Relatório referente ao teste de intrusão executado do dia 12/04 a 28/04 de 2021.

Relatorio Pentest

SrAl1ss0n Pentesting Ltda

SrAl1ss0n.com.br

TryHackMe

tryhackme.com

2021

Termo de Responsabilidade

Este relatório é inteiramente fictício e tem como propósito servir como um estudo prático de Ethical Hacking, visando simular uma consultoria de Pentest representado por "SrAl1ss0n Pentesting Ltda" (entusiasta de segurança da informação) e tendo como contratante "Ben Spring" (Co-Fundador do TryHackme e criador dos ambientes vulneráveis descritos nesse documento)

Essa atividade foi proposta durante as aulas da 1ª turma de Ethical Hacking do bootcamp da **Uniciv** em 2021 ministrado pelo professor **Victor de Queiroz**, e todos os testes executados foram realizados em escopos controlados e com vulnerabilidades propositais providos por TryHackMe.com disponível em https://tryhackme.com/room/owasptop10.

Declaramos por meio desse documento que nenhum dos ambientes testados e documentados são reais, e tem como objetivo ensinar estudantes de segurança informação a encontrar falhas em ambientes web.

Contratante:

Ben Spring

TryHackMe Co-founder
Room Creator

Indice

Relatório Executivo

04 Sumário Executivo & Escopo dos testes

05 Resultados Simplificados

06 Recomendações executivas

Relatório Técnico

08 PT01: Execução de comandos exposta

09 PT02: Invasão do sistema através de falhas conhecida.

10 PT03: Invasão do servidor & Exposição de dados sensíveis.

11 PT04: Leitura de arquivos sigilosos

12 PT05: Quebra de autenticação

13 PT06: Banco de dados de senhas exposto na internet

14 PT07: Leitura não autenticada de anotações de usuários

15 PT08: Uso de senha padrão na aplicação.

16 PT09: Inserção de códigos maliciosos na aplicação web.

17 Material de Apoio

18 Material de Apoio

19 Metodologias && Ferramentas utilizadas

Sumário executivo

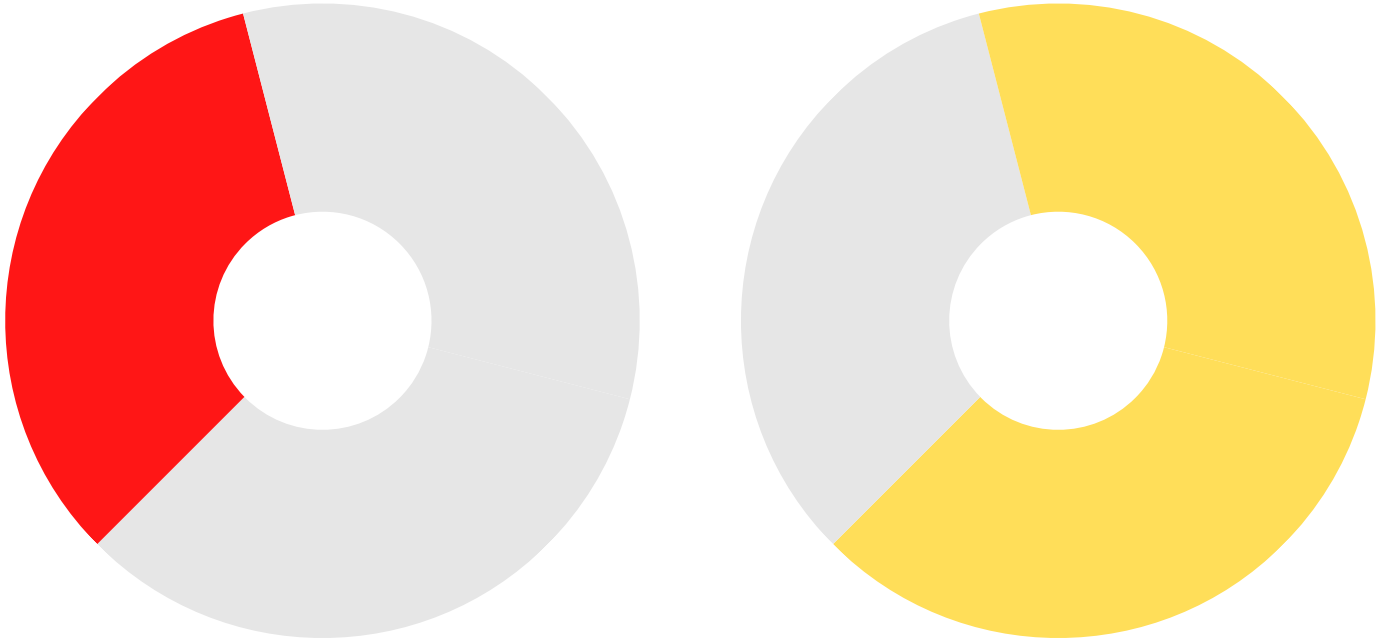
Após às 13:00 do dia 12/04/2021 foi iniciado os testes de intrusão nos ambientes cibernéticos da empresa TryHackMe tendo como acordo total permissão para que a empresa SrAl1ss0n Ltda simule ataques cibernéticos em seu escopo de 09 máquinas até as 00:00h do dia 24/04/2021

Escopo

- 10.10.169.55
- 10.10.121.2
- 10.10.127.189
- 10.10.88.227
- 10.10.31.184
- 10.10.251.57
- 10.10.36.35
- 10.10.76.249
- 10.10.130.80

Resultado Simplificado

Após os testes de invasão cibernética foram encontradas encontradas 9 vulnerabilidades dentro da estrutura do ambiente cibernético acordado anteriormente, deles tendo um total de **3** vulnerabilidades **críticas**, 6 vulnerabilidades **altas**.



Legendas

Falhas Críticas:

Foram consideradas **Vulnerabilidades Críticas** toda e qualquer falha que dê acesso ao sistema do servidor e que por consequência permita o controle total ou parcial do próprio.

Falhas Altas:

Foram consideradas **Vulnerabilidades Altas** toda e qualquer falha que dê acesso a informações sensíveis ou até mesmo acesso não autorizado a alguma aplicação.

Recomendações Executivas

Será necessário realizar a contratação de recursos tecnológicos para a proteção do ambientes

Devido à criticidade das vulnerabilidades encontradas e exploradas, recomendamos que uma equipe interna de resposta a incidentes, ou perícia forense, analise os ambientes explorados com a finalidade de evidenciar possíveis comprometimentos durante o período de exposição dos ambientes anterior aos testes de intrusão.

Relatório Técnico

PT01: Execução de comandos exposta.

Severidade: Crítico

Host: 10.10.169.55

Após a realização do processo de reconhecimento na aplicação web, foi possível encontrar um vetor de execução de comandos, tornando possível a invasão parcial ou completa do sistema.

FIG01: evidencia de comandos sendo executados em: http:10.10.169.55/evilshell

Impacto:

Com a possibilidade de executar comandos no servidor da empresa é possível ter controle total ou parcial do sistema do mesmo, ter acesso a arquivos sigilosos, configurações e até mesmo possibilitando outros ataques, como deface, vazamento de dados e etc.

Correções / Mitigações:

Recomendamos que implemente um método de autenticação para acessar a página de execução de comandos para que apenas administradores tenham acesso à função, se possível a remoção da mesma, combinada com a implementação do uso do serviço SSH corretamente.

PT02: Invasão do sistema através de falhas conhecida.

Severidade: Crítico Host: 10.10.130.80

Após a realização do processo de reconhecimento na aplicação web, foi possível encontrar exploits funcionais para a tecnologia utilizada no web-site Book Store 1.0

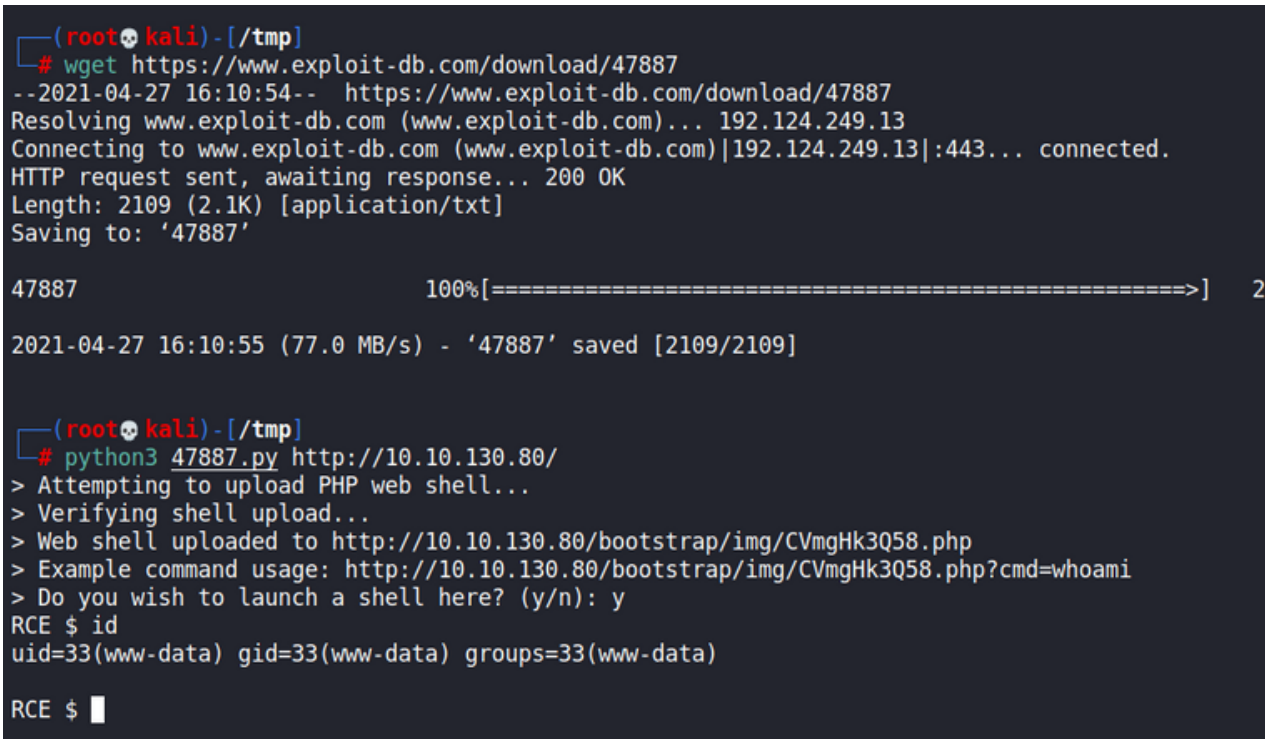


FIG02: evidencia da execução do exploit que gerou a possibilidade de executar comandos no servidor

Impacto:

Com a possibilidade de executar comandos no servidor é possível ter controle total ou parcial do sistema do servidor da empresa, ter acesso a arquivos sigilosos, configurações e até mesmo possibilitando outros ataques, como deface, vazamento de dados e etc.

Correções / Mitigações:

Recomendamos que realize atualizações na tecnologia Book Store 1.0, será necessário a implementação de WAF, Firewall, SIEM, para protegerem o servidor da empresa.

PT03: Invasão do servidor & Exposição de dados sensíveis.

Severidade: Critico Host: 10.10.76.249

Foi possível decodificar os dados passados através dos cookies da web aplicação, permitindo a leitura de dados sigilosos como a senha dos usuários, e realizar a modificação dos dados como por exemplo o parâmetro userType podendo modificar as permissões do usuário permitindo acesso administrativo, e o mais importante o parâmetro encodedePayload possibilitou executar comandos no servidor.

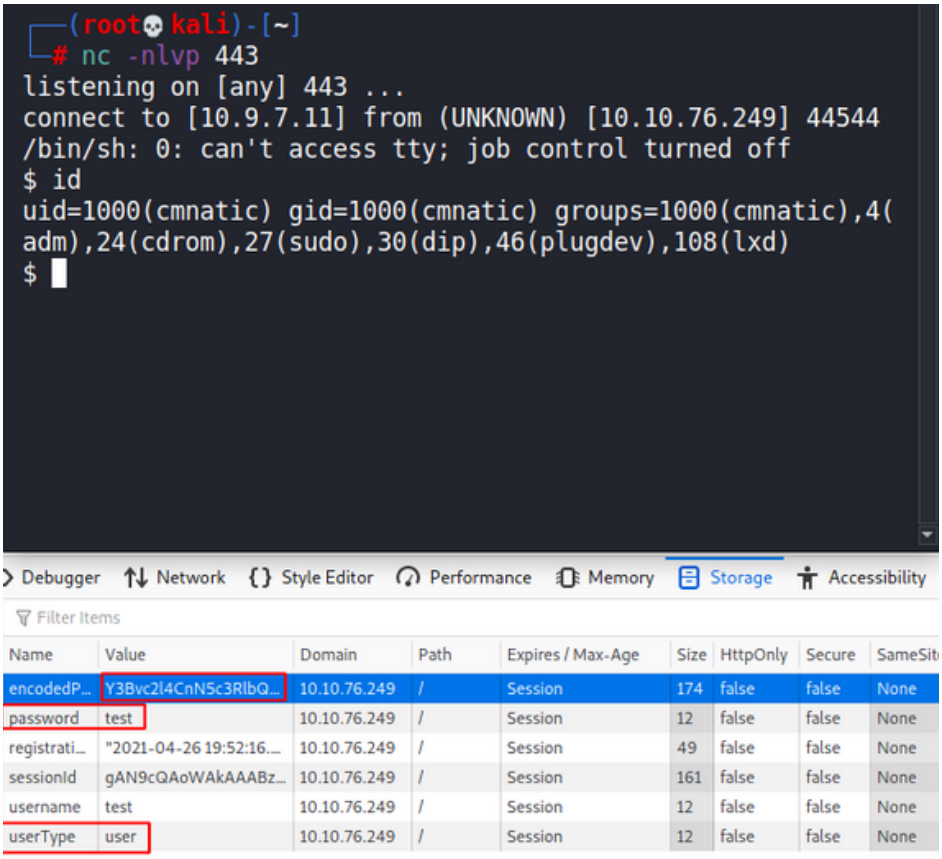


FIG03: evidencia de dados exposto && execução de comandos

Impacto:

Com essas falhas um invasor pode ter acesso administrativo da página web, vazar dados de usuários, executar ataques de Man-in-The-Midle para ter acesso a contas, e ter controle total ou parcial do servidor através do comandos.

Correções / Mitigações:

É recomendado a utilização de um método criptográfico mais forte no campo de cookies, desabilitar a modificação de cookies por parte do cliente, realizar um codeoverview para que a execução de comandos nos cookies sejam desabilitada.

PT04: Leitura de arquivos sigilosos da empresa e servidor.

Severidade: Alta

Host: 10.10.88.227

Foi encontrada uma falha de XXE, com a possibilidade de inserção e execução de XML no servidor o que permitiu a leitura de arquivos sigilosos de sistema do servidor e da empresa.

FIG04: evidencia de dados exposto através de XXE

Impacto:

Com essas falhas há a possibilidade de ler arquivos sigilosos do sistema/servidor, o que acarreta em uma quebra de confidencialidade da empresa, tendo a habilidade de leitura no servidor é possível acessar arquivos de configurações.

Isso habilita um atacante executar outros ataques, podendo até mesmo invadir o sistema, vazar dados e etc.

Correções / Mitigações:

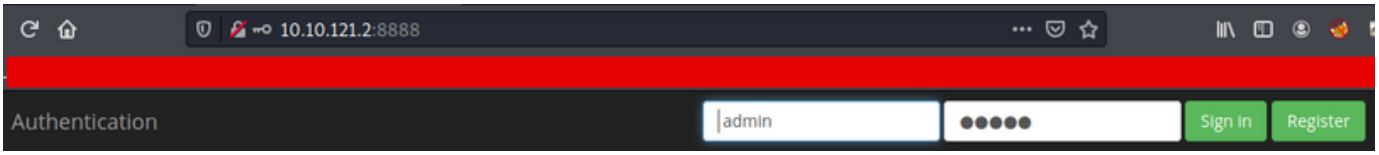
É recomendado desabilitar a execução de códigos XML, implementação de um WAF com regras para que códigos maliciosos sejam bloqueados , ou se for necessário a execução de códigos XML seria recomendado que os códigos fossem executados em um servidor com menos privilégios .

PT05: Quebra de controle de autenticação

Severidade: Alta

Host: 10.10.121.2

Após a criação de um usuário com um espaço antes do nome foi possível ter acesso a conta do usuário com o mesmo nome utilizando a senha do usuário criado.



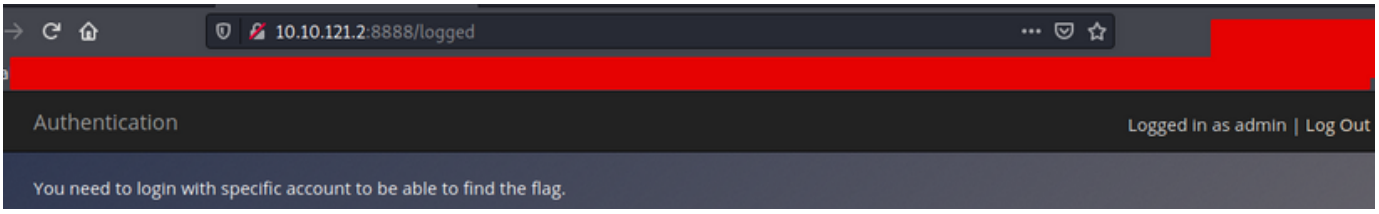


FIG05,06,07: criação de usuário e login na conta do alvo

Impacto:

Com essas falhas se fez possível ter acesso total a área administrativa da web aplicação e também ter acesso a qualquer conta de qualquer usuário.

Correções / Mitigações:

É recomendado realizar um codeoverview na área de criação e login de usuário tanto no banco de dados quanto na programação da aplicação web.

PT06: Banco de dados de senhas exposto na internet

Severidade: Alta Host: 10.10.127.189

Após o processo de reconhecimento foi possível encontrar o banco de dados da aplicação armazenado de forma exposta à internet, habilitando a quebra de hashs o que viabilizou a obtenção de todas as senhas.

FIG 08,09,10: localização do banco de dados e quebra dos hashs

Impacto:

Com essas falhas se fez possível ter acesso a todas as senhas de todos os usuários da aplicação web, quebrando não só a confidencialidade da aplicação quanto a integridade da aplicação

Correções / Mitigações:

É recomendado que desabilite a função index off do serviço apache2, utilizar métodos de criptografia mais forte como DES, AES, RSA, solicitar mudança de senha de todos os usuários da aplicação, pois podem ter tido suas senhas vazadas.

PT07: Leitura não autenticada de anotações de usuários

Severidade: Alta

Host: 10.10.31.184

Após a modificação do parametro "?note=" nas requisições se fez capaz a leitura das anotações de todos os usuários de forma não legítima, quebrando a confidencialidade da aplicação.

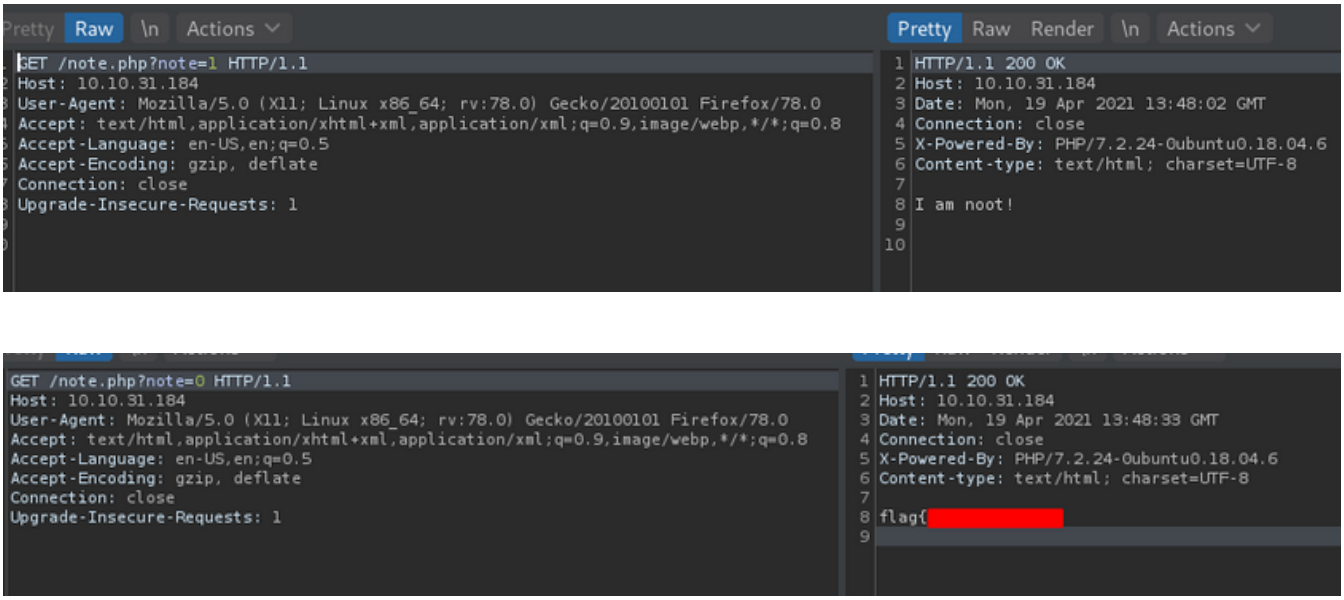


FIG 11,12: Requisições e Respotas da aplicação de acordo com a modificação do parametro "?note="

Impacto:

Com essas vulnerabilidade houve a possibilidade de ter acesso a anotações de todos o usuários, quebrando a confidencialidade da aplicação web, criando-se o risco de vazamento de dados, e dados sensíveis como por exemplo de empresas terceiras que armazenam informações importantes na aplicação.

Correções / Mitigações:

É recomendado a implementação de uma método ou ferramenta de verificação se a anotação que está sendo requisitada é do usuário que está solicitando.

PT08: Uso de senha padrão na aplicação.

Severidade: Alta

Host: 10.10.251.57

Após pesquisar na internet à respeito da tecnologia utilizada no web site foi possível encontrar usuário e senha padrão na documentação oficial (https://github.com/NinjaJc01/PensiveNotes) da aplicação e devido a falta de configuração foi possível realizar login com as credenciais padrões

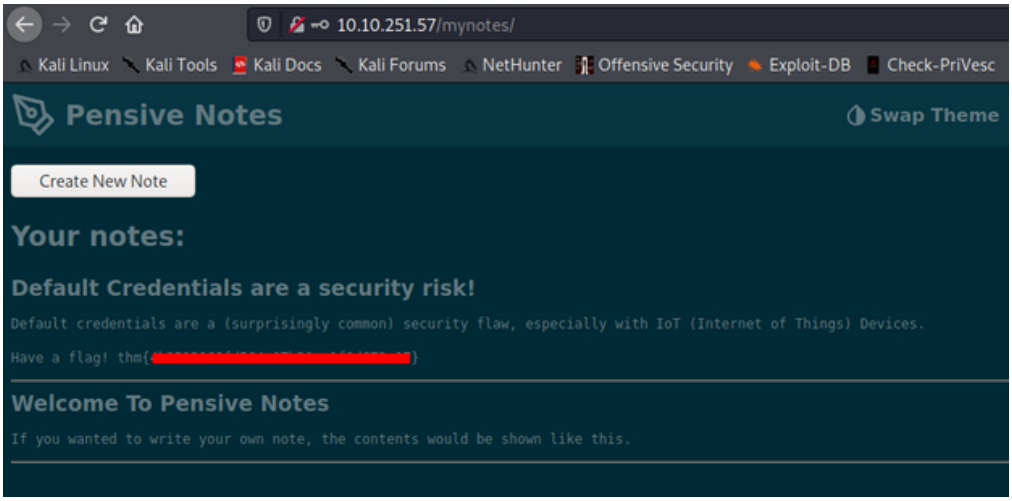


FIG13: Acesso total a aplicação após o login com as credenciais encontradas na internet

Impacto:

Com essa falta de configuração correta da tecnologia utilizada é possível ter acesso total a área administrativa da aplicação web, supondo que um invasor tenha acesso a essa área é provável que ele mude dados da empresa, vaze dados, ou até mesmo execute mais ataques a longo prazo.

Correções / Mitigações:

É recomendado que altera as credenciais de autenticação, desabilite as padrões e que implemente um sistema mais rígido de autenticação como um 2FA (2 Factore authentication) ,por exemplo.

PT09: Inserção de códigos maliciosos na aplicação web.

Severidade: Alto Host: 10.10.36.35

Devido ao fato da falta de uma sanitização da entrada de dados dos usuários foi possível executar comandos HTML e script de JS viabilizando que um ataque de XXS ocorra.

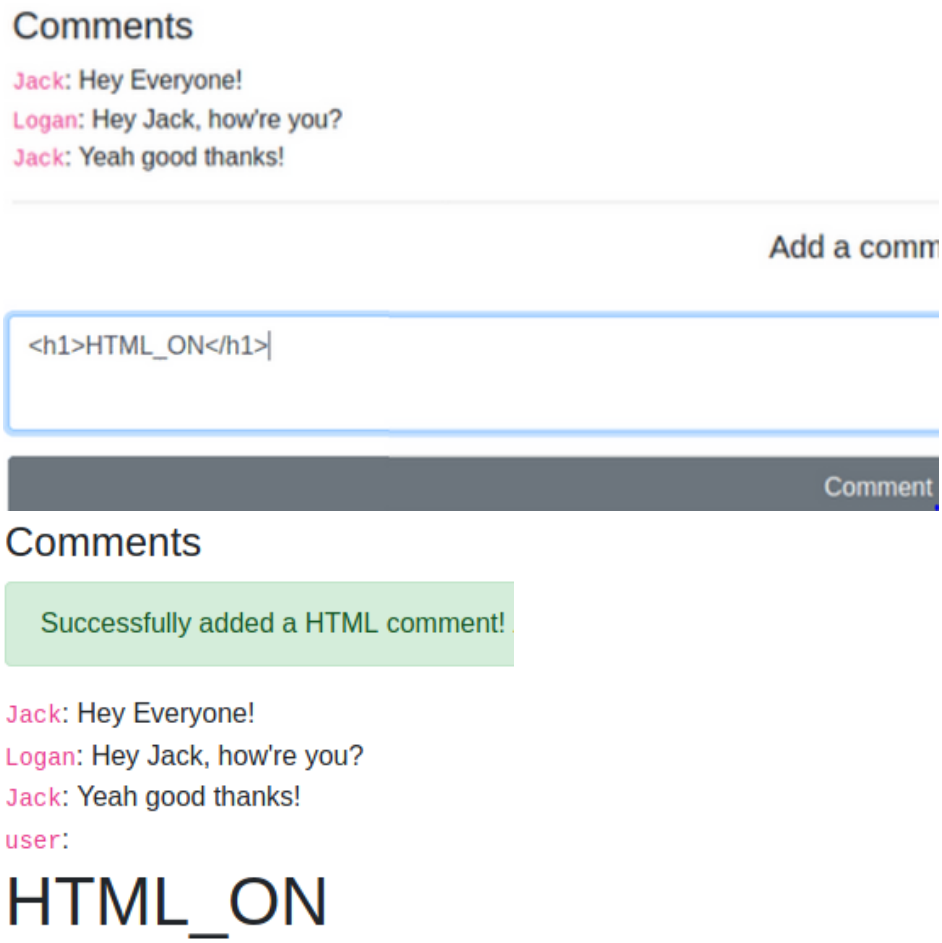


FIG 14, 15: Inserção e execução por parte do browser de codigo HTML.

Impacto:

Com essa vulnerabilidade é possível que um atacante realize ações capazes de indisponibilizar o sistema do servidor, alterar informações presentes no site (daface) e até mesmo injetar um código de keylogger para capturar tudo que é digitado no site.

Correções / Mitigações:

É recomendado que seja desabilitado a execução de HTML na página, e que se caso for necessário a inserção de códigos HTML que haja uma sanitização, evitando que por exemplo a tag <script/> seja executada dificultando a exploração do ambiente, além da implementação de WAF, Firewall, SIEM que já foram recomendados em outros casos anteriores.

Materiais de apoio

Materiais de apoio de acordo com cada vulnerabilidade e citações:

PT01

https://www.php.net/manual/pt_BR/function.passthru.php

https://subscription.packtpub.com/book/networking_and_servers/9781785284588/6/ch06lvl1sec59/remote-code-execution

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

PT02

https://projectworlds.in/free-projects/php-projects/online-book-store-project-in-php/

https://www.exploit-db.com/exploits/47887

https://github.com/projectworldsofficial/online-book-store-project-in-php

PT03

https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization
https://portswigger.net/web-security/deserialization/exploiting

PT04

https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

PT05

https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Materiais de apoio

PT06

https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/

https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard

https://www.clienteoba.com.br/index.php/knowledgebase/439/Desabilitando-a-listagem-de-diretorios-no-Apache.html

PT07

https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control

PT08

https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration
https://github.com/NinjaJc01/PensiveNotes

PT09

https://owasp.org/www-community/attacks/xss/

https://www.welivesecurity.com/br/2018/12/27/cross-site-scripting-xss-entenda-o-que-e-e-saiba-como-estar-protegido/

https://portswigger.net/web-security/cross-site-scripting

https://rafaelomarques.wordpress.com/2015/12/08/como-criar-um-keylogger-em-javascript-com-apenas-4-linhas-de-codigo/

Metodologias e Ferramentas utilizadas

Durante todo o período do teste de intrusão foram utilizado metodologias como:

Foi utilizado a metodologia de testes da owasp para realizar as análises de vulnerabilidades web.

https://owasp.org/www-project-web-security-testing-guide/

https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-pt_pt.pdf

Para a realização dos testes de intrusão foi utilizado a metodologia PTES.

http://www.pentest-standard.org/index.php/Main_Page

Durante a realização dos testes foram utilizadas as ferramentas contida no sistema operacional Kali Linux.

https://www.kali.org/