**CENÁRIO CONTROLADO NO CODEIGNITER**

[1] Andiparos – 2 minutos

[2] Nessus – 15 minutos

[3] Ratproxy – 10 minutos

[4] Uniscan – 8 minutos

[5] Wapiti – 2 minutos

[6] Grabber – 2 minutos

[7] Paros proxy – 8 minutos

[8] Skipfish – 5 minutos

[9] Vega – 2 minutos

[10] Zed attack proxy – 6 minutos

TABELA 1 - VULNERABILIDADES DETECTADAS CONFORME RELATÓRIO DE SAÍDA

|  |  |  |
| --- | --- | --- |
| Vulnerabilidades | Ferramentas | Gravidade |
| X-frame-options header not set | [10] | Média |
| X-content-type-options header missing | [10] | Baixa |
| Cookie no httpOnly flag | [6] | Baixa |
| Password autocomplete in browser | [2,7,9] | alta |
| Incorrect or missing MIME type | [8] | Médio |
| External contente embedded on a page | [8] | Médio |
| Http trace support detected (apache 2.4.27) | [1,2,9] | Médio |
| Cleartext Password over http | [2,9] | Alta |
| Directory listing | [4,8,9] | Baixa |
| Directory browsing | [1,7] | Médio |
| Lotus domino default files | [1,7] | Médio |
| Sql injection | [1,4, 7] |  |
| Identificação de versão de tudo (SO, VERSÕES, etc) | [1,2] | Médio |
| Web Browser XSS Protection Not Enabled | [10] | Baixa |
| Signature match detected | [8] | Alto |
| Sql injection fingerprinting | [1,7] | Alta |
| Clickjacking | [2] | Média |

TABELA 2 - VULNERABILIDADES DETECTADAS E SUAS CATEGORIAS

|  |  |  |
| --- | --- | --- |
| Vulnerabilidades | Ferramentas | Categoria top 10 |
| X-frame-options header not set | [10] | Cross site scripting |
| X-content-type-options header missing | [10] | Cross site scripting |
| Web Browser XSS Protection Not Enabled | [6] | Má configuração de segurança - security misconfiguration |
| Cookie no httpOnly flag | [2,7,9] | Cross site scripting |
| Password autocomplete in browser | [8] | Exposição de dados sensíveis - Sensitive data exposure |
| Incorrect or missing MIME type | [8] | Má configuração de segurança - security misconfiguration |
| External content embedded on a page | [1,2,9] | Falso-positivo, era apenas uma outra página do apache |
| Http trace support detected (apache 2.4.27) | [2,9] | Cross site scripting (xss) |
| Cleartext Password over http | [4,8,9] | Exposição de dados sensíveis - Sensitive data exposure |
| Directory listing | [1,7] | Má configuração de segurança - security misconfiguration |
| Directory browsing | [1,7] | Má configuração de segurança - security misconfiguration |
| Lotus domino default files | [1,4, 7] | Apenas um arquivo, nada de vulnerabilidade. Falso-positivo |
| Sql injection | [1,2] | Injeção de código |
| Identificação de versão de tudo (SO, VERSÕES, etc) | [10] | Using components with known vulnerabilities -Usando componentes com vulnerabilidades conhecidas |
| Signature match detected | [8] | Exposição de dados sensíveis e insuficiente ataque de proteção |
| Sql injection fingerprinting | [1,7] | injeção de código |
| Clickjacking | [2] | Cross-Site Request Forgery |

|  |  |
| --- | --- |
| **VULNERABILIDADE TOP 10** | **SCANNERS QUE DETECTARAM** |
| INJEÇÃO DE CÓDIGO | [1,2,7] |
| CROSS SITE SCRIPTING | [2,7,9,10] |
| Quebra de autenticação e gerenciamento de sessão | [] |
| Quebra de controle de acesso - broken access control | [] |
| Má configuração de segurança | [1,6,7,8] |
| Exposição de dados sensíveis | [4,8,9] |
| Cross site requesty forgery (CSRF) | [2] |
| Insufficient attack protection | [8] |
| Using components with known vulnerabilities | [2] |
| APIs desprotegidas | [] |