FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Gestão de Vulnerabilidades

Carlos Friaças
ASA / SEG
20-Nov-2018

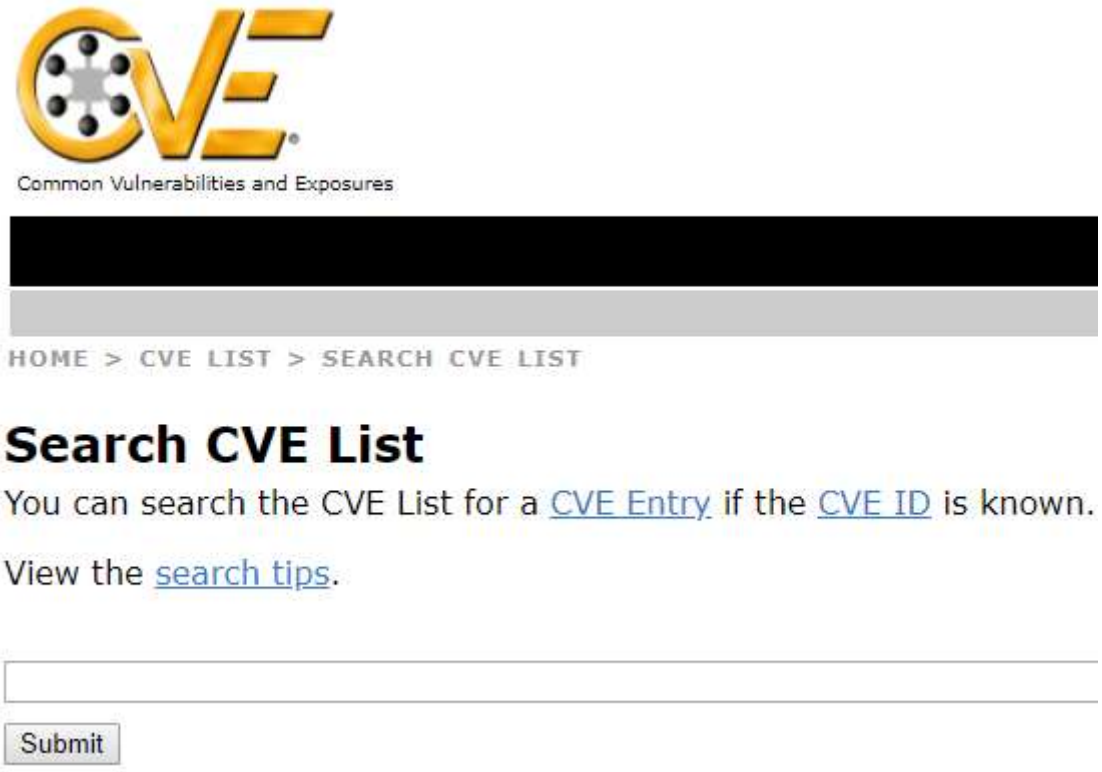
Porta aberta?

- O número de vulnerabilidades conhecidas é imenso
- Todos os dias são descobertas novas vulnerabilidades
- Os serviços web são um target óbvio

Mitre CVEs

- Common Vulnerabilities and Exposures

- Descrição de casos



Mitre CVEs - Exemplo

CVE-ID	
CVE-2018-10969	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

SQL injection vulnerability in the Pie Register plugin before 3.0.10 for WordPress allows remote attackers to execute arbitrary SQL commands via the invitation codes grid.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

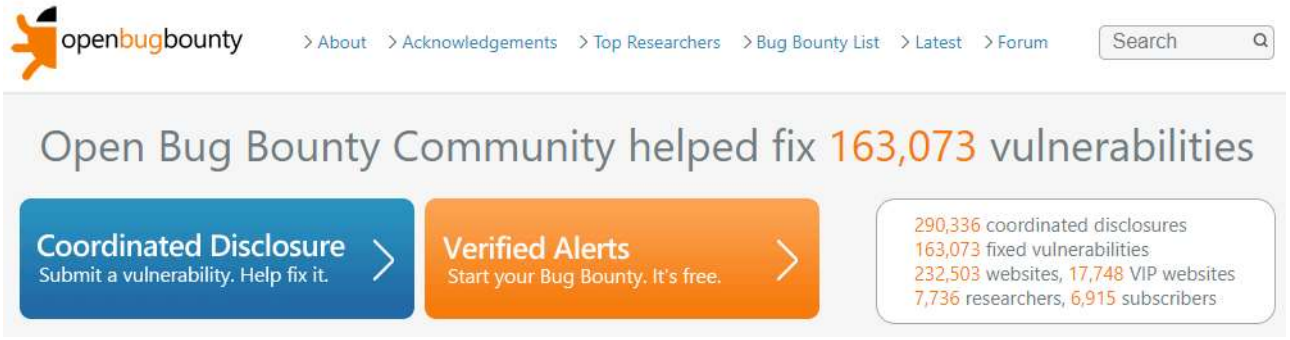
- EXPLOIT-DB:44867
- URL:https://www.exploit-db.com/exploits/44867/
- MISC:https://wordpress.org/plugins/pie-register/#developers

Assigning CNA

MITRE Corporation

«Bounties»

- *Disclosure* responsável
- Permitir ao dono do *asset* a rectificação do problema



«Bounties» - Exemplo

Open Bug Bounty ID: OBB-355996

Security Researcher **c0rtePentest**, a holder of 2 badges for responsible and coordinated disclosure, found a security vulnerability affecting **vodafone.pt** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147** standard, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**vodafone.pt**
Open Bug Bounty Program:	**Create your bounty program now.** It's open and free.
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**c0rtePentest**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
http://www.vodafone.pt/NR/rdonlyres/68463169-A34D-4228-8DB2-D83F684514D0/0/VDF_BannerTV_570x250.swf?ClickTag=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTUE9TRUQnKTwvc2NyaXB0Pg==
```

Research's Comment:

```
Click to trigger XSS
```

Mirror:

Click here to view the mirror

Coordinated Disclosure Timeline

Vulnerability Reported:	21 October, 2017 00:56 GMT
Vulnerability Verified:	23 October, 2017 06:48 GMT
Website Operator Notified:	23 October, 2017 06:48 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Public Report Published [without any technical details]:	23 October, 2017 06:48 GMT
Vulnerability Fixed:	21 December, 2017 10:48 GMT
Public Disclosure:	20 November, 2017 00:56 GMT

Inteligência como fonte

- Recolha de fontes externas, para a RCTS

- Uma semana má…

Relatórios Semanais

- Por instituição/membro da RCTS
- A partir de report@cert.rcts.pt
- Todas as segundas-feiras, às 00:30
- Em formato .CSV
- Quando a instituição não recebe significa que nada foi detectado nas últimas semanas ☺

Nessus – Vulnerability Scanner

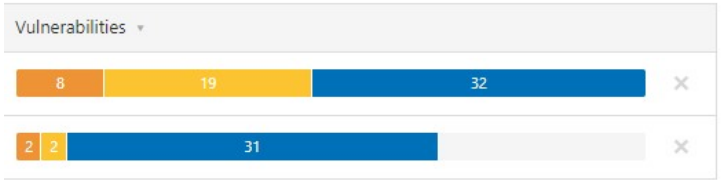
- Adquirida licença no ano passado
- Ferramenta que executa análises em profundidade
- Pode estar 24/7 a analisar diversos websites, de forma automatizada
- Hoje a FCCN analisa ~15 websites semanalmente
- Poderão ser adquiridas mais licenças, se necessário

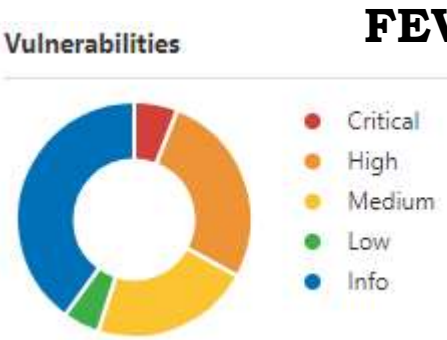
Relatórios

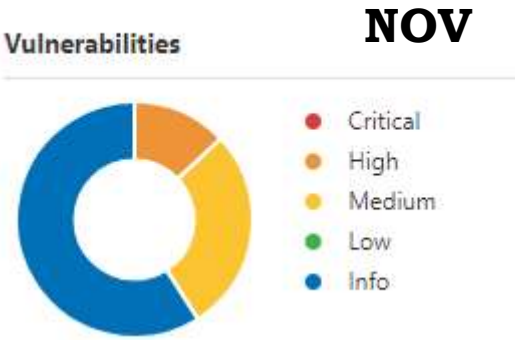
- Classificação por gravidade
- Duração & tipo de testes
- Exemplo de dois *hosts*
- Evolução…

Scan Details

Name:	[redacted]
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Start:	November 15 at 4:00 AM
End:	November 15 at 5:32 AM
Elapsed:	2 hours







Próximos passos?

- Há interesse neste serviço?
- Que/Quantos websites pretendem avaliar?
- Que periodicidade?

Perguntas

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Obrigado pela atenção!

info@cert.rcts.pt