej technológie, ktorá je základom aplikácie (schémy)
- využívanie kódov tretích strán bez znalosti o ich fungovaní
- publikovanie citlivých informácií bez realizácie ich ochrany (šifrovanie)
- nedôveryhodné federácie



Sieťové prostriedky/technológie

- Next Generation Firewall
- Network design
 - segmentation





Ešte niečo iné ?



Vývoj a proces nasadenia web aplikácie

- Proces pre vývoj
 - informácie o spôsobe bezpečného programovania
 - kontrola kódu tretích strán
- Nasadenie do prostredia
 - podľa postupu
 - preverenie správnosti
- TESTOVANIE
 - funkčné
 - bezpečnostné
 - penetračné





I. Prečo by som mal riešiť webovú
bezpečnosť?

II. Aké prostriedky použiť?

III. Bude mi to vôbec stačiť?



III. Bude mi to vůbec stačit?

Bezpečnost – proces - komplexnost



Čo ďalšie ?

- bezpečný vývoj a nasadenie aplikácií (SDL) a aplikovanie tohto procesu na subdodávateľov
- správny postup nasadzovania konfiguračných zmien komponentov (technológií) webovej ochrany, rovnako ako sieťovej
 - (napr. dvojité kontrola, testovacie prostredie)
- sledovanie chýb používaných technológií a ich odstraňovanie
- budovanie bezpečnostného povedomia zamestnancov
- TESTOVANIE všetkých častí aplikácie, súčasťou ktorej musia byť aj prvky bezpečnosti





Čo ďalšie ?

- Iné vstupy do organizácie
 - E-mail
 - Dns
 - Manažment !!!
 - VPN, bezpečné protokoly v kombinácii so silnejšou autentizáciou
- Zamestnanci a ich pracovné stanice a servery
 - administrátori, autorizovaní používatelia
 - technológie na ochranu staníc a serverov
 - AntiMalware
 - Šifrovanie
 - White image, sandbox
- Monitorovanie
 - SIEM





Ďakujem za pozornosť

Ing. Ján Odzgan

Mobil: 0905767951 | E-mail: lynx@lynx.sk, jan.odzgan@lynx.sk

LYNX - spoločnosť s ručením obmedzeným Košice

www.lynx.sk



???

